Joint Publication 2-01

Joint and National Intelligence Support to Military Operations

5 July 2017

PREFACE

1. Scope

This publication provides doctrine for joint and national intelligence products, services, assessments, and support to joint military operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and it provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs), and prescribes joint doctrine for operations and training. It provides military guidance for use by the Armed Forces in preparing and executing their plans and orders. 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 objectives.

3. Application

a. Joint doctrine established in this publication applies to the Joint Staff, commanders of combatant commands, subunified commands, joint task forces, subordinate components of these commands, the Services, and combat support agencies.

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 unless the CJCS, 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 US, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

4. Contribution

The following staff, in conjunction with the Joint Doctrine Development Community, made a valuable contribution to the revision of this Joint Publication: Lead Agent and Joint Staff Doctrine Sponsor LtCol Glen Weaver, Joint Staff J-2; Joint Analysis Division Action Officer Mr. Mark Brown, Joint Staff J-7, Joint Doctrine Analysis Division; and Joint Doctrine Action Officer LTC Gregory Browder, Joint Staff J-7, Joint Doctrine Division.

For the Chairman of the Joint Chiefs of Staff:

KEVIN D. SCOTT
Vice Admiral, USN
Director, Joint Force Development

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 2-01
DATED 05 JANUARY 2012

- **Clarifies the difference within a joint intelligence operations center (JIOC) between a red team and a red cell.**

- **Adds appendices: "Target Intelligence," "Global Intelligence, Surveillance, and Reconnaissance Management," and "Joint Exploitation Support to Intelligence."**

- **Describes information operations intelligence integration as a military capability that supports information operations.**

- **Clarifies identity intelligence, identity intelligence production, and associated identity activities.**

- **Restructures Chapter III, Section B, "Collection," and clarifies collection management, collection requirements management, and collection operations management functions.**

- **Clarifies the role of joint intelligence planners to coordinate the planning and direction portion of the joint intelligence process.**

- **Describes intelligence support to cyberspace operations and cyberspace intelligence, surveillance, and reconnaissance considerations.**

- **Clarifies the roles and responsibilities of the JIOC with increased emphasis on the intelligence mission management function.**

- **Emphasizes the role of the J-2 to ensure the integration of intelligence resource management within the operations cycle of the joint force.**

- **Defines the Defense Intelligence Agency's roles and responsibilities as the defense intelligence collection manager.**

- **Describes each of the Service intelligence organizations and their capabilities.**

- **Clarifies the difference between an intelligence, surveillance, and reconnaissance activity and an intelligence collection capability or asset.**

- **Expands the discussion of counterintelligence activities to include protecting information and information systems and combatting transnational organized crime.**

- **Describes weapons technical intelligence as a subcategory of technical intelligence.**

TABLE OF CONTENTS

APPENDIX

GLOSSARY

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Explains the Role of Intelligence in Military Operations**
- **Describes Joint and National Intelligence Organizations, Responsibilities, and Procedures**
- **Discusses Intelligence Operations and the Intelligence Process**
- **Describes Intelligence Support to Joint Operation Planning**

The Role of Intelligence in Military Operations

The goal is to maximize intelligence support to military operations by increasing the efficiency of the intelligence process and the effectiveness of the intelligence organizations that support the joint force commander.

The objective of joint intelligence operations is to provide accurate and timely intelligence to commanders. The intelligence staff must provide the joint force commander (JFC) with an understanding of the operational environment (OE), particularly with regard to the adversary's forces, capabilities, and intentions.

Joint intelligence doctrine describes the roles and relationships of intelligence organizations at the national, combat support agency (CSA), combatant command (CCMD), and subordinate joint force levels.

The intelligence directorates of a joint staff (J-2s), CCMD joint intelligence operations centers (JIOCs), subordinate joint force J-2s, and joint intelligence support elements (JISEs) are all parts of a mutually supporting intelligence enterprise.

Intelligence Challenges

Globalization and technology advancements enable adversaries to challenge the economy and security of the US and its allies. Some adversaries seek to develop or acquire capabilities that have the potential to produce catastrophic results. Small groups or individuals can harness chemical, biological, or even crude radiological or nuclear devices to cause extensive damage and harm. Adversaries may also conduct cyberspace operations to disrupt commercial activities, daily life, and military operations; cause economic damage; compromise sensitive and/or technical information; and interrupt critical infrastructure such as power grids and information networks. The inherent deniability of dual-

use technologies, particularly in the chemical and biological industries, continues to make technical assessments and estimates difficult. Agile intelligence processes and procedures must be understood and utilized across the intelligence enterprise. Intelligence organizations need to be prepared to respond to a myriad of requirements in a wide variety of situations across the range of military operations.

Exploitation and dissemination of information now occur nearly simultaneously as multimedia products resident in knowledge bases are automatically updated with new information as it is collected and processed.

Intelligence Support to Military Operations

Intelligence support functions primarily focus on adversary military capabilities, violent extremist organization threat capabilities, centers of gravity, and potential courses of action in order to provide commanders with the necessary information to plan and conduct operations. Intelligence analysts must also consider and fuse other relevant aspects of the OE, such as sociocultural factors, into the overall assessment in order to ensure commanders fully understand the OE.

A crucial aspect of intelligence support to ongoing operations is the integration of intelligence resource management within the joint operations center.

Of particular importance to force protection is the timely sharing of counterintelligence (CI), law enforcement information, and other actionable intelligence regarding threats from terrorism, weapons of mass destruction (WMD), information operations, and cyberspace.

Counterintelligence support is crucial to protecting US forces, protecting information and information systems, and combating terrorism and transnational organized crime, and it must be fully integrated into planning and execution.

CI activities are conducted to detect, identify, assess, exploit, and counter or neutralize the threat posed by foreign intelligence entities, or by individuals engaged in espionage, sabotage, subversion, terrorism, or transnational organized crime. The Defense Intelligence Agency (DIA) Directorate for Operations and CI elements from the Services and Department of Defense (DOD) agencies participate in this multidisciplined effort and facilitate information sharing among CCMDs, interagency partners, and law enforcement organizations.

Weapons of Mass Destruction Counterproliferation and Nonproliferation Activities

Intelligence is a critical enabler of efforts to protect the homeland, DOD, and allies from WMD attacks and supports 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 their associated materials, technology, and expertise necessary to create and sustain a WMD program) 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 proliferation attempts.

Information Operations

By providing population-centric sociocultural intelligence and physical network architecture, including the information transmitted via those networks, intelligence can greatly assist information operations planners in determining the proper effects. The utilization of information operations intelligence integration greatly facilitates an understanding of the interrelationship between the physical, informational, and cognitive dimensions of the information environment.

Cyberspace Operations

Intelligence activities are a key enabler providing commanders and planners with a better understanding of an adversary's use of cyberspace, an adversary's vulnerabilities, and reliance on cyberspace and potential exploitation opportunities.

Joint and National Intelligence Organizations, Responsibilities, and Procedures

Joint Intelligence

The Joint Staff J-2 [Directorate of Intelligence] is under the authority, direction, and control of the Chairman of the Joint Chiefs of Staff (CJCS) and is resourced by the DIA. It provides all-source intelligence and intelligence staff support to the Secretary of Defense (SecDef), CJCS, other Joint Staff directorates, CCMDs, and the Services. It also serves as the single focal point for crisis intelligence support to national and theater decision makers, along with managing the worldwide defense warning system.

Combatant Command Intelligence Organizations and Responsibilities

CCMD J-2 provides the combatant commander (CCDR), higher echelons (up to and including the National Joint Operations and Intelligence Center [NJOIC]), and subordinate commands with a common, coordinated, timely, all-source intelligence picture in a form that the primary user requires.

CCMD JIOC is the focal point for the CCMD's intelligence planning, collection management, analysis, and production effort and is organized as directed by the CCDR through the CCMD J-2. The CCMD JIOC supports joint planning and conducts intelligence operations in support of the commander and staff, subordinate component commands, and joint task forces (JTFs). The JIOC integrates all DOD intelligence from external defense and national intelligence organizations, partner nations, nongovernmental organizations (NGOs), United States Government (USG) department and agencies, and law enforcement to ensure accurate, timely, and complete intelligence is available to support CCMD joint planning, execution, and assessment.

Subordinate Joint Force Intelligence Organizations and Responsibilities

In order to accomplish the assigned mission, the joint force J-2 uses a combination of the following elements:

JISE. At the JTF level, a JISE is normally established. The JISE provides the JTF with tailored intelligence products and services with a continuous analytical capability.

Operational-Level JIOC. In a particularly large or protracted campaign, the JTF commander may decide to employ an operational-level JIOC. The JIOC incorporates the capabilities inherent in a JISE but is generally more robust.

Joint Force Counterintelligence and Human Intelligence Staff Element (J-2X). This organization integrates human intelligence (HUMINT) and CI by combining the HUMINT operations cell, the task force CI coordinating authority, a HUMINT analysis and requirements cell, and a CI analysis cell, all of which comprise the J-2X.

Geospatial Intelligence (GEOINT) Cell. GEOINT support includes imagery, imagery intelligence (IMINT), and geospatial information and services.

National Intelligence Agency Support. The JFC, at the recommendation of the J-2, may request that the national intelligence community (IC) analysts or subject matter experts deploy to support a JISE or operational-level JIOC.

National Intelligence

The IC had its origin in the National Security Act of 1947, amended by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, and guided by Executive Order 12333, *United States Intelligence Activities*, as amended. It refers in the aggregate to those executive branch agencies and organizations that are funded in the National Intelligence Program (NIP). The IC consists of the Director of National Intelligence (DNI) and 16 member organizations.

IRTPA established the Office of the Director of National Intelligence (ODNI) with specified authority over the NIP budget, appointment of certain IC agency heads, IC personnel policies, tasking for collection and analysis, foreign liaison, and protection of intelligence sources and methods.

Department of Defense Intelligence and Combat Support Agency Organizations and Responsibilities

The **Under Secretary of Defense for Intelligence** serves as the principal staff assistant to SecDef and Deputy Secretary of Defense regarding intelligence, CI, security, sensitive activities, and other intelligence-related matters.

The **NJOIC** is an integrated Joint Staff J-2/J-3 [Operations]/J-5 [Strategic Plans and Policy] element that monitors the global situation on a continual basis and provides the CJCS and SecDef a DOD planning and crisis response capability. The NJOIC is located within, and is an integral part of, the National Military Command Center. The intelligence component of the NJOIC maintains an Alert Center that consists of the deputy director for intelligence, regional desks corresponding to each geographic CCMD, and representatives from each Service intelligence staff element, the intelligence defense agencies, and the Central Intelligence Agency (CIA). If a developing situation escalates into a crisis, the relevant Alert Center regional desk officer is augmented with analytical

support; an intelligence cell, intelligence working group, or intelligence task force is formed.

DIA is an intelligence CSA under SecDef and a member of the national IC. The Director, DIA, reports to SecDef through the CJCS. DIA's combat support mission is to provide support for operating forces planning for, or conducting, military operations, including support during conflict or in the conduct of other military activities related to countering threats to US national security. DIA conducts overt and clandestine HUMINT collection focusing on requirements of importance to DOD. DIA also leads efforts to align intelligence activities and links and synchronizes national, defense, and military intelligence.

National Security Agency/Central Security Service is a unified organization structured to provide the signals intelligence mission of the US and ensure the protection of national security systems for all USG departments and agencies. The National Security Agency is an intelligence CSA under SecDef and is dual-tasked as a member of the national IC under the DNI. Through the National Security Agency/Central Security Service representative, the National Security Agency provides direct cryptologic and cyberspace support to the CCMD JIOCs through the Central Security Service (comprised of the Service cryptologic components).

National Geospatial-Intelligence Agency (NGA) is an intelligence CSA under SecDef and is dual-tasked as a member of the national IC under the DNI. The Director, NGA, serves as the functional manager for GEOINT and is the principal GEOINT advisor to the DNI, SecDef, CJCS, and CCDRs. As functional manager, NGA develops GEOINT tradecraft standards, develops strategic guidance and procedures, and develops and enforces information technology architecture and standards. NGA also ensures coordination across intelligence disciplines and IC elements. GEOINT consists of imagery, IMINT, and geospatial information. GEOINT exploitation includes analysis of electro-optical, infrared, and radar imagery; full motion video; moving target indicators; geospatial information; and spectral, laser infrared, radiometric, polarimetric, spatial, and temporal data.

National Reconnaissance Office (NRO) is a DOD agency and a member of the national IC. The Director, NRO, reports to both the DNI and SecDef. NRO is responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data-processing facilities to collect intelligence and information to support national and departmental missions and other USG needs.

Service Intelligence Organizations. The Chiefs of the Services provide intelligence support for DOD missions related to military systems, equipment, training, and national intelligence activities. The Services also provide support to DOD entities, including CCMDs and their components and each CCMD's JIOC.

National Intelligence Community Organizations and Responsibilities

The IRTPA created the ODNI to improve information sharing, promote a unified and strategic direction for the IC, and ensure integration of effort across the IC. ODNI is led by the DNI. The DNI serves as the principal advisor to the President, National Security Council, and Homeland Security Council for intelligence matters related to national security and oversees and directs the implementation of the NIP. The ODNI is comprised of several components, including the National Counterterrorism Center, the National Counterproliferation Center, the National Counterintelligence Executive, and the National Intelligence Council.

The **CIA** is the largest producer of all-source national security intelligence to senior US policy makers and provides extensive political and economic intelligence to DOD senior decision makers. The CIA also oversees the Open Source Enterprise.

The **Department of State** 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 Bureau of Intelligence and Research provides all-source intelligence primarily to support both foreign policy and national security with an emphasis on terrorism and foreign law enforcement activities, including proliferation concerns.

The **Federal Bureau of Investigation (FBI)** has multiple domestic and global law enforcement and

investigative roles. The FBI also has an intelligence branch with domestic and foreign partner engagement capabilities. The FBI has primary responsibility for CI and counterterrorism operations conducted in the US. FBI CI operations overseas are coordinated with the CIA. The FBI shares law enforcement/CI information with appropriate DOD entities and CCMDs. The FBI foreign partner engagement program focuses on communications coordination and cooperation with designated foreign law enforcement, intelligence, and public/private partners to enable intelligence and information sharing.

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

The **Department of Energy** analyzes foreign information relevant to US energy policies and nonproliferation issues and the national science laboratories under its authority.

The **Department of Homeland Security (DHS)** 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 DHS, operates as an armed force, a law enforcement organization, and an IC element. The USCG's Intelligence Coordination Center and maritime intelligence fusion centers operate under the direction of the Assistant Commandant for Intelligence. The USCG Intelligence Coordination Center is the central hub for collection, fusion, analysis, and dissemination of maritime intelligence and information to USCG operating units, DHS, and all members of the IC, including DOD and key decision makers at the national level.

The **Drug Enforcement Administration** 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.

Interagency, Intergovernmental, and Multinational Intelligence Sharing

The fundamentals of command and control are influenced through trust and shared understanding of the OE by the force, including mission and multinational partners. Trust and understanding occur through open intelligence and information sharing, while ensuring protection of US sources and methods are paramount. Most sharing is bilateral due to partner nation requirements or sensitivities. In operations involving multinational, interagency, international, or nongovernmental entities, one of the most critical functions of the JFC is establishing a common view of the problem and shared situational awareness among all entities. Although intelligence sharing is accomplished at all levels during crises, in most operations the requirement expands with proximity to the operational forces.

Multinational Intelligence Collaboration

Typically, in a multinational operation, allied military partner intelligence counterparts may locate or colocate around the JTF headquarters in the form of national intelligence cells. Allied nations also bring valuable intelligence contributions and can often provide niche capabilities in support of the overall JTF mission. Different participants in a multinational organization can contribute unique intelligence sources and useful perspectives on intelligence problems. However, US analysts should be aware that different nations have differing standards for assessing the reliability, validity, and confidence of their raw and processed intelligence. In addition, some participants may be limited by policy in what they may provide to the effort, and their analysis may be slanted due to national biases.

International Intelligence Sharing

Synchronizing USG departments and agencies with joint or multinational military operations, international organizations, NGOs, and contractors enables US forces to gain access to specialized knowledge, significant access, or insight and understanding that these organizations possess. Inclusiveness with partners leads to a common understanding of this environment, the associated military challenge, and determination of necessary conditions to achieve success. This analysis helps provide common visualization and better achieve unity of effort with our partners—bridging the gap between all instruments of national and international power.

Interorganizational

The role of DOD intelligence elements in an operation

Intelligence Collaboration

involving USG interagency partners is dictated by the nature of the support relationship. DOD operations, in conjunction with other USG departments and agencies, such as DHS, within the US or its territories can be characterized as either homeland defense or defense support of civil authorities. At the national level, the National Operations Center, operated by DHS, is the primary node for incident management across the federal government.

Intelligence Operations

These intelligence operations should focus on the commander's mission and support the commander's decision-making 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 facilitates an understanding of the wide variety of intelligence operations and their interrelationships.

Planning and Direction. Joint intelligence planners, through participation in the joint planning and assessment processes, lead development of the priority intelligence requirements and concept of intelligence operations. Intelligence planning provides a methodology to coordinate, integrate, and synchronize all available intelligence capabilities to meet the CCDR's intelligence requirements for joint planning and assessment.

Collection. Collection operations acquire information about relevant aspects of the OE and provide that information to intelligence processing and exploitation elements. Collection management, which occurs at all levels of intelligence, is the process of converting information requirements into collection requirements, tasking, or coordinating actions with appropriate collection organizations or agencies, and monitoring results and retasking as required.

Processing and Exploitation. The processing and exploitation components of the intelligence process convert the collected raw data into information that can be readily disseminated and used by all-source intelligence analysts to produce multidiscipline intelligence products.

Analysis and Production. The analysis and production portion of the intelligence process integrates, evaluates,

analyzes, and interprets information from single or multiple sources into a finished intelligence product that may be as little as a few textual lines in message format, or a multipage, multisource, multimedia electronic file.

Dissemination and Integration. The timely dissemination of critical information and finished intelligence to appropriate consumers is paramount to attaining and maintaining information superiority. Properly formatted intelligence products are disseminated to the requester, who integrates the intelligence into the decision-making and planning processes.

Evaluation and Feedback. All intelligence operations are interrelated, and the success or failure of one operation may impact the rest of the intelligence process. It is imperative that intelligence personnel and consumers at all levels honestly evaluate and provide timely feedback throughout the intelligence process on how well the various intelligence operations perform to meet the commander's intelligence requirements.

CONCLUSION

This publication provides doctrine for joint and national intelligence products, services, assessments, and support to joint military operations.

Intentionally Blank

CHAPTER I
THE ROLE OF INTELLIGENCE IN MILITARY OPERATIONS

"We will rebalance investments toward systems that are operationally responsive and effective in highly contested environments, while sustaining capabilities appropriate for more permissive environments in order to support global situational awareness, counterterrorism, and other operations."

Quadrennial Defense Review 2014

1. Introduction

a. The objective of joint intelligence operations is to provide accurate and timely intelligence to commanders. Joint and Service intelligence organizations produce intelligence products that rely on timely and integrated intelligence from national agencies. This joint intelligence effort promotes information superiority throughout the operational environment (OE), enabling the successful conduct of operations. The intelligence staff must provide the joint force commander (JFC) with an understanding of the OE, particularly with regard to the adversary's forces, capabilities, and intentions. To ensure timely and accurate intelligence is provided or available to the JFC, subordinate commands, and components, the intelligence staff performs the following tasks:

(1) Clearly understand and be aware of the intelligence requirements (IRs) of their superior and subordinate commands and components.

(2) Identify intelligence capability shortfalls and knowledge gaps to the JFCs they support.

(3) Task and utilize theater, Department of Defense (DOD), and national capabilities to address identified shortfalls and gaps.

b. Joint intelligence doctrine describes the roles and relationships of intelligence organizations at the national, combat support agency (CSA), combatant command (CCMD), and subordinate joint force levels. The intelligence directorates of a joint staff (J-2s), CCMD joint intelligence operations centers (JIOCs), subordinate joint force J-2s, and joint intelligence support elements (JISEs) are all parts of a mutually supporting intelligence enterprise. This intelligence enterprise supports the JFC through intelligence federation in order to accomplish intelligence support missions. **The goal is to maximize intelligence support to military operations by increasing the efficiency of the intelligence process and the effectiveness of the intelligence organizations that support the JFC.** Intelligence resources, methodologies, and products for every military option and scenario should be developed, reviewed, and exercised regularly. Intelligence that is anticipatory, timely, accurate, complete, relevant, objective, and available is a crucial enabler of unified action and successful military operations. Observations and insights generated during operations should be captured during after action reviews and shared to further maximize intelligence support.

2. Intelligence Challenges

a. **Today's complex world presents a variety of intelligence challenges.** Over the past century, the predominant threat to the US was understood to be in the form of a military attack from a belligerent nation-state. US dominance in warfare has given adversaries, particularly non-state actors and any state sponsors, a strong motivation to adopt asymmetric methods to counter US advantages. Globalization and technology advancements enable adversaries to challenge the economy and security of the US and its allies. Some adversaries seek to develop or acquire capabilities that have the potential to produce catastrophic results. Small groups or individuals can harness chemical, biological, or even crude radiological or nuclear devices to cause extensive damage and harm. Adversaries may also conduct cyberspace operations (CO) to disrupt commercial activities, daily life, and military operations; cause economic damage; compromise sensitive and/or technical information; and interrupt critical infrastructure such as power grids and information networks. Although much emphasis has been placed on irregular warfare and chemical, biological, radiological, and nuclear (CBRN) attacks, the intelligence community (IC) needs to be wary of the prospect of regional conflicts with nation-states with the capability of challenging US interests. Global availability of emerging technology provides regional powers with a means to rapidly develop military capabilities without traditional indicators. The inherent deniability of dual-use technologies, particularly in the chemical and biological industries, continues to make technical assessments and estimates difficult. **Agile intelligence processes and procedures must be understood and utilized across the intelligence enterprise. Intelligence organizations need to be prepared to respond to a myriad of requirements in a wide variety of situations across the range of military operations.** At the same time, the quality of intelligence products remains of paramount importance and should be sufficiently detailed and timely to satisfy the commander's decision-making needs.

b. Today's information environment offers unparalleled technological opportunities for meeting these challenges by dramatically increasing the timeliness of relevant information and by integrating operations and intelligence. Advances in data processing, such as artificial intelligence, large data-set analytics, knowledge bases, and iterative search tools, have created a new paradigm in which the timelines of intelligence operations and the intelligence process are greatly compressed. Likewise, the traditional delineations among the various types of intelligence operations have been blurred. **Exploitation and dissemination of information now occur nearly simultaneously as multimedia 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 systems that enhance situational understanding through a common operational picture (COP) enable intelligence personnel to quickly exploit, analyze, produce, and disseminate relevant intelligence. Secure digital communication links and automated exploitation tools now make it possible to immediately process a significant amount of collected data, disseminate the resulting information in support of the commander's decision-making requirements, and routinely provide timely feedback required to dynamically manage intelligence collection assets. Likewise, direct sensor-to-shooter connectivity enables the timely transmission of

"To navigate today's turbulent and complex strategic environment we must:

(1) Execute our mission smartly and identify ways to better leverage the substantive work of our partners and potential partners;

(2) Continue to integrate, transform, and strengthen the IC's [intelligence community's] support to national security;

(3) Protect privacy and civil liberties and adhere to the Principles of Professional Ethics for the IC; and

(4) Adapt to changing needs and resources and innovate to provide unique anticipatory and strategic intelligence."

National Intelligence Strategy, 2014

precise information, which increases the ability to successfully engage time-sensitive targets.

3. Intelligence Support to Military Operations

Intelligence plays a critical role to assist commanders in making decisions across the range of military operations. Commanders use intelligence to anticipate, visualize, and understand the OE to influence the outcome of operations, focus combat power, and provide force protection as needed. Figure I-1 depicts the primary support functions of joint intelligence. Joint operations span the three levels of warfare, strategic, operational, and tactical, which require specific and focused intelligence support at each level.

a. Intelligence support functions primarily focus on adversary military capabilities, violent extremist organization threat capabilities, centers of gravity (COGs), and potential courses of action (COAs) in order to provide commanders with the necessary information to plan and conduct operations. Intelligence analysts must also consider and fuse other relevant aspects of the OE, such as sociocultural factors, into the overall assessment in order to ensure commanders fully understand the OE.

b. The role of the J-2 is to 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 peace enforcement operation should any of the belligerents fail to honor the terms of a truce. A crucial aspect of intelligence support to ongoing operations is the integration of intelligence resource management within the joint operations center (JOC). This function of the J-2 ensures the intelligence resource management element is actively participating in the operations cycle of the joint force. Therefore, intelligence resources at every echelon should be structured to provide support that is proactive, is flexible, identifies opportunities, and meets the commander's intent.

Primary Joint Intelligence Support Functions

- Aiding commanders to frame the operation by identifying the nature of the problem and contributing to the development of the operational approach.
- Effective intelligence planning to integrate, synchronize, and manage all available intelligence capabilities to support joint force commander decision-making needs.
- Early warning of the potential for adversarial elements or factors in the operational environment to negatively or positively impact current or planned operations.
- Joint intelligence preparation of the operational environment using all available resources to continuously monitor and update the operational environment to evaluate the adversary and other relevant actors and estimate adversary courses of action most likely and most dangerous to friendly forces.
- Intelligence architecture planning that enables interoperability and information sharing, supports fusion of single-source information, and feeds decision-making tools.
- Continuous maintenance of intelligence data visualization input for knowledge boards, common operational picture, etc.
- Collection and requirements management that identifies gaps in information and formulates strategies to proactively acquire needed information from the most appropriate source.
- Providing target intelligence in support of the command targeting function to enable appropriate target selection in line with the commander's priorities, and assess the effectiveness of targeting.
- Providing direct intelligence liaison support to joint force staff functions such as information operations and joint targeting boards.

Figure I-1. Primary Joint Intelligence Support Functions

c. The intelligence function also supports force protection and homeland defense (HD) through the production of threat assessments. The timely integration and sharing of intelligence and appropriate law enforcement information among CCMDs, interagency members, and multinational partners is vital to this effort. To attain such an end state, DOD works with the Department of Homeland Security (DHS), the Department of the Treasury, 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 threats from terrorism, weapons of mass destruction (WMD), information operations (IO), and cyberspace.

(1) **CI Activities. CI support is crucial to protecting US forces, protecting information and information systems, and combating terrorism and transnational**

organized crime, and it must be fully integrated into planning and execution. The DOD CI program has five separate but interrelated functions: investigations, collection, operations, analysis and production, and functional services. All five functions will be incorporated into CI planning and support activities. CI activities are conducted to detect, identify, assess, exploit, and counter or neutralize the threat posed by foreign intelligence entities, or by individuals engaged in espionage, sabotage, subversion, terrorism, or transnational organized crime. An effective CI program uses a multidisciplined approach that relies on the timely fusion of information from law enforcement, CI, and other intelligence sources. The Defense Intelligence Agency (DIA) Directorate for Operations and CI elements from the Services and DOD agencies participate in this multidisciplined effort and facilitate information sharing among CCMDs, interagency partners, and law enforcement organizations.

Basic CI policy is contained in Department of Defense Directive (DODD) 5240.02, Counterintelligence (CI). *Additional information on CI support to operations can be found in Joint Publication (JP) 2-01.2,* Counterintelligence and Human Intelligence in Joint Operations.

(2) **Law Enforcement Information.** Threats to the OE in the US and foreign countries often are received by law enforcement personnel, who are the primary responders to threats in most countries. Law enforcement information originates from the Federal Bureau of Investigation (FBI), DHS, legal attaches, INTERPOL [International Police], and other law enforcement agencies. Because law enforcement information focuses on threats that are traditionally nonmilitary, it can be an important source of information that can fill intelligence gaps about the OE and in particular gaps directly related to force protection.

(3) **WMD Counterproliferation and Nonproliferation Activities. Intelligence is a critical enabler of efforts to protect the homeland, DOD, and allies from WMD attacks and supports 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 their associated materials, technology, and expertise necessary to create and sustain a WMD program) 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 proliferation attempts. Locating WMD and/or toxic industrial materials (TIMs) (chemical, biological, or radiological) in the area of concern are critical aspects since they can create an environment requiring extraordinary protection and produce long-term health hazards with massive environmental damage.

Additional information on intelligence support to countering WMD and operations in CBRN environments can be found in JP 3-40, Countering Weapons of Mass Destruction, *and JP 3-11,* Operations in Chemical, Biological, Radiological, and Nuclear Environments.

(4) **IO.** Intelligence is a vital military capability that supports IO. By providing population-centric sociocultural intelligence and physical network architecture, including the information transmitted via those networks, intelligence can greatly assist IO planners in determining the proper effects. The utilization of information operations intelligence integration (IOII) greatly facilitates an understanding of the interrelationship between the physical, informational, and cognitive dimensions of the information environment.

For more information, see JP 2-0, Joint Intelligence, *and JP 3-13,* Information Operations.

(5) **CO.** Operations conducted by US military forces and adversaries are increasingly conducted in cyberspace. Intelligence support to CO is covered by appropriate authorities, particularly those regarding cyberspace intelligence, surveillance, and reconnaissance (ISR). Cyberspace ISR includes ISR activities in cyberspace that are conducted to gather intelligence that may be required to support future operations. These activities synchronize and integrate the planning and operation of cyberspace systems in direct support of current and future operations. Cyberspace ISR focuses on tactical and operational intelligence and on mapping adversary cyberspace to support military planning. Cyberspace ISR requires appropriate deconfliction and cyberspace forces that are trained and certified to a common standard with the IC. ISR in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other United States Government (USG) departments and agencies. Intelligence activities are a key enabler providing commanders and planners with a better understanding of an adversary's use of cyberspace, an adversary's vulnerabilities, and reliance on cyberspace and potential exploitation opportunities.

For more information, see JP 3-12, Cyberspace Operations.

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

"The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to 'connect the dots.' No one component holds all the relevant information."

The 9/11 Commission Report

1. Introduction

JFCs exercise control over a vast array of assigned, allocated, and attached intelligence collection and analytic capabilities. Nevertheless, these alone will not be capable of satisfying all the joint force's IRs. The joint force J-2 relies on intelligence from theater, defense, national, partner nation (PN), and law enforcement organizations to satisfy the JFC and staff requirements. The resources from these organizations integrate defense intelligence capabilities into a comprehensive intelligence effort designed to support the joint force. The J-2 should understand the organization, procedures, production responsibilities, and expertise resident in the various multinational and national intelligence agencies 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 defense and national intelligence.

SECTION A. JOINT INTELLIGENCE

2. Overview

IRs are driven by the mission and the commander's guidance and intent. To fulfill these IRs, the J-2 conducts operations within the context of the joint intelligence process.

3. Joint Staff, Directorate for Intelligence

The Joint Staff J-2 [Directorate of Intelligence] is under the authority, direction, and control of the Chairman of the Joint Chiefs of Staff (CJCS) and is resourced by the DIA. It provides all-source intelligence and intelligence staff support to the Secretary of Defense (SecDef), CJCS, other Joint Staff directorates, CCMDs, and the Services. It also serves as the single focal point for crisis intelligence support to national and theater decision makers, along with managing the worldwide defense warning system. The Joint Staff J-2 coordinates and develops joint intelligence doctrine and architecture. The Joint Staff J-2 coordinates with the IC coordinator for support to military operations.

4. Combatant Command Intelligence Organizations and Responsibilities

a. **CCMD J-2.** The CCMD J-2 is responsible to the combatant commander (CCDR) and supports the staff in developing strategy, planning major operations and campaigns,

coordinating the intelligence structure and architecture, recommending and managing appropriate command relationships for ISR assets, and supervising the production and dissemination of appropriate intelligence products in accordance with (IAW) command relationships authorities. Additionally, the J-2 determines the requirements and direction needed to enable unity of the intelligence effort in support of the commander's objectives. The J-2 provides the CCDR, higher echelons (up to and including the National Joint Operations and Intelligence Center [NJOIC]), and subordinate commands with a common, coordinated, timely, all-source intelligence picture in a form that the primary user requires. The J-2 accomplishes this by employing joint force intelligence resources and identifying and integrating intelligence from various sources, including senior and subordinate commands, the IC, international partners, USG departments and agencies, law enforcement, and nongovernmental organizations (NGOs). Specifically, the CCMD J-2 should:

(1) Normally exercise staff supervision over the JIOC and manage collection through allocation and integration of intelligence capabilities, while synchronizing external capabilities with other CCMD JIOCs.

(2) Plan and coordinate the joint intelligence architecture designed to support intelligence collection activities for the CCDR, staff, subordinate component commanders, and joint task forces (JTFs).

(3) Establish an intelligence systems architecture that supports intelligence production and effective dissemination throughout the command, to include tactical levels and multinational partners.

(4) Determine and recommend prioritized intelligence needs based on mission analysis and commander's planning guidance, specifically priority intelligence requirements (PIRs) (focusing on the adversary and the OE to drive collection and production requirements [PRs]) to support the commander's decision making.

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

(6) Identify available intelligence and information resources, match assets against requirements, and identify potential analytic or collection resource shortfalls.

(7) Request, as required, external collection resources and analysis and production support from defense and national intelligence organizations.

(8) If applicable, assume modernized integrated database (MIDB) responsible production authority in crisis/wartime for the area of responsibility (AOR) and properly delegate responsibilities to federated producers. In conjunction with DIA, produce orders of battle (OBs) in electronic databases.

(9) Coordinate the intelligence effort of subordinate commands.

(10) Assist the operations directorate of a joint staff (J-3) and plans directorate of a joint staff (J-5) in development of mission objectives and determine the availability, quality, and quantity of intelligence assessments, knowledge, and information relative to the joint mission.

(11) Inform and support the CCDR's decisions, guidance, and intent.

(12) Provide target intelligence for plans and operations, ensuring the IC, federated relationships, component intelligence directorates, and PNs are leveraged to support target intelligence production.

(13) Manage no-strike lists.

b. **CCMD JIOC.** Each CCMD; United States Cyber Command (USCYBERCOM), a subordinate unified command under United States Strategic Command (USSTRATCOM); and the United States Forces, Korea (USFK), a subordinate unified command under United States Pacific Command (USPACOM), have assigned JIOCs to integrate intelligence capabilities in support of the command mission. The JIOC is the focal point for the CCMD's intelligence planning (IP), collection management, analysis, and production effort and is organized as directed by the CCDR through the CCMD J-2. The CCMD JIOC supports joint planning and conducts intelligence operations in support of the commander and staff, subordinate component commands, and JTFs. The JIOC integrates all DOD intelligence from external defense and national intelligence organizations, PNs, NGOs, USG department and agencies, and law enforcement to ensure accurate, timely, and complete intelligence is available to support CCMD joint planning, execution, and assessment. The CCMD JIOC maintains visibility on all intelligence collection resources available to the command, aids the CCDR and staff in determining knowledge gaps and intelligence capabilities shortfalls, and recommends solutions to mitigate them. The JIOC also seeks to ensure timely support by submitting requests to IC production centers through the defense intelligence component representatives in direct support to the command.

(1) **Organization.** A JIOC is organized as directed by the CCDR through the CCMD J-2. A notional CCMD JIOC organizational structure is shown in Figure II-1. Normally, a JIOC responds to crisis situations by shifting its focus and assets, rather than by altering its organizational structure. Although there is no "standard" JIOC organizational structure, and each JIOC will vary depending on CCMD requirements, JIOCs are organized around a set of key principles and functions. These include:

(a) Integrate intelligence capabilities to effectively support joint planning, execution, and assessment.

(b) Institutionalize IP as the intelligence component of the Adaptive Planning and Execution (APEX) enterprise.

(c) Improve Reserve Component integration.

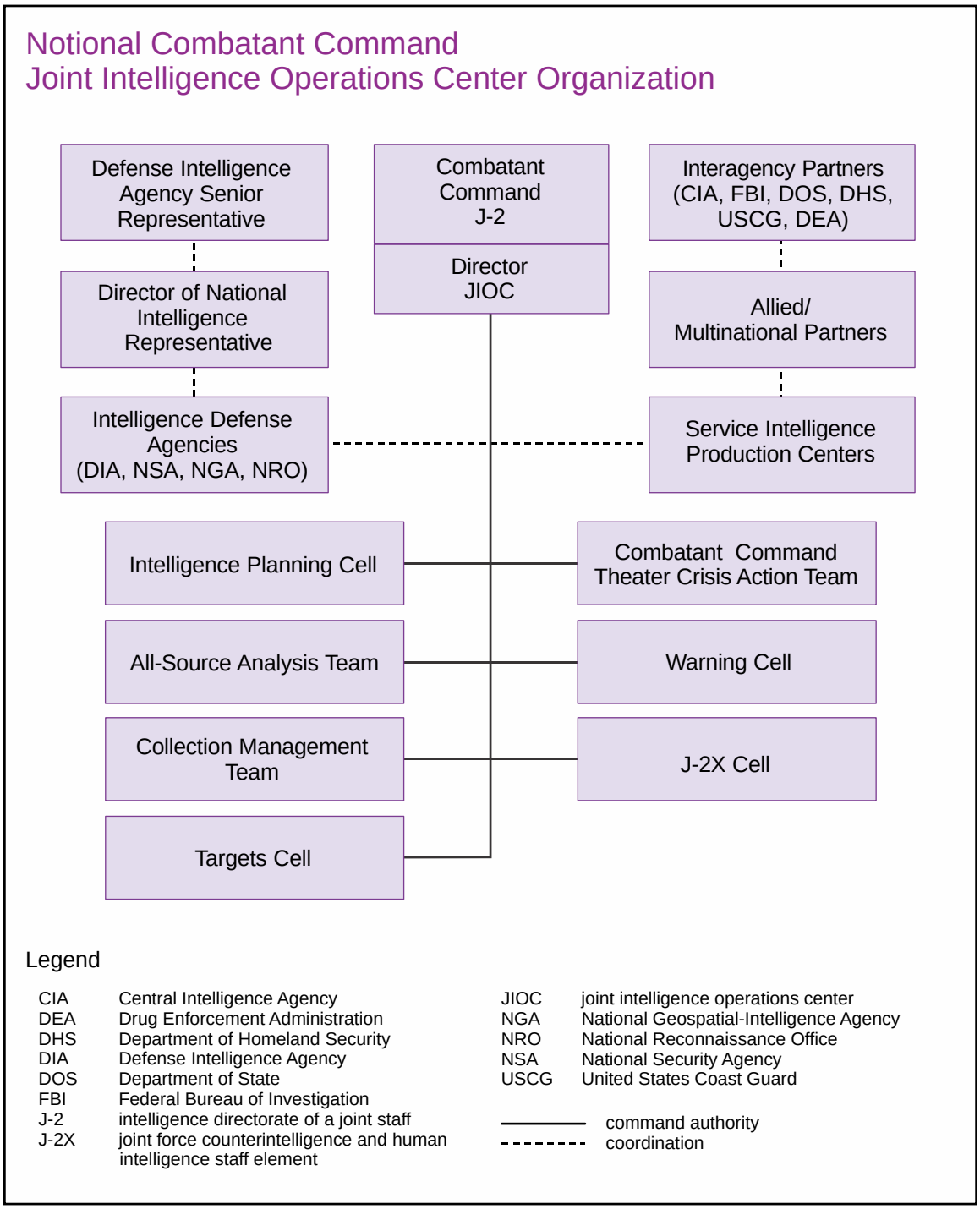


Figure II-1. Notional Combatant Command Joint Intelligence Operations Center Organization

(d) Share PN information and intelligence and collaborate intelligence support operations with allies and PNs.

(e) Facilitate intelligence mission/collection management.

(f) Expand alternative analysis capabilities.

(g) Improve all-source analysis and multidiscipline intelligence.

(h) Establish a horizontal integration/collaborative information technology (IT) enterprise in a net-centric environment.

(i) Improve training, education, and readiness.

(j) Integrate national intelligence and CSAs' capabilities.

(2) **Responsibilities.** The primary responsibility of the JIOC is to integrate defense intelligence capabilities and facilitate access to all sources of intelligence in a prescribed timeline and appropriate format to effectively support CCMD joint planning, execution, and assessments. Other responsibilities include, but are not limited to:

(a) Coordinate with the Joint Staff J-2 and DOD portion of the IC to address PIRs and collection and analysis PRs effectively to support joint planning, execution, and assessment.

(b) Determine and close knowledge gaps and mitigate intelligence capabilities shortfalls.

(c) Develop and maintain an integrated intelligence architecture that supports joint planning, targeting operations, and assessments.

(d) Maintain and coordinate execution of the CCMD intelligence collection plan with components and other IC agencies.

(e) Conduct IP in support of CCMD plans, in coordination with external intelligence organizations as determined by the CCMD J-2.

(f) Ensure target intelligence and battle damage assessment (BDA) are being produced by the appropriate echelon within the CCMD organizational structure, and, if target intelligence and BDA cannot be produced with assigned assets, coordinate target intelligence production requests and BDA requirements with the appropriate defense intelligence enterprise and national IC organizations via the Joint Staff J-2.

(g) Provide warning intelligence assessments, maintain awareness, and provide amplification as required of intelligence-derived threat warning events and actions.

(h) Direct the joint intelligence preparation of the operational environment (JIPOE) effort. Integrate analyses with products produced by subordinate commands and other organizations, and ensure the JIPOE process encompasses a systematic analysis of all relevant aspects of the OE. Continuously develop and update tailored products to support the planning and assessment efforts.

(i) Provide intelligence support and augmentation to subordinate joint forces.

(3) **Concept of Operations (CONOPS).** CCMD JIOCs use a task-oriented approach utilizing personnel resources assigned, allocated, or attached to the command; military and civilian personnel detailed to the command from other commands and Services; and personnel from DOD agencies in direct support of the command mission. The defense attaché office and Service CI elements are in general support and are expected to respond to JIOC requirements consistent with national priorities.

(a) JIOCs coordinate intelligence mission management functions to conduct intelligence operations to fill information gaps, identify intelligence capabilities shortfalls and develop mitigation options, and produce all-source intelligence products to support CCDR and senior leader decision making. The CCMD JIOC coordinates with subordinate JTF and Service component intelligence staff directorates, as well as external defense and national intelligence organizations, to accomplish this mission. The JIOC leverages the efforts of the IC and interagency partners to achieve an integrated, all-source intelligence mission operations capability. The JIOC is organized in a manner to facilitate fusion of all information and intelligence received from available sources. The JIOC coordinates with all mission partners, including CCMD and Service component staffs, the defense intelligence component representatives, and the CCMD's Director of National Intelligence (DNI) representative to actively task and integrate intelligence from all sources and levels to satisfy command PIRs.

(b) JIOCs plan for the transition from peacetime to wartime. IP for rapid response to possible crises occurs as part of a command's overall joint planning process (JPP). The planning effort includes determining the personnel, equipment, and intelligence architecture essential for generic support to deployed forces.

(c) JIOCs conduct analysis-driven collection management. Through participation in CCMD battle rhythm, intelligence planners coordinate with JIOC collection managers, all-source analysts, and intelligence information systems managers to assess intelligence capabilities shortfalls, identify information gaps, and develop collection and analysis and production plans to mitigate intelligence capabilities shortfalls and to fill known information gaps. The CCMD IP team works with joint intelligence planners at the subordinate component commands and JTFs, and, through the Joint Staff J-2, the defense intelligence enterprise, and appropriate national agencies to mitigate intelligence capabilities shortfalls and fill knowledge gaps to satisfy CCDR requirements. The JIOC executes collection management authority (CMA) on behalf of the J-2 and exercises collection requirements management (CRM) for certain assets and all national resources. Through the joint collection management board (JCMB), the CCMD J-2 and J-3 develop CCMD operation orders (OPORDs) and fragmentary orders that delegate CMA for subordinate components and JTFs.

(d) A red team exists intellectually and institutionally separate from the JIOC's conventional analysts. The red team is comprised of experienced personnel with knowledge of known and potential adversaries who are specifically trained in appropriate

concepts and methodologies. In contrast with the J-2 red cell, which performs threat emulation, the red team reviews key intelligence assessments and operation plan (OPLAN) assumptions in order to provide alternative analysis and reduce risk. Red teams adopt a comprehensive, multi-perspective approach to assessing an adversary and then devise alternatives for operational planning. Red teams assist joint planning by validating assumptions about the adversary and participating in the wargaming of friendly and adversary COAs.

For more information about red teams, refer to JP 5-0, Joint Planning.

(e) The JIOC establishes working relationships for exchanging intelligence with all potential intelligence contributors, including national intelligence agencies, Service intelligence production centers, Service and functional component intelligence elements, and joint reserve intelligence centers. If applicable, the JIOC establishes and maintains ties and connectivity with interagency partners such as the Central Intelligence Agency (CIA), FBI, Department of State (DOS) and country teams, DHS, United States Coast Guard (USCG), and the Drug Enforcement Administration (DEA). IAW the CCMD theater or functional campaign plan, CCMD JIOCs establish intelligence exchange relationships with multinational partners to ascertain their potential and willingness to contribute to a combined intelligence effort.

5. Subordinate Joint Force Intelligence Organizations and Responsibilities

a. The size and organizational structure of a subordinate joint force's intelligence organization is determined by the JFC based on the situation, mission, and available intelligence resources. The roles and functions of a JTF's J-2 are varied based upon the scope of the JTF's mission and required support relationships. The JTF's J-2 activities include:

(1) **Plan and direct the overall intelligence effort on behalf of the JFC.** The J-2 develops and recommends PIRs based on the JFC's guidance, identifies intelligence capabilities shortfalls and knowledge gaps, 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, or JTF's JIOC, including personnel, information, and physical security.

(2) Provide situational awareness to the JTF commander, battle staff, and other staff elements, including components, if applicable. Integrate all-source intelligence and relevant information into the JTF-specific COP.

(3) Manage the JTF collection plan using all assigned collection capabilities and assets in direct support. Request additional collection capabilities through the CCMD J-2. Request additional intelligence capability through the CCMD J-2.

(4) Request production of JTF JIPOE products by the CCMD JIOC. Integrate separate intelligence preparation of the battlespace efforts into JIPOE products to better support JTF intelligence assessments.

(5) Provide continuous threat warning to the JTF commander, battle staff, component units, and multinational forces, as appropriate.

(6) Provide target intelligence and intelligence inputs for BDA, as necessary.

(7) Conduct liaison and provide intelligence products and support to the following JTF entities, as applicable:

(a) Joint targeting coordination board.

(b) JCMB.

(c) IO cell.

(d) Joint personnel recovery team.

(e) Civil-military J-3.

(f) Joint planning group.

(g) Geospatial intelligence (GEOINT) cell.

(h) Red team.

(i) JIPOE coordination cell.

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

b. In order to accomplish the assigned mission, the joint force J-2 uses a combination of the following elements:

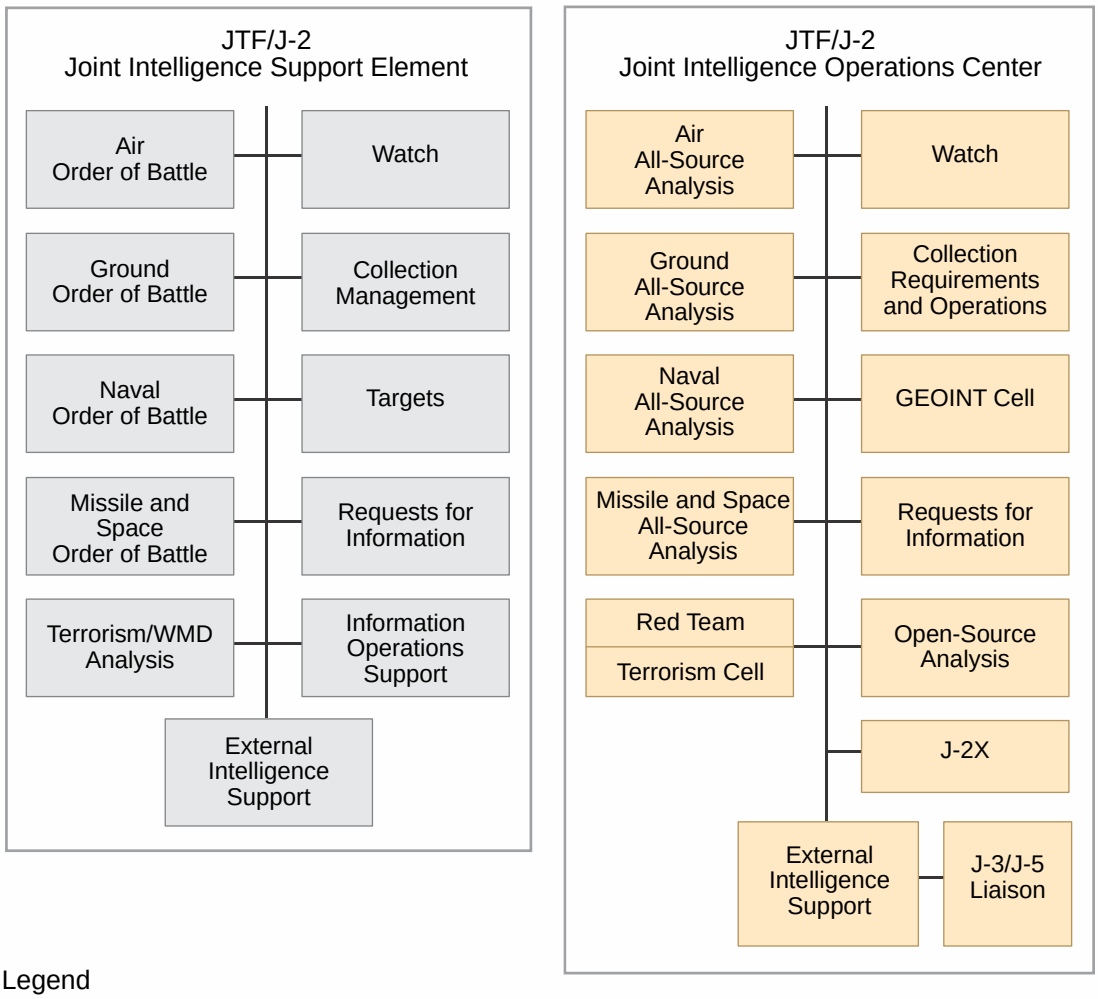
(1) At the JTF level, a JISE is normally established; however, a JIOC may be established at the direction of the JFC based on the scope, duration, and mission. For the remainder of this document "JISE" will be used as the standard term to describe the intelligence organization at the JTF level. Working together, these organizations play the primary role in managing and controlling the various types of intelligence functions and operations that comprise the intelligence process. The JISE provides the JTF with tailored intelligence products and services with a continuous analytical capability. Capabilities of the JISE may include OB analysis, collection management, target intelligence, IO analysis, a warning intelligence watch, and a request for information (RFI) desk.

(2) Alternatively, in a particularly large or protracted campaign, the JTF commander may decide to employ an operational-level JIOC. An operational-level JIOC incorporates the capabilities inherent in a JISE, but is generally more robust. The JTF JIOC may incorporate liaison elements from the supported CCMD JIOC, as well as

defense intelligence components and IC organizations not present in the JTF JISE. A notional JISE and JIOC organizational structure is provided in Figure II-2.

(3) **Joint Force Counterintelligence and Human Intelligence Staff Element (J-2X).** In coordination with the CCMD J-2, the JFC normally establishes a J-2X. This organization integrates human intelligence (HUMINT) and CI by combining the HUMINT operations cell, the task force counterintelligence coordinating authority

Notional Joint Intelligence Support Element and Joint Intelligence Operations Center



Legend

GEOINT	geospatial intelligence	J-3	operations directorate of a joint staff
J-2	intelligence directorate of a joint staff	J-5	plans directorate of a joint staff
J-2X	joint force counterintelligence and human intelligence staff element	JTF	joint task force
		WMD	weapons of mass destruction

Figure II-2. Notional Joint Intelligence Support Element and Joint Intelligence Operations Center

(TFCICA), a HUMINT analysis and requirements cell, and a CI analysis cell, all of which comprise the J-2X. The J-2X should also include an operational support cell staffed to operate continuously. The J-2X may also include an operational support element to provide services of common concern to the HUMINT operations cell and TFCICA, such as report and source administration, linguistic support, 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 manages, coordinates, and deconflicts HUMINT and CI collection within the joint operations area. The J-2X maintains the command source registry, deconflicts source matters, and performs liaison functions with external organizations. It is imperative 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, Counterintelligence and Human Intelligence in Joint Operations.

(4) **GEOINT Cell.** The JFC may establish a GEOINT cell and designate a GEOINT officer to manage the framework for accessing GEOINT data to enhance the joint force's COP for situational awareness and decision making. GEOINT support includes imagery, imagery intelligence (IMINT), and geospatial information and services (GI&S).

For more detailed guidance, see JP 2-03, Geospatial Intelligence in Joint Operations.

(5) **National Intelligence Agency Support.** The JFC, at the recommendation of the J-2, may request that the national IC analysts or subject matter experts deploy to support a JISE or operational-level JIOC.

c. The JTF J-2 should assist subordinate component command directors of intelligence in achieving their objectives through integration with the CCMD J-2, JIOC, and JTF J-2 processes. Subordinate directors of intelligence have the capability, either organically or via Service reachback, to provide support to the joint force through the following functions:

(1) Interface with CCMD J-2-directed intelligence systems architecture and targeting automation.

(2) Integrate into CCMD J-2-directed intelligence collection strategy.

(3) Notify CCMD and/or JTF J-2 regarding component commands' commander's critical information requirements (CCIRs), PIRs, and essential elements of information (EEIs).

(4) Support CCMD J-2 and/or JTF J-2 warning intelligence processes.

(5) Develop RFIs to fill intelligence gaps, and process those RFIs through the CCMD J-2-directed RFI process.

(6) Participate in the CCMD J-2 or JTF J-2 JIPOE process.

(7) Develop collection for the CCMD J-2 or JTF J-2 collection management board.

(8) Integrate in CCMD J-2 GI&S process and architecture.

(9) Participate in CCMD J-2 document and media exploitation (DOMEX) and interrogation processes.

(10) Produce target intelligence products as required and formulate target nomination lists that support their component commander's objectives.

(11) Integrate into and support CCMD J-2 OB and electronic OB processes.

(12) Provide battle damage indications and other directed information to support CCMD J-2 and federated processes as directed.

(13) Provide mensurated coordinates to support subordinate forces per CCMD J-2 guidance and obtain CCMD J-2 point mensurated certification as required IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3505.01, *Target Coordinate Mensuration Certification and Program Accreditation.*

(14) Provide intelligence support to, and augment the intelligence infrastructure of, subordinate joint forces.

(15) Maintain awareness and provide amplification as required of intelligence-derived threat warning events and actions.

SECTION B. NATIONAL INTELLIGENCE

6. Overview

The IC had its origin in the National Security Act of 1947, amended by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, and guided by Executive Order (EO) 12333, *United States Intelligence Activities*, as amended. It refers in the aggregate to those executive branch agencies and organizations that are funded in the National Intelligence Program (NIP). The IC consists of the DNI and 16 member organizations.

a. **IC Governance.** The IRTPA established the Office of the Director of National Intelligence (ODNI) with specified authority over the NIP budget, appointment of certain IC agency heads, IC personnel policies, tasking for collection and analysis, foreign liaison, and protection of intelligence sources and methods.

b. National intelligence organizations conduct extensive collection, processing, analysis, production, and dissemination activities. These intelligence organizations employ specialized resources and dedicated personnel to gain information about

adversaries, events, and other worldwide IRs. 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. As determined by the joint force J-2 during IP, the integration of national intelligence capabilities can substantively enhance intelligence support to JFC decision making.

For more information on IP, see JP 2-0, Joint Intelligence; *CJCSI 3110.02,* (U) Intelligence Planning Objectives, Guidance, and Tasks; *and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3314.01,* Intelligence Planning.

c. Successful support to JFCs by national IC elements and defense intelligence enterprise components that are not national IC elements (e.g., CCMD JIOCs and the Joint Staff J-2).

7. Department of Defense Intelligence and Combat Support Agency Organizations and Responsibilities

a. The **Under Secretary of Defense for Intelligence (USD[I]).** USD(I) serves as the principal staff assistant to SecDef and Deputy Secretary of Defense regarding intelligence, CI, security, sensitive activities, and other intelligence-related matters. USD(I) also exercises SecDef's authority, direction, and control over, and oversees the activities of, DIA, the National Geospatial-Intelligence Agency (NGA), the National Security Agency/Central Security Service (NSA/CSS), the National Reconnaissance Office (NRO), and the Defense Security Service and exercises planning, policy, and strategic oversight over all DOD intelligence, CI, and security policy, plans, and programs. The USD(I) manages all-source defense intelligence analytical efforts through the Defense Intelligence Analysis Program (DIAP). On behalf of SecDef, USD(I) consults and coordinates with the Under Secretary of Defense (Comptroller/Chief Financial Officer) on military intelligence program (MIP) budgetary matters and DNI on NIP budgetary matters; coordinates with ODNI to develop, synchronize, and implement annual NIP and MIP priorities; and coordinates with the CJCS to ensure defense intelligence, CI, and security components within the operating forces (Services and CCMDs) are resourced to support DOD missions and are responsive to collection and advisory tasking by the DNI. The USD(I) monitors MIP implementation and execution by the Services and the defense intelligence components.

b. The **NJOIC.** The NJOIC is an integrated Joint Staff J-2/J-3 [Operations]/J-5 [Strategic Plans and Policy] element that monitors the global situation on a continual basis and provides the CJCS and SecDef a DOD planning and crisis response capability. The NJOIC is located within, and is an integral part of, the National Military Command Center. The intelligence component of the NJOIC maintains an Alert Center that consists of the deputy director for intelligence, regional desks corresponding to each geographic CCMD, and representatives from each Service intelligence staff element, the intelligence defense agencies, and the CIA. The Alert Center is a continuously manned, all-source, multidiscipline intelligence center providing defense intelligence situational awareness, warning intelligence, and crisis management intelligence support to the President of the

United States, SecDef, Joint Chiefs of Staff (JCS), CCMDs, deployed forces, Services, and other intelligence consumers during peace, crisis, and war. It provides planning, management, and infrastructure for intelligence working groups (IWGs) and intelligence task forces (ITFs) that provide direct intelligence support during major conflicts. To provide intelligence analytical depth, DIA maintains a 24/7 direct support element (DSE) at the NJOIC, tailored to the current global situation and operations tempo. The NJOIC coordinates the intelligence response to immediate crises and contingencies.

c. If a developing situation escalates into a crisis, the relevant Alert Center regional desk officer is augmented with analytical support; an intelligence cell, IWG, or ITF is formed. Thus, support may range from a few additional analysts in an intelligence cell to a continuously staffed IWG or ITF augmented as required.

(1) **Intelligence Cell or Focus Group.** A cell or focus group is established based on indications that a threat to US interests or personnel may exist or when other potential crisis situations arise. The cell or group is formed to respond to the requirements levied by the NJOIC or CCMD JIOCs. The cell monitors and provides a continuous assessment of the developing situation. An intelligence cell is generally formed with personnel from the Joint Staff J-2, and the size of the cell or unit is determined by the crisis. While the cell or focus group is not continually manned, extended duty hours or 24-hour operations and augmentation from DIA may be warranted.

(2) **IWG.** As a crisis develops, an IWG may be established within the NJOIC 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 Office of the Secretary of Defense (OSD), CJCS, Joint Staff, Services, CCMDs, and deployed operational forces; and is normally manned from Joint Staff J-2 and DIA resources with reserve augmentation. The IWG is continually manned if warranted by the level of crisis.

(3) **ITF.** If a crisis situation continues to escalate, or SecDef orders a significant military response to the crisis, 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. The intelligence defense agencies, CIA, and other national IC 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:

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

(b) Provides time-critical responses to requirements from the OSD, CJCS, Joint Staff, Services, CCMDs, and deployed operational forces.

(c) Provides timely warning to the OSD, CJCS, Joint Staff, Services, and CCMDs of hostilities or potential threats to US interests in the ITF's area of concern.

(d) Develops and tailors an all-source intelligence collection strategy for the DOD response to the crisis.

(e) Responds to requirements from other USG departments and agencies responsible for crisis response activities.

(f) Responds to requirements of the United Nations (UN) and/or foreign governments consistent with ODNI guidelines and in coordination with the DIA Foreign Disclosure Office.

(g) Coordinates tasking of other USG departments and agencies in support of OSD, CJCS, CCDRs, subordinate JFCs, and other consumers.

d. **DIA.** DIA is an intelligence CSA under SecDef and a member of the national IC. The Director, DIA, reports to SecDef through the CJCS. DIA's combat support mission is to provide support for operating forces planning for, or conducting, military operations, including support during conflict or in the conduct of other military activities related to countering threats to US national security. DIA also provides SecDef and the Deputy Secretary of Defense, the CJCS, the DNI, and other US decision makers with all-source intelligence to improve decision making and prevent strategic surprise. Through regional and functional centers, DIA facilitates federated intelligence support to military operations in response to intelligence customer needs and requirements. DIA conducts overt and clandestine HUMINT collection focusing on requirements of importance to DOD. DIA also leads efforts to align intelligence activities and links and synchronizes national, defense, and military intelligence. DIA analytical and operational support includes:

(1) CI and HUMINT.

(2) Counterterrorism.

(3) Counterdrug operations.

(4) CO.

(5) Personnel recovery.

(6) Counterproliferation of WMD and associated delivery means.

(7) UN peacekeeping and multinational support.

(8) Measurement and signature intelligence (MASINT).

(9) Noncombatant evacuation operation efforts.

(10) Warning intelligence.

(11) Target intelligence (including BDA).

(12) Current intelligence.

(13) Collection management.

(14) Intelligence architecture and systems support, including program management of community on-line intelligence system for end-users and managers (COLISEUM).

(15) DOMEX.

(16) Counterinsurgency support (including the forensic collection and exploitation of improvised explosive devices [IEDs] and other weapons systems derived from weapons technical intelligence [WTI]).

(17) IO.

(18) Threat finance intelligence.

(19) Counter-transnational organized crime.

(20) Foreign military OB.

(21) Defense critical infrastructure.

(22) Global intelligence analysis through open-source intelligence (OSINT) integration.

(23) Integration of foreign partner intelligence capability.

(24) Facilitation of multinational intelligence sharing for unity of effort and understanding.

e. **Additional functions of DIA:**

(1) **Collection Management.** The Director, DIA, operates as the defense intelligence collection manager to:

(a) Support DOD and the CCDRs by developing and recommending globally optimized sourcing solutions for intelligence units and personnel capabilities (excluding platform/sensor based intelligence collection and associated processing, exploitation, and dissemination [PED] capabilities).

(b) Perform mission analysis on emerging crisis IRs and recommend the appropriate office of primary responsibility to respond.

(c) Receive, validate, and prioritize collection requirements from the CCMDs, and coordinate collection and production responsibility with appropriate agencies.

(d) Maintain global visibility of DOD intelligence operations and capabilities.

(e) Provide an intelligence operation global situation awareness display.

(f) Assess effectiveness of intelligence operations.

(g) Deconflict competing requirements for intelligence collection and processing resources, and forward recommendations to resolve conflicts to SecDef, through the CJCS, for approval.

(2) **IP.** The DIA planning and exercise organization supports the CCMD IP process led by the Joint Staff J-2 IP Functional Manager to develop dynamic threat assessments and theater intelligence assessments (TIAs) and national intelligence support plans (NISPs) to support the development and execution of President-, SecDef-, or CJCS-directed CCDR plans and orders and assists the CCMDs in evaluating NISP production requirements matrixes (PRMxs).

For more information on IP, see Chapter III, "Intelligence Operations."

(3) **Support to CCMD JIOCs and JFCs.** The Director, DIA, develops and recommends, through the Joint Staff deputy director for intelligence operations, plans, and policy, globally optimized sourcing solutions for intelligence units, personnel, and capabilities, not including platform/sensor-based intelligence collection capabilities and associated PED issues; provides personnel and resources to support CCMD intelligence directorates and JIOCs; provides a DIA senior representative to each CCMD JIOC to advise on collection capabilities and IP; serves as the defense intelligence enterprise global force manager for military intelligence personnel; and, along with the Services, prepares, equips, trains, and deploys military intelligence personnel in support of CCMD or JFC requirements.

f. **NSA/CSS.** NSA/CSS is a unified organization structured to provide the signals intelligence (SIGINT) mission of the US and ensure the protection of national security systems for all USG departments and agencies. The National Security Agency (NSA) is an intelligence CSA under SecDef and is dual-tasked as a member of the national IC under the DNI. Through the National Security Agency/Central Security Service representative (NCR), NSA provides direct cryptologic and cyberspace support to the CCMD JIOCs through the Central Security Service (comprised of the Service cryptologic components). The Director, National Security Agency (DIRNSA)/Chief, Central Security Service (CHCSS):

(1) The general/flag officer serving as the Director, NSA, serves concurrently as the Commander, USCYBERCOM, a subordinate unified command under USSTRATCOM.

(2) Acts as the principal SIGINT advisor to SecDef, the DNI, and the JCS.

(3) Is designated as the national manager responsible for securing the USG's national security telecommunications and information systems.

(4) Exercises operational control (OPCON) over the United States Cryptologic System (USCS)—the SIGINT and cybersecurity activities of the USG.

g. **NGA.** NGA is an intelligence CSA under SecDef and is dual-tasked as a member of the national IC under the DNI. The Director, NGA, serves as the functional manager for GEOINT and is the principal GEOINT advisor to the DNI, SecDef, CJCS, and CCDRs. As functional manager, NGA develops GEOINT tradecraft standards, develops strategic guidance and procedures, and develops and enforces IT architecture and standards. NGA also ensures coordination across intelligence disciplines and IC elements. GEOINT consists of imagery, IMINT, and geospatial information. GEOINT exploitation includes analysis of electro-optical, infrared, and radar imagery; full motion video; moving target indicators; geospatial information; and spectral, laser infrared, radiometric, polarimetric, spatial, and temporal data. It employs ancillary data, signature information, and fused data products. NGA conducts GEOINT analysis to combine imagery, IMINT, and geospatial information to produce tailored, actionable intelligence to support customers across a broad range of DOD and the USG. NGA provides direct support to the CCMD JIOCs and procures and disseminates commercial, remotely sensed imagery for DOD and the IC.

h. **NRO.** The NRO is a DOD agency and a member of the national IC. The Director, NRO, reports to both the DNI and SecDef. NRO is responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other USG needs. NRO activities support warning intelligence, monitoring of arms control agreements, access to denied areas, and the planning and execution of military operations. NRO provides direct support to the CCMD JIOCs.

i. **Service Intelligence Organizations.** The Chiefs of the Services provide intelligence support for DOD missions related to military systems, equipment, training, and national intelligence activities. The Services also provide support to DOD entities, including CCMDs and their components and each CCMD's JIOC.

(1) **Army Intelligence.** The Army Deputy Chief of Staff for Intelligence (G-2) is responsible for policy formulation, planning, programming, budgeting, management, staff supervision, evaluation, and oversight of intelligence, weather support, and geospatial activities for the Department of the Army. The Army intelligence enterprise includes intelligence staffs and military intelligence units assigned or attached at echelons from theater army, through corps and division, down to battalion level. The G-2 also exercises staff supervision over the United States Army Intelligence and Security Command (INSCOM). INSCOM provides intelligence support to commanders in the

areas of GEOINT, SIGINT, tactical and strategic HUMINT, CI, IO, and general military and scientific and technical intelligence (S&TI). The INSCOM elements include:

(a) National Ground Intelligence Center responsible for the production of all-source intelligence for S&TI and general military intelligence on foreign ground forces.

(b) Army Operations Group conducts HUMINT operations.

(c) Army Cryptologic Operations lead the Army's cryptologic effort to satisfy SIGINT requirements.

(d) The 1st Information Operations Command provides information and cyberspace operational support.

(e) 116th Military Intelligence Brigade conducts tasking, collection, processing, exploitation, dissemination, of multiple organic and joint intelligence aerial-ISR missions.

(f) 300th Military Intelligence Brigade provides trained and ready linguist and military intelligence personnel.

(g) 704th Military Intelligence Brigade conducts SIGINT operations.

(h) 780th Military Intelligence Brigade conducts SIGINT and computer network operations.

(i) 902nd Military Intelligence Group provides direct and general CI support to Army activities and major commands.

(j) 66th, 207th, 470th, 500th, 501st, 505th, and 513th Military Intelligence Brigades conduct theater level, multidiscipline intelligence collection and analysis operations.

(2) **Air Force (AF) Intelligence.** The Deputy Chief of Staff of the Air Force for Intelligence, Surveillance, and Reconnaissance (AF/A2) is responsible for policy formulation, planning, evaluation, oversight, and leadership of AF global integrated ISR capabilities. As the AF's senior intelligence officer (SIO) in the IC, the AF/A2 is directly responsible to the USD(I). 25th AF, a subordinate to Air Combat Command, is responsible for executing AF/A2's global integrated ISR responsibilities. 25th AF organizes, trains, equips, and presents assigned forces and integrates their all-source intelligence capabilities to the AF, CCDRs, and CSAs. 25th AF provides multisource ISR products, applications, capabilities and resources, to include cyberspace and geospatial forces and expertise. Additionally, it is the Service cryptologic component responsible to the NSA/CSS for AF matters involving the conduct of cryptologic activities, including the full spectrum of missions directly related to both tactical warfighting and national-level operations. 25th AF organizations include:

(a) The AF Technical Applications Center, which performs nuclear treaty monitoring and nuclear event detection.

(b) The 9th Reconnaissance Wing, which provides national and theater command authorities with timely, reliable, high-quality, high-altitude reconnaissance products.

(c) The 55th Wing mission responsibility includes ISR, electronic attack, command and control (C2), presidential support, nuclear treaty verification, and precision awareness to national leadership and warfighters.

(d) The 480th and 70th ISR Wings provide global distributed and reachback ISR. The 70th ISR Wing works closely with the NSA/CSS, leveraging the net-centric capabilities of a worldwide cryptologic enterprise. The 480th ISR Wing capabilities include national cryptologic, IT, cyberspace ISR, tactical analysis, joint force air component commander-support, and SIGINT integration.

(e) The 363rd ISR Wing, which provides targeting-related intelligence to air component forces.

(f) Additional AF intelligence organizations include:

1. The National Air and Space Intelligence Center, DOD's center of excellence for foreign air and space threats. The mission of the National Air and Space Intelligence Center is to make sure the nation is at the cutting edge of understanding foreign threats to US air and space operations.

2. 688th Cyberspace Wing, which provides IO-related intelligence.

3. The AF Office of Special Investigations, which is responsible to the US AF Inspector General, provides a full range of CI and criminal investigative services.

(3) **Navy Intelligence**

(a) The Director of Naval Intelligence is the Navy's intelligence executive to the Chief of Naval Operations and the Operational Navy staff. As such, the Director of Naval Intelligence exercises overall authority through the Department of the Navy on matters pertaining to intelligence, cryptology, CI, and special security. The Director of Naval Intelligence manages the Navy portion of the NIP, sets naval intelligence policy, and directs naval IP and programs. The Commander, Fleet Cyber Command, serves as the Navy's Service cryptologic component commander. The Naval Criminal Investigative Service provides law enforcement and security services in the form of combating terrorism programs to the Navy and Marine Corps on a worldwide basis.

(b) The Office of Naval Intelligence (ONI) is the leading provider of maritime intelligence to the US Navy and joint forces, as well as national decision makers and other consumers in the IC. ONI specializes in the analysis, production, and

dissemination of vital, timely, and accurate scientific, technical, geopolitical, and military intelligence information to key consumers worldwide. ONI organizations include:

1. **Nimitz Operational Intelligence Center.** The Nimitz Operational Intelligence Center functions to meet the increasing demand for rapid access to operational intelligence by aligning with globally netted maritime operation centers. The Nimitz Operational Intelligence Center is composed of cells and detachments that support numbered fleets and naval warfare enterprises.

2. **Farragut Technical Analysis Center.** The Farragut Technical Analysis Center is focused on foreign science and technology research, development, and proliferation. The Farragut Technical Analysis Center's mission is to deliver knowledge of current and future foreign navy capabilities to enable long-range planning and research, guide future acquisitions, and prevent technological surprise.

3. **Kennedy Irregular Warfare Center.** The Kennedy Irregular Warfare Center functions to meet the expanding demands of Naval Special Warfare Command and Navy Expeditionary Combat Command. It is comprised of two cells: a deployed forces cell, which embeds into navy special warfare squadrons, and a global analysis cell, which provides all-source operational intelligence reachback and imagery services to expeditionary forces.

4. **Hopper Information Services Center.** The Hopper Information Services Center provides mission-related IT services and ensures the rapid and reliable delivery of intelligence to operational forces and intelligence customers worldwide through service oriented architecture.

(c) Naval Information Forces is an echelon command under Commander, US Fleet Forces, which is responsible to staff, train, and equip intelligence entities (to include SIGINT) for afloat and shore-based commands.

(d) The Navy IO commands produce IOII.

(4) **Marine Corps Intelligence**

(a) The Director of Intelligence is the Commandant of the Marine Corps' principal intelligence staff officer, the functional manager for intelligence and cryptologic activities, and the chief architect for the Marine Corps Intelligence Activity (MCIA) and the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE), encompassing all aspects of the intelligence warfighting function. As such, the Director of Intelligence serves as the Service Intelligence Chief for joint intelligence matters and formulates policy for intelligence, CI, and electronic warfare.

(b) The Headquarters, Marine Corps (HQMC) Intelligence Department is responsible for policy, plans, programming, budgets, and staff supervision of intelligence and supporting activities within the US Marine Corps. The HQMC Intelligence Department supports the Commandant of the Marine Corps in his role as a member of the JCS, represents the Service in joint and IC matters, and exercises supervision over the

MCIA. The HQMC Intelligence Department has Service staff responsibility for GEOINT, SIGINT, HUMINT, MASINT, CI, OSINT, and the tactical exploitation of national capabilities program (TENCAP), and ensures there is a single synchronized strategy for the development of the Marine Corps ISR capabilities.

(c) MCIA is the Service intelligence center fully integrated into the DIAP. Through this program, MCIA provides expeditionary warfare intelligence to support national, theater, or operational requirements. MCIA serves as the hub of the Marine Corps ISR enterprise; is the focal point for Marine Corps distributed common ground/surface system (DCGS) intelligence product exposure to the DOD DCGS enterprise; and provides reachback for collection management, analysis and production, and targeting support to MCISRE units.

(d) The Marine Corps Information Operations Center is the responsible service center for the production of IOII.

(5) **National Guard (NG) Intelligence.** While the NG is not a separate Service, NG incident awareness and assessment (IAA) intelligence assets can provide a dissemination and communications bridge between state/local authorities and DOD agencies. These forces can serve as a liaison between DOD and state/local agencies, provide augmentation and liaison to state and local agencies, as well as serve the needs of the DOD for IAA local intelligence support. The NG Bureau J-2 provides national-level support and coordination on intelligence issues with Joint Staff J-2, defense intelligence components, National Guard joint force headquarters-state (NG JFHQs-State), CCMDs, Service intelligence components, and USG departments and agencies. The NG Bureau J-2 provides intelligence products, policy guidance, training, tools, and enabling forces for foreign intelligence, IAA, and special security activities to the NG JFHQ-State and NG forces in Title 32, United States Code, or state active duty status. Many NG units are embedded with their active duty counterparts, particularly throughout the AF DCGS. A handful of NG entities own their own DCGS and operate in direct support to their active duty counterparts. In both aspects, the source of AF intelligence offerings is transparent to the warfighter.

For more information on NG intelligence activities, see Chief National Guard Bureau Instruction, 2000.01, National Guard Intelligence Activities.

8. National Intelligence Community Organizations and Responsibilities

a. The IRTPA created the ODNI to improve information sharing, promote a unified and strategic direction for the IC, and ensure integration of effort across the IC. ODNI is led by the DNI. The DNI serves as the principal advisor to the President, National Security Council (NSC), and Homeland Security Council for intelligence matters related to national security and oversees and directs the implementation of the NIP. The DNI and the presidentially appointed, Senate-confirmed Principal Deputy Director of National Intelligence work closely with their leadership team, core mission enablers, and oversight offices to effectively integrate foreign, military, and domestic intelligence in defense of the homeland and in support of US national security interests at home and abroad. The

ODNI is comprised of several components, including the National Counterterrorism Center, the National Counterproliferation Center, the National Counterintelligence Executive, and the National Intelligence Council.

(1) The IRTPA also established national mission managers under the DNI. Mission managers are the principal IC officials overseeing all aspects of national intelligence related to their respective mission areas. Mission areas are enduring problem sets involving either a regional actor or a transnational issue, such as proliferation of WMD. The mission managers are tasked with understanding the requirements of their customers and ensuring intelligence capabilities are appropriately tasked, information is processed, and analysis is performed to satisfy those requirements. Where intelligence gaps are identified, mission managers are tasked to plan strategies to collect the data and to evaluate IC performance in fulfilling assigned tasks.

(2) The National Intelligence Coordination Center (NICC) is the DNI's central node to deconflict national and DOD intelligence activities and enhance collection management efforts across the IC.

b. The **CIA** is the largest producer of all-source national security intelligence to senior US policy makers and provides extensive political and economic intelligence to DOD senior decision makers. CIA also oversees the Open Source Enterprise.

(1) The Director, CIA, serves as the National HUMINT Manager and coordinates, deconflicts, and evaluates clandestine HUMINT operations across the IC.

(2) The Director, CIA, is also responsible for the National Clandestine Service, directing clandestine collection (primarily HUMINT) of foreign intelligence that is not obtainable through other means. The National Clandestine Service also conducts CI to protect US activities and institutions from penetration by hostile foreign organizations and individuals.

(3) The CIA Directorate of Intelligence analyzes all-source intelligence and produces finished intelligence products on key foreign intelligence issues. This information comes from a variety of sources and methods, including US personnel overseas, HUMINT reports, satellite imagery, open-source information, and other sensors.

(4) The Directorate of Science and Technology accesses, collects, and exploits information to facilitate the execution of the CIA's mission by applying innovative scientific, engineering, and technical solutions to the most critical intelligence problems.

c. The **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 Bureau of Intelligence and Research provides all-source intelligence primarily to support both foreign policy and national security with an emphasis on terrorism and foreign law enforcement activities, including proliferation concerns.

d. The **FBI** has multiple domestic and global law enforcement and investigative roles. The FBI also has an intelligence branch with domestic and foreign partner engagement capabilities. The FBI has primary responsibility for CI and counterterrorism operations conducted in the US. FBI CI operations overseas are coordinated with the CIA. The FBI shares law enforcement/CI information with appropriate DOD entities and CCMDs. The FBI foreign partner engagement program focuses on communications coordination and cooperation with designated foreign law enforcement, intelligence, and public/private partners to enable intelligence and information sharing.

e. The **Department of the Treasury** analyzes foreign intelligence related to US economic policy and participates with DOS in the overt collection of general foreign economic information. The Department of the Treasury provides intelligence support through their Office of Intelligence and Analysis focused on counter threat finance, analyzing economic support for illicit networks, and economic intelligence for economic sanctions determination. The counter threat finance efforts support DOS and DOD through collection and analysis of economic knowledge of terrorist networks, proliferation of WMD, narcotics trafficking, and illicit finance.

f. The **Department of Energy** analyzes foreign information relevant to US energy policies and nonproliferation issues and the national science laboratories under its authority.

g. The **DHS** 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. DHS is also a member of the NICC.

h. The **USCG,** a component of DHS, operates as an armed force, a law enforcement organization, and an IC element. The USCG's Intelligence Coordination Center (ICC) and maritime intelligence fusion centers operate under the direction of the Assistant Commandant for Intelligence. The USCG ICC is the central hub for collection, fusion, analysis, and dissemination of maritime intelligence and information to Coast Guard operating units, DHS, and all members of the IC, including DOD and key decision makers at the national level.

i. The **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. The 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 efforts 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.

9. Joint and National Intelligence Support Forums

a. **CCMD JIOCs.** The CCMD JIOC is the first stop for CCMD staff, component Service commands, and subordinate joint force headquarters (HQ) IRs. For non-time-sensitive requirements, JIOCs receive RFIs from CCMD staff elements and subordinate intelligence organizations through COLISEUM. The RFIs are validated and researched to determine whether the information exists in either theater or national intelligence databases that are accessible to the JIOC. If the JIOC determines that the RFI asks for information that is unavailable or represents an intelligence collection gap, the JIOC RFI manager forwards it for action to the JIOC element that performs mission operations. The JIOC employs intelligence planners to validate the requirement and theater analysts and collection managers to conduct mission analysis on the requirement, choose the best COA for requirement satisfaction, and task theater intelligence collection assets or request national collection agency support to obtain the information. Requests for national agency support are normally forwarded to DIA using COLISEUM. Time-sensitive collection requirements may go directly to the appropriate national intelligence agency using its on-site representative, with a follow-up request using the requested intelligence discipline's requirements management tool. Time-sensitive RFIs that require production may also go directly to the appropriate national intelligence agency with a follow-up request in COLISEUM.

b. **DNI Representative.** The DNI provides representatives to each of the CCMDs to coordinate national IC support to the command and to facilitate access to IC resources. DNI representatives also advise and assist the command regarding secondary and follow-on dissemination of originator-controlled material and HUMINT control system information.

c. **DIA.** DIA maintains senior representatives at each of the CCMDs, USFK, Supreme HQ Allied Powers Europe, and North Atlantic Treaty Organization (NATO) HQ. Each DIA senior representative organization includes a SIO who serves 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 DIA senior representative organization typically includes a HUMINT support element consisting of one or more DIA HUMINT personnel, an intelligence production liaison officer (LNO), and a measurement and signature intelligence liaison officer (MASLO). Some DIA senior representative organizations also have IT and Defense Combating Terrorism Center representatives. The DIA senior representative, as the forward representative of DIA, enhances and expedites the exchange of information between DIA and the supported command. It provides an on-site interface between DIA and the command, advising them on the roles, missions, and capabilities of DIA while ensuring that command requirements are understood by DIA.

(1) **The National Measurement and Signature Intelligence Office (NMO) LNO.** NMO provides MASINT representatives to the CCMDs in the form of MASLOs. The MASLO helps expedite a broad spectrum of MASINT operational support between NMO and the supported command. For example, the MASLO provides technical assistance on MASINT capabilities available to support military operations.

Additionally, MASLOs are the means for providing feedback on the commander's operational needs for integration into MASINT-related current operations and future acquisition requirements.

(2) **DSE.** The DSE, located in the NJOIC, serves as the crisis management office for the DIA Directorate for Analysis (DI). The DSE is the single point of contact (POC) 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 DSE transitions to 24-hour operations as required, and the size and number of DSE watch teams varies depending upon the nature and duration of each crisis.

d. **National Agency CCMD Representatives.** CIA, NSA/CSS, NGA, and NRO support CCDRs on a full-time basis through representatives. Some of these representatives are located full time at the command JIOC. These representatives serve as the CCDR's advisors on how to best employ their organization's capabilities and provide liaison with their parent organizations. The CCDR and J-2 should fully utilize these representatives to ensure the command is familiar with the current responsibilities, capabilities, and operations of the representative's parent organization.

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

(a) NCRs are senior representatives of DIRNSA/CHCSS accredited to the CCMDs, other senior military commands, DOS, and DOD. The NCRs at the military commands are the senior cryptologic authorities in the region and are the special advisors to the CCDR for all cryptologic matters.

(b) CSGs are extensions of the National Security Operations Center and are the primary mechanism for the supported organization to gain entrance into and support from the 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.

(2) **NGA Representatives.** NGA provides representatives to the CCMDs in the form of National Geospatial-Intelligence Agency support teams (NSTs) composed of staff officers, imagery analysts, and geospatial analysts. The NST is the central POC for all operational and training support from NGA. In addition, the NST helps CCMDs understand emerging GEOINT concepts, technologies, and procedures; supports developing GEOINT system services; coordinates geospatial support; and arranges meteorological and oceanographic (METOC) support from the joint METOC officer.

(3) **NRO Representatives.** NRO provides field representatives to the CCMDs. These NRO field representatives provide technical assistance relating to the capabilities of NRO systems to support operations. These field representatives also provide insights

on warfighter operational needs for integration into NRO present operations and future acquisitions.

e. **National Intelligence Support.** National intelligence agencies can provide support to commanders during crisis or contingency operations. Joint force J-2s—through their CCMD JIOCs and IC liaisons—should submit requests for allocation of intelligence support capabilities through the Global Force Management Allocation Plan (GFMAP) and through annex B to APEX plans and orders as determined by the CCMD J-2. Joint Staff J-2 should communicate support requirements to the IC, defense intelligence officers (DIOs), and national intelligence managers (NIMs).

(1) **Composition and Size.** The composition of national intelligence agency support 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 supporting effort should be reviewed and modified as required in coordination with the supported commander. Each supporting agency is responsible for communication equipment and workstations.

(2) **Required Support from Supported Commands.** Supporting national intelligence agencies may require infrastructure, transportation, logistic, and bandwidth support from the supported command. At a minimum, it will require electric power, adequate workspace within a temporary SCIF, and expendable administrative supply items. The supported command arranges the transportation for personnel and equipment from the continental US marshalling area to the operational area during initial deployment and redeployment. Lodging and dining facilities are provided and funded by the supported command. Additionally, the supported command may need to provide mission-specific military equipment.

(3) **National IC Support and Joint Force Relationship.** Forward national intelligence agency assets are deployed in direct support of the JFC, under the staff supervision of the J-2, and perform functions as designated. Subject to restrictions based on security clearance and program access, all intelligence generated should be available to the J-2 organization and JFC.

f. **Crisis Intelligence Federation.** In response to an unforeseen situation, joint forces may garner support from the IC through the crisis intelligence federation process. Based on J-2 staff estimates, the supported CCMD J-2 coordinates crisis intelligence federation support with the NJOIC.

Specific planning guidance for crisis intelligence federation is discussed in Chapter III, "Intelligence Operations," Section A, "Planning and Direction."

g. **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-2 Global Force Management Branch coordinates the specialized intelligence support provided by various organizations to supported CCMDs

in order to preclude redundancy with any support being provided by crisis federation partners.

(1) 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 GEOINT or MASINT support. Augmentees may also provide specialized support in areas such as DOMEX, WTI, forensic-enabled intelligence (FEI), and biometrics-enabled intelligence (BEI) specifically related to counterinsurgency and countering IEDs. These capabilities may deploy with other supporting joint force units as requested.

(2) NSA/CSS can provide support teams for crisis response missions. The teams provide enhanced situational awareness, threat warning, personnel recovery support, and tailored intelligence products as required. During the initial stages of crisis or sensitive joint operations, a CCDR can request the immediate deployment of a support team to provide remote, limited access to NSA threat warning and intelligence networks. To further expedite augmentation during time-sensitive planning, support team notification procedures for activation and deployment of a team can be predetermined by a memorandum of agreement between NSA/CSS and the supported command. The team requires logistics and transportation support, and usually redeploys after arrival of J-2 elements or other augmentation.

(3) **NIM.** NIMs oversee and integrate all aspects of the IC's collection and analytic efforts against a particular region or function. Each NIM serves as a single focal point within ODNI for the integration of all activities related to a particular region or function, as well as being the DNI's personal representative on the issue. NIMs maintain senior-level contacts with the intelligence, policy making, and warfighting communities so that a full range of IRs for a particular function or region are met on a daily basis. NIMs also establish strategic guidance to improve long-term IC collection and analysis.

(4) **DIOs.** DIOs serve as the primary advisers in their areas of expertise to the Director and Deputy Director of DIA. They are the DOD counterparts to the NIMs. DIOs coordinate with CCMD J-2s and DIA senior representative organizations to advise and assist them with mission and resource decisions.

10. Intelligence and the Department of Defense Information Network

a. The Department of Defense information network (DODIN) is the set of information capabilities, associated processes, and personnel to collect, process, store, disseminate, and manage information on demand to joint forces and support personnel. The DODIN includes all communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. This environment supports all DOD and IC missions and functions, in war and peace, and at all operating locations. The DODIN provides interfaces to multinational and non-DOD users and systems.

b. The DODIN enables intelligence and operations information and schematics to provide a COP that facilitates interoperability between Service information systems and provides assured, secure, and tailorable information on demand to all appropriate users. The modern communications and IT that make the DODIN possible are undergoing continuous and rapid evolution. This technological dynamism affects all the various subarchitectures, systems, and applications resident in the DODIN. 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) DIA establishes DOD-wide intelligence priorities for attaining interoperability among the tactical, theater, and national intelligence systems and the respective communications systems at each level. 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 CCMD then takes this standard "package" and, in coordination with DIA, builds a theater intelligence architecture based on the mission, CCDR guidance, and command requirements.

(2) Developers, installers, and other information systems professionals should continuously improve the quality of their support to commanders by successfully creating and refining communications and information systems. However, technological development may be realistically tempered by the limitations of fielded and deployed systems and of the consumers themselves.

c. **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 CSA intelligence processes rely on a communications backbone consisting of Joint Worldwide Intelligence Communications System (JWICS) and SECRET Internet Protocol Router Network (SIPRNET). This infrastructure is supplemented by a distributed, common exploitation and dissemination system, tactical data links, and intelligence broadcast services to enable information sharing and collaboration.

(1) **JWICS.** JWICS is the IC's global communications network that provides DOD and IC users a mature, reliable, and flexible sensitive compartmented information (SCI) communications architecture. JWICS is designed to deliver secure, assured, efficient, interoperable information on a global basis to national and defense intelligence consumers. JWICS provides real-time SCI data and video teleconferencing (VTC) capability and connects deployed forces, on land and at sea, with their parent commands, the Services, national intelligence producers, senior DOD leadership, and other USG departments and 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. JWICS operates in three modes (i.e., fixed, containerized, and mobile) with the capability of supporting a joint force, and associated national IC support, in a fixed structure and/or field site.

(b) The complementary architecture of JWICS (data and/or video) and joint deployable intelligence support system (JDISS) workstations (data) spans strategic, operational, and tactical levels. The major JWICS applications are electronic publishing, VTC, and bulk data transfer, including large file imagery.

(c) The **Containerized Joint Worldwide Intelligence Communications System (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 the National Secure Telephone System.

(d) The **Joint Worldwide Intelligence Communications System mobile integrated communications system (JMICS)** provides a scalable, deployable JWICS that is self-contained on a heavy, high-mobility, multipurpose, wheeled vehicle for rapid deployment in all-weather, austere environments. Key features include satellite connectivity, fax, Non-classified Internet Protocol Router Network (NIPRNET), SIPRNET local area network (LAN), SCI LAN workstations, JDISS network servers, and SCI VTC equipment. Deployment of JMICS is coordinated by Joint Staff J-2 in support of national or joint force requirements.

(2) **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 e-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) **Integrated Broadcast Service (IBS)** disseminates near real time (NRT) tactically/operationally significant intelligence and information to the warfighter, providing situational awareness, rapid threat warning, friendly force tracking, combat search and rescue, missile defense and theater missile warning, and other vital data to the decision-making processes. IBS is a theater-tailored information and intelligence dissemination architecture with global connectivity that uses a standardized broadcast data format and a common receiver family and is interoperable with current and programmed tactical and strategic warfare systems. IBS is an interactive service that provides intelligence producers the means to disseminate strategic, operational, and

tactical information to the warfighter via multiple transmission paths IAW dynamic, user-generated dissemination priorities. This information is continually refined by data from strategic, operational, and tactical sensors.

(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 C2 system requirements.

(5) The Organizational Messaging Service provides the ability to exchange official information between military organizations and allied nations, USG activities, and the IC.

d. **Intelligence-Related Information Processing, Storage, and Management Systems.** These components of the DODIN consist of information processing, storage, and management applications specifically tailored to meet the broad array of intelligence activities supporting joint military operations.

(1) **Global Command and Control System-Integrated Imagery and Intelligence (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 OE 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 on both SCI and collateral networks.

(2) **Advanced Global Intelligence Learning Environment (AGILE)** is an IC-wide learning environment that encourages the sharing of learning solutions in the shared space and enables the IC training community to operate cohesively as a single enterprise. AGILE is available on JWICS, SIPRNET, and NIPRNET and offers an expanded choice of course offerings.

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

(4) **National Measurement and Signature IR System** provides national and DOD intelligence organizations with a common MASINT requirements submission and tracking system.

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

(6) The **Collection Management Tool** is accessed through JWICS and SIPRNET and comprises a tailorable suite of interoperable automated tools designed to enhance the collection planning, execution, and ISR battle management capability of CCMDs, subordinate joint forces, and components. The Collection Management Tool includes the Planning Tool for Resource, Integration, Synchronization, and Management, which is used in collection planning, operations, and managing of intelligence collection assets that are deployed to all CCMDs and USFK.

For more information on ISR management, see Appendix B, "Global Intelligence, Surveillance, and Reconnaissance Management."

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

(8) **Web Secure Analyst File Environment** provides intelligence analysts with the means of retrieving classified message traffic, intelligence information reports (IIRs), and abstracts of hard copy 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 and military infrastructure 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.

(11) **Special Operations Forces Exploitation Site** is a Web-based architecture that enables global submission of identity-based collections, including biometrics and DOMEX, NRT responses, and intelligence reachback support.

e. **Other Communications Resources**

(1) **The Joint Communications Support Element (JCSE).** The JCSE is a unique communications organization that provides contingency and crisis communications to meet the operational and support needs of the JCS, Services, CCMDs, DOD agencies, and non-DOD agencies. Requests for support should be completed IAW CJCSI 3110.10, *(U) Communications Systems Supplement to the Joint Strategic Capabilities Plan (JSCP).* 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 forces and special operations forces (SOF) use TROJAN SPIRIT II. Marine Corps forces use the High Bandwidth Special Intelligence-Palletized Terminal and the Expeditionary Command and Control System. Army, Marine Corps, and SOF all use JMICS and tactical LAN in support of joint requirements for intelligence support to subordinate joint forces. These systems provide communications connectivity to support

full JWICS, JDISS data, secure voice, and other unique intelligence communications needs.

(3) Liaison with other agencies or Service elements with communications capabilities, such as NSA/CSS 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 communications system directorate of a joint staff (J-6), may arrange to temporarily share their circuits to meet critical needs.

11. Intelligence Communications Architecture Planning

A wide range of national, theater, and component intelligence and communications systems are available to a JFC. The existence of this capability does not, however, ensure intelligence and communications systems can be deployed without significant planning and coordination. Supporting and supported communications paths should be established through prior coordination to extend DODIN services to the JFC. The CCMD J-2 should understand current systems 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 communications 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 should effectively coordinate communications architecture requirements with the J-6 and coordinate with the logistics directorate of a joint staff (J-4) and other logistic elements for the timely delivery and installation of intelligence and communications systems.

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-time/NRT intelligence continues to be a critical factor.

(1) **Step 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 and adversary's cyberspace attack capabilities. 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) **Step 2.** In step 2, the specific communications 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.

(3) **Step 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 intelligence information flow from one node to another.

(4) **Step 4.** During step 4, the joint force J-6 staff should 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 manpower and personnel directorate of a joint staff, J-3, J-4, J-5, and J-6 staffs at each security level.

b. **Architecture Planning.** The CCMD 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. 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 communications systems (e.g., JWICS). This architecture links the subordinate joint force with the Service components and multinational force units as well as with the CCMDs and the NJOIC.

c. **System Planning**

(1) Communications asset requirements should 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, application software, and communications bandwidth needed to provide simultaneous transmission of secure, interactive VTC; 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 CCMD JIOC, the subordinate joint force and components, and multinational partners).

(3) Requests to the CCMD J-6 for Defense Information Systems Agency (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 on-call circuitry activation IAW an approved OPLAN.

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

d. **Planning Considerations**

(1) Joint intelligence dissemination relies on a federated architecture across many agencies and systems. This allows JFCs access to relevant intelligence when needed, based on their mission and the specific phase of the ongoing operation, using services or service-oriented architectures to access intelligence data physically located and maintained at various locations. Additionally, the theater JIOC should determine the desired intelligence and enable access to the information directly to all echelons requiring it. It is vital that the JIOC prioritize its data exchanges according to CCMD and JTF guidance to enable the appropriate allocation of scarce resources.

(2) Every 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 collection resources among the major elements of the deployed joint force and supporting intelligence organizations worldwide.

SECTION C. INTERAGENCY, INTERGOVERNMENTAL, AND MULTINATIONAL INTELLIGENCE SHARING

12. Overview

Operations with a wide variety of partners are becoming the norm, making intelligence sharing with interagency and multinational partners increasingly important. The fundamentals of C2 are influenced through trust and shared understanding of the OE by the force, including mission and multinational partners. Trust and understanding occur through open intelligence and information sharing, while ensuring protection of US sources and methods are paramount. Most sharing is bilateral due to PN requirements or sensitivities. See Figure II-3 for examples of common entities and organizations with which DOD intelligence forces may form relationships. In operations involving

Figure II-3. Common Entities Encountered in Multinational Operations

multinational, interagency, international, or nongovernmental, entities, one of the most critical functions of the JFC is establishing a common view of the problem and shared situational awareness among all entities. Although intelligence sharing is accomplished at all levels during crises, in most operations the requirement expands with proximity to the operational forces. Therefore, it is imperative that the JFC, staff, J-2, subordinate units, mission, and multinational partners understand the permissions and restrictions on information sharing.

a. All operations conducted in conjunction with interagency, international, nongovernmental, or multinational partners involve intelligence sharing to some degree. The amount of intelligence required to be shared varies widely based on the nature of the military operation. In general, combat operations with multinational partners require much more robust intelligence sharing than humanitarian or peacekeeping operations. The joint force J-2 should scale the organization's capability to provide intelligence sharing accordingly.

b. The foreign disclosure officer (FDO) of the CCMD plays a key role in any intelligence sharing plan with multinational, interagency, or nongovernmental entities. The FDO is versed in all relevant national disclosure policy (NDP) and can guide the JFC and staff in the proper procedures for the release of classified or sensitive information. The FDO provides staff review and advises the JFC on approval of sanitized or downgraded military intelligence products. In the absence of an on-site FDO, intelligence products that require sanitization or downgrading for release to third parties should be referred to the producing agency through the command representative from that agency or may be coordinated through the RFI process. Since this process may be time-consuming, the JTF/J-2 should request deployed FDO support to optimize timely intelligence sharing requirements.

c. For most contingencies, the DNI may issue guidelines to the IC, covering:

(1) The types of intelligence products that may be shared, while protecting sources and methods.

(2) Guidelines for protecting sources and methods when sharing intelligence products.

(3) Who is authorized to prepare intelligence products determined for sharing.

(4) Organizations authorized to receive US intelligence.

(5) Manage classification markings to use on shared intelligence products.

(6) Procedures in case of unauthorized disclosure.

(7) Organizational responsibilities.

d. The FDO uses NDP and the DNI guidance to promulgate directives to CCMD intelligence analytical elements on preparation processes and procedures, including tear line reporting for intelligence shared with foreign partners. Tear line reports are derived from US intelligence products and written in such a way as to readily and quickly provide essential operational information without revealing the information's source. Tear line reporting is a mechanism for analytical elements at the CCMD, JTF/J-2, and component levels to provide intelligence-derived reporting and warnings to partners (multinational members without established intelligence sharing agreements; state, local, and tribal elements; and international and nongovernmental entities). CCDRs are delegated authority to conduct tear line reporting, which can be further delegated in writing to the JTF commander and below. The J-2 should use the principle of "write to release" when deciding whether to produce a tear line. That is, the information should be provided to the interagency, international, nongovernmental, or multinational partners if it is determined that the information contained in the report is relevant to the partner's mission and can be released to the partner.

13. Multinational Intelligence Collaboration

a. Typically, in a multinational operation, allied military partner intelligence counterparts may locate or colocate around the JTF HQ in the form of national intelligence cells. It is imperative for the JTF/J-2 in this environment to establish good working relationships with multinational partners to encourage a shared view of the OE. Allied nations also bring valuable intelligence contributions and can often provide niche capabilities in support of the overall JTF mission. Different participants in a multinational organization can contribute unique intelligence sources and useful perspectives on intelligence problems. However, US analysts should be aware that different nations have differing standards for assessing the reliability, validity, and confidence of their raw and processed intelligence. In addition, some participants may be limited by policy in what they may provide to the effort, and their analysis may be slanted due to national biases.

b. There is no standard template for a JTF/J-2's relationship with multinational partners, since it is situation-dependent. Although each situation is different, there are

certain issues that may be addressed before multinational intelligence collaboration can proceed. In addition to release and disclosure authorities and procedures, intelligence architecture and workspaces can become major issues. The policies and laws of each member of the multinational organization should also be considered. For example, some nations' laws may forbid participation in certain types of operations, and this could impact what sorts of intelligence those nations will contribute to the effort at different points, what general issues, individual operations, or specific missions their intelligence analysts can support; and even what their personnel may report or observe via full motion video. As levels of access may differ between participants in the multinational organizations, the J-2 needs to ensure the variations in access do not jeopardize the J-2's relationship with multinational partners needed for multinational access.

c. Detailed planning for information sharing should be accomplished well in advance of operations with PNs, if possible. A JTF/J-2 may decide how much intelligence can be provided and the mechanisms to use for sharing. This is made more complicated by the multiple classification levels allowed by the nature of the partners involved in the operation. Some allied countries have established intelligence-sharing agreements with the US, which permit almost seamless two-way flow of intelligence. A presidential decision directed access for Commonwealth allies (Great Britain, Australia, New Zealand, and Canada) to information at the collateral level via a Commonwealth releasable segment of the US SIPRNET in order to enhance information sharing. STONEGHOST is an encrypted communications network designed to support collaboration and intelligence sharing between the US defense IC and its Commonwealth allies during combat operations. Other allies have long-standing relationships with US Services and intelligence agencies, but release of US-produced intelligence is subject to review by the FDO. The United States Battlefield Information Collection and Exploitation System (US BICES) and United States Battlefield Information Collection and Exploitation System Extended (US BICES-X) provide US intelligence services and agencies a mechanism for sharing intelligence with foreign partners who have the appropriate agreements with the US. US BICES is an intelligence system that is the US gateway to the 28-member nation battlefield information collection and exploitation system (BICES); although not a NATO system, all 28 BICES member nations are part of NATO and each nation provides its own gateway for sharing collectively with all other members. By mutual agreement, BICES also allows nations to utilize the system for bilateral or multilateral intelligence sharing by implementing additional security measures. US BICES-X provides these same capabilities in support of intelligence sharing requirements for CCMDs outside the broader BICES community. For example, US BICES-X services in support of USPACOM are known as the Asia Pacific Intelligence Information Network. Within the United States Central Command's (USCENTCOM's) AOR, the system is referred to as the USCENTCOM Partner Network. US BICES-X is implemented with PNs or a grouping of nations in alignment with CCMD requirements and the appropriate policy, security, and technical agreements with the PN(s).

d. There exist a number of robust, multinational networks used as a backbone for intelligence exchange. Examples include Combined Enterprise Regional Information Exchange System (CENTRIXS); BICES and US BICES-X; and the Supreme HQ Allied

Powers, Europe's LAN, Cronos. These networks provide multiple intelligence applications, typical office software and Web browsing capabilities, and may also include collaboration and NRT data access tools, as well as secure voice over Internet protocol telephony. CENTRIXS, in particular, uses commercially available computers, software applications, and network equipment that are generally releasable to foreign partners. CENTRIXS, BICES, and US BICES-X all have the advantage of having a direct interface with national intelligence producing agencies such as NGA and DIA for direct insertion of products and databases.

e. If no existing information system network is in place for the multinational partners providing forces, either the multinational HQ or the JTF may establish a LAN. BICES, US BICES-X, CENTRIXS standards are used as the model for establishing and maintaining multinational connectivity at the tactical and operational level. The basic CENTRIXS operational architecture framework is the same for all CCMDs and leverages existing networks, technology, and network centers. Similarly, the basic US BICES and US BICES-X framework is the same for all CCMDs. The JTF/J-2 should request network connectivity through the JTF commander and should identify resources and establish procedures to transfer appropriate, releasable intelligence from US systems to the shared network as expeditiously as possible.

f. In an extended or large-scale operation involving multinational forces, the JTF commander may elect to establish a multinational intelligence center. The multinational intelligence center is manned by members of the multinational force who can contribute intelligence capabilities and is normally equipped and funded by the JTF or multinational command. Its function is to fuse all-source intelligence from multinational force members, create a COP, provide early warning to the multinational command and operational forces, and conduct JIPOE. The presence of a multinational intelligence center does not alleviate the need for a US JISE or operational JIOC at the JTF to receive and process US-only intelligence information in support of the JTF commander and staff. In many cases, the US JISE or JIOC responds to requests for information from the multinational intelligence center.

Note: NATO uses fully developed and coordinated doctrine, contained in Allied joint publications and standardization agreements. When the Armed Forces of the United States participate in multinational operations, US commanders should follow multinational doctrine and procedures that have been ratified by the US.

14. International Intelligence Sharing

a. JFCs recognize the complex, interconnected, and largely unpredictable nature of the OE and the need to better understand it and the military challenge. Synchronizing USG departments and agencies with joint or multinational military operations, international organizations, NGOs, and contractors enables US forces to gain access to specialized knowledge, significant access, or insight and understanding that these organizations possess. Inclusiveness with partners leads to a common understanding of this environment, the associated military challenge, and determination of necessary conditions to achieve success. This analysis helps provide common visualization and

better achieve unity of effort with our partners—bridging the gap between all instruments of national and international power.

b. Depending on the nature of the relationship with these organizations, US forces may consider revealing specific information needs or simply establish an information exchange. Fostering relationships with host nation organizations may enable a deeper understanding of local issues, and, over time, enable commanders to directly influence perceptions and behaviors.

15. Interorganizational Intelligence Collaboration

a. The role of DOD intelligence elements in an operation involving USG interagency partners is dictated by the nature of the support relationship. DOD operations, in conjunction with other USG departments and agencies, such as DHS, within the US or its territories can be characterized as either HD or defense support of civil authorities (DSCA). DOD intelligence organizations should expect to operate alongside interorganizational partners when assigned to conduct authorized intelligence functions in support of operations conducted in the homeland IAW EO 12333, *United States Intelligence Activities;* DODD 5240.01, *DOD Intelligence Activities;* and DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons.*

b. At the national level, the National Operations Center (NOC), operated by DHS, is the primary node for incident management across the federal government. The NOC operates 24/7 and includes IC LNOs. One of the primary functions of the NOC is providing situational awareness of potential incidents and threats to the US. The NOC maintains continuous contact with other federal agency operations centers, including the NJOIC, and issues situation reports on emerging crises.

c. During HD, military forces are used to counter threats and aggression against the US. DOD will be designated as the lead federal agency (LFA), supported by other USG departments and agencies, in defending against traditional threats/aggression. When ordered to conduct HD operations, United States Northern Command (USNORTHCOM) or USPACOM will normally designate a JTF, functional component, or single-Service task force, to command US military operations and coordinate with other agencies. The JTF normally coordinates an interagency response to the crisis through the joint interagency coordination groups. In addition, the JTF may request the presence of liaison elements representing other USG departments and agencies.

d. DSCA is support provided by US federal military forces, DOD civilians, DOD contract personnel, DOD component assets, and NG forces in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. In DSCA missions, DOD capabilities will always be used in a support role. DHS or the Federal Emergency Management Agency (FEMA) will designate an LFA to coordinate the USG response. The nature of the emergency drives the selection of the LFA, with the FBI taking the lead in terrorism or security-related incidents in most cases. The LFA will

establish a joint field office (JFO) in proximity to the emergency area. The JFO may be thought of as a rough equivalent to the DOD JTF and includes local, state, and federal agencies involved in emergency response. If the crisis is a response to a security incident, the FBI may activate a JOC and colocate the JOC within the JFO. The JOC will act as the lead for all investigative and intelligence issues. National intelligence agencies will work with the JOC to provide and receive situational awareness. Additional information on the structure and concepts of operation for the JOC and JFO can be found in the DHS's National Response Framework.

e. USNORTHCOM or USPACOM designates a defense coordinating officer (DCO) upon receipt of a request for assistance from the LFA. The USNORTHCOM DCOs are typically Army North, O-6-level staff officers who are in support of one of the nine FEMA regions and have interagency experience. USPACOM DCOs (based in Hawaii and Guam) work closely with US Army North Region IX DCO via a memorandum of agreement. The DCO works to integrate DOD efforts in support of the operation and serves as the on-scene military POC for the JFO and principal representatives of other USG departments and agencies, and NGOs. The DCO may have a defense coordinating element at the JFO consisting of a staff and LNOs to help coordinate military support. The defense coordinating element may include an intelligence officer. All DOD organizations, providing direct support to the JFO, coordinate their support with the DCO. This includes DOD intelligence CSAs that have received requests for support from the LFA or JFO.

f. Intelligence sharing between interagency participants frequently occurs on an ad hoc basis (see Figure II-4). It is imperative the JTF J-2, if designated, dedicate sufficient resources to provide liaison to interagency IC elements to encourage more robust exchange of information. The lack of an LFA J-2 staff function in most USG crisis response operations means there is little pre-planning for intelligence operations. The DHS uses its Homeland Security Information Network (HSIN) as its primary C2 and situational awareness tool. The HSIN includes a classified intelligence module that provides a COP, an RFI management tool, and collaboration software. However, each responding interagency partner brings their own internal communications system and databases and interacts primarily with their respective home agencies. Therefore, national IC agencies often lack connectivity at the JFO level.

g. The JFO may require a broad array of intelligence. In HD operations, interagency partners require warning information and intelligence concerning threats originating from abroad, especially concerning international terrorist groups and WMD proliferation issues. During DSCA missions, the most common request is for GI&S of the area around the incident scene. The NGA may deploy a forward element with connectivity to NGA data in support of a DSCA operation. NGA can provide reachback to national databases for products and analysis.

h. Several USG departments and agencies outside of DOD have imagery collection means that may be employed in the incident scene area. DHS may activate the interagency remote sensing coordination cell at the national level to coordinate and deconflict collection efforts. Any DOD intelligence collection of imagery within the US

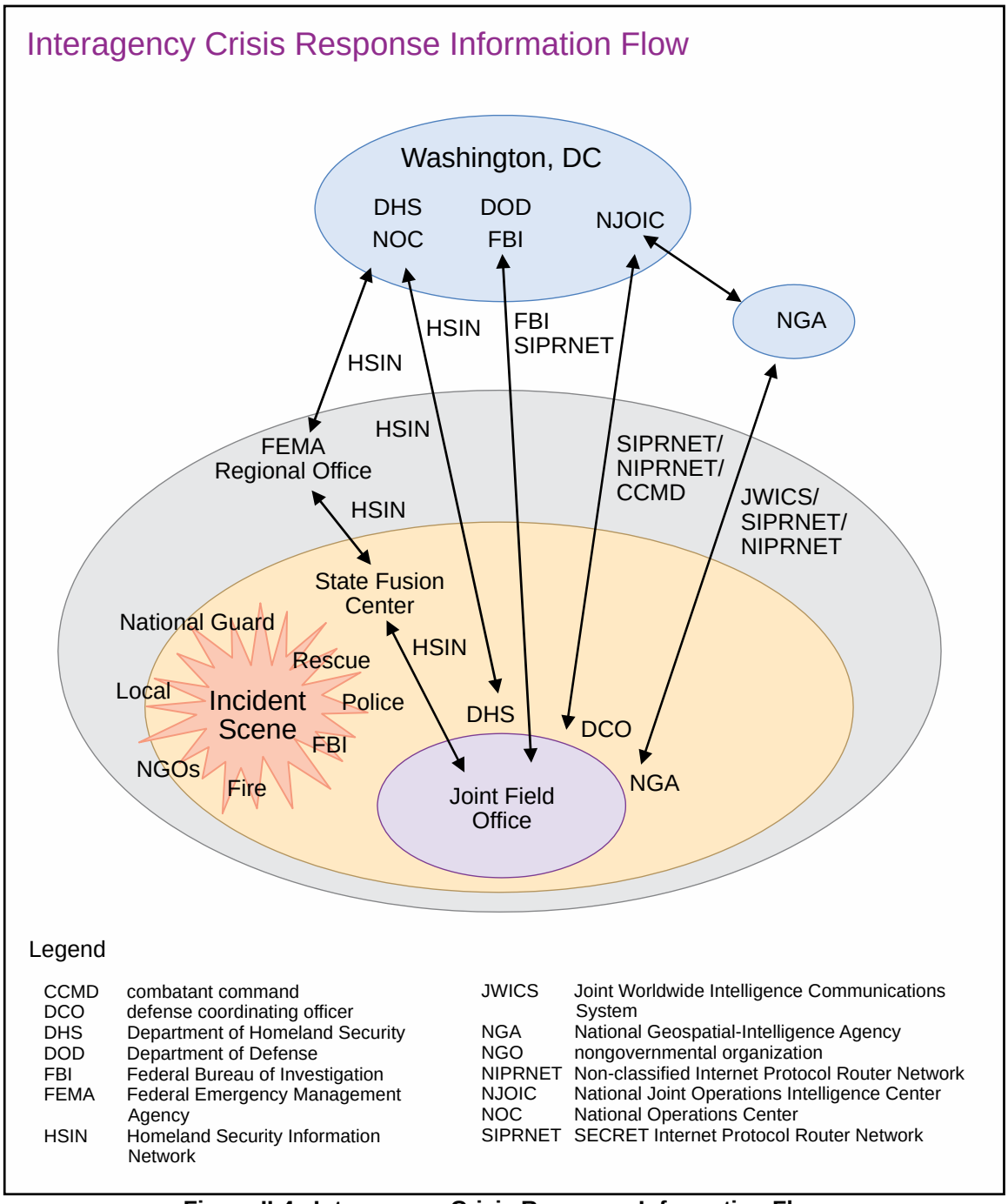


Figure II-4. Interagency Crisis Response Information Flow

must conform to US laws and DOD policies. During DSCA operations, military IAA elements should coordinate efforts with the DHS interagency remote sensing coordination cell.

i. In some cases, high-profile events, such as presidential inaugurations and Olympic games hosted in the US, are designated as national special security events, allowing for detailed pre-planning of a government-wide security operation. Depending on the venue

and purpose of the event, the US Secret Service, FBI, or DHS normally acts as the LFA and establishes a JFO and/or JOC. These events normally call for increased IC participation, including DOD intelligence elements in support of USNORTHCOM or USPACOM. The NJOIC may stand up a CAT with a corresponding ITF or working group in response.

j. Most states and many major local jurisdictions have established fusion centers (also known as information sharing and analysis centers) in support of the homeland security mission and the 9/11 Commission guidance to share information. These entities are designed to support collection, analysis, and dissemination of intelligence to meet standing information needs. Many operate 24/7 watch centers. State and local fusion centers are typically structured to include the following mission areas:

(1) Information collection and threat recognition.

(2) Intelligence fusion and analysis.

(3) Information sharing and collaboration.

(4) Risk analysis.

k. A number of cleared federal representatives may be available to assist in communication with these centers, including representatives from FBI, DHS, and state NG elements. The FBI has made an effort to place special agents and analysts in state fusion centers with access to the FBI's secure network, SIPRNET, and JWICS. Sensitive but unclassified connectivity to these centers is provided through a variety of shared situational awareness and collaboration tools, including HSIN.

CHAPTER III
INTELLIGENCE OPERATIONS

"Our challenges range from highly capable, near-peer competitors to empowered individuals, and the concomitant reduction in our own capacity will make those challenges all the more stressing on our defense and intelligence establishments. This strategic environment will be with us for some time, and the threat's increasing scope, volatility, and complexity will be the 'new normal'."

Vincent R. Stewart, Lieutenant General, US Marine Corps,
Director, Defense Intelligence Agency,
Worldwide Threat Assessment, February 2015

1. Introduction

Joint and national intelligence supports military operations by providing information, finished intelligence products, and targeting information to the CCMD, 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. Intelligence also contributes heavily to understanding the OE. The intelligence process is comprised of a wide variety of interrelated intelligence operations: planning and direction, tasking and collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. These intelligence operations should focus on the commander's mission and support the commander's decision-making process (see Figure III-1).

2. The Intelligence Process

a. 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 facilitates an understanding of the wide variety of intelligence operations and their interrelationships. There are no firm boundaries delineating where each operation within the 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 DCGS while simultaneously cross-cueing additional platforms for further 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 or other source, without first undergoing detailed all-source analysis and intelligence production. It is also important to note that in some instances the collector, processor, or exploiter may not be an intelligence element, instead belonging to the operational or law enforcement elements of the conventional force, interagency partner, or PN. These elements, however, feed the intelligence architecture and process of the JFC. Regardless of the source, the increased tempo of military operations requires an unimpeded flow of automatically processed and exploited data that is both timely and

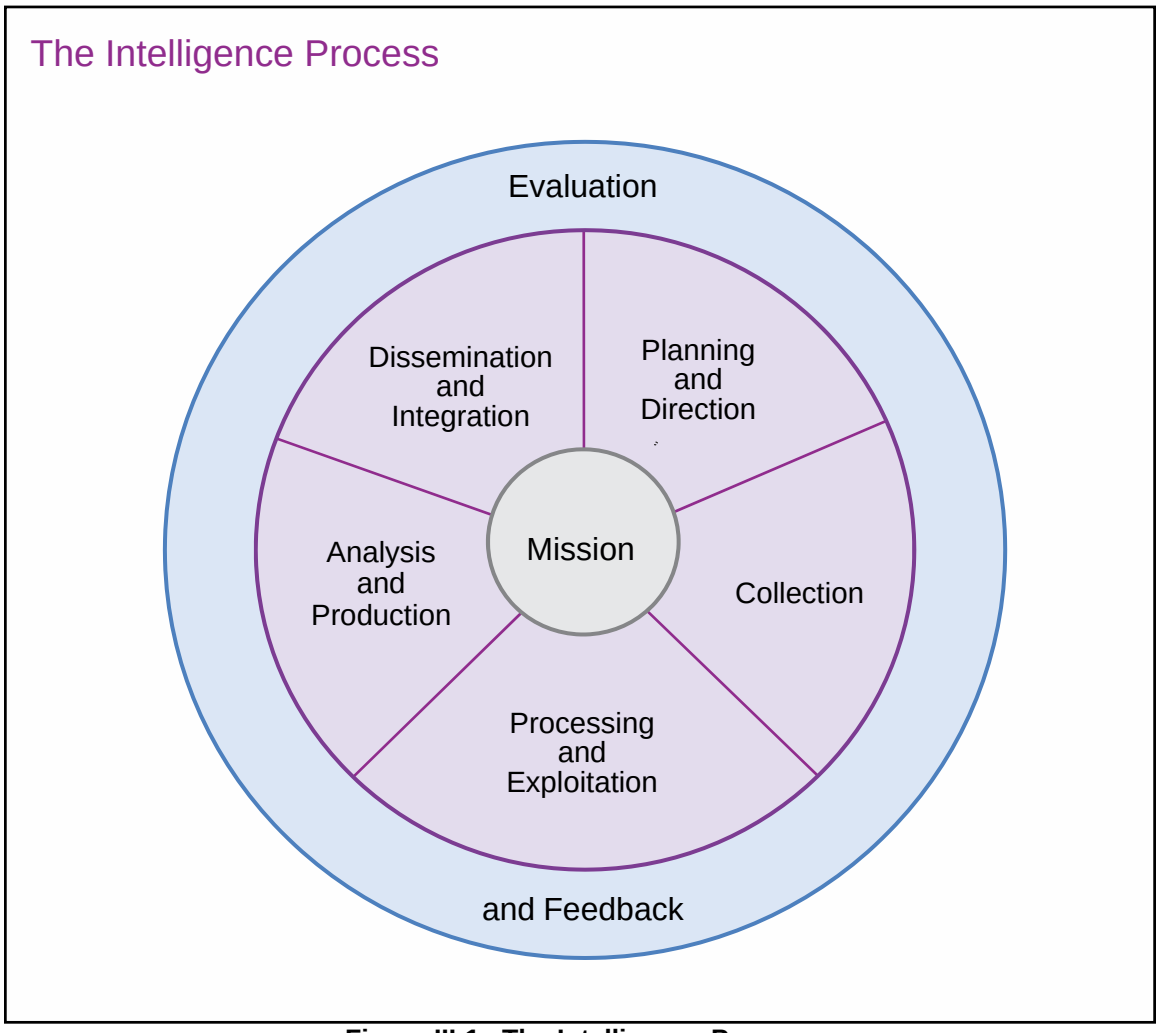


Figure III-1. The Intelligence Process

relevant to the commander's needs. This unanalyzed combat information should 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 should be accomplished in time to support the commander's decision-making needs. Many collection system products require some level of processing and exploitation to render the information intelligible to the customer.

b. Joint intelligence operations are founded on an understanding of the commander's mission and intent. This understanding also provides the basis for the identification of intelligence gaps regarding relevant aspects of the OE. These intelligence needs are identified by the commander and all joint force staff elements, are formalized by the J-2 as IRs throughout the JPP, and are coordinated by intelligence planners throughout the planning and direction portion of the intelligence process.

c. The tasking and collection element of the intelligence process involves tasking appropriate collection assets. Tasking and collection includes the identification, coordination, and positioning of assets and/or resources and levying tasking against them to satisfy collection requirements.

d. The processing and exploitation components of the intelligence process convert the collected raw data into information that can be readily disseminated and used by all-source 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 and associated processing and exploitation architectures. For example, some intelligence collection systems accomplish processing and exploitation automatically and nearly simultaneous with collection, while other collection assets, such as HUMINT teams, may require substantially more time. In addition, some collection sensors create data files unique to that sensor and platform and may require re-processing and/or re-formatting prior to exploitation. Processing and exploitation requirements are prioritized and synchronized with the commander's PIRs. National-level exploitation and production priorities should be in line with their associated collection priority, if applicable.

e. The analysis and production portion of the intelligence process integrates, evaluates, analyzes, and interprets information from single or multiple sources into a finished intelligence product that may be as little as a few textual lines in message format, or a multipage, multisource, multimedia electronic file. Depending on exploitation requirements (a last look at a target for situational awareness, monitoring activity levels at a high-value target, in-depth targeting, etc.), analysis and production of products may require immediate dissemination. Moreover, the demands of the modern OE 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 should be immediately communicated directly to those forces, platforms, or personnel identified at risk so that the appropriate responsive action can be taken once such notification has been acknowledged.

g. Intelligence operations, activities, and products are continuously evaluated. These evaluations are essential to the process and may lead to actions that focus the performance of intelligence operations and the overall functioning of the intelligence process. Feedback from the requester to the collection asset on the information or product provided enhances the overall IC effectiveness. Intelligence planners at the CCMDs, Joint Staff, CSAs, and Service production centers play a critical role to enhance IC effectiveness to the JFCs through IP that coordinates the provision of intelligence support to the joint planning and operation assessment processes.

SECTION A. PLANNING AND DIRECTION

3. Overview

The planning and direction portion of joint intelligence operations occurs continuously as the intelligence component of the command's shaping and contingency adaptive planning effort. Joint intelligence planners, through participation in the joint planning and assessment processes, lead development of the PIRs and concept of intelligence operations. They coordinate the planning and direction of joint intelligence operations on behalf of the joint force J-2 to satisfy the intelligence needs of the commander and staff. As the foundation for effective IC support, a continuous JIPOE process that produces timely tailored products to facilitate JFC decision making is the culminating capstone of joint intelligence operations. Planning and direction involves the activities shown in Figure III-2.

4. Intelligence Planning

As the intelligence component of the APEX enterprise, IP provides a methodology to coordinate, integrate, and synchronize all available intelligence capabilities to meet the CCDR's IRs for joint planning and assessment. It ensures the intelligence system is focused on providing the commander with the intelligence required to create desired

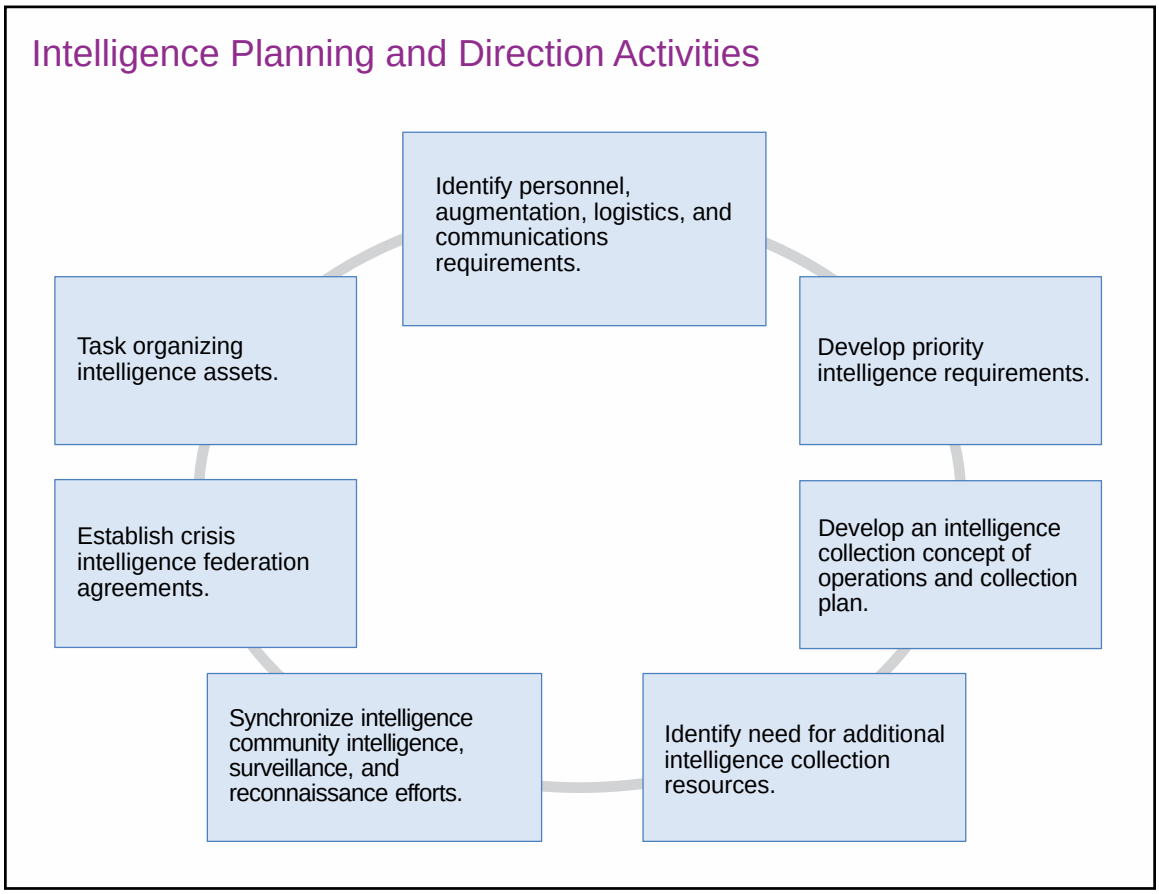


Figure III-2. Intelligence Planning and Direction Activities

effects and achieve operational objectives. Planning for the optimal employment of assets, sensors, and PED systems across the full spectrum of joint operations across all intelligence disciplines and throughout the OE is a challenge for the joint force. The coordinated activity used by staffs to synchronize the employment of sensors against anticipated collection targets and to ensure raw data can be converted into usable information is known as ISR. The IP construct is shown in Figure III-3 and includes three major products described below:

a. **Dynamic threat assessment (DTA) or TIA** is a defense strategic intelligence assessment developed by DIA that identifies enemy or adversary capabilities and intentions for top-priority plans. DIA produces and provides the CCMD an updated DTA prior to mission analysis and updates DTAs as strategic factors in the OE change. For theater campaign plans, DIA produces a TIA. The TIA is a theater-wide, defense-strategic intelligence assessment, which identifies the capability and intentions of key actors with particular emphasis on how these actors are affected by the strategic environment. The TIA enables development of the CCMD intelligence staff estimate and informs mission analysis and COA development.

b. **Annex B** is the intelligence annex to a plan or order that provides detailed information on the enemy or adversary situation, establishes priorities, assigns intelligence tasks, identifies required intelligence products, requests support from higher echelons, describes the concept of intelligence operations, and specifies intelligence procedures. CCMD J-2s lead development of annex B (Intelligence). The format and guidance for annex B (Intelligence) are contained in CJCSM 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance.* Figure III-4 depicts annex B (Intelligence) contents. Two critical processes inform annex B (Intelligence): the intelligence estimate and the J-2 staff estimate.

(1) An **intelligence estimate** is an appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the COAs open to the enemy or adversary and their order of probability of adoption.

(2) The **J-2 staff estimate** is an assessment of intelligence and CI capabilities of all assigned and attached intelligence assets available to support the operation. It identifies and addresses known or anticipated factors pertaining to CI or intelligence collection, processing and exploitation, analysis and production, and dissemination and integration that may limit the intelligence staff function's ability to support proposed friendly COAs.

c. The **NISP** is a supporting plan to a CCMD plan that details how the intelligence capabilities of CSAs, Services, and other DOD intelligence organizations should be employed to meet the CCDR's IRs. It facilitates the integration of theater and national intelligence capabilities and assures synchronization of intelligence operations by the CCMD J-2. The Joint Staff J-2, in close coordination with the supported CCMD J-2, coordinates, integrates, and synchronizes the activities of the defense intelligence enterprise to develop and staff a NISP for approval by the supported CCDR or their

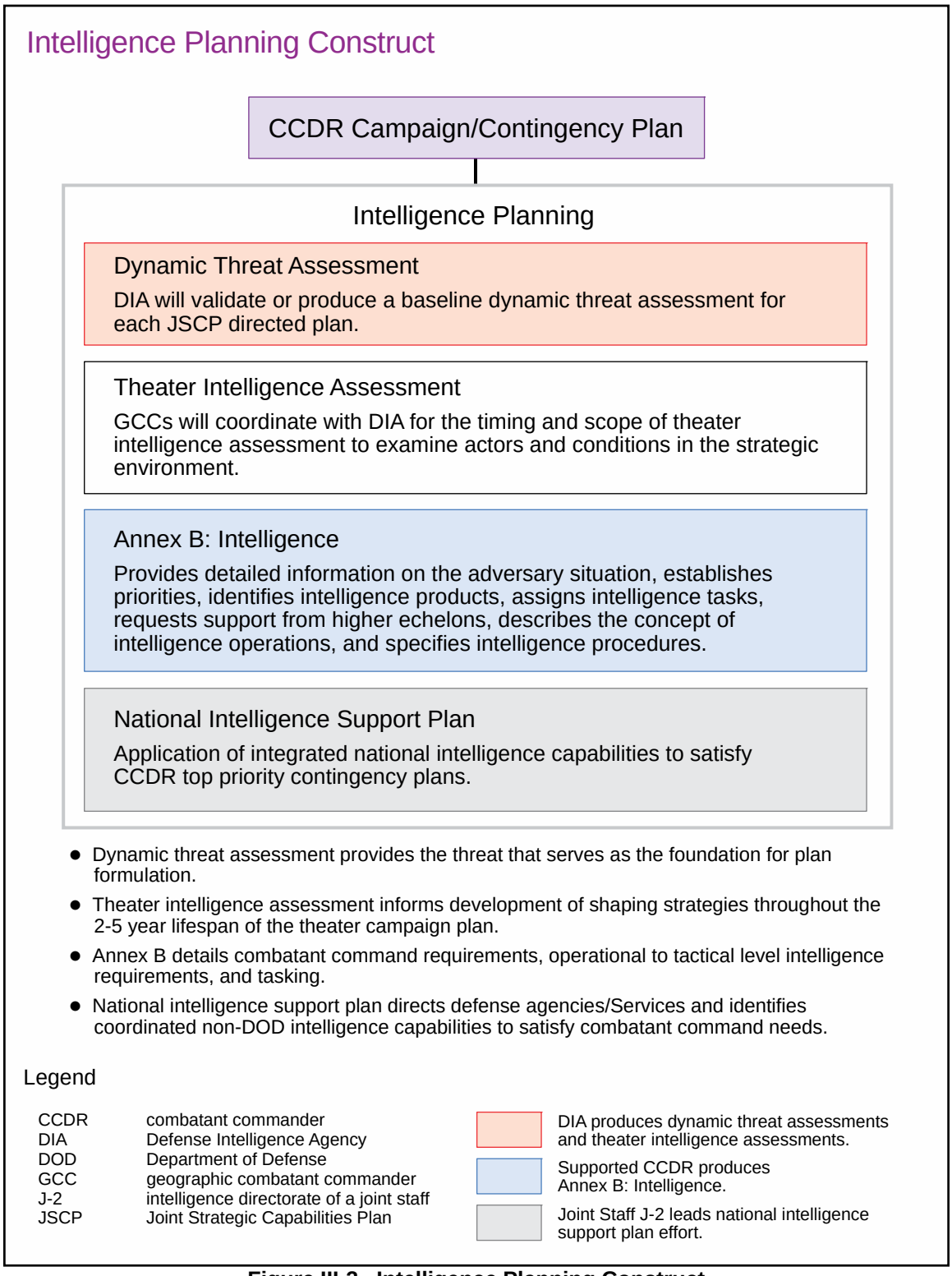


Figure III-3. Intelligence Planning Construct

designated representative. The NISP also identifies tasks requiring non-DOD intelligence entities support. It contains annexes from applicable defense intelligence agencies/organizations that detail their concept for function support. A NISP consists of

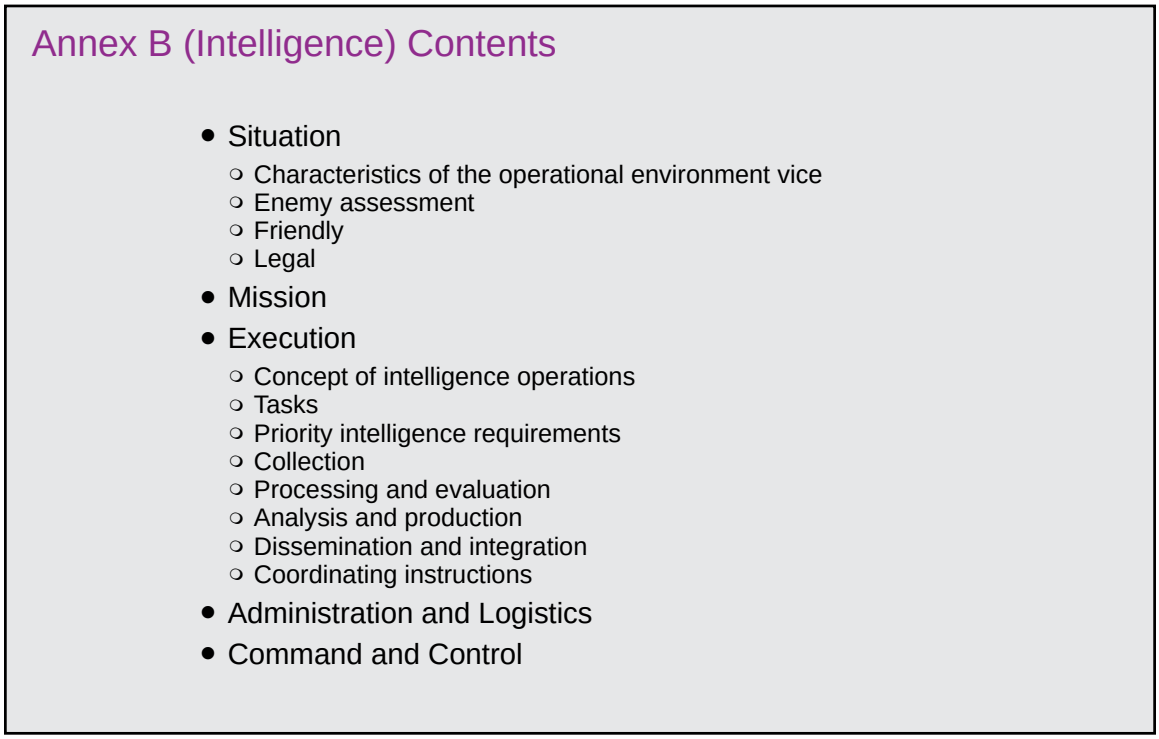


Figure III-4. Annex B (Intelligence) Contents

four primary components: the NISP base plan, command IRs (PRMx/collection requirements matrix [CRMx]), capability assessments, and functional support plans (FSPs).

(1) The **NISP base plan** provides overall guidance to integrate and synchronize the defense intelligence enterprise effort for the supported CCMD plan. It contains the concept of intelligence operations, assigns tasks and responsibilities, requests interagency support as required, and identifies major gaps and shortfalls.

(2) The **PRMx** is a compilation of prioritized CCMD all-source intelligence analysis and identified PRs that support the CCDR's decisions and are organized in a two-tier hierarchy of tasks and subtasks. When completed, the PRMx reflects the essential elements of a federated production plan that is intended to optimize the employment of all available defense intelligence enterprise analytic resources. The PRMx is intended to be a living document and maintained accordingly.

(3) The **CRMx** is a list of anticipated collection requirements (PIRs, EEIs, specific information requirements [SIRs]), and observables to support CCDR decision making. The CRMx should be used to correlate the identified requirements with the collection capabilities that are best suited to satisfy the task. If appropriate, tipping and cueing indicators should be identified. The intent of the CRMx is to optimize use of all available collection resources.

(4) A **capability assessment** is a brief evaluation of a CCMD JIOC, CSA, or Service intelligence center's capability and capacity to satisfy CCMD IRs, recorded in

matrix format. These assessments form the basis for identification of capability shortfalls and knowledge gaps.

(5) An **FSP** is an intelligence agency/organization's annex to a NISP that describes the intelligence capabilities and concept for their employment in support of the CCMD plan. The FSP also assesses agency/organizational capabilities and identifies significant knowledge gaps and capability shortfalls in supporting the CCMD mission and identifies mitigation strategies where appropriate.

For more information on IP products and processes, see CJCSM 3314.01, Intelligence Planning, *and JP 2-0,* Joint Intelligence.

5. Intelligence Requirements and Information Requirements Planning

a. CCMD JIOC intelligence planners lead IP teams to develop and staff annex B and co-chair IP steering groups to develop and staff NISPs, as appropriate, to support CCDR decision making. The CCMD J-2 participates fully in the planning and decision-making process, contributing through JIPOE products to the CCDRs' understanding of the OE and receiving guidance to help focus the intelligence effort. Through participation in JPP and CCMD battle rhythm events, CCMD JIOC intelligence planners help develop mission success criteria (i.e., desired effects, operational objectives, and end states) and their associated metrics to determine what intelligence support and information may be required to facilitate CCDR decision making.

b. As an output of JPP, all elements of the staff nominate CCIRs to the commander for approval. CCIRs comprise a limited number of information requirements that enable the staff to focus limited resources on those aspects of the operation the commander is interested in closely monitoring and upon which a decision may be based. CCIRs consist of PIRs and friendly force information requirements (FFIRs). During planning prior to execution, the J-5 is the overall staff proponent to develop and monitor FFIRs. During execution, the J-3 is the overall staff proponent to monitor FFIRs. The J-2 is the overall staff proponent to develop and monitor PIRs. The J-2 leads the development of IRs (general or specific subjects upon which there is a need for the collection of information or the production of intelligence to fill intelligence gaps) and the development of information requirements (items of information regarding the enemy or adversary and other aspects of the OE that need to be collected and processed to meet the IRs). **IRs that are deemed most important to understand the adversary or other aspects of the OE are identified by the commander as PIRs. Information requirements that are also critical or that would answer PIRs are known as EEIs.** EEIs may require answering numerous specific questions regarding the collected area/target, such as threat OB, operational status and readiness of troops and equipment, or identification of unique signature information as well as human factor analysis and IOII.

c. The categories, types, and level of detail of IRs differ from echelon to echelon. Intelligence necessary to support the operational level might be inappropriate at the tactical level. With some exceptions, the higher echelon commander's IRs 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.

d. An RFI response disseminates existing products; integrates or tailors on-hand information; or schedules, tasks, and collects data for original production to satisfy customer requirements. The information should 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 DIAP as a PR. If it is determined that insufficient information exists to answer an RFI, then a collection requirement is prepared and entered into the appropriate CRM application.

(1) Requirements that cannot be satisfied are submitted as RFIs or collection requirements to the next higher echelon. Each echelon validates, prioritizes, and, if possible, satisfies the RFI or collection requirement before forwarding it to the next level. In certain cases, staffing simultaneously through the multiple echelon submissions is necessary when the request is time sensitive. 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 confirms that an intelligence collection or PR is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and may not be satisfied by previous collection or production. Information copies of the requirement should be forwarded to supporting intelligence organizations to alert potential respondents to the requirement.

(3) The intelligence federation process enables CCMDs to form support relationships with other JIOCs, Service intelligence centers, reserve organizations, multinational partners when appropriate, or other intelligence agencies to assist with the accomplishment of the joint force's mission. The supported CCMD J-2 should coordinate with the NJOIC to establish an ad hoc crisis intelligence federation. For deliberate and crisis action requirements, CCMDs initiate the federation process by assessing their intelligence shortfalls and requesting federated partnership support through the NJOIC for crisis action requirements or through the Joint Staff J-2 IP Functional Manager for deliberate planning requirements. 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 geographic combatant commander's (GCC's) AOR, thereby freeing the supported command's assets to refocus on crisis support.

(a) Supporting JIOCs, Service intelligence centers, and intelligence agencies should be considered as being in direct support of the supported CCMD J-2. **For crisis intelligence federation requirements, the NJOIC coordinates and directs via APEX order specific command relationships. Crisis intelligence federation**

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). Deliberate intelligence federation relationships are coordinated by the Joint Staff J-2 IP Functional Manager and specified in annex B to the OPLAN, NISPs, or memoranda of agreement as appropriate, following joint planning and execution community review coordination.

(b) For crisis intelligence federation requirements, the NJOIC coordinates the establishment of crisis intelligence federation requirements, recommends re-prioritized support, and specifies temporary supporting relationships as necessary through CJCS orders or fragmentary orders. Figure III-5 depicts the process for crisis intelligence augmentation and federation support.

6. Resource Allocation

Intelligence support is provided by joint force providers with individuals and units consisting of civilians and military members. The personnel supporting CCMD JIOCs are assigned to the CCMDs by SecDef via the Forces for Unified Commands Memorandum. When emergent IRs exceed the capabilities or capacity of assigned intelligence forces, additional intelligence forces can be allocated to the CCMD by SecDef in response to near-term risks. In both cases, SecDef specifies the command relationship authorities over assigned and allocated intelligence forces by the CCDR. For allocation of intelligence forces, the Director, DIA, through the Joint Staff J-25 [Deputy Directorate for Intelligence, Operations, Policy and Plans], supports DOD and CCDRs by developing and recommending globally optimized sourcing solutions for intelligence units and personnel capabilities, not including platform/sensor based intelligence collection and associated PED capabilities, and coordinates directly with the intelligence CSAs, the Joint Staff, and other DOD agencies for CCDR-requested intelligence capabilities. The Joint Staff coordinates with the Military Departments/Services, CCDRs, and intelligence agencies to identify and recommend joint global platform/sensor-based ISR and associated PED capabilities sourcing solutions.

7. Requesting National Intelligence

a. **National Intelligence Production Support.** The JIOC is the primary focal point for providing intelligence support to the CCMD. Based on continuous J-2 staff estimates coordinated by JIOC intelligence planners, the CCMD J-2 determines whether CCMD and subordinate components' intelligence needs can be met with assigned resources or may require national-level assistance. If national-level production assistance is required, a formal RFI request should be prepared. The flow of RFIs from JIOCs to national intelligence agencies differs only slightly from peacetime to crisis. As approved by the CCMD J-2, JIOC intelligence planners coordinate with Joint Staff J-2 intelligence planners who coordinate, represent, and advocate CCMD IRs to CJCS, OSD, and the ODNI for requesting national-level intelligence production support. The Joint Staff J-2 intelligence planners should interface with other DOD intelligence agencies or the national IC through the NICC to provide support. If determined that the information

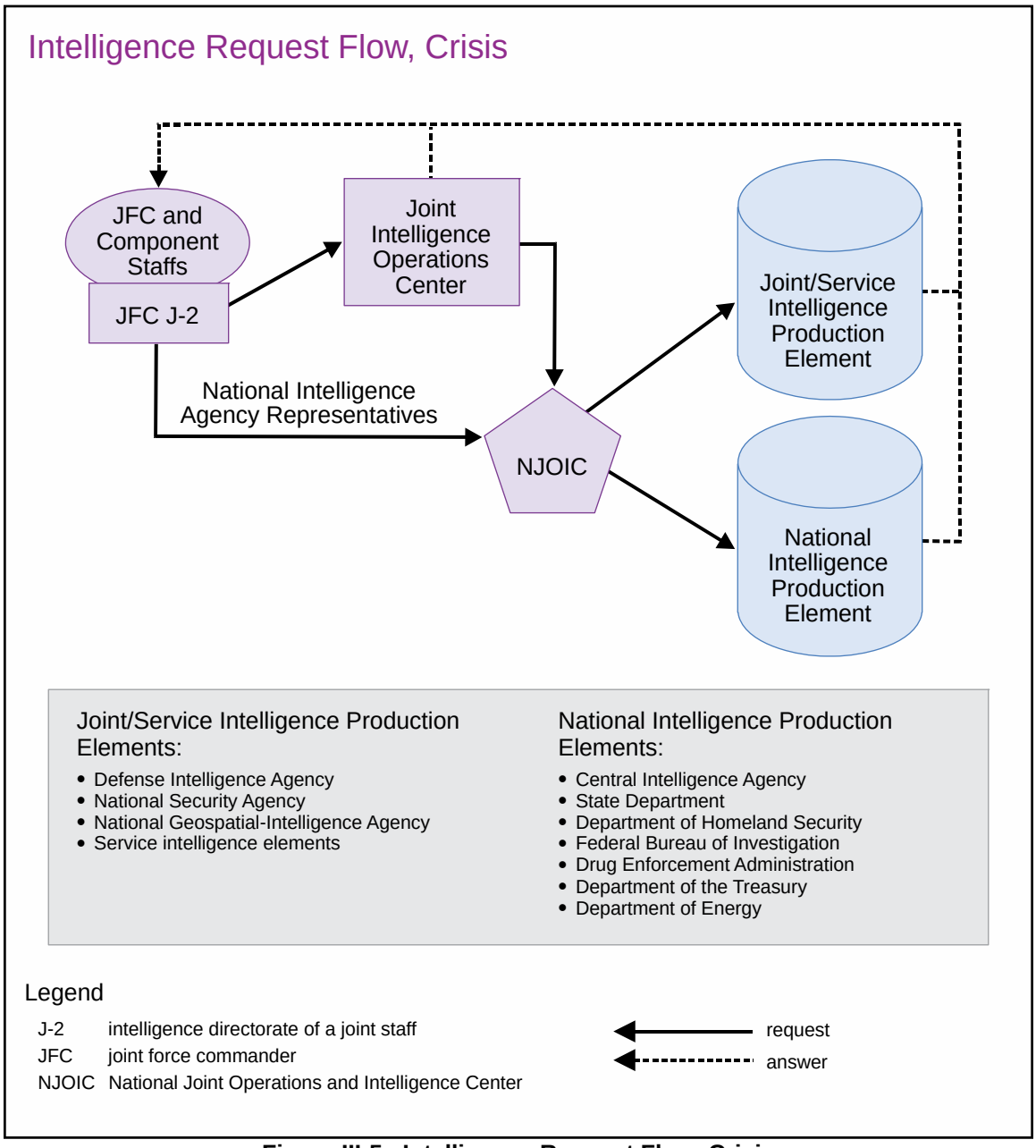


Figure III-5. Intelligence Request Flow, Crisis

required has not been produced by any agency in the IC, the Joint Staff J-2 intelligence planners should coordinate with the CCMD JIOC intelligence planners and NICC to recommend an appropriate strategy to collect, process, analyze, produce, and disseminate the required information. This strategy should be included in annex B to the plan or order and in a NISP, as appropriate.

(1) **Noncrisis Request Procedures.** DIA ensures the expeditious flow of intelligence from the national level through the JIOCs to deployed forces during peacetime (see Figure III-6). RFIs are forwarded from the JIOC to DIA and/or the production agency. If the JIOC determines national-level intelligence collection is

required to meet theater intelligence PRs, a formal collection request should be prepared and forwarded to the Joint Staff J-2.

(2) **Crisis Request Procedures.** The NJOIC is the focal point for all crisis intelligence federation requirements, as required. Additionally, deployed national agency representatives may serve as direct links to their parent organizations, when the joint force J-2 intelligence planners recommend and the CCMD J-2 determines that NJOIC coordination is required for time-sensitive collection requirements or RFIs require national support. For tracking purposes, the JIOC should monitor the status of all RFIs originating from theater.

b. **National Intelligence Augmentation Support.** CCMDs coordinate with the Joint Staff J-2 via record message all requests for external support, 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 the Joint Staff J-2 via the CCMD J-2 for validation and subsequent action. Requests for CIA personnel/equipment support should be submitted via the ODNI representative to the CIA for action.

c. **The National Intelligence Priorities Framework (NIPF)** is the DNI's sole mechanism for establishing national intelligence priorities. Intelligence topics reviewed by the NSC Principals Committee and approved by the President annually form the basis of the NIPF and the detailed priorities established by the DNI. The ODNI and the IC elements use the NIPF to allocate national collection and analytical resources. **The NIPF is the DNI's guidance to the IC** on the national intelligence priorities for planning, collection, and analysis. The NIPF serves as the basic guidance for US foreign intelligence collection and analysis. It balances intelligence issues, countries, non-state actors, and terrorist organizations to formulate a global standing priority matrix. National collection requirements and analysis and production efforts are tied to the NIPF priorities. The Deputy DNI for Intelligence Integration oversees NIPF development and management. The development and management process includes input from Services, OSD, and CCMDs. The NIPF matrix reflects customers' priorities for intelligence support and ensures enduring and emerging national intelligence issues are addressed. The NIPF is reviewed quarterly, is published annually, and may be updated on an ad hoc basis to address emerging issues. The contents of the NIPF are classified.

d. The Integrated Defense Intelligence Priorities process is managed by USD(I) to consolidate and prioritize DOD's operational, policy-related, and acquisition-related intelligence priorities to integrate DOD intelligence priorities into the NIPF.

e. The DIAP is a framework to focus analysis and determine levels of effort for the DOD portion of the IC. When new NIPF priorities are approved, or as threats evolve, DIAP analytical efforts are adjusted by the DIAP Board of Governors.

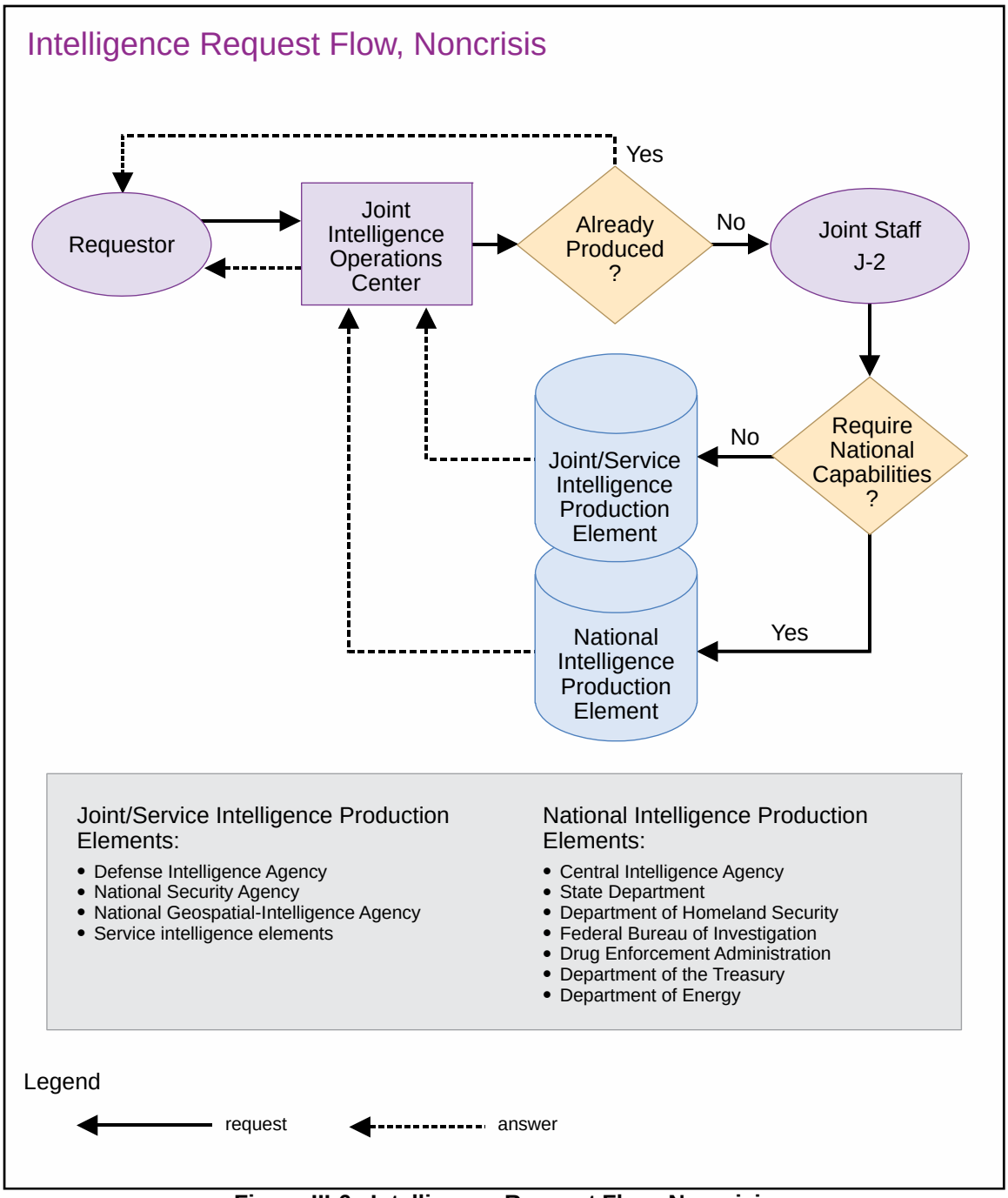


Figure III-6. Intelligence Request Flow, Noncrisis

SECTION B. COLLECTION

8. Overview

a. Collection operations acquire information about relevant aspects of the OE and provide that information to intelligence processing and exploitation elements. Collection management, which occurs at all levels of intelligence, is the process of converting information requirements into collection requirements, tasking, or coordinating actions

with appropriate collection organizations or agencies, and monitoring results and retasking 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 supporting, assigned, or attached to a particular commander, unit, or echelon while a collection resource is not assigned or attached to a specific commander, unit, or echelon and must be requested and coordinated through the chain of command of the unit that directs and controls them.

9. Collection Management

a. **Principles of Collection Management.** Collection managers develop collection strategies and plans based on validated IRs of commanders and decision makers. Collection strategies discuss what must be collected and specify broadly which organizations or intelligence disciplines have been tasked to support IRs. Collection plans discuss how those IRs will be supported, specifying what collection assets and resources will be used. Intelligence planners support the collection management process by coordinating with collection managers and intelligence analysts to identify intelligence gaps and submit RFIs. The collection manager's task is to first validate the new requirements and ensure there are no existing collection requirements covering the same requested information and, if not, draft and submit the new requirement. Once they have been validated, the collection manager begins the process to obtain the intelligence necessary to best answer the requirement. To do this, the collection manager:

(1) If necessary, develops and manages a multi-discipline collection strategy that integrates discipline-specific collection requirements with target characteristics.

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

(3) In coordination with the J-3, forwards collection requirements to the component commander, Service, defense intelligence components, or national agency exercising control over the collection resources, who then tasks the resource(s) to satisfy the collection requirement.

(4) Directs processing and dissemination of collected data. Collection managers should understand the capabilities and limitations of each intelligence discipline, the sensors, platforms, PED architecture, product format, and procedures for ensuring target coverage by the appropriate collection asset and its associated PED assets. Collection managers keep analysts and 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.

(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 to new collection requirements in a timely manner, ensures thorough planning, and increases flexibility in the choice of disciplines and systems. Early requirement identification also allows the collection manager time to accomplish needed research, run predictive analysis tools if required, and establish and/or refine a POC list.

(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 risks to joint operations 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 NIPF priorities, the commander's PIRs, and the current situation ensures 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 routine collection operations. If collection does not occur at the lower priority, the requirement should be reviewed for a possible increase in stated priority.

(a) The CCMD J-2 determines and recommends prioritized intelligence needs based on mission analysis and commander's planning guidance.

(b) The collection manager for national tasking purposes is required to associate a collection requirement to an appropriate NIPF issue in order to establish a numerical tasking priority value. Depending on the intelligence issue, urgency, and criticality, priority exceptions may be applied in order to satisfy a requirement.

(c) The collection manager may have an additional, locally established, tiered priority framework to further refine the ranking of identical NIPF priority requirements.

(d) Short-term priority exceptions that support crisis issues, such as personnel recovery, time-sensitive targeting, and response to natural disasters, may also be submitted on a case-by-case basis.

(3) **Multidisciplinary Approach.** Collection disciplines complement each other, and the collection manager should resist favoring or becoming too reliant on a particular sensor, human source, technical system, or technique. Each discipline's limitations can be mitigated by the capabilities of the others, as different systems provide additional, and alternative, insights into the requirement. Collection gathered from additional disciplines is often necessary to corroborate or increase friendly force confidence in gathered intelligence. While a sensor, human source, and/or technical 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 requirements and information gaps that are most likely to be satisfied by a particular collection operation (e.g., HUMINT and/or SIGINT can capture enemy intent, but GEOINT

cannot). Rigid dependence on a single source of information or operational methodology may result in mission failure or become an operational vulnerability, especially if that source becomes unavailable or if the enemy becomes aware of the use of that single source and takes denial and deception countermeasures. The use of a multidisciplinary approach minimizes the enemy's ability to detect discernible patterns and thus may hamper their CI or denial and deception efforts. The CCMD J-2/JIOC directs, supervises, and guides the execution of the strategic theater collection management process across all available intelligence disciplines. The CCMD JIOC performs integrated collection management to determine, validate, and task multidiscipline collection requirements based on CCDR mission needs and PIRs. Collection managers define multidiscipline collection requirements, followed by the theater collection strategy, plan, and CONOPS. Multidiscipline CRM can be done by the theater or CCMD collection managers, with the CCMD collection managers exercising validation and prioritization authority via the CCMD's CMA. The CCMD collection managers/planners then develop a collection plan and task collection requirements to appropriate, available theater collection assets; collection requirements that are not able to be satisfied by theater assets are forwarded for collection by Service or national-level collection resources.

(4) **Task Available Collection Assets First.** Use of available 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 available assets, the collection manager should request collection support from higher, adjacent, and subordinate units, agencies, and organizations.

c. **Collection management has two distinct functions:** CRM, which determines what intelligence systems must collect, and collection operations management (COM), which specifies how to satisfy those requirements. CRM focuses on the requirements of the customer, is multidiscipline oriented, and advocates what information is necessary for collection. COM focuses on the selection of the specific systems within a discipline to collect information to satisfy the customer's request. COM is conducted by organizations to determine which collection assets can best satisfy the customers' requests (see Figure III-7).

(1) Depending on the size of the collection management element, the CRM and COM functions may not be organizationally distinct and may in fact be performed by a single individual. Although considered separate to facilitate the understanding of their different objectives, in practice, there may be no distinction between them. If performed by separate individuals/staffs, constant interaction should be maintained between the two.

(2) **CRM and COM 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. CRM is conducted by all echelons. Each organization establishes their own collection requirements for themselves and their supported units, validates and prioritizes them, and then determines if they can be satisfied using organic assets. Collection requirements

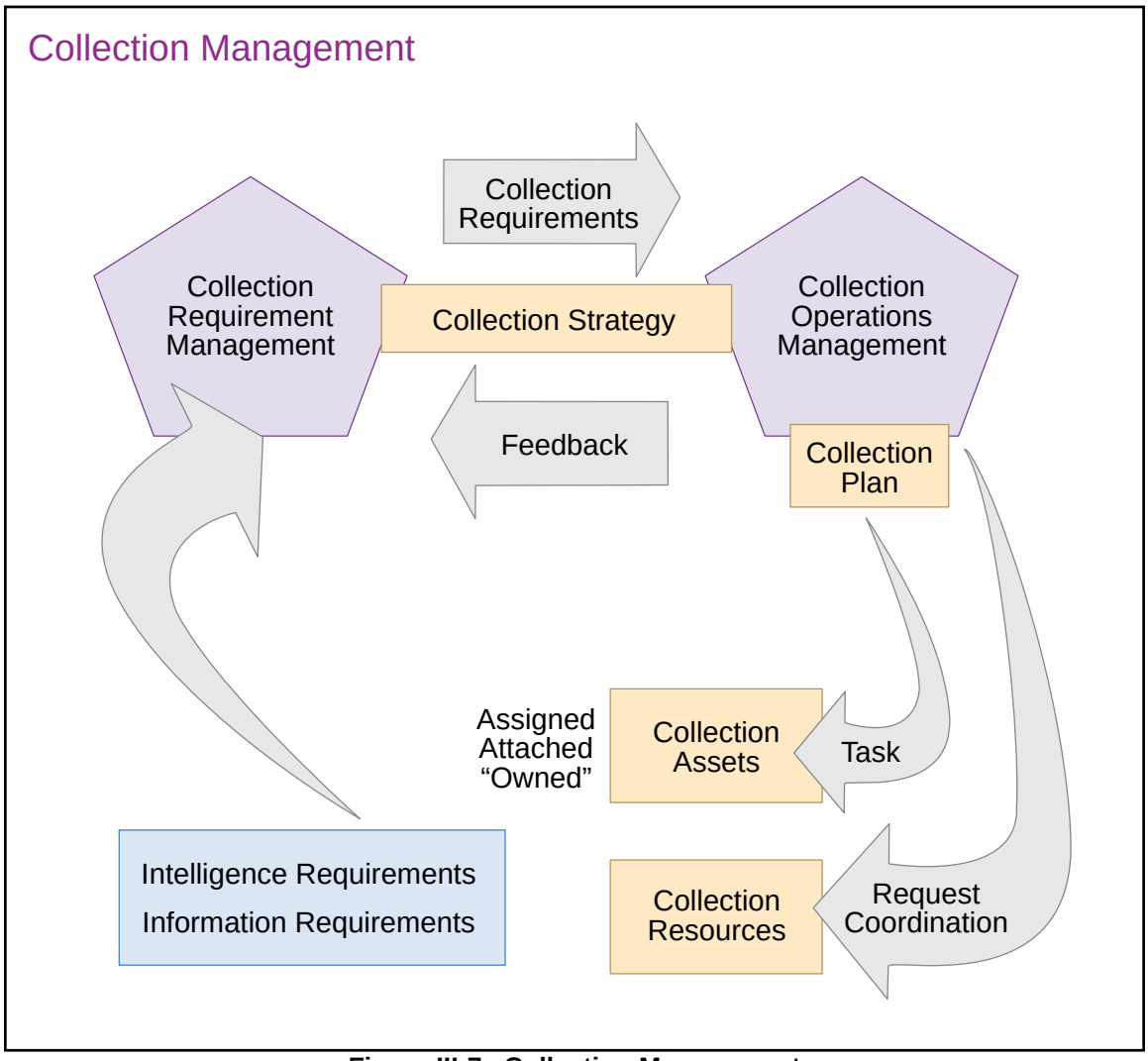


Figure III-7. Collection Management

should be satisfied at the lowest possible level. Requirements that cannot be satisfied at the tactical or theater level and that have been validated by the CCMD's collection manager or J-2 are then forwarded to the next higher (or lateral supporting) 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 should be forwarded for action to the theater intelligence collection management office. COM is conducted by organizations possessing collection assets to determine which collection assets can best satisfy the customers' product requests.

(3) **CMA.** Within DOD, CMA constitutes the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater-wide collection policies. CMA ensures unity of collection effort, effectively employs synchronized collection to support combat operations, and assesses the collection process. It is important to note that CMA is an authority held by a single leader and not one exercised by all collection managers. The CCMD J-2 exercises CMA

RELATIONSHIP BETWEEN COLLECTION MANAGEMENT AND OPERATIONS

The joint force commander's (JFC's) collection management staff prioritizes validated collection requirements, defines the required collection parameters (i.e., provides direction to collection platforms necessary to conduct the mission), and recommends the appropriate asset to be assigned to collect against a particular target via a collection plan. Once the JFC approves the collection plan, the collection management staff, in coordination with the operations directorate, forwards collection requirements to the component commander exercising operational and/or tactical control over the theater collection 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 technical or human intelligence (HUMINT) assets that can satisfy the collection requirement based on such operational consideration as maintenance schedules, training, experience, or in the case of HUMINT, placement and access of collectors and/or sources.

Various Sources

for a given CCMD and acts as the executive for collection management. CMA may also reside at the JTF level or may be delegated to components. CMA is often exercised via decisions made at the JCMB.

(4) **Joint Staff J-2.** The Joint Staff J-2 is the principal intelligence advisor to the CJCS and provides crisis intelligence to OSD, CJCS, and the Joint Staff. The Joint Staff J-2 also manages crisis response for the Joint Staff and staffs the intelligence portion of the NJOIC. The Joint Staff J-2 advocates for CCMD IRs to the Joint Staff, the intelligence CSAs, OSD, and ODNI.

(5) **Theater Collection Management.** The theater J-2 should be kept apprised of all intelligence collection requirements being levied on assets and resources within the GCC's AOR, including other IC agencies with their own assets. This is important in order to prevent redundancy in collection, deconfliction of targets, and coordination of friendly forces in the AOR. **The theater J-2 retains full CMA (specifically, the authority to validate, modify, or non-concur) over all intelligence collection requirements within the AOR.** This authority may be delegated to a subordinate JFC.

10. Collection Requirements Management

a. **Requirements Origination.** The subordinate joint force tactical units develop collection requirements in support of current and future operations and commander's priorities and objectives and send those requirements to the subordinate joint force J-2 for validation and tasking to tactical collection assets. Subordinate component J-2s submit requests for additional collection resources to the CCMD J-2 if they do not have the capability to collect the data. The CCMD J-2 validates or modifies standing collection

requirements submitted by subordinate joint force or component commands. The CCMD J-2 tracks the status of research, validation, submission, and satisfaction of all collection requests received. **At the JFC's discretion, a 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 serves as the GCC's decision-making body for all collection management issues within the AOR, to include requirement validation, asset allocation, and collection plan approvals. All collection requirements received and validated by the CCMD collection managers are included in a joint integrated prioritized collection list (JIPCL). The CCMD J-2 collection manager may use the JCMB as the conduit for obtaining CCDR approval of the JIPCL.

b. **Management and validation of requests for theater collection reside at the CCMD level.** The CCMD J-2 collection manager directs all collection management over theater collection requirements and operations. The validation process should be responsive to operational requirements. The CCMD J-2 collection managers validate and submit collection requirements to DIA when they cannot be satisfied by theater assets. Validated collection requirements from subordinate components and units become part of the theater collection plan.

c. **Collection strategy development and planning is a continuous process that coordinates and integrates the efforts of all collection units and agencies.** Collection strategy development is the responsibility of the collection manager. Collection strategy development begins with an understanding of the commander's PIRs to provide context to the overall intelligence problem. Based on the PIRs, the intelligence staff (usually the intelligence planner and the analyst) develops more specific questions, known as EEIs. From the EEIs, the collection strategists and analysts then develop SIRs and observables. These observables are often grouped into a geographic area or system node or link that is referred to as a named area of interest. Once this process is completed, the collection strategists can develop a thorough collection strategy that identifies the collection gaps for each PIR and which collection disciplines should be tasked against the requirements. Collection managers should determine which collection assets have the capabilities to collect the information needed and have access to the named areas of interest or collection targets. Coordination between the collection strategists, the operators, and the all-source analysts is critical to the development of collection strategies.

d. Collection managers use the finished collection strategy to develop an actionable collection plan detailing what collection targets should be tasked—based on time, space, and purpose.

e. For national-level requirements, the collection requirements manager will input a SIR using the system application term of EEI for submission into each CRM database of record.

11. Collection Operations Management

a. **The COM process organizes, directs, and monitors the equipment and personnel that collect the data to satisfy requirements.** COM personnel develop collection plans against requirements in cooperation with CRM personnel, predict how well a system can satisfy requirements, monitor and report the operational status of technical collection systems, allocate and task technical collection assets and processing and/or exploitation systems or HUMINT collection assets with the capability to collect, and evaluate the performance of the collection systems or platforms. (See Figure III-8).

b. **Collection Planning**

(1) Collection planning **identifies, schedules, and controls collection assets and/or resources.** The collection manager performing COM reviews mission requirements for sensor and target range, system responsiveness, timeliness, threat, weather, source placement, access and availability, and reporting requirements. These elements are considered with the detailed technical, administrative, and logistical data of the collection system or platform to identify and determine asset and/or resource availability and capability. The requirements are then translated into specific mission tasking orders issued to a commander with tactical control of the assets in question.

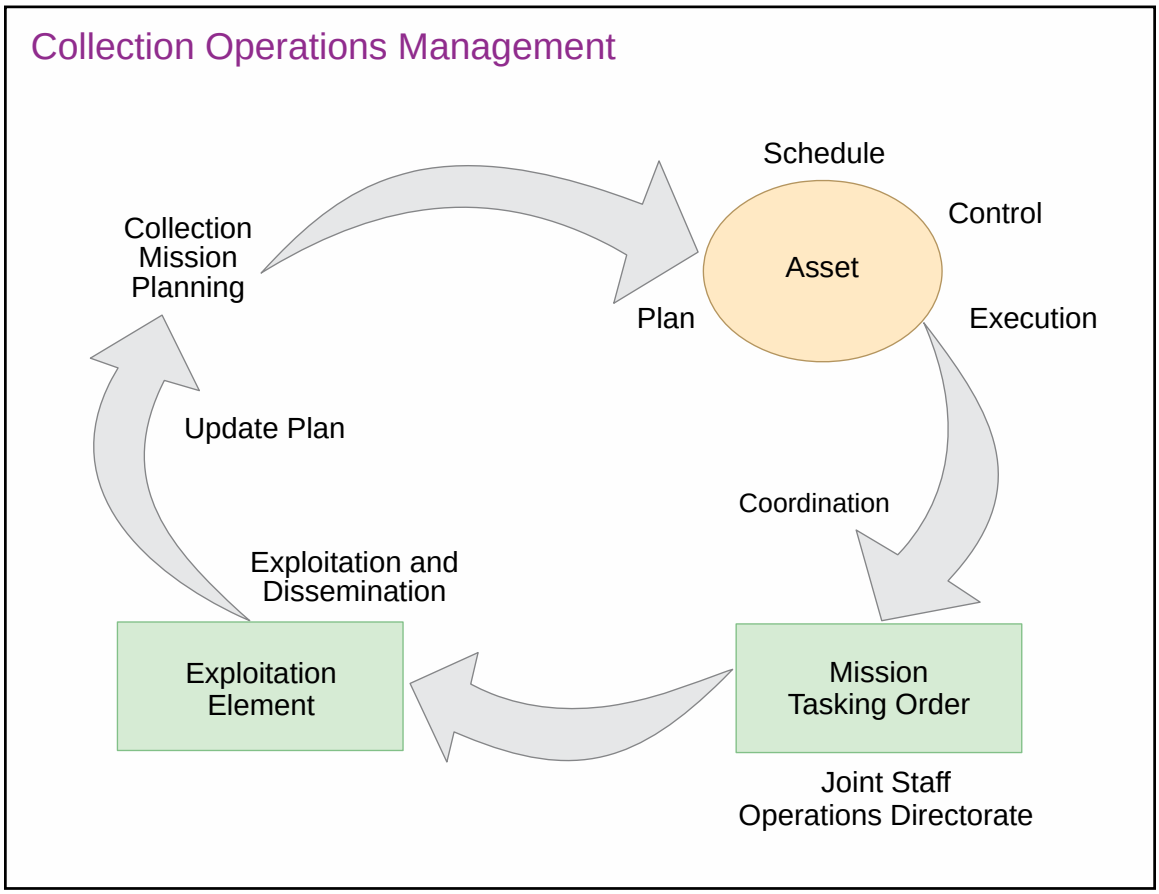


Figure III-8. Collection Operations Management

(2) **The Collection Plan.** Collection system effectiveness is predicted by analyzing the capability and availability of intelligence collection assets and resources to collect against specific targets. Collection system efficiency is predicted by comparing the appropriateness of all available and capable intelligence collection 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 RC-12 Guardrail or an unmanned aircraft system 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 plan considers all outstanding IRs, their relative priority, and the immediate tactical situation.

(3) The collection plan may be either a simple, single-discipline spreadsheet or a complex, multidiscipline document containing various spreadsheets and other documents, such as the reconnaissance, surveillance, tasking, and acquisition annex to the air tasking order produced by a theater air operations center. The collection asset allocation plan includes PIRs, their associated EEIs and related indicators, collection requirements and their SIRs, collection assets to be tasked or additional collection resources to be requested, when the information report is needed, and who is to receive it. The completed collection plan forms the basis for further collection actions. (See Figure III-9 for a sample integrated collection planning matrix.)

(4) 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 a 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. To determine collection platform or sensor suitability, a set of key SIRs is analyzed and compared with both key element sets of the target and collection capability factors of available assets or resources. The result informs the selection of the most appropriate asset to satisfy the SIR (see Figure III-10).

(1) **Collection Asset Selection Considerations.** Key elements of the asset selection process 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 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.

Sample Integrated Collection Planning Matrix

	Primary	Alternate	Tip/Queue	NAI/TAI	LTIOV	Collection Agencies											
						Collection Assets (Assigned, Apportioned, Allocated Capabilities)						Collection Resources (Requested Capabilities)					
						SIGINT	HUMINT	CI	GEOINT	MASINT	Other	SIGINT	HUMINT	CI	GEOINT	MASINT	Other
Phase 0																	
OP OBJ 1																	
PIR 1.1																	
EEI 1.1.1																	
Indicator 1.1.1.1																	
SIR 1.1.1.1.1																	
SIR 1.1.1.1.2																	
SIR 1.1.1.1.3																	
Indicator 1.1.1.2																	
SIR 1.1.1.2.1																	
SIR 1.1.1.2.2																	
EEI 1.1.2																	
Indicator 1.1.2.1																	
SIR 1.1.2.1.1																	
SIR 1.1.2.1.2																	
Indicator 1.1.2.2																	
SIR 1.1.2.2.1																	
SIR 1.1.2.2.2																	
SIR 1.1.2.2.3																	
PIR 1.2																	
EEI 1.2.1																	
Indicator 1.2.1.1																	
SIR 1.1.1.1.1																	
SIR 1.1.1.1.1																	
Indicator 1.2.1.2																	
SIR 1.1.1.1.1																	
SIR 1.1.1.1.1																	
SIR 1.1.1.1.1																	
EEI 1.2.2																	
Indicator 1.2.2.1																	
SIR 1.1.1.1.1																	
Indicator 1.2.2.2																	
SIR 1.1.1.1.1																	
SIR 1.1.1.1.1																	
SIR 1.1.1.1.1																	
OP OBJ 2																	
PIR 2.1																	
EEI 2.1.1																	
Indicator 2.1.1.1																	
SIR 2.1.1.1.1																	
SIR 2.1.1.1.2																	
SIR 2.1.1.1.3																	
Indicator 2.1.1.2																	
SIR 2.1.1.2.1																	
SIR 2.1.1.2.2																	
EEI 2.1.2																	
Indicator 2.1.2.1																	
SIR 2.1.2.1.1																	
SIR 2.1.2.1.2																	
Indicator 2.1.2.2																	
SIR 2.1.2.2.1																	
SIR 2.1.2.2.2																	
SIR 2.1.2.2.3																	

Collection Agency: Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (JP 2-01)

Collection Asset: A collection system, platform, or capability that is supporting, as assigned, or attached to a particular commander. (JP 2-01)

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.

Legend

CI	counterintelligence
EEI	essential element of information
GEOINT	geospatial intelligence
HUMINT	human intelligence
LTIOV	latest time information is of value
MASINT	measurement and signature intelligence
NAI	named area of interest
OP OBJ	operational objective
PIR	priority intelligence requirement
SIGINT	signals intelligence
SIR	specific information requirement
TAI	target area of interest

Figure III-9. Sample Integrated Collection Planning Matrix

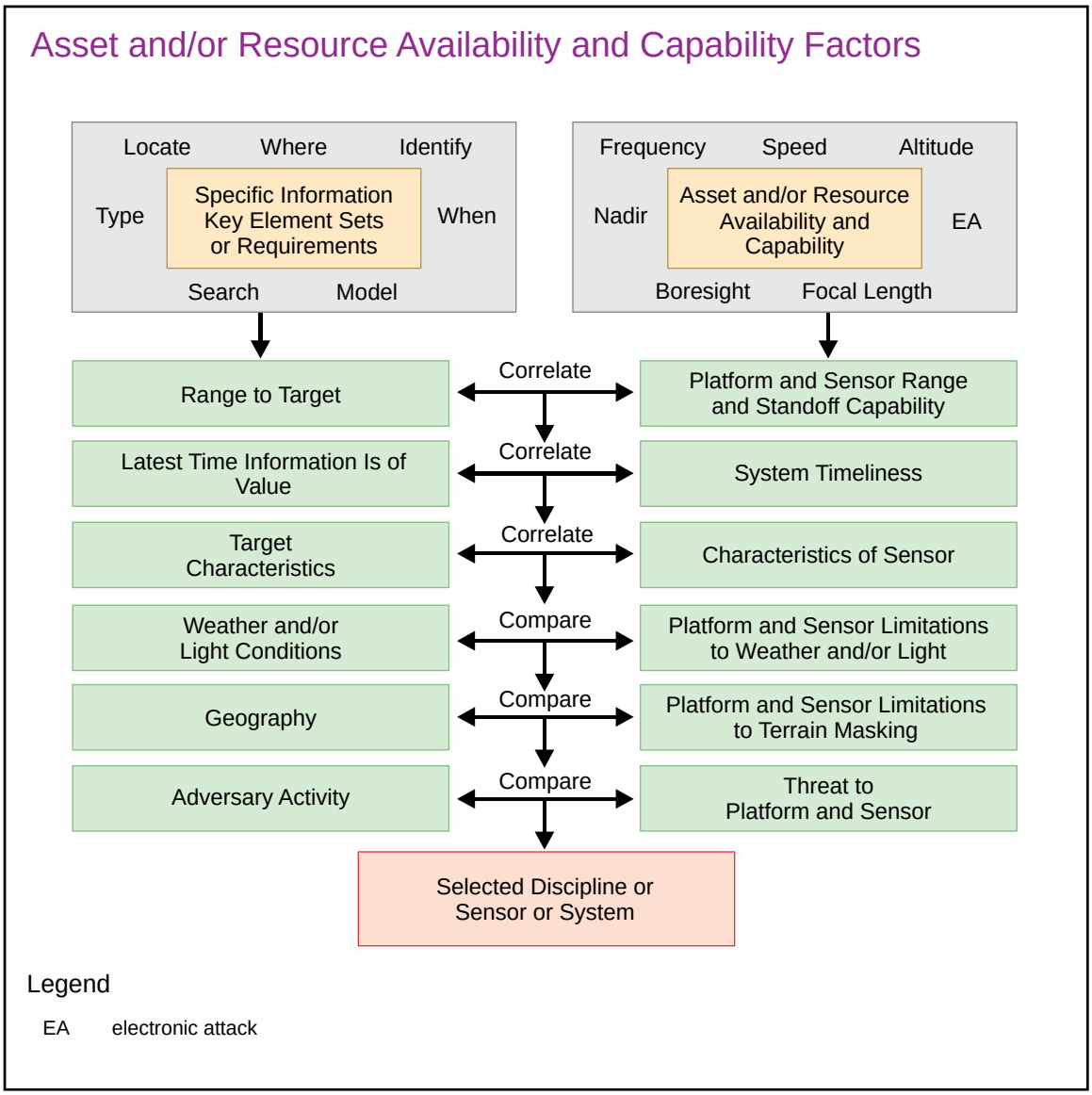


Figure III-10. Asset and/or Resource Availability and Capability Factors

(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 GEOINT, HUMINT, and CI. Collectibles, in contrast, are associated with SIGINT. Both observables and collectibles are associated with MASINT and OSINT. One or more target characteristics may be associated with a key element, and these characteristics can be compared to a sensor or sensors' capability to collect. From the continuation of 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 and CI, the analogous consideration would be the source's access.

(c) **Timeliness** is when the information requested should be received in order to be of value (latest time information is of value [LTIOV]). In order to ensure timeliness, collection managers performing COM should consider the entire intelligence process—not only collection time, but also the lead time required to process and exploit collected data and disseminate the resulting information.

(2) **Collection Capabilities Factors.** COM personnel should know the capabilities and limitations of the available sensors, systems, and disciplines so they can use collection capability factors to directly compare key element sets. The capabilities and limitations of various disciplines and systems are considered, together with their availability, to decide whether they should be tasked. **Sensor capability factors are technical or performance characteristics, range, dwell time, revisit times, and timeliness. CI and/or HUMINT capability factors include placement and access of sources and operational access or freedom of movement of human collectors or their sources.**

(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; therefore, if the enemy or 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 target engagement purposes, particularly in support of coordinate-seeking weapons, demands greater locational accuracy than information collected for updating OBs.

(b) **Platform/sensor range** considers the system's ability to provide target coverage. This characteristic is used to determine which platforms are capable of reaching a location to bring its sensors to bear on the target area. This location is determined by limitations of the OE (primarily weather and threats), commander's guidance and rules of engagement, the physical capability of the platform to reach the specified location, platform altitude and noise reduction considerations, and, where applicable, platform/sensor data transmission/receive ranges (e.g., airborne tether). The

collection manager performing COM assesses combinations of these various range factors 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) **Revisit time** is the period an asset or resource can return and acquire additional collection against a specific target or issue. Revisit times may be hours to days and may have a direct impact on a requirement that calls for multiple collections within a specified timeframe. In some cases, a delay between collection events is built into the plan in order to acquire indications of change that may be suspected.

(e) **Timeliness** considers 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-11). 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, which is then compared with the LTIOV. If the system's timeliness exceeds the LTIOV, then it fails to contribute to satisfying the specific requirement and should not be considered for collection planning purposes.

(3) **Correlation.** Target collection and 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) **OE Factors.** After correlation, the candidate sensors are compared with OE factors to support final sensor selection. Those OE factors include the threat, terrain, contamination, solar position, electromagnetic interference, and weather that might influence the particular discipline or sensor selection. Depending on the OE factors, a technically capable sensor may be dropped from consideration.

(a) Sensor vulnerability is the degree to which enemy countermeasures may affect the collection platform and/or sensor. In general, the sensor platforms that penetrate enemy territory or airspace are the most vulnerable, stand-off sensors less so, and satellite sensors the least vulnerable (though not completely invulnerable). 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 enemy reactions that may require a threat warning alert.

See CJCSI 3250.01., (U) Policy Guidance for Intelligence, Surveillance, and Reconnaissance and Sensitive Reconnaissance Operations.

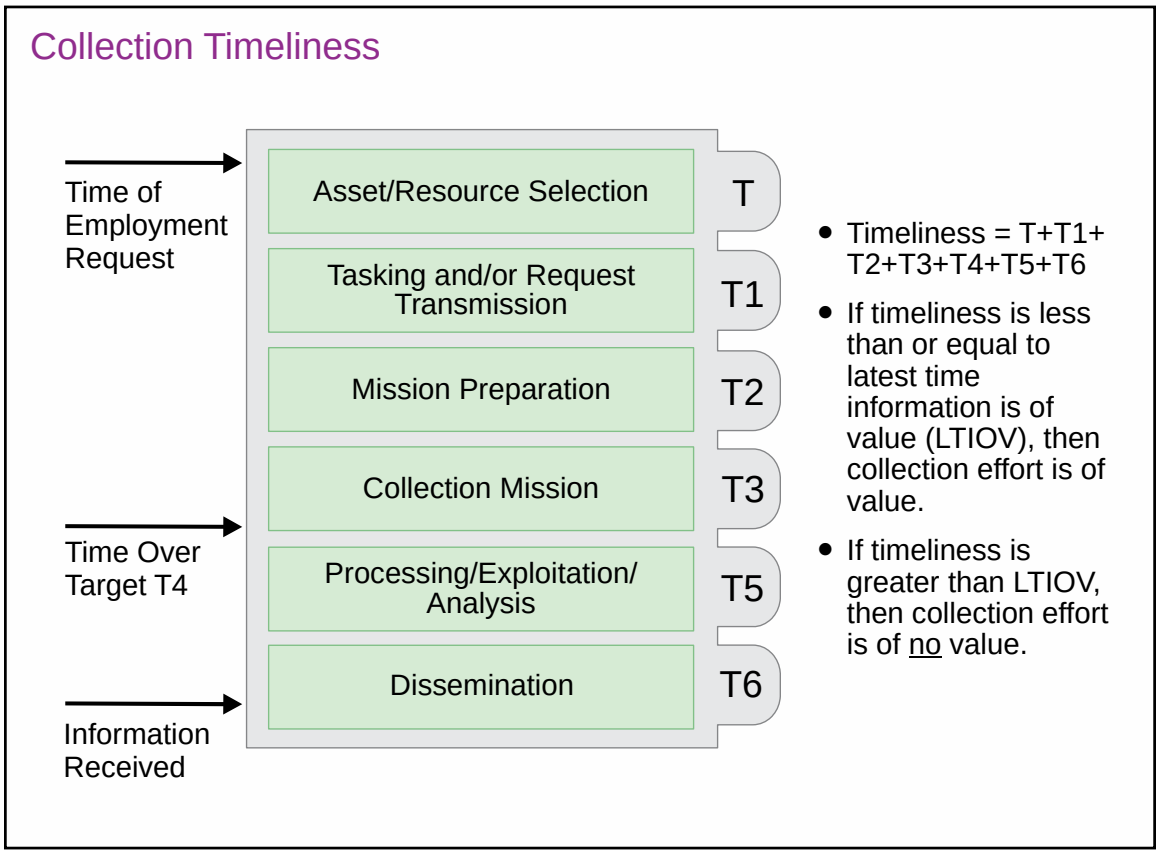


Figure III-11. Collection Timeliness

(b) Weather and light conditions are also considerations, particularly with electro-optical sensors. Weather conditions in and around the collection area may affect the collection platform and/or sensor capability to "see" the area.

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

(d) CBRN hazard understanding is the dynamic individual and collective comprehension of the implications of CBRN incidents and resulting conditions within the OE, facilitating the framing of CBRN problems and decision making. Selection criteria for sensors should 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 (to include estimated downtime, if not available) and the addition or deletion of capabilities. Coordination with adjacent and higher HQ and national agencies should 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, and then proceeds through the active requirements list to determine how

each request can be satisfied (see Figure III-12). The collection manager performing CRM transmits the requirements and any recommendations for planning and scheduling

Collection Tasking Worksheet

Collection Tasking Worksheet

Organization: _____ Registration Number: _____

DTG: _____ Collection Manager: _____

Specific Information Requirements: _____

Time: _____ Priority: _____ 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 _____

Legend

CI	counterintelligence	HUMINT	human intelligence
COMINT	communications intelligence	IMINT	imagery intelligence
DTG	date-time group	MASINT	measurement and signature intelligence
ELINT	electronic intelligence	TECHINT	technical intelligence

Figure III-12. Collection Tasking Worksheet

of the prioritized list to the collection manager performing COM. The collection manager then develops the collection plan based on the command's guidance. 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 that is to be reported. Collection tasking includes PED, tasking, guidance, and instructions. In many cases, the demand (number of collection requirements) exceeds the capacity (number of collection requirements that collection assets can be expected to satisfy). In these cases, the collection managers for CRM and COM should coordinate on how to proceed. In some cases, the untasked requirements may simply be tasked on a subsequent day or after other collection priorities have been completed. In other cases, the collection requirement should be submitted to other organizations with collection resources tasked to support the command. Command guidance should specify the command's policy on what to do in these instances.

(2) Collection to satisfy a validated requirement may occur at any level. CRM includes validation, which confirms that an intelligence collection requirement or PR is sufficiently important to justify the dedication of intelligence resources at each echelon. For example, if a CCDR determines the information needed to answer an RFI is unavailable, the commander may task collection assets 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) A mission tasking order or mission type order is sent to the unit selected for the accomplishment of the collection operation.

(4) Collection support request forms or messages are methods of requesting collection support, for time-sensitive situations, from pre-determined sensors and/or weapons on resources of the supporting force. These are dependent on the tactical situation, type of sensor, and type of resource (i.e., supporting, theater, national, or multinational). Many specific data elements in these requests and the transmission procedures are classified. In the case of assigned and direct support assets, requesters follow instructions provided in the OPLAN or OPORD intelligence annex or by message. In addition, the *Joint Tactical Exploitation of National Systems Manual,* DIA manuals, and the classified *Defense Human Intelligence (HUMINT) Enterprise Manual, Volume I, Collection Requirements, Reporting, and Evaluation Procedures* provide guidance for requesting support from DOD and national CI and HUMINT resources, establishing procedures, and authorizing responsibilities within the CI and HUMINT collection enterprise. In preparing requests for national resources, the collection manager should consider the guidelines in Figure III-13. It is important to note that, in most cases, supported units should request specific information, rather than a specific asset. If the asset is unavailable, the support may be able to be satisfied with an available, if less suitable, asset. It is the responsibility of the collection manager performing COM to maximize the number of requests satisfied while still satisfying requirements completely.

Guidelines for Requesting National Resource Collection

Areas of Interest	National systems are best employed against high-priority targets outside the range of 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 request for information, address why current information does not satisfy the requirement, and identify any required unique sensor capabilities that are unattainable from other assets.
Sensor Capabilities	Target descriptions must place minimum restrictions on systems' use, unless specific parameters are required.
Sensor Accessibility	The targets' accessibility must be determined when possible before a collection request is forwarded.
Exploitation and/or Analysis Requirements Clarity	Specific information requirements directly related to the target (including concise, explicit exploitation guidance) will provide clarity to collection and exploitation personnel. These may be labeled essential elements of information in existing collection management systems and tools.
Exploitation and/or Analysis Requirement Purpose	Exploitation and/or analysis requirements must state the purpose of the information desired and how 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-13. Guidelines for Requesting National Resource Collection

(a) 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. "Tipping and cueing" refers to the use of one intelligence discipline, asset, or sensor type to cross-cue or initiate collection by a more precise sensor. In some cases, cueing, tasking, and collection activities may be semiautomatic to optimize and speed the intelligence process.

(b) **Asset Mix and/or Redundancy.** A collection manager uses a combination of assets of differing disciplines (asset mix) or similar disciplines (asset

redundancy) against high-priority targets. 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 is required to increase 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.

(c) **Persistent Surveillance.** Across the range of military operations, collection strategies against high-value targets should emphasize and provide for the near-continuous, all-weather, day/night surveillance of the target through the efficient utilization of all appropriate collection assets in persistent surveillance, as opposed to periodic reconnaissance, mode. Persistent surveillance, as part of a collection strategy, enables timely decisions by the commander and the effective use of precision-guided munitions and is critical to countering the enemy's use of military deception. Long-dwell collection platforms, such as unmanned aircraft systems, distributed undersea and unattended ground sensors, battlefield surveillance radars, and SOF, have enabled a paradigm shift in which it is possible to provide continuous surveillance over large portions of the area of interest to monitor, tag, track, characterize, and report on movements and activities associated with the target. Persistent surveillance is facilitated by the effective integration and synchronization of all theater and national collection assets and resources in a coherent collection strategy. Because persistent surveillance depends heavily on resources that are in high demand and usually few in number, requirements for persistent surveillance should be prioritized.

(d) **Asset Convergence and Dispersion.** When developing a collection plan, collection managers should consider whether to maximize efficiency by dispersing collection assets across the widest geographic area in order to maximize collection, or place them in nearby or the same geographic areas to overlap their sensor ranges for synergistic effects, thus providing more opportunities for dynamic tipping and cueing, asset mix, and/or asset redundancy. In many instances, these events may not be pre-planned for specific targets, though the value of allowing these ad hoc tipping events to unfold may outweigh the value of maximizing the number of collection requirements. Convergence can be used to increase the confidence of target identification, classification, or location data, or to collect upon different observable or measurable target characteristics (such as a GEOINT and SIGINT mix). Convergence is the deliberate use of multiple assets at the same time to exploit a target. Dispersion is distributing assets to cover a large geographic area with a diverse set of targets without sacrificing quality, or separating assets in a manner that allows for collection against the greatest number of targets.

e. **The CCMD J-2 staff/JIOC and J-3/joint reconnaissance center need to dynamically manage theater collection assets.** They also need to ensure collection support is synchronized with the CCDR's intent, national requirements, campaign objectives, operational objectives, and other guiding priorities as established by the Service components. In parallel, the CCDR, through the battle staff and supporting intelligence analysts, obtains and maintains access to processed and unprocessed intelligence data and products to determine mission accomplishment and/or requirement satisfaction. With airborne collection platforms in particular, many different staff

elements are involved: operations, weather, maintenance and logistics, and communications. They need to be closely integrated into the mission planning effort. Intelligence sensor planners and managers of processing and exploitation elements should 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 that are responsible for tasking reconnaissance assets.

f. **Execution.** During mission execution, collection managers performing a combination of CRM/COM authorities are often tasked to monitor, and in certain circumstances when external factors cause a change to the collection plan, control (via delegated tactical control) collection assets during the collection operation. These circumstances include when threats, weather, or CBRN dangers deny collection assets the ability to operate in certain operational areas. They also include development of time-sensitive collection opportunities and urgent force protection or personnel recovery requirements. In these instances, the collection manager should review any incoming collection requirements for completeness and urgency, validate and prioritize them as appropriate, then retask collection assets as appropriate.

(1) **Resource Integration.** 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 may augment and clarify ongoing threat warning events, a rapid intelligence gain/loss assessment should be made and collection planners (i.e., the collection managers performing COM who developed the collection plan) should be, when possible, consulted prior to retasking of collection missions already in progress. Situations may warrant such dynamic retasking of intelligence assets to support the commander's urgent force protection as opposed to IRs. Deviations to the pre-mission collection plan should be documented in after action mission summaries and updates to the mission plan. This enables collection actions which were not performed to be retasked at the earliest available opportunity. When integration of a new collection requirement with current or already planned missions is not feasible, a new mission should be planned.

(2) **ISR Visualization.** ISR visualization is a subset of the COP available in tools such as the Global Command and Control System (GCCS) and Service C2 communications 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 situational awareness 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 OE. ISR visualization enables collection managers performing COM to monitor and control collection missions and update the collection plan during mission execution. ISR visualization optimizes the use of limited ISR collection assets, contributing NRT ISR information that promotes persistent surveillance of the area of interest and enhances the JFC's battle management of the operation. Successful ISR visualization is contingent on timely reporting of ISR asset 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 collection assets, their capabilities, their field of regard, and their tasked targets. ISR visualization requires continuous feedback regarding the current and projected locations of all collection 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 collection asset tasked to collect on each target. ISR visualization displays also depict the effects of the OE, to include METOC effects, on the collection capabilities of individual airborne collection 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 SCI-level displays.

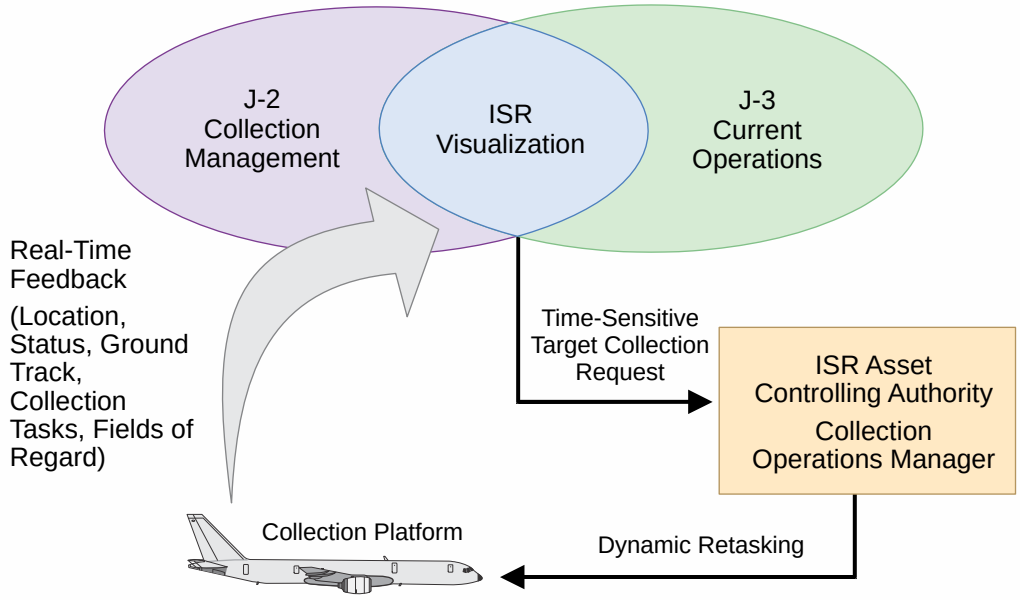
(b) **ISR Visualization and Current Operations.** ISR visualization is integrated in NRT with current military operations. From planning through execution, ISR visualization provides the J-2/J-3 a valuable tool for conducting ISR operations and rapidly responding to changing collection requirements. ISR visualization is merged with JIPOE products such as event and decision support templates. The interface between ISR visualization and JIPOE 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 operations, ISR visualization includes current intelligence overlays depicting changes in adversary defensive capabilities. ISR visualization facilitates the integration and synchronization of the joint force's and component commands' ISR activities and capabilities.

For a more detailed discussion of the JIPOE process, JIPOE products, and ISR visualization, see JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

(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 enemy time-sensitive targets that may warrant dynamic retasking of collection platforms or retasking 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 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-

Intelligence, Surveillance, and Reconnaissance Visualization

- J-2/J-3 team effort synchronizing ISR and operations
- Real-time visualization of ISR asset status
- Integrates current ISR picture with current military situation and JIPOE products
- Identifies fleeting collection opportunities
- Facilitates time-sensitive decision making (e.g., dynamic retasking)
- Resident on GCCS/COP



Legend

COP	common operational picture
GCCS	Global Command and Control System
ISR	intelligence, surveillance, and reconnaissance
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
JIPOE	joint intelligence preparation of the operational environment

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

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 retasking to the controlling authority of the most appropriate collection asset. The collection manager performing COM controlling the collection platform accomplishes the actual retasking 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 colocation or by virtual connectivity. Likewise, the joint force's ISR visualization

operation may 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 GCCS and Service C2 communications system variants may be fully integrated into these battle management operations and should support the commander's information requirements through the COP.

(3) **Collection Plan Update.** The collection manager performing CRM/COM in a dynamic environment updates the collection plan continuously during the mission and finalizes a post-mission collection plan update based on what actually happened. The collection managers who developed the pre-mission collection plan review the post-mission update and determine how to satisfy planned-but-unsatisfied collection requirements. Collection requirements can be unsatisfied after a collection mission for a variety of reasons (e.g., asset unavailability, maintenance, sensor failure, weather, threat). These collection managers should determine whether the requirements can be canceled, retasked to a future mission, or if they may coordinate with collection managers performing CRM to submit the requirement to a higher or lateral echelon.

(a) **Exploitation.** Exploitation of collected information is closely associated with the management of collection assets and resources. **Generally, the staff that allocated a collection capability also controls the sensor-unique PED equipment.** Exploitation is discussed further in Section C, "Processing and Exploitation," and dissemination in Section E, "Dissemination and Integration."

(b) **Evaluate Reporting. The evaluation process tracks the status of collection requirements and provides feedback to the requesters and collectors.** Monitoring outstanding requirements ensures that orders and requests for 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 the requesters receive a copy; and determines, in conjunction with the requester, if the requirement has been satisfied. The collection manager should also let the collector know if the information collected is of value to the requester. Requester feedback establishes customer satisfaction, permits tasking deletion, and frees collection assets and resources to be redirected to satisfy other active requirements.

(4) 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 supporting organizations and other units or agencies that own and operate collection and exploitation assets or resources. 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.

12. Types of Collection Operations

a. Collection is conducted via a variety of means and in a variety of broad categories.

(1) Collection includes those activities related to the acquisition of data required to satisfy the requirements specified in the collection plan. The collection plan is modified and revised as needed to satisfy the most pressing and evolving IRs. Collection operations acquire information about the adversary and the OE and provide that information to intelligence assets and elements.

(2) It is crucial for collection managers to understand the collection capabilities and limitations of various collection assets and resources in order to properly include collection management products such as collection strategies, collection plans, and tasking. Collection assets and resources are collection systems, platforms, or capabilities designed to collect information. Collection assets and resources can be categorized by three types: technical collection (not to be confused with technical intelligence [TECHINT]), human-derived collection, and a combination of these two.

(a) **Technical Collection Platforms.** Technical collection platforms conduct collection by use of various collection sensors. Technical collection platforms predominantly use the GEOINT, MASINT, or SIGINT disciplines

(b) **Human Collection Assets and Resources.** Intelligence collection that is tasked to trained human collectors and obtained through their interaction with human sources or through the collector's observations of the OE.

(c) **Combination of Technology and Human Collection.** The combination of technology and human collection requires the interaction of these two asset categories for collection to occur such as TECHINT, OSINT, and identity activities.

1. **TECHINT.** TECHINT is derived from the exploitation of foreign material and scientific information. TECHINT begins with the acquisition of a foreign piece of equipment or foreign scientific/technological information. The item or information is then exploited (i.e., analyzed) by specialized, multi-Service collection and analysis teams.

2. **OSINT.** OSINT is based on information that any member of the public can lawfully obtain by request, purchase, or observation. Examples of open sources include unofficial and draft documents, published and unpublished reference material, research, or online databases, and Web-based networking platforms or repositories. Other sources include foreign print, radio, television, and Internet broadcast messages.

3. **Identity Activities.** Identity activities leverage intelligence, operations, and law enforcement elements to collect identity information, forensic materials, and documents and media through site exploitation or directly from encountered individuals. Collected information and materials are processed and

exploited using a combination of technical capabilities, scientific processes, and analytic methods and provided to identity intelligence (I2) analysts for analysis and production.

(3) The most important components of collection are what the sensor capabilities or assets are. The range, sensitivity, frequency ranges, and other asset characteristics should be known in sufficient detail so the collection manager can determine what types of indicators the sensor can and/or is best suited to observe/collect. When a collection manager is conducting research on a systems capability, it is valuable to understand how the system conducts its collection mission to include the mission participants.

13. Collection Agencies and Sources

a. Each member of the Defense Collection Management Enterprise (DCME) maintains a primary customer set and performs collection management within its responsibility or leverages collection of other IC organizations to meet intelligence customer requirements. This occurs under the guidance and oversight of the defense collection manager (DCM) IAW DODD 5105.21, *Defense Intelligence Agency (DIA)*, and Department of Defense Instruction (DODI) 3325.08, *DOD Intelligence Collection Management.*

b. The Office of the Under Secretary of Defense (Intelligence) oversees DOD collection management plans, policies, and programs, including training, certification, and professional development programs. It provides direction and guidance to DOD components conducting collection management activities.

c. The SIOs of the Services organize, train, equip, and deploy forces to support CCMD and component command joint intelligence warfighting and collection management operations. The Services, as part of planning, programming, and acquisition efforts, ensure Service and command intelligence systems and architectures make data and exploitation products accessible to all CCMD JIOCs; other DOD and IC organizations; and designated, multinational partners via the DODIN, DCGS, enterprise services, and other capabilities.

d. The CCMD JIOCs execute theater collection management activities in coordination with DIA, subordinate joint force commands, other DOD components, other defense intelligence components, and multinational partners. The CCMDs develop the theater collection plan and employ theater-assigned and supporting collection sensors and platforms.

e. In parallel, the CCMDs develop and maintain databases supporting planning, operations, and targeting; validate assessments from higher, lower, and adjacent sources; conduct ISR visualization; and operate as a cohesive mission management team with the operations directorates of the CCMDs, Services, and other DOD IC elements. This ensures dynamic and integrated management of theater and tactical collection management and ISR activities.

f. The JIOCs participate in the JCMB and support JCMB working groups to manage and direct CCMD collection requirements and operations to support mission needs. The JCMB is the CCMD's theater process, enabling needs prioritization, collection strategies and plans, CRM, ISR asset planning, synchronization, operations, PED, and assessment.

g. The Director, DIA, serves as the DCM and is the DOD lead for coordinating intelligence collection support to meet CCMD requirements; leading efforts to align analysis and collection activities with ongoing and planned operations; and linking and synchronizing military, defense, and national intelligence collection capabilities. The Director, DIA, also appoints a functional manager for collection management, who sets standards for DOD training, certification, and professional development programs, and advocates for resources required for DOD intelligence collection.

h. DIA reviews and updates DOD collection management documentation and proposes doctrine to accurately reflect, align with, and optimize joint collection management activities, concepts, and principles directly supporting intelligence priorities. DIA equips collection managers with integrated architecture and state-of-the-art tools and applications to address customers' intelligence needs. DIA should assess new technology and make recommendations for the inclusion of new technology that may advance the DCME capabilities.

i. DIRNSA/CHCSS manages the SIGINT and Cryptologic Enterprise and ensures these capabilities are fully integrated into the lager defense intelligence enterprise. NSA/CSS provides direct support to the CCMD JIOCs, DIA, and other DOD and national intelligence collection operations and mission management by integrating SIGINT capabilities, expertise, and personnel.

j. NSA/CSS develops FSPs in support of IP NISP development efforts. SIGINT mission management capabilities enable integrated SIGINT tasking, collection, and processing, including effective tipping/cross-cueing from one sensor/discipline to another within the DCME. NSA/CSS SIGINT mission management involves requirements validation, tasking, collection, and PED activities.

k. The Director, NGA, manages the national system for the Geospatial-Intelligence Enterprise and ensures its capabilities are integrated into the larger defense intelligence enterprise. NGA provides direct support to CCMD/JIOC, DIA, and collection management operations by integrating GEOINT capabilities/expertise and/or personnel. NGA may develop FSPs in support of IP NISP development efforts. NGA serves as the manager responsible for validating, tasking, and satisfying DOD and national geospatial-IRs via the National GEOINT Committee and emerging GEOINT Information Management System.

l. The NGA Functional Manager for Source Management exercises GEOINT mission management responsibilities involving policies, plans, requirements, tasking, collection, PED, and GEOINT information, products, and services that support joint warfighters, other DOD components, and national intelligence customers. NGA GEOINT mission management also provides timely, relevant, and accurate GEOINT and

effective tipping and cross-cueing from one sensor or discipline to another in the defense intelligence enterprise.

m. The Director, NRO, manages and operates the NRO and its programs and activities and acquires NRO systems. The NRO provides DOD, the IC, and USG with global situational awareness, real-time engagement support, SIGINT and NRT imagery, and access to denied areas. The NRO accomplishes this support through the direction and management of all assigned resources to provide peacetime, contingency, crisis, and combat overhead reconnaissance support to DOD and delivers intelligence capabilities, information products, services, and tools in response to national-level tasking in coordination with the functional managers.

n. The Director, NRO, receives and implements SecDef and DNI guidance and direction by establishing strategic guidance policy and procedures for executing the NRO mission and accomplishing the Director, NRO, National Security Space responsibilities.

SECTION C. PROCESSING AND EXPLOITATION

14. Overview

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 to decision makers (to facilitate timely operations) and to intelligence personnel (for all-source intelligence analysis). Processed data should be automatically integrated with existing information in the GCCS COP to provide the most current view of the OE (see Figure III-15).

For more information on exploitation, see Appendix F, "Joint Exploitation Support to Intelligence."

a. At the CCMD level, the J-2 manages theater processing systems and capabilities. Prior planning is critical to ensure system interoperability with joint, interagency, and multinational communications systems. The potential for operations involving both nonmilitary organizations and NGOs complicates this environment. The J-2 should consider these factors and be flexible in developing work-around procedures. Intelligence processing elements should be prepared to set up both US-only and multinational segments.

b. Processing and exploitation of collected information by the components and their subordinate units is closely associated with effective management of collection assets. Traditionally, processing and exploitation was performed by the collection operation element because of sensor-unique requirements. Increasingly, improved communications capability and open standards for sensors permit processing and exploitation at other locations. Processing and exploitation can now be performed either in reachback or expeditionary environments. Expeditionary processing and exploitation is performed

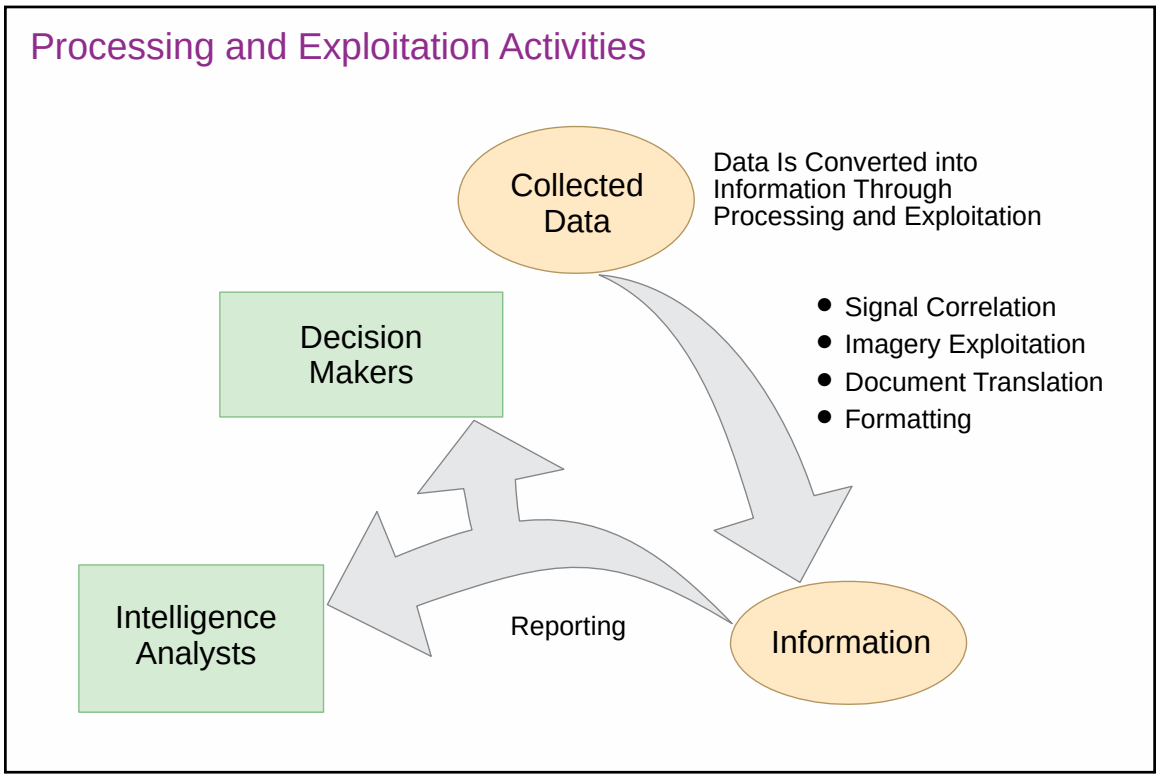


Figure III-15. Processing and Exploitation Activities

while colocated with the collection operation element in a forward environment. This type of processing is required when collection occurs in a disconnected, interrupted, or low-bandwidth environment. Reachback processing can be performed at a centralized or federated location. Reachback enables efficiencies by allowing processing and exploitation resources to be actively managed and transitioned between collection assets to provide the most effective and efficient allocation of processing and exploitation capabilities. The type of processing and exploitation applied to collected information is determined by mission requirements, the collection asset, collection environment, and the resources available.

15. Human Intelligence

HUMINT is a category of intelligence derived from information collected and provided by human sources. HUMINT supports operations across the range of military operations at all levels of warfare. 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 HUMINT is conducted by the JIOC and joint force analytical and/or production activities. This activity primarily involves analyzing HUMINT reporting for inclusion in all-source production and for database maintenance, and supports HUMINT and CI targeting and source validation. Documents and media captured by US and multinational personnel are processed outside HUMINT channels at J-2 joint document exploitation centers (JDECs), if established. All captured documents and media should be forwarded to the JDEC for centralized processing and safeguarding.

Additional information on the J-2X organization and responsibilities can be found in JP 2-01.2, Counterintelligence and Human Intelligence in Joint Operations.

For more information on DOMEX, refer to Appendix C, "Document and Media Exploitation."

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 rocket and V-2 ballistic missiles.

In the spring of 1945, as the outcome of World War 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 a full description of yourself and 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, and Military Intelligence: Its Heroes and Legends,* compiled by Diane L. Hamm, US Army Intelligence and Security Command History Office, October 1987

16. Geospatial Intelligence

a. GEOINT is an intelligence discipline that has evolved from the integration of imagery, IMINT, and geospatial information to a broader cross-functional effort in support of national and defense missions and international arrangements. Advances in technology and the use of geospatial data throughout the joint force have created the ability to use geography by integrating more sophisticated capabilities for visualization, analysis, and dissemination of fused views of the OE. This capability provides many advantages for the warfighter, national security policy makers, homeland security personnel, and IC collaborators by precisely locating activities and objects, enabling safe navigation over air, land, and sea, assessing and discerning the meaning of events, and providing context for decision makers.

b. GEOINT includes imagery, that may be processed and exploited at multiple locations simultaneously, both in and out of theater, by the JIOC or equivalent, component command intelligence units, Service intelligence centers, and national intelligence organizations. The JIOCs, or other organizations, process the digital data and display the down-linked imagery on a workstation for immediate exploitation. The imagery can also be sent to a digital library for later use. Imagery exploitation results, such as reporting, annotated images, and shape files, 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-I3.

For additional information on GEOINT see JP 2-03, Geospatial Intelligence in Joint Operations.

17. Signals Intelligence

SIGINT support to joint operations includes communications intelligence, ELINT, and foreign instrumentation signals intelligence (FISINT). Communications intelligence 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 JIOCs, 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 CCMD JIOCs. 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 NJOIC for tasking to the appropriate organizations. Where applicable, requests for SIGINT support should be entered into approved systems such as the Planning Tool for Resource, Integration, Synchronization, and Management, for approval by the designated SIGINT operational tasking authority.

18. Measurement and Signature Intelligence

MASINT provides technically derived intelligence to detect; tag, track, and locate; 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 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 warning intelligence, JIPOE, force protection, and foreign materiel exploitation. In addition, MASINT provides intelligence on WMD capabilities as well as weapons system capabilities based on analysis of collected telemetry data.

19. Open-Source Intelligence

a. OSINT is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific IR.

b. Publicly available information is information that anyone can lawfully obtain by request, purchase, or observation.

c. OSINT is developed using media and Web-based sources. 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 ODNI Open Source Enterprise provides translations of foreign broadcast and print media. OSINT is also developed from information collected by commercial companies that use their own assets or purchase information from independent contractors who monitor media.

20. Technical Intelligence

a. Exploitation of captured enemy equipment can provide critical information on enemy strengths and weaknesses that may favorably influence planning. Exploitation of enemy equipment, excluding computer storage media, video and digital recording media, and media equipment, is generally performed in the CCMD by a joint captured materiel exploitation center (JCMEC), which is staffed by Foreign Materiel Program personnel from the Services' TECHINT organizations and Naval Explosive Ordnance Disposal Technical Division. CCMDs or subordinate joint forces should notify the NJOIC through command channels when they require JCMEC support. This may help ensure appropriate Service component resources are requested to meet the support requirement.

b. As a subcategory of TECHINT, WTI addresses the challenges of operating in an asymmetric environment in which the enemy employs improvised weapons. WTI leverages an enterprise architecture that spans from tactical collection through strategic forensic/technical exploitation and intelligence analysis and focuses on improvised weapon, associated components, and other weapons systems. WTI both feeds and leverages I2 production. Through analysis of captured material and improvised weapons, WTI feeds these capabilities and applications and likewise, they leverage WTI through the fusion of information that links people, places, and things in greater context.

For more information on WTI, refer to the JP 3-15.1, Counter-Improvised Explosive Device Operations, *and the* Weapons Technical Intelligence Handbook.

21. Counterintelligence

CI uses collection methodologies that are similar to HUMINT. However, CI, in contrast to HUMINT, has a more narrow focus and targets those entities that are targeting friendly forces and information. Nonetheless, exploitation of data collected by CI assets can yield information critical to warning intelligence and force protection. Service component CI elements conduct CI collection using liaison; elicitation; passive collection; review of open sources; military CI collections; and screening, interviews, and debriefing of displaced persons, defectors, refugees, and US persons with access to information of CI interest. Additionally, law enforcement information and 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-2X.

For more detailed information regarding CI processing, exploitation, and reporting, see JP 2-01.2, Counterintelligence and Human Intelligence in Joint Operations.

SECTION D. ANALYSIS AND PRODUCTION

22. 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, rendered through a continuous JIPOE process, support the JFC's decision making regarding the critical requirements; vulnerabilities; COGs of adversary forces; current military capabilities of adversary, friendly, and neutral forces; and estimates of the most likely/most dangerous adversary COAs.

b. **Intelligence is produced through the integration, evaluation, analysis, and interpretation of information from single or multiple sources.** Intelligence production should 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 the CCDR 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).

23. Conversion of Information into Intelligence

a. Data initially received from theater or national sensors arrives in various forms depending on the nature of the sensing device. Depending on the source, the raw input may be in the form of digitized data, unintelligible voice transmissions, large digital files containing unrectified images of the Earth, or spools of unprocessed film. In order to be usable for a planner, decision maker, or intelligence analyst, this raw data must first be processed into an intelligible form. Trained intelligence specialists resident at JIOCs, JISEs, Service components, Service intelligence centers, and intelligence DOD agencies typically convert raw data into usable information by processing and exploiting the data (see Figure III-17). The amount of time required to complete this process depends on the type of sensor and data transmission method. It could range from minutes to days.

(1) In the first step, collection output is converted by sensor-specific processing measures into visual, auditory, or textual information that is intelligible to humans.

(2) A separate process is required to further translate and contextualize the information that results from initial processing. It is not until the end of this step that the planner, decision maker, or intelligence analyst can cognitively assimilate the information.

b. CCDRs require timely access to crucial, relevant information; therefore, intelligence should continually balance access requirements with the need to protect sources and methods. Intelligence-producing agencies should make information

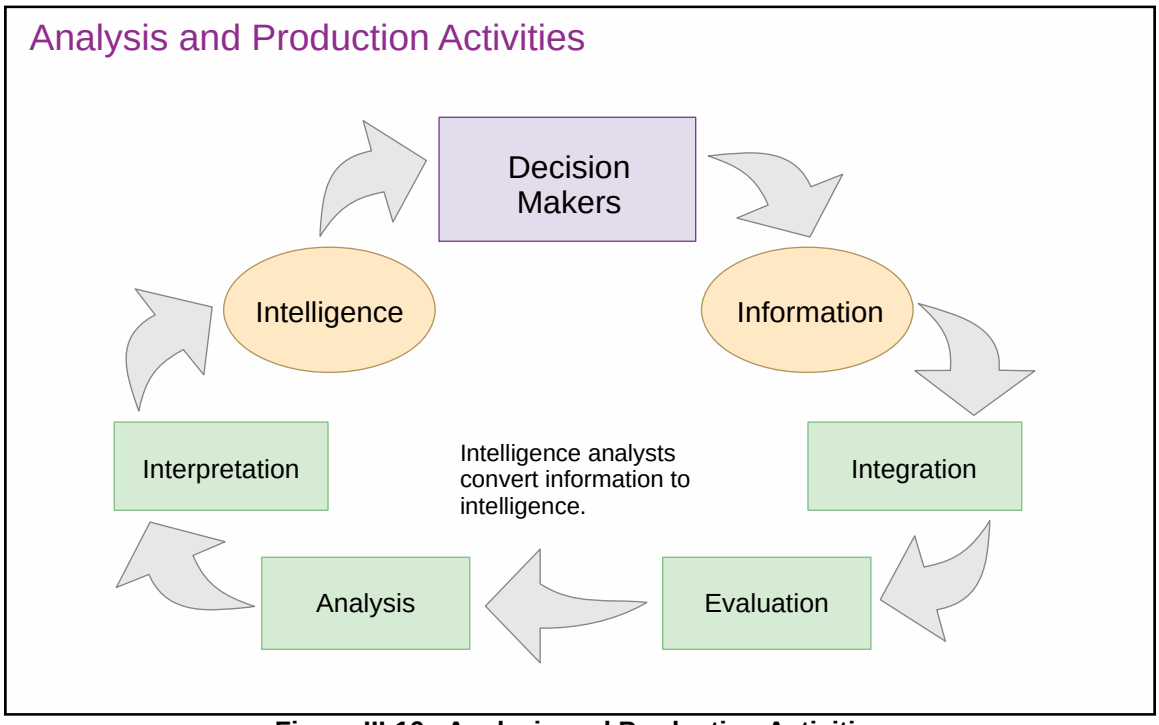


Figure III-16. Analysis and Production Activities

available to intelligence analysts and other intelligence users at the earliest time possible. Service components, intelligence centers, or intelligence CSAs processing and exploiting collected data should make the resulting information available in libraries, Web pages, databases, or message traffic as soon as the information can be understood by the consumer.

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

(1) **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 JIOCs 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.

(2) **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.

(3) **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.

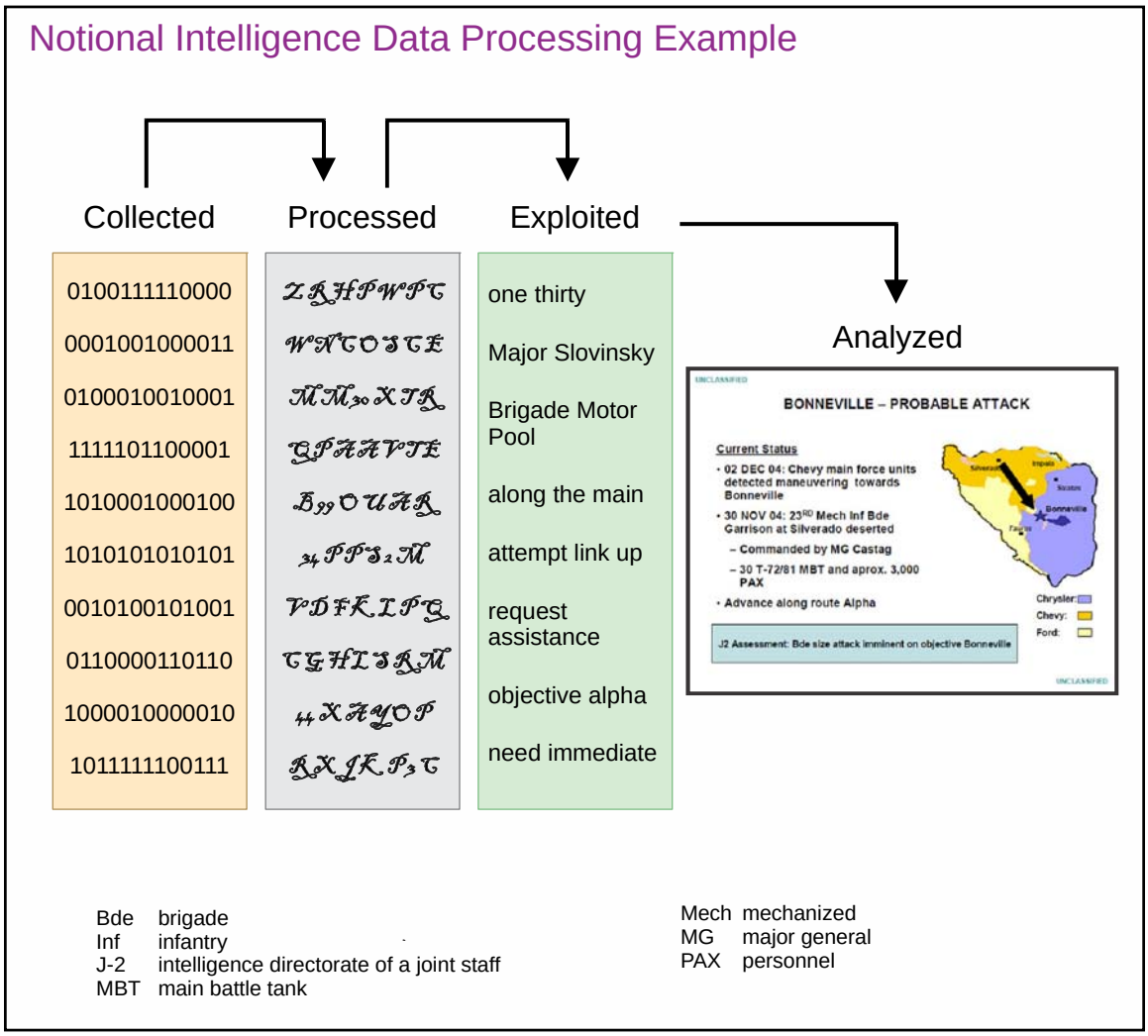


Figure III-17. Notional Intelligence Data Processing Example

(4) **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, recognizing the absence of activity, and a postulation regarding the significance of that activity.

24. Collaboration

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.**

a. During crisis situations or contingency operations, some formal collaboration may be facilitated by preplanned federated intelligence partnerships. However, even in the

absence of a federated support arrangement, JIOC analysts and their counterparts in other theaters and at the national level should collaborate as the situational requirements dictate. During peacetime, routine, informal collaboration among intelligence analysts should be encouraged within guidelines established by the JFC or joint force J-2.

b. The IC has incorporated a variety of tools on both JWICS and SIPRNET to foster greater collaboration within the IC.

c. Interorganizational document coordination, in contrast to informal IC collaboration, is a more formal staff process in which official organizational positions are obtained or confirmed.

25. Databases and Virtual Knowledge Bases

a. **Intelligence databases are repositories of collected data, processed information, and finished intelligence products that 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 segregated according to intelligence disciplines. For example, the NGA National Exploitation System is the repository for imagery analysis and production, and the NSA Pulse contains current and historical finished SIGINT products. Similarly, the Biometrics Identity Intelligence Resource contains BEI products on encountered individuals, and the Harmony database maintains DOMEX information of assessed intelligence value. The segregation 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.**

b. **Virtual knowledge bases** are essentially 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.

26. Products

Categories of intelligence products produced by or for the subordinate joint force are described as follows and in Figure III-19.

Virtual Knowledge Bases

A Virtual Knowledge Base maintains the published analytical conclusions of the Intelligence Community in an electronically accessible form organized according to a taxonomy.

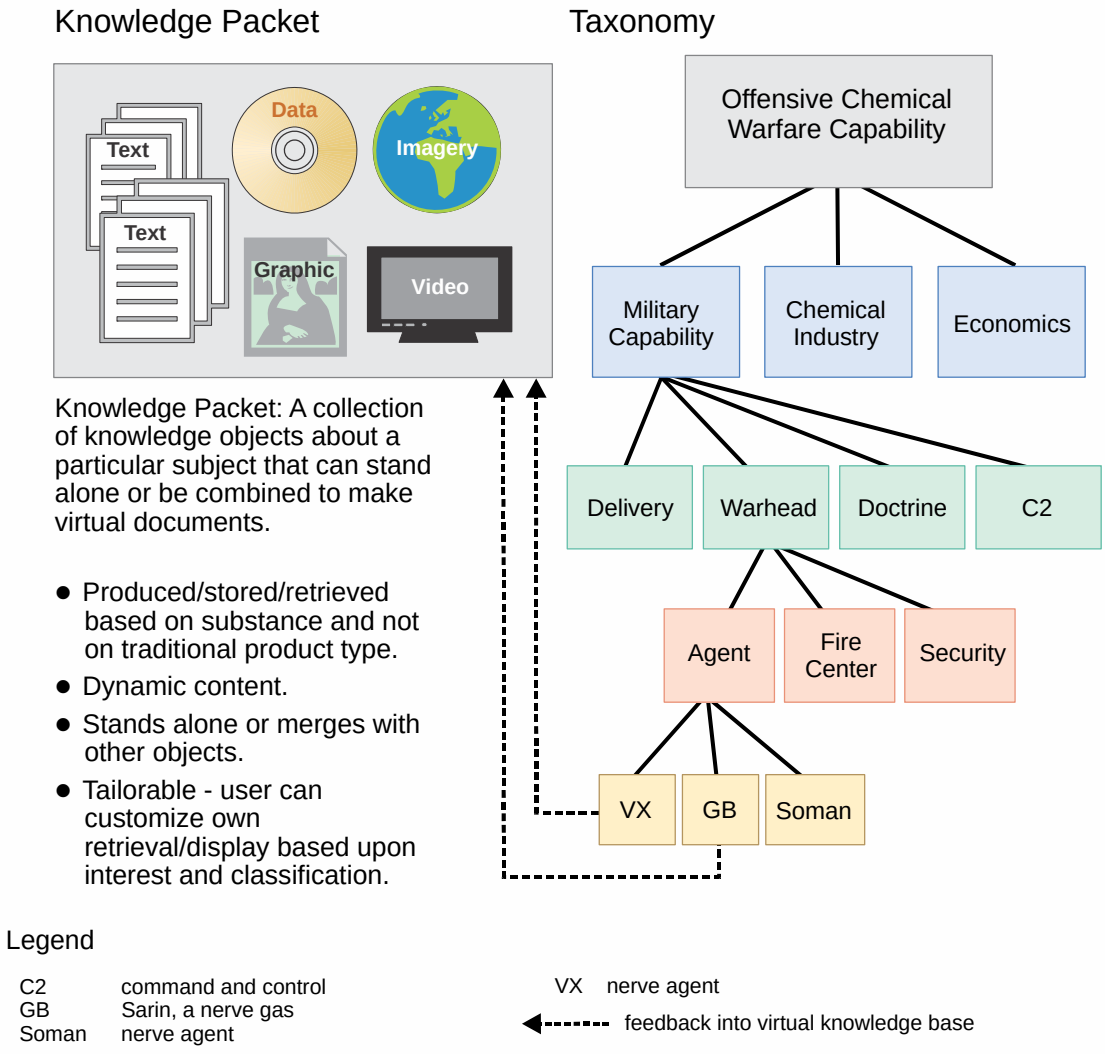


Figure III-18. Virtual Knowledge Bases

a. Warning Intelligence

Intelligence Products

Warning Intelligence

- Current intelligence reports from theater assets, theater warning intelligence support, and correlation of force movements in the joint operations area (JOA).
- National level provides tip-off and warnings of imminent or hostile activity.

Current Intelligence

- Military and political events of interest from joint intelligence operations center (JIOC), joint intelligence support element (JISE), and national sources. Counterintelligence on current foreign intelligence activities.
- Reports on joint force operations.
- Summaries and briefings by JIOC, JISE, and national organizations.
- Open-source intelligence in the JOA.

General Military Intelligence

- Tailored to specific mission: Political, economic, and social aspects of countries in the JOA. Information on organization, operations, and capabilities of foreign military forces in the JOA. Counterintelligence on foreign intelligence capabilities and activities, as well as terrorism, which impacts the force protection mission.
- Formats: Military Capabilities Assessment, Military-Related Subject Assessment, Adversary Course of Action Estimate, Foreign Intelligence Threat Assessment.

Target Intelligence

- Target systems analyses.
- Electronic target folders containing target materials describing characteristics of selected targets.
- Target lists.
- Combat assessment products.

Scientific and Technical Intelligence

- Adversary weapon system capabilities and vulnerabilities.
- Medical capabilities and health services available in the JOA.
- Potential collateral effects from attacking weapons of mass destruction sites.

Counterintelligence

- Counterintelligence analyzes the threats posed by foreign intelligence and security services and the intelligence activities of non-state actors.

Estimative Intelligence

- Estimates provide forecasts on how a situation may develop and the implications for planning and executing military operations.

Identity Intelligence

- Biometric enabled watchlist.
- Document and media exploitation search results.
- Forensics studies.

Figure III-19. Intelligence Products

(1) The warning intelligence process analyzes and integrates operations and information to **assess the probability of hostile actions and provides sufficient warning to preempt, counter, or otherwise moderate their outcome.** The focus of

THREAT WARNING

Threat warning is closely associated with, but functionally distinct from, warning intelligence. Threat warning is the urgent communication and acknowledgment 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 acknowledgment of receipt of the alert. Although often 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.

Various Sources

warning intelligence varies at each echelon—from least specific at the strategic level, to most specific at the operational and tactical levels.

(2) Subordinate joint force warning intelligence relies on tip-offs from sources at all levels. An integrated, responsive intelligence architecture should be established to satisfy theater requirements. Warning IRs include:

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

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

(c) Enemy or adversary motivations, allegiance networks, possible triggering events, goals, and objectives.

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

(e) Information-related capabilities (IRCs) in the region.

(f) Activities related to preparations for malicious cyberspace activities by regional and international actors with interests in the area.

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

(h) 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 TIMs.

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

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 warning intelligence, in that both depend upon continuous monitoring of world events and specific activities in the GCC'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 CCMD JIOC 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 may 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 or enemy capabilities, probable intentions, and will to use military force, where, when, in what strength, and with what forces and weapons.

(b) The adversary's or enemy's operational plans.

(c) The adversary's or enemy's COGs.

(d) The adversary's or enemy's vulnerabilities.

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

(f) The impacts of 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 or enemy WMD assets, WMD-related facilities, and activities (e.g., movement of WMD materials, technology, and expertise). Location and characterization of TIMs resident in or transiting the area of interest. Potential dual-use

facilities (e.g., pharmaceutical plants, fertilizer-production facilities, nuclear reactors), including those with legitimate industrial or military functions.

(j) Adversary or enemy foreign intelligence and security activities.

(k) Adversary or enemy or potential adversary cyberspace capabilities.

(l) Adversary or enemy use of the information environment including cyberspace.

(m) Adversary or enemy counterspace capabilities.

(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. **GMI**

(1) GMI is tailored to specific subordinate joint force missions and includes information on the organization, operations, facilities, and capabilities of selected foreign military forces and pertinent information concerning the OE (political, economic, topographic, geodetic, demographic, and sociological aspects of foreign countries). Increasingly, GMI may become more concerned with non-traditional aspects of the OE to include cultural aspects and cyberspace capabilities. Specifically, GMI includes, but is not limited to, information on the items listed in Figure III-20.

(2) Fused joint intelligence assessments are:

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

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.** OB identifies force components and assesses the strengths, structures, and dispositions of the personnel and equipment of the opposing military and other forces, to include cyberspace capabilities and WMD.

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, evasion, resistance, and escape (personnel recovery, combat search and rescue, tactical recovery of aircraft and personnel, etc.)
- Government control

Figure III-20. General Military Intelligence Concerns

3. **Force Readiness and Mission.** Assesses the enemy's or adversary's readiness, as well as the doctrine it would follow, and the 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 required mission activity (i.e., industrial, transportation, fuel and military infrastructure, supply status, attrition rates, and the enemy's or adversary's morale) necessary to achieve objectives.

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

(b) **OE Assessment.** This type of assessment can provide indicators enhancing situational understanding of the full array of an adversary's capabilities and vulnerabilities, including warfighting sustainability. Examples are as follows:

1. **Communications System and Cyberspace Capabilities.** An assessment of the adversary's communications system (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, C2 system, and reconstitution capability.

3. **Energy.** A listing of power and fuel sources and their 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 operational area.

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. Sociocultural analysis (SCA) is particularly useful for understanding the cultural aspects of the population. SCA is used for analyzing things such as the society, social structure, culture, power and authority, and motivations of the various groups and individuals.

For additional information on SCA, see JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

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 activities.

7. **Space Systems.** An assessment of the adversary (red), allied (green), and neutral (grey) inherent and available space capabilities and infrastructure.

8. **Environmental Considerations.** An assessment of environmental factors that could affect military operations such as oil dumping/fires, industries producing/using TIMs and storage/waste sites, trash/waste dumping, and even space debris. This assessment should also include any cultural/historical/religious sites and even endangered species habitats. The CCMD JIOC is the primary source for the latest intelligence assessments of environmental considerations.

9. **Medical.** Availability and capability of foreign military and civilian medical facilities, equipment, and supplies, as well as professional medical personnel to treat casualties. Availability and capability of a PN to provide or assist with aeromedical evacuation. Infectious disease and environmental health risks, and scientific and technical (S&T) developments in biotechnology and biomedical subjects of military importance. An assessment of preventive medicine efforts and the medical environment in which multinational forces might operate is important to ensure the correct medicine,

clothing, and immunizations are available to the friendly forces and the local population. Particular attention should be paid to biological warfare threats because they may be difficult to detect. Due to the potential use of vectors, to include humans, and the limitations of automated biological warfare detection systems, medical intelligence and epidemiological reporting may provide the first indication of a biological attack.

10. **METOC.** Climatology and METOC conditions 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 atmospheric conditions, so assessing when METOC conditions are favorable for employment of these weapons can identify windows in which the adversary may conduct these types of operations. The joint METOC officer is the designated source for assessing climatological and METOC effects on friendly and adversary capabilities.

d. **Target Intelligence.** Target intelligence portrays and locates the components of a target or target complex, networks, and support infrastructure in support of joint targeting. Specific target intelligence products may include characterizing the target's physical or functional construct, significance, location, vulnerability, and other attributes. Intelligence forms the basis for target analysis and development, tracking and fixing information for moving or perishable targets, and weaponeering. It is critical that intelligence analyses supporting targeting remain consistent throughout the joint force and component commands. The COP and its supporting GCCS capability promote this unity of effort in providing a common set of data, information, and intelligence. Target development information for all target types is resident in MIDB.

For additional information on targeting intelligence, see Appendix D, "Target Intelligence."

e. **S&TI.** S&TI looks at foreign S&T 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 supports the research and development of friendly systems and countermeasures to known or postulated threats. Obtained through the foreign materiel exploitation, foreign materiel acquisition, and captured enemy equipment programs, the information is analyzed to preclude scientific and technological surprises and advantages by an adversary that could be detrimental to friendly personnel and operations.

f. **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 JIPOE.

g. **Estimative Intelligence.** Once a basic understanding of the threat and pertinent military-related subjects has been gained, it is necessary to try to view the situation

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, subversion, 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 among many other benefits. A commander can request and use CI information to protect personnel, equipment, and facilities.

Various Sources

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 CCMD JIOC are the primary sources of information in support of these estimates.

h. **I2**

(1) I2 combines the synchronized application of biometrics, forensics, and DOMEX capabilities with intelligence and identity management processes to establish identity, affiliations, and authorizations in order to deny anonymity to the adversary and protect US/PNs assets, facilities, and forces. I2 products result from the collection, analysis, exploitation, and management of identity attributes and associated technologies and processes. All-source analysts fuse identity attributes (biologic, biographical, behavioral, and reputation) and other information and intelligence associated with those attributes collected as a result of information collection tasks. I2 may include reporting from all intelligence disciplines, as well as collections from operational and law enforcement elements. I2 products include, but are not limited to, biometric intelligence analysis reports, behavioral influence analysis products, and I2 support packets. The JFC receives current identity information and derogatory reporting from all levels of the joint force, IC, interagency partners, and PNs concerning known or suspected terrorists, foreign fighters, foreign intelligence agents, criminals, opportunists, and persons of interest (POIs). This information is fused together to identify and assess threat networks, their capabilities and capacity, COGs, objectives and intent, and potential COAs in support of the commander's decision-making process. The I2 operations process results in discovery of true identities; links identities to events, locations, and networks; and reveals hostile intent. These outputs enable tasks, missions, and actions that span the range of military operations. Typical I2 assessments and products are:

(a) **Biometric-Enabled Watchlist (BEWL).** A list of POIs in which individuals are identified primarily by their biometrics sample instead of their name or other biographic information for screening, vetting, persistent targeting, or population management purposes. The BEWL can be customized depending on mission.

(b) **Biometric Intelligence Analysis Report.** An assessment focused on an individual resulting from the fusion of an individual's biometric data with all-source intelligence.

(c) **Tactical Visual Intelligence Product.** An all-source graphic product that fuses BEWL encounters, matches to IEDs, I2, network information, and other geospatial layers to highlight ideal geographic locations to conduct tactical biometrics collection operations and for use for targeting support.

(d) **Visual Intelligence Product.** Primarily graphic assessment that provides brief summaries of key persons and networks of interest. Generally produced for senior leaders and policy makers.

(e) **Networks and Identities Assessment.** Assessment that is an all-inclusive, long-term product that provides an in-depth profile of a key person and/or network of interest.

(f) **Quiktel.** Short assessments that address time-sensitive emerging, high-interest identity, network, and biometrics capability topics with limited available collection.

(g) **Biometric Rollup.** An analytic summary in response to tactical biometrics submissions. This product provides an analytic summary of the match results in response to the submissions, as well as any reporting found from a cursory name search against IC databases. The product is e-mailed to the submitter and subsequently posted to the case documents for the enrollment. The biometric rollup is designed to support analytic requirements in austere environments with limited bandwidth.

(h) **Behavioral Influences Analysis (BIA).** A baseline and descriptive analytic product that supports the development of the BIA individual behavioral profile and complements the BIA group behavioral profile and organizational behavioral profile. Individual biographies identify the significance of operational-level foreign air, space, and missile forces leadership, commanders, and key personnel, as well as critical individual roles and responsibilities. IO planners and US military or diplomatic delegations are the primary audience for this product.

1. **BIA Individual Behavioral Profile.** An in-depth analysis of a specific operational-level foreign air, ground, naval, space, or missile commander or key unit member focused on assessing command or unit climate and individual decision-making calculus. This product relies heavily on a sophisticated remote profiling methodology and is intended for IO planners.

2. **BIA Group Behavioral Profile.** An in-depth analysis of specific groups within operational-level foreign air, ground, naval, space, or missile forces focused on assessing group traits, behavioral influences, and potential vulnerabilities within and between groups. Though this product has many applicable audiences, it is written with IO planners in mind.

3. **BIA Organizational Behavioral Profile.** An in-depth analysis of operational-level foreign air, space, or missile units and organizations focused on assessing organizational behavior and influences on leadership and decision making. This product relies heavily on an organizational psychology-based methodology and is intended for IO planners.

(i) **Identity Intelligence Support Packet (I2SP), Pre-Operational.** A tailored, multi-intelligence, technical exploitation in support of DOD requirements and find, fix, finish, exploit, analyze, and disseminate (F3EAD) focusing on I2. Location-based analysis to provide full-spectrum, all-source analysis focused on a defined location in support of JIPOE and provide nontraditional views of targets or identify new targets and links through I2.

(j) **I2SP, Post-Operational.** A tailored, multi-intelligence, technical exploitation in support of DOD requirements and F3EAD focusing on I2. The I2SP provides tailored multi-intelligence technical exploitation in support of F3EAD and I2. The products are sent to the requestor and shared via collaboration tools. The products are typically completed within two weeks of the request, but can be produced more quickly if required.

(k) **POI Packets.** POI packets provide I2 analytic support to the initial and recurrent vetting of foreign personnel working with forward deployed military and/or USG personnel. POI packets provide tailored summaries of significant derogatory information on individual POIs, combining biometric, DOMEX, and screening information in an easily briefed format.

(2) BEI is derived from the collection, processing, and exploitation of biometrics signatures; the contextual data associated with those signatures; and other available information that answers a commander's or other decision maker's information needs concerning persons, networks, or populations of interest. BEI supports the development of I2 by biometrically baselining and characterizing the identity of an individual encountered in the OE so that it can be referenced and used to inform decision making across time and geography and in all future phases of the operation.

(3) FEI is derived from the collection, scientific analysis, and exploitation of materials, weapons, equipment, output signals, and debris that link persons, places, and events to produce tactical and strategic intelligence in support of the JFC and national decision makers. FEI includes, but is not limited to, the following scientific areas: deoxyribonucleic acid, CBRN analysis, chemistry, metallurgy, firearms and tool marks, fingerprint analysis (record and latent prints), facial and voice recognition, image

analysis, video forensics, captured documents, and trace material analysis. FEI supports the characterization and tracking of individual actors encountered in the OE.

(4) DOMEX is the processes, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under the USG's physical control. It includes all digital media capable of storing fixed information, to include computer storage material and cell phones. Captured documents and media, when processed and exploited, may provide valuable information such as enemy plans, intentions, locations, capabilities, and status. DOMEX may be conducted by any intelligence personnel with appropriate technical exploitation and language support.

For more information on DOMEX see Appendix C, "Document and Media Exploitation."

27. Support to Operational Commanders

a. CCMD, Service, and DOD agency production centers 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 CCMD J-2s (see Figure III-21) include:

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

(2) To coordinate with JIOC intelligence planners to develop a PRMx, if necessary, to include in annex B for CCMD campaign plans and level 3, 3T, and 4

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 MOD [Ministry of Defense] and various communications nodes. In addition to blueprints 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**

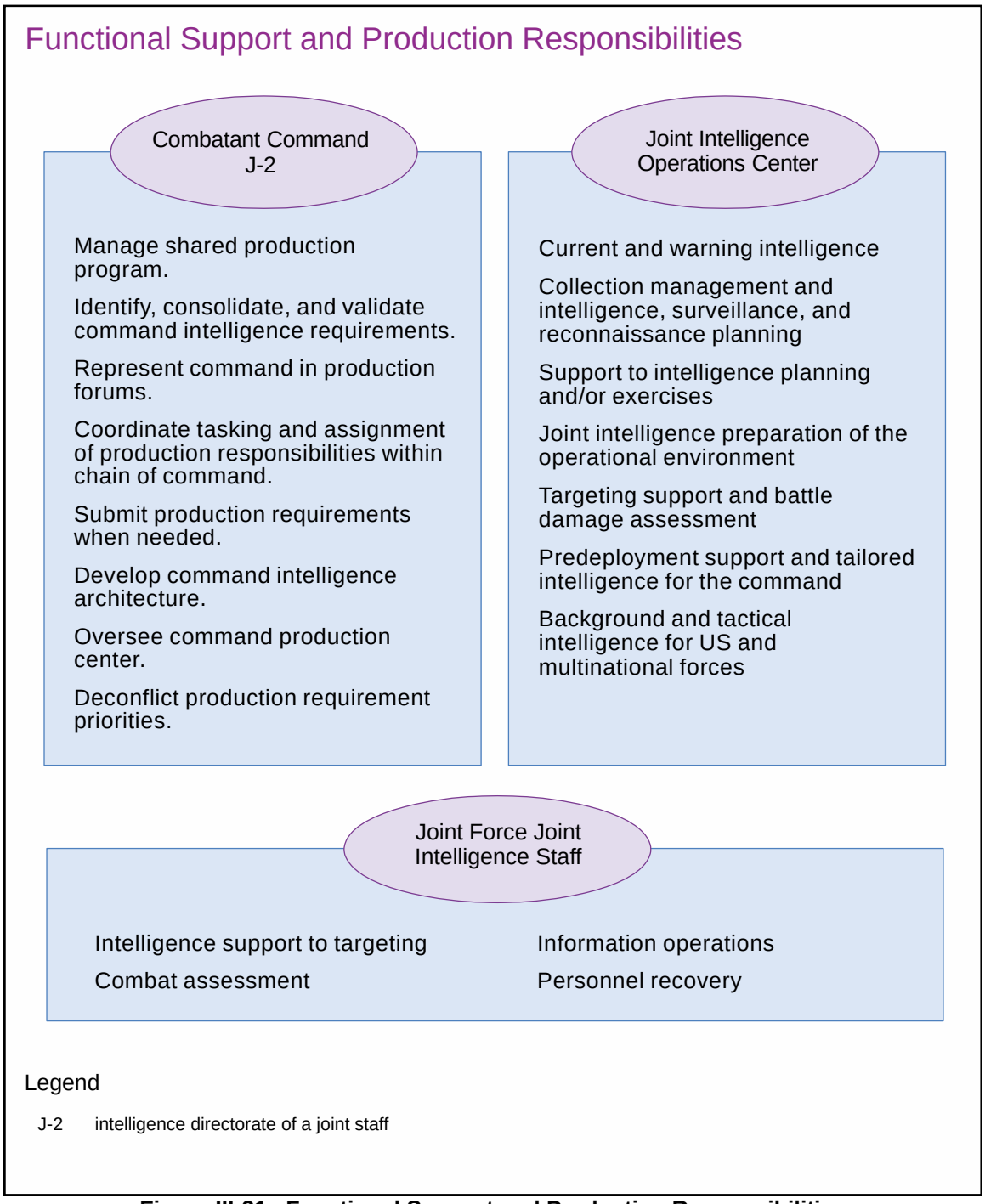


Figure III-21. Functional Support and Production Responsibilities

contingency plans and to develop the PRMx and analysis and production capability assessments in annex A for an NISP, as appropriate, on behalf of the CCMD J-2.

(3) To coordinate with CCMD JIOC intelligence planners to validate and consolidate command IRs for which intelligence production may be satisfied by maintenance and entry of data in command automated databases.

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

(5) To coordinate the tasking and assignment of production responsibilities to the production center within the command's chain of command. For areas beyond the CCMD JIOC capabilities, coordinate with the CCMD JIOC intelligence planners in the IP team(s) to produce J-2 staff estimates that inform the CCMD J-2 regarding the need for analysis and production intelligence federation support.

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

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

(8) To deconflict PR priorities.

b. **The CCMD's intelligence analysis and production is performed by its JIOC.** JIOCs are the cornerstones for fulfilling the IRs of CCDRs and their subordinate commanders. The JIOCs provide tailored, finished intelligence products to support CCDR and senior staff decision making regarding joint planning and operational assessments. Production-related responsibilities of the JIOC include analysis and production of the following:

(1) Current and/or warning intelligence for forces deployed in a GCC's AOR.

(2) Support to IP through planning and direction coordination with the CCMD JIOC intelligence planners.

(3) ISR planning in collaboration with CCMD J-3 COM personnel.

(4) JIPOE in support of joint planning and ongoing operations.

(5) In close coordination with CCMD, JIOC intelligence planners support target intelligence PRs, such as supporting development of target materials (TM), target analysis, and maintaining no-strike lists in appendix 4 (Targeting) to annex B (Intelligence) as required.

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

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

(8) 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.** JFCs may utilize a joint targeting

coordination board (composed of senior JIOC targeting element and J-3 fires element representatives) battle rhythm event to plan, execute, and assess joint fires operations at all echelons of assigned and direct support joint fires capabilities. The joint force J-2 is responsible for target intelligence. Target intelligence utilizes target systems analysis to provide the foundation for target mensuration, development, weaponeering, strike lists management, and collateral damage estimation (CDE).

A detailed description of joint procedures for intelligence support to targeting is found in JP 3-60, Joint Targeting.

d. **Combat assessment (CA) is the determination of the overall effectiveness of force employment during military operations.** CA is composed of three related elements: BDA, munitions effectiveness assessment (MEA), and reattack recommendation (RR). Intelligence production support for CA includes detailed assessments of any physical and/or functional damage to the enemy's target systems and combat capability, analysis of collateral damage, estimative weapon effectiveness, and targeting recommendations for future operations. The J-3, with input from component commanders and the J-2, has primary responsibility for CA. The J-2 has the responsibility to accumulate, consolidate, and report information regarding battle damage inflicted on the enemy as a result of combat operations. Timely and accurate BDA facilitates current and future operations. 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 3-60, Joint Targeting.

e. **IOII.** IOII is a vital military capability that supports IO. The utilization of IOII greatly facilitates understanding the interrelationship between the physical, informational, and cognitive dimensions of the information environment as a part of the OE. Resources include the information itself and the materials and systems employed to collect, analyze, apply, disseminate, and display information and produce information-related products such as reports, orders, and leaflets. Intelligence uses a variety of tools to assess the OE, thereby providing insight into a threat assessment. Due to the long lead time needed to establish information baseline characterizations, provide timely intelligence during IO planning and execution efforts, and properly assess effects in the information environment, intelligence planners and collection managers must be intimately involved in the planning process. DIA/NSA/CIA/NGA, Service intelligence and IO centers, and the national S&TI centers provide technical, analytical, and database information to the CCMDs in a variety of recurring and ad hoc documents and reports to support IO.

28. 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 responsible or collaborative.**

(1) **Responsible production centers produce the bulk of finished intelligence products.** A center designated as responsible is the authoritative source within the DIAP 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 DIAP 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 are to:

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

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

(c) Assume lead or contributing production center responsibilities for validated PRs.

(d) Request collection for any essential information gaps.

(e) Complete original research on the topic.

(f) Produce assigned categories in shared national-level databases (such as MIDB) within the topic and/or geographical area.

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

b. **The CCMD J-2 identifies and validates command IRs.** The command's production center (e.g., JIOC) schedules and accomplishes production activities, focusing on producing tailored, finished intelligence in support of mission planning and execution.

c. **At the subordinate joint force level, production focuses on the fusion of all-source intelligence from components, the CCMD JIOC, and national sources to support the joint force mission and operations.** The CCMD JIOC 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.

d. **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 CCMD 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."

29. Request Management

Customers communicate requirements to their supporting intelligence office at an existing military element, 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, TM, and hard copy 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 DIAP procedures for registration and assignment of RFIs and subsequent tracking of the RFI.

a. 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 supporting intelligence center (SIC) at the next level in the Service, CCMD, or DIA chain. **At the joint force command or Service component, the next level SIC is resident at the CCMD JIOC. DIA/DI, each Service, and each CCMD has a SIC to process and validate the RFIs submitted by their organizations' supporting intelligence offices.** The CCMD SIC normally accepts RFIs via e-mail or other informal means. However, the SIC should input the RFI into COLISEUM to initiate IC production. The validation process may 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).

b. Upon validation, the SIC 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 SIC 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, who is an element of DIA/DI.

c. 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 DIAP 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.

d. 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 should produce and citing a final response date. Copies of the response are sent simultaneously to the assigning SICs, the collaborating production centers, and the defense intelligence production functional manager.

30. Prioritizing Requirements

a. **All requirements should 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 should be in a format that the customer can understand and apply.

b. **The joint force J-2 is the office of primary responsibility for all IRs 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 available collection assets. If internally generated requirements cannot be satisfied by available joint force assets, the joint force J-2 should validate and prioritize these requirements and submit them as RFIs to the CCMD JIOC. This includes production and/or collection requirements that can be satisfied only by CCMD resources or by national agencies. If a CCMD JIOC cannot satisfy these RFIs, it should forward them directly to DIA or the DIAP responsible organization 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

31. Overview

The timely dissemination of critical information and finished intelligence to appropriate consumers is paramount to attaining and maintaining information superiority. **Intelligence should 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 mission application. GCCS 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 should 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. When a joint force J-2 is supported by national agencies,

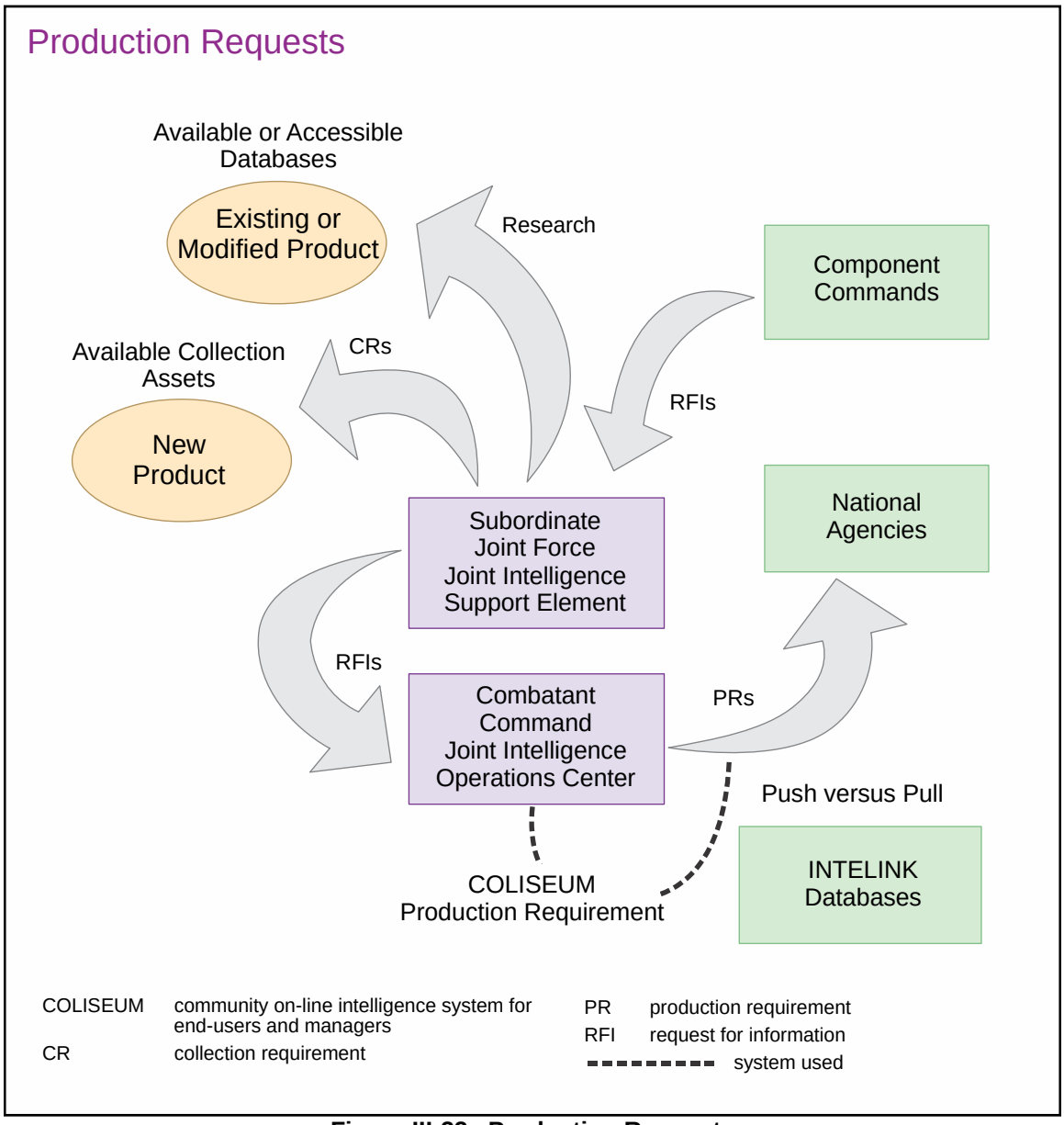


Figure III-22. Production Requests

RFIs are routed to the agency representatives for immediate action, in addition to the NJOIC. The national agency and NJOIC personnel deconflict RFIs. The joint force J-2 or CCMD JIOC maintain the responsibility to enter the RFIs into COLISEUM.

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 that satisfies standing information requirements by a subordinate unit; or specially prepared studies requested in advance by the subordinate joint force J-2. The "pull" concept involves direct electronic access to databases, intelligence files, or other

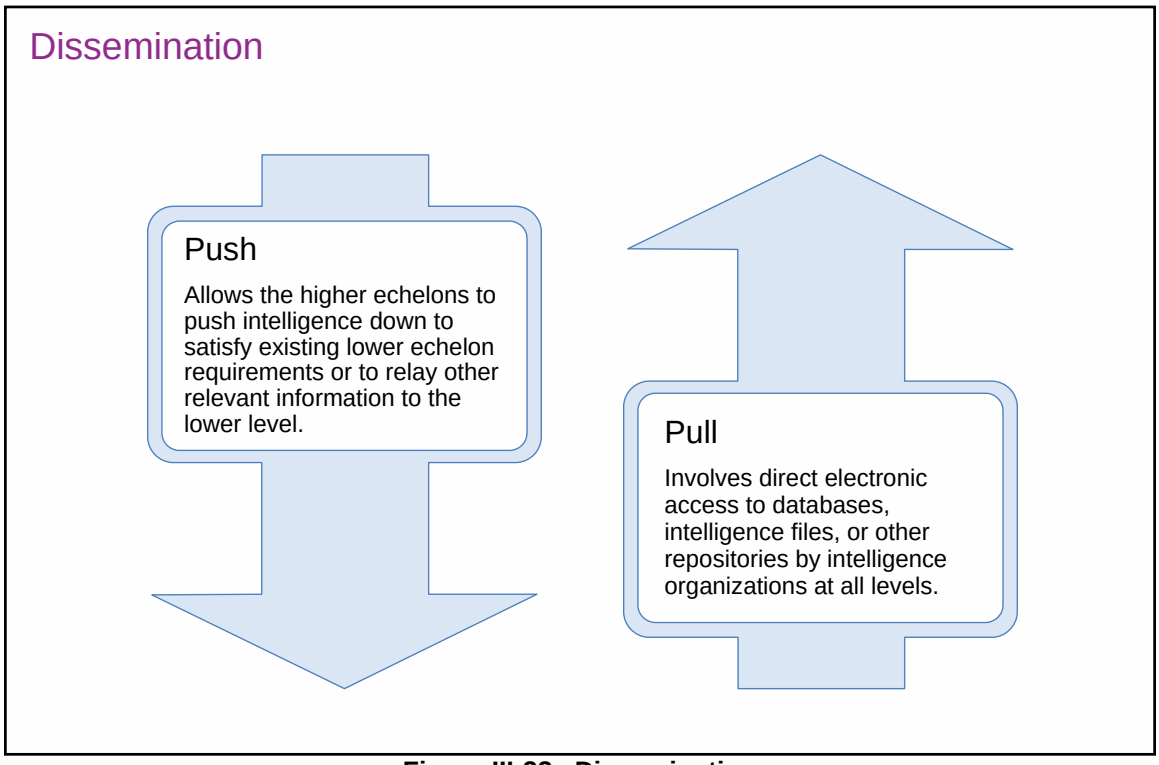


Figure III-23. Dissemination

repositories by intelligence organizations at all levels. An increasing number of intelligence "pull" products are available on Intelink or Intelink-S (collateral version), STONEGHOST (FIVE-EYES version of Intelink), Intelink-P (Policynet), and other national and theater file servers. One means of improving the pull method across the IC is establishment of the Library of National Intelligence. The Library of National Intelligence has several million documents and includes disseminated analytic reports from the CIA, DIA, NGA, NSA/CSS, USCG ICC, CIA's Open Source Center, Service intelligence centers, and others. The "pull" method is far quicker and more streamlined 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 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 a collection source to those friendly assets most at risk. Similarly, the utilization of collaborative tools and related capability of secure Internet relay chat enables the collective "pull" of threat warning information by all subscribers.

c. The J-2 should be involved with the other staff elements to ensure the logistic and communications infrastructures are capable of supporting intelligence operations and dissemination. Special dissemination planning considerations may be required when assets and infrastructure are austere and LOCs are 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 CCMD's DPM, should ensure appropriate mailing addresses, Organizational Messaging Service addresses and routing indicators, and special security office security accreditation are requested and established for those units. This administrative information may be communicated to and validated by the command DPM, who provides the information to DIA and other supporting national agencies. Further, the subordinate joint force J-2 should coordinate communications requirements with the J-6 during the planning phase of the operation.

32. Dissemination Methods

a. **Digital Dissemination**

(1) **Digital 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 hard copy 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 and intelligence systems such as the JWICS, SIPRNET, JDISS, NIPRNET, GCCS, Intelink and/or Intelink-S, and IBS are being integrated within the DODIN 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 IIRs and imagery, are also being posted to servers (e.g., Intelink, Intelink-S, NIPRNET [unclassified only]) for access by the CCMDs and subordinate joint forces. Other digital products include messages and intelligence databases maintained by national-level agencies or theater JIOCs.

(4) Media for the dissemination of electronic documents may include CD-ROM and DVD, depending on the requirements of the end user. For example, JIOCs 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

"Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space."

Sustaining US Global Leadership: Priorities for 21st Century Defense

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 electronic document should in turn be placed on the dissemination server for requester pull or electronic push.

(6) **The Services and CCMDs are integrating digital 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. They are designed to provide commanders with timely intelligence information derived from national, commercial, DOD, and combined force intelligence collection nodes via a variety of point-to-point, broadcast, and Web-based communications networks.

b. **Hard Copy Dissemination. The capability to deliver intelligence by fax, message, or courier in hard copy still remains a requirement in many situations.** The use of hard copy dissemination via fax messaging may be necessary during multinational operations as US intelligence equipment and system architectures are often not compatible with multinational systems or at the same security level. Additionally, some products, such as maps, are often available only in hard copy when large quantities are required.

(1) CCMDs manage the movement of hard copy intelligence to deployed subordinate joint forces in coordination with the J-3, J-4, the DPM, and the dissemination manager. Past operations and communications limitations associated with transmitting large format and/or color products have validated the continuing requirement to ship some critical hard copy products to consumers. However, many Service elements are equipped with large format plotters with the ability to print from digital sources. The DPM should check for availability and coordinate access for intelligence personnel.

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

33. Integration of Intelligence and Operations

a. 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 planning. The primary vehicle for integrating intelligence and operations is the COP. Intelligence should 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 OE.

b. 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 SecDef policy decisions to joint force 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 digitized raster graphics (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 IBS ELINT feeds from orbiting satellites and other passive ELINT sensors is automatically plotted on COP graphic displays.

SECTION F. EVALUATION AND FEEDBACK

34. Overview

All intelligence operations are interrelated, and the success or failure of one operation may impact the rest of the intelligence process. **It is imperative that intelligence personnel and consumers at all levels honestly evaluate and provide timely feedback throughout the intelligence process on how well the various intelligence operations perform to meet the commander's IRs.** 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 should not be considered satisfied and, time permitting, the requirement should be extended and/or retasked for collection or production. Concurrently, remedial action should be immediately initiated to identify the reasons why the intelligence process failed to satisfy the requirement and to ensure that such failure is not repeated.

35. Evaluation

All operations in the intelligence process are interrelated and should 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 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 intelligence excellence. To achieve the highest standards of excellence, intelligence products must be anticipatory, timely, accurate, usable, complete, relevant, objective, and available. 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 intelligence excellence, see JP 2-0, Joint Intelligence.

36. 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 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

APPENDIX A
JOINT FORCE INTELLIGENCE DIRECTORATE QUICK REACTION CHECKLIST

1. Overview

This checklist can assist a CCMD or 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 and military operations required, many of these variables may or may not apply. Other considerations not listed may also become factors.

2. Conduct Intelligence Planning

a. Provide intelligence support to planning. In many cases, an OPLAN or CONPLAN may already exist and require modification, but often a crisis is unanticipated and crisis action plans are developed in the days or months before military action. The following are steps toward effective intelligence support to planning.

(1) Direct a detailed JIPOE effort and notify command planners immediately of any changes in the situation.

See JP 2-01.3, Joint Intelligence Preparation of the Operational Environment, *for more information.*

(2) Coordinate with the command J-3/J-5 to develop the **commander's estimate.** Report major capability limiting factors (shortfalls) in any area for possible inclusion in the commander's estimate.

See JP 5-0, Joint Planning, *and CJCSM 3130.03,* Adaptive Planning and Execution (APEX) Planning Formats and Guidance, *for more information on the commander's estimate.*

(3) Prepare annex B to the commander's operations plan or concept plan, as required (refer to *CJCSM 3130 Series*). Identify in annex B all possible requirements for intelligence collection, production, processing, reporting, and/or dissemination assistance. State what assistance may be required, when it would normally be needed, and the duration of the requirement.

(4) Coordinate geospatial requirements with appendix 7 (GEOINT) to annex B (Intelligence), to the commander's operation or concept plan, as required.

(5) Coordinate with the Joint Staff J-2 Intelligence Planning Functional Manager to develop a NISP, if required (see CJCSM 3314.01, *Intelligence Planning*).

b. Prepare commander's **PIRs.** Produce an ISR CONOPS in coordination with the joint force J-3. Disseminate general collection priorities and requirements for subordinate joint force support and coordinate requirements with the subordinate J-2.

Coordinate with the Joint Staff J-2 to notify them of impending national IRs and to determine the availability of ISR resources.

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

(2) Coordinate with DIA for MASINT support or augmentation.

(3) Coordinate with the CCMD J-2X for CI and HUMINT support and augmentation requirements and submit a request for forces (RFF) through the command J-3.

(4) Coordinate with the command NSA/CSS representative to obtain required SIGINT support.

(5) Coordinate with NGA for GEOINT support.

(6) 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** should be coordinated with and processed through J-3 operations channels IAW DODD S-5210.36, *(U) Provision of DOD Sensitive Support to DOD Components and Other Departments and Agencies of the US Government.* All intelligence and other USG departments and agencies affected by or involved with sensitive support should also be kept informed.

c. **Establish effective external liaison relationships** with required national and DOD intelligence elements, interagency partners, and multinational entities.

(1) Coordinate with USSTRATCOM and Joint Functional Component Command for Space for space support. The designated space coordinating authority should ensure space support is provided to the commander. The space coordinating authority should reach back to the Joint Space Operations Center for any additional space support requirements.

(2) Coordinate through USCYBERCOM, as appropriate, for augmentation support to CO and planning.

(3) Coordinate with the Joint Information Operations Warfare Center through the Joint Staff for augmentation support to IO, OPSEC, and MILDEC.

(4) Request liaison support from interagency or multinational partners as appropriate to the operation.

(5) Coordinate with USSTRATCOM and the Joint Electronic Warfare Center for joint electromagnetic spectrum operations expertise.

(6) Coordinate with USSTRATCOM and the Joint Navigation Warfare Center for navigation warfare expertise.

(7) Coordinate with USSTRATCOM and the Joint Warfare Analysis Center for precision-targeting for selected networks and nodes expertise.

d. Determine intelligence collection and associated PED requirements and coordinate with the Joint Staff for allocation recommendations. Determine intelligence unit and personnel capabilities requirements and coordinate with DIA for allocation recommendation.

(1) Coordinate with NJOIC for intelligence augmentation, federation, or national agency 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.

(2) If required, request 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.

(3) Request assessments on disease threats, environmental and industrial health hazards, and foreign military and civilian health care capabilities from DIA's National Center for Medical Intelligence.

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

(1) 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.

(2) Coordinate a joint restricted frequency list with the command J-2, J-6, and NSA/CSS.

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

(4) Establish new Organizational Messaging Service addressee lists for receiving and sending pertinent subordinate joint force J-2 message traffic.

f. Consult with the Joint Staff J-2 on the status of possible multinational actions and associated intelligence support requirements.

(1) Identify, in coordination with the J-3 and J-4, requirements and/or requests from foreign countries for assistance or information.

(2) Establish POCs with multinational forces. Determine if any special language or translation requirements exist which may necessitate linguist augmentation. Inform the command J-2 of anticipated augmentation requirements with specific language skills. The J-2 should include specific language skills requirements in the command's RFF, the joint manning document, or the annual collection requirements submission.

(3) Begin planning to establish a multinational intelligence architecture, using CENTRIXS capabilities as a model.

(4) Coordinate requests for foreign disclosure and/or release issues with DIA and NGA, as appropriate. Request release approval from ODNI through DIA, and request a forward deployed FDO through the global force management (GFM) processes. Obtain waivers for release of appropriate levels of intelligence to multinational partners if required.

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

3. Establish Missions and/or Tasks

a. As required, the CCMD 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 CCMD J-2 and begin organizing, equipping, and preparing for the impending mission. CJCSI 1301.01, *Joint Individual Augmentation Procedures,* prescribes the guidance for requesting joint individual augmentation. The CCDR validates the joint augmentation personnel requirements in a joint manning document and the requirements are filled either by a Service component or through the joint force provider. Reserve Component forces should be included in sustainment plans for long-term joint force requirements.

(1) Intelligence responsibilities should be clearly delineated among subordinate joint force, CCMD, and national levels. Determine whether any subordinate joint force units (SOF in particular) require intelligence support from the CCMD or national level that the theater JIOC cannot provide.

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

(3) 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.

b. 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.

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

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

e. Verify all intelligence personnel and equipment are listed in the appropriate priority on the time-phased force and deployment list.

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

(1) Joint reconnaissance operations (J-3).

(2) IO (J-3).

(a) The IO staff includes IO planners and a complement of IRC planners and specialists to facilitate seamless integration of IRCs to support the JFC's CONOPS.

(b) IRC specialists can include, but are not limited to, personnel from the joint electromagnetic spectrum operations, CO, military information support operations, civil-military operations, deception cells, intelligence, and public affairs communities.

(3) Counterproliferation (J-3).

(4) CI (J-2).

(5) Personnel recovery (J-3).

(6) Counterterrorism (J-3).

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

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

(9) Interrogation operations and exploitation of captured documents and equipment (J-2/J-3/J-4).

(10) Debriefing operations (J-2/J-3).

(11) Transportation intelligence (US Transportation Command/J-2 and DIA for red force transportation assessments).

(12) Enemy employment of WMD (J-3 and/or CBRN officer). See JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*, for further detail.

(13) Target intelligence production, to include target systems analysis, electronic target folder (ETF) production, target list management, and BDA.

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

(15) Civil-military operations (J-9).

(16) Barrier and mining operations (J-3).

(17) Language, regional expertise, and cultural awareness skills.

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

(19) GI&S officer.

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

4. Identify Support Needed

a. **Intelligence Services and 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 intelligence defense agency support (e.g., personnel augmentation, JWICS, DOMEX). If so, identify entities to be tasked and mix of skills and capabilities needed. Use RFF process for augmentation.

(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 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 CCDR's staff.

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

(4) Assume the operation for which the subordinate joint force was established should 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, regional/area expertise, CI and HUMINT collection, Service and intelligence defense agency expertise, communications, tactical or in-depth analysis, debriefing, DOMEX, and polygraph support.

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

c. **Logistics**

(1) In concert with the CCMD J-2 and the subordinate joint force J-2, J-3, and J-4, ensure transportation requirements for high-priority personnel and materiel are documented and prioritized. If this is an unforeseen contingency or crisis, there is normally not an existing time-phased force and deployment data for personnel and materiel, and the J-2 should assist the J-4 to ensure intelligence needs are documented and met.

(2) Ensure 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 CCMD GI&S staff of the GI&S support POC in the subordinate joint force.

(3) Identify subordinate joint staff GI&S requirements to the CCMD 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 CCMD GI&S staff: the production schedule; status of products and digital data required and date of first shipment; status of host-nation support for GI&S products, digital data, and capabilities; and status on disclosure and/or release of geospatial information to multinational forces.

(5) Verify and/or submit GI&S requirements detailed in appendix 7 (GEOINT) to annex B (Intelligence).

(6) Request supporting forces provide a GI&S distribution plan. Ensure CCMD 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 CCMD GI&S staff. Forward unit line number to the CCMD GI&S staff.

(9) Establish map depot inventory quantities to include reorder levels. Report results to the CCMD GI&S staff via Organizational Messaging Service, e-mail, or JDISS.

(10) Request that the CCMD 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 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 or open sources that could supplement the METOC database.

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

g. **DOMEX Support.** DOMEX support should 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.

5. Establish a Forward Joint Intelligence Operations Center or Joint Intelligence Support Element

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

See Chapter II, "Joint and National Intelligence Organizations, Responsibilities, and Procedures," for more information on JIOC/JISE.

b. Determine whether a JIOC or JISE is to be established. A JIOC should normally be larger than a JISE and include additional plans personnel, a robust intelligence mission management functionality with extensive liaison with JFC COM personnel and intelligence agencies, and an active red team. Considerations for establishing a JIOC or JISE include:

(1) Facility location and physical security requirements.

(2) JISE requirements:

(a) Collection management section.

(b) Intelligence analysis section.

(c) Target intelligence section.

(d) CI.

(e) Communications and information systems support.

(f) Electronic and hard copy product dissemination to components.

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

(3) JIOC requirements:

(a) Intelligence mission operations center.

1. Collections requirements and collections operations.

2. Warning intelligence.

3. JFC's J-3 liaison elements.

4. J-2X.

5. External liaison elements (joint targeting board, IO cell, collection management board, provisional reconstruction team, and civil-military operations center).

6. Interagency and multinational liaison elements.

(b) All-source analysis center.

1. HUMINT, SIGINT, GEOINT, MASINT, OSINT, and CI analysis.

2. Air, ground, maritime, IO, electromagnetic spectrum, cyberspace, space, and missile, and terrorism analysis.

3. Regional/cultural subject matter experts.

4. JIPOE production cell.

5. Collection management liaison.

(c) Intelligence plans center (joint OPLAN, annex B, and as required, NISP development and coordination).

(d) Red team.

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

6. Intelligence Collection Management

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

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

c. Identify available 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 IRs. Ensure collection requirements to cover such shortfalls are developed and forwarded through the CCMD JIOC to DIA for subsequent national resource tasking.

e. **Prepare an ISR CONOPS in collaboration with the command J-3** that fully integrates the capabilities of organic and nonorganic collection assets and resources and that maximizes the efficiency of the tasking and PED architecture. Forward ISR CONOPS to the Joint Staff J-2/J-3, with all RFFs and with all OPLANs.

f. Ensure collection activities are coordinated with DIA through the CCMD JIOC for subsequent national resource tasking.

g. **CI and HUMINT Collection**

(1) Determine the need for a subordinate J-2X to manage, coordinate, and deconflict HUMINT, CI, country team, and/or joint force unit operations.

(2) Determine the need for a joint interrogation and debriefing center (JIDC) to conduct joint interrogation operations, a JCMEC, and JDEC (see Appendix C, "Document and Media Exploitation") to satisfy subordinate joint force and CCMD PIRs. Request staffing through the RFF process, as required.

(3) Determine the need for and request further CI and HUMINT collection augmentation and support through RFF.

h. **GEOINT Collection**

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

(2) Make all imagery or image products available to the requestor. The requestor should be notified of product availability.

(3) Establish the need for and request further GEOINT collection augmentation and support from the Services or NGA/CSS.

(4) Initiate coordination with NGA as early as possible. Shortfalls in GEOINT products, data, and services may adversely impact planning and analysis and may hinder operations during execution.

For more information, see JP 2-03, Geospatial Intelligence in Joint Operations.

i. **SIGINT Collection**

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

7. Intelligence Production Management

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

(1) As needed, in concert with J-3 and theater JIOC**, tailor PIRs for the current situation**.

(2) Keep PIRs current and update periodically.

b. **Develop or acquire a complete intelligence assessment of the situation.**

(1) **Conduct a JIPOE effort** to support operational planning, including identification of enemy and adversary COGs and assisting in developing potential COAs. See JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment.*

(2) Periodically update situation assessment using ongoing JIPOE assessments.

(3) Submit periodic situation assessments to the commander and chain of command.

c. Ensure regional and threat assessments are current.

d. Ensure key friendly and neutral forces are identified and SCA is performed.

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

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

g. Closely track intelligence collection and PRs to completion.

8. Communications System Support (for Subordinate Joint Force Intelligence)

a. **Identify the common intelligence systems, programs, Web portals, collaboration tools, and processes** that may be utilized by the joint force to conduct intelligence operations. Ensure personnel are trained to operate these systems.

b. The joint force J-2 should establish and maintain regular dialogue with the CCMD J-2 and the Service component intelligence staff officers.

c. Request JCSE support/augmentation.

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

e. Know the capacity of communications paths serving the subordinate joint force, between the subordinate joint force and its components, and with multinational force units.

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

(2) **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 JIOC and national organizations.

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

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

h. Ensure communications lines have sufficient rate capacity or bandwidth.

i. If necessary, establish a tactical SCIF.

j. Identify communications security needs (devices, keying material) and determine availability.

k. Ensure all router tables are updated.

l. Ensure all Organizational Messaging Service addresses are updated, complete, and used.

m. Eliminate duplicate data being disseminated to the same users by different means.

n. Ensure information systems security measures are employed properly.

o. Determine reporting/production times and types of reports.

9. Multinational Interaction

a. **Establish liaison** between joint and multinational force intelligence organizations.

b. Ensure foreign disclosure procedures include write-for-release guidance to **expedite sanitization and sharing** of US-generated intelligence products with allies and multinational partners.

c. Ensure friendly objectives, intentions, and plans are fully communicated to appropriate intelligence organizations.

d. Ensure interoperability of communications 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.

Additional information on multinational operations may be found in JP 3-16, Multinational Operations.

10. Counterintelligence

a. In coordination with the J-3 and multinational intelligence and/or CI elements, develop and implement CI and counterterrorism plans.

b. The CICA, through the J-2-X, should recommend to the J-2, or JFC, appointment of the TFCICA or CI 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 CCMD CICAs 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 military CI collection 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, Counterintelligence and Human Intelligence in Joint Operations.

11. Security

a. Ensure facilities, 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
GLOBAL INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE MANAGEMENT

1. Introduction

a. CCDRs should develop a coherent, cohesive, and synchronized intelligence collection plan that links theater or functional campaign PIRs and its employed platforms. It should embrace joint (and even combined) sourcing. It should resist the oversimplified desire for the "persistent stare" with a single type of platform in a single domain and embrace the intricacies of matrixed and multi-intelligence capabilities throughout the OE.

b. As there will always be fiscal constraints and operational competition for intelligence collection resources, and requirements often exceed capabilities, a CCMD's planning staff should critically think through its intelligence collection requirements to ensure its most pressing needs are met without compromising a force provider's ability to sustain capacity for the global effort.

2. Intelligence, Surveillance, and Reconnaissance Planning

a. **Establishing Requirements.** Today's CCMD has many named operations, operational and contingency plans, or lines of effort (LOEs). Each has unique PIRs, and each mandates a unique approach (or approaches) to answering it. It is important that ISR planners take a systematic approach to ISR planning to ensure an efficient use of its collection platforms. Thus, a CCDR's ISR planning staff may prioritize its named operations/OPLANs/LOEs, identify PIRs, and link the PIRs to collection capability requirements.

(1) Prioritization is influenced by many factors, but three of the most significant are the CCDRs' theater campaign objectives, SecDef's prioritization of operations as prescribed by the Guidance for Employment of the Force (GEF) and the associated force allocation decision matrix (FADM), and national strategy prioritizations as espoused by the President or the NSC staff. Usually, these three priorities match, but there are situations where they do not; for example, one CCMD's objectives for security cooperation dovetails well with the SecDef prioritized campaign against organized transnational terrorist organizations, but are incongruous with NSC staff prioritizations.

(2) PIRs should be developed with enough specificity to be answered through discrete collection requirements which can be met through the use of intelligence disciplines.

(3) Collection planners link PIRs and collection requirements to existing intelligence disciplines and capabilities. Assuming the airborne capabilities are the gap filler to all the other capabilities within the OE based upon competition for airborne intelligence collection capabilities, the collection capabilities in the other aspects of the OE should be accounted for first. Only then can the airborne requirements—known as airborne ISR capabilities requirements—be identified. Airborne ISR capabilities

requirements are not doctrinally pure in definition but are defined in a manner to assist GFM planners in identifying the platform best suited for a particular ISR mission.

(4) Each desired airborne ISR capability requirement should be realistically defined in a manner and with sufficient fidelity to allow strategic ISR managers to allocate resources and assets to meet the requirement. Defined collection capabilities requirements are influenced by degree of desired persistence, desired periodicity, collection swath, prosecution timelines, and target development. Normally, each capability requirement is defined in hours per month. To ascertain that fidelity, CCMD ISR planners should apply a systematic process to ensure a coherent linkage of PIRs/collection requirements to airborne ISR capability requirements is made. To that end, the strategic ISR management enterprise Joint Staff J-3 and J-2 have collaboratively established a CCMD collection and ISR CONOPS template with associated guidance on its development.

b. **CCMD ISR CONOPS**

(1) A CCMD's ISR CONOPS is a powerful tool to synchronize a CCDR's IRs with collection capabilities to allow the efficient and effective employment of ISR resources and assets (with the associated PED systems) in support of missions conducted within a GCC's AOR. An annual ISR CONOPS should inform the GFM process on the collection requirements that remain unfilled after exhausting other available collection options, including ISR capabilities throughout the AOR and inclusive to organic/assigned forces, PNs, and interagency contributions.

(2) The ISR CONOPS is a requisite product that accompanies a CCMD's annual ISR requirements submission, as directed by SecDef's Global Force Management Implementation Guidance and associated GFM business rules and as specified by the current GFMAP planning cycle planning order. During the annual GFM planning cycle, the ISR management enterprise will issue guidance on developing the ISR CONOPS. This guidance directs that the following elements be addressed in the CONOPS development: assumptions, constraints, PIR diagnostics, collection capability requirements and operational risk, and PED requirements.

(a) **Assumptions.** A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the COA.

(b) **Constraints.** A requirement placed on the command by a higher command that dictates an action, thus restricting freedom of action.

(c) **PIR Diagnostic.** A graphical depiction of the relative utility of each type of intelligence discipline or collection method with the potential to collect against the EEIs associated with related PIRs and collection requirements.

(d) **Airborne ISR Capability Requirement.** CCMD's identification of the airborne ISR capability and capacity required to fulfill an anticipated collection

requirement after considering all other available collection capabilities to include ground-based and sea-based collectors; friendly units in vicinity of anticipated collection targets; expected national or multinational technical means of verification and reachback support; multinational, interagency, and organic collection capabilities already provided or anticipated; and applying CCMD operational constraints such as basing, target access, and airspace.

(e) **Operational Risk.** A subjective assessment of risk (measured as low, moderate, significant, or high) of not sourcing or partial sourcing. The subjectivity of this risk may be reduced by comparing the current collection capability requirement to what was sourced in the previous allocation cycle and then comparing the previous collection capability to measured operational gains or losses. For any risk assessment above moderate, the methodology, data, and justification used to support the CCMD's assessment should be provided to Joint Staff.

(f) **PED.** PED capability which may or may not be organic to a platform, system, Service, or CCMD. CCDR's ISR requirements should address specific PED requirements, especially the need for advanced finished products and/or constrained timelines. PED availability will be addressed in the platform force offering.

3. Global Force Management of Intelligence, Surveillance, and Reconnaissance

GFM is a process and set of procedures used to allocate ISR platforms to optimally source a CCMD's ISR requirements, whether it is an annual requirement or an emergent requirement (those not accounted for within the annual requirements). Annual requirements are submitted almost 18 months prior to the year of execution and are predicated on a command's ISR plan and named operations as codified in its ISR CONOPS. Global changes could impact the time period leading up to or during the execution of the annual allocation may result in emergent requirements. Thus, ISR allocation is a dynamic and continuous process.

a. Annual Allocation

(1) The annual allocation process is composed of four steps: identification of CCMD ISR requirements, identification of force provider platform/PED availability, the allocation "build," and sourcing adjudication.

(2) CCMD J-2 and J-3 ISR planners collaboratively generate airborne ISR capability requirements for each of its LOEs and submit them to the Joint Staff J-3 for review and validation via the Joint Capabilities Requirements Manager (JCRM) system. (Note that specific ISR platforms are not directly requested because most ISR platforms can source various collection capabilities, have unique basing requirements, and may compete for shared PED resources. Generating capability requirements allows the allocation/sourcing enterprise more flexibility in generating an integrated global allocation plan.) Each capability requirement should be discrete enough to be assigned its own force tracking number, used for ease of requirement management. The Joint Staff should validate the requirement before it is advanced for sourcing. It is essential the

JCRM capability requirements match those identified in the ISR CONOPS. Following force tracking number validation, the joint force providers—Services and CCMDs with assigned forces—are queried for their "force offering," that is, those forces available for deployment. With the force offerings come unique restraints and caveats, such as basing, PED, and operational, manpower, and funding limitations.

(3) The sourcing recommendation developed and managed by the Joint Staff aligns the CCMD requirements with available force capacity. Sourcing solutions are iteratively staffed through all force providers and CCMDs, ensuring feasibility and eliminating sources of contention when possible. The goal is to provide a near 100% sourcing solution acceptable to the CCMDs and Services.

(4) Finally, the best solution is presented at a Joint Staff-led Global Force Management Board for adjudication. Any remaining contentious sourcing issues are either reconciled or left unresolved. If reconciled, no further actions are required, other than CJCS recommendation and SecDef approval. If unresolved, two more senior forums are available for reconciliation. If still unresolved, the plan goes to the CJCS for recommendation before going to SecDef for final decision and ultimate approval.

b. **Emergent Allocation**

(1) The annual allocation plan should not be considered inflexible. Ongoing operations evolve, while new crises appear. Often, a CCMD will need to modify its ISR plan. The emergent allocation process is also four stages: A CCMD RFF or a request for sourcing (RFS), a sourcing drill, Joint Staff adjudication, and an approved SecDef order authorizing the transfer of forces.

(2) When confronted with situational change that renders the current ISR allocation inadequate, a CCMD may levy an RFF or an RFS to the Joint Staff. The distinction between the RFF and RFS is subtle, but important. An RFF is designed to source a new requirement while an RFS is designed to modify an existing requirement. Both require specific information pertaining to the situational change (since previously adjudicated/sourced) requiring new or additional capacity, the capability required, and the inclusive dates. The RFF/RFS should be validated by the Joint Staff prior to sourcing.

(3) Once released for sourcing, the ISR Joint Force Coordinator (Joint Staff) will determine the best platform/system to satisfy the requirement and subsequently query the force provider for the capacity to support. If capacity exists, then any limitations should be identified as a sourcing constraint. If capacity does not exist, then a reallocation schema should be looked at, considering changing OPCON of existing allocation from one CCMD to another. When considering reallocation, considerations include the FADM comparison of the gaining and losing CCMDs.

(4) All sourcing COAs, whether they are allocation of new capacity, reallocation of existing capacity, or even recommendations to close the request without sourcing, should be iteratively staffed through the Joint Staff, addressing the concerns of all CCMDs and Services with equities. Ultimately, the sourcing COAs—with a primary

recommendation—are advanced through the CJCS and SecDef for adjudication and approval.

(5) The approved COA is published in SecDef's orders book. Corresponding orders lines are pushed to the Services and affected CCMDs for execution. Internal deployment orders are published, ordering Service forces forward or transferring OPCON between CCMDs.

4. Processing, Exploitation, and Dissemination Management

a. **PED** is a key component of ISR. PED and collection components (sensors, assets) of ISR should be fully synchronized. PED capability encompasses the equipment that receives, processes, relays, and stores or transmits collected data; the communications systems architecture and associated bandwidth/throughput that moves collected data to an exploitation center; the exploitation center that receives processed data, turns it into a usable form, and disseminates information to customers; and the personnel that satisfy specific CCMD PED requirements. PED capabilities may also include remote or distributed sensor control and data link operations, depending on the force provider and the technical design and employment CONOPS of the specific ISR capability in question.

b. **PED Types.** Different PED constructs support global ISR.

(1) **PED enterprise** is a networked system-of-systems that includes architecture, manpower, and other resources to provide PED capability in support of global ISR requirements.

(2) **Crew-based PED** is provided onboard the collection platform or collection activity (e.g., RC-135, EP-3) and may be augmented by capacity in the larger global enterprise.

(3) **Deployed PED** capability is forward-deployed to support commanders and ISR assets that do not have access to reachback PED. It may be required due to a disconnected, interrupted, low bandwidth environment or lack of reachback capability on the collection platform. Deployed PED can support high-priority, time-sensitive requirements for conventional and SOF operations and includes, but is not limited to, quick reaction capabilities and emergent ISR requirements where reachback PED infrastructure is lacking or does not exist.

(4) **Reachback PED** capability is outside of a theater at a location with robust communications architecture, enabling national to tactical multi-disciplined intelligence capability support to theater commanders at all levels. PED nodes can be enterprise capabilities or single exploitation units within a Service, CSA, or CCMD. Reachback PED nodes can also be either inside or outside the US and are not considered as part of the overall military footprint in a given AOR and can include distributed PED, federated PED, and reach in PED.

(a) **Distributed PED** is the capability of one or more PED nodes within an enterprise that uses a centralized control and decentralized execution structure to support global ISR PED requirements. The centralized control element retains the reporting and mission management responsibilities. That is, all PED nodes report back through the centralized control element.

(b) **Federated PED** is capability leveraging an enterprise of interconnected PED elements within or among Services, CCMDs, CSAs, or multinational partners to support AOR-specific ISR requirements. Each contributing PED node is responsible for reporting any mission requirements for their given target set.

(c) **Reach in PED** is a node pulling data from and pushing products to forward-based ISR assets or data storage.

(5) **Service-retained (formerly organic) PED** supports Service-tasked ISR and is usually deployed forward. Service-retained PED is divided into offered and not offered PED capabilities.

(a) **Service-retained PED–offered** is capability retained by a Service that is offered by that Service to support theater ISR assets ordered to a CCMD in the GFMAP.

(b) **Service-retained PED–not offered** is capability retained by a Service that is not offered to support theater ISR assets and is instead retained by the Service to support its assets tasked against Service requirements, usually corps and below.

c. **PED Management**

(1) PED systems are managed in the context of their relationship with ISR capabilities. The processes for addressing annual, emergent, and time-urgent PED requirements; how sourcing recommendations are made; and how gaps and shortfalls are identified and addressed are a part of PED systems management.

(2) The challenge of high demand for the limited capacity of the unmanned aircraft systems requires deconfliction of operational, communications, and PED resources.

(3) USSTRATCOM's Global Force Management of Processing, Exploitation, and Dissemination Resource Allocation CONOPS focuses on aligning ISR available PED capacity with theater-level airborne ISR assets via the GFM process.

d. **PED Awareness.** Effective planning should be based on accurate situational awareness of the OE. For the global PED mission, this OE can be understood through the allocation of PED forces. Situational awareness may enable focusing PED weight of effort in a manner best suited to optimize PED capacity and meet CCMD needs. Effective situational awareness of global PED operations may require visibility, transparency, and feedback, including close coordination with force providers and CCMDs to ensure synchronization of weight of effort with developing operations,

development of close working relationships with CSAs to enable a clear understanding of the PED capabilities and capacity that CSAs provide to support CCMDs, and close communication between PED force providers and their C2 centers.

e. **PED Prioritization.** Multiple contingency and crisis operations revealed the need to prioritize limited global PED capabilities among CCMDs. Unless overridden by the President or SecDef, the GEF/FADM may dictate how PED capabilities should be prioritized among CCMDs. Emergent requirements may require rearranging priorities as they arise. PED is a finite resource. Lack of transparency of PED capability and capacity within DOD hampers efficient and effective resource allocation.

5. Intelligence, Surveillance, and Reconnaissance Assessments

a. **Introduction**

(1) ISR assessments evaluate the performance of intelligence collection operations in order to improve collection effectiveness in meeting intelligence and operational requirements. Assessments drive a continual improvement process through all phases of the intelligence process by identifying actionable recommendations to influence the ISR strategy, as well as collection asset/resource allocation and employment. Continuous and timely assessment is crucial to monitor and measure progress toward mission accomplishment.

(2) The cornerstone of an ISR assessment is the intelligence problem being answered. To be effective, assessments should be purpose driven in order to determine the value of intelligence gain, the reasons why ISR activities were or were not successful in answering the intelligence problem, how well the intelligence problem was answered, and what actions need to be taken to address poor performance or limited effectiveness. Therefore, collection measures of performance (MOPs) and measures of effectiveness (MOEs) are the main components of a comprehensive ISR assessment.

(3) ISR assessments should evaluate performance and effectiveness.

(a) **Performance** represents a quantitative measure and answers two questions: whether the ISR capability performed within technical standards and whether the planned collection was accomplished. Evaluators should identify the root causes for performance below technical standards and for uncollected or unsatisfied collection.

(b) **Effectiveness** represents a qualitative measure and answers whether the collection that was accomplished satisfied the requirement. If it did not, the evaluators should assess the reasons.

b. **Assessments Inputs.** While the cornerstone of an ISR assessment is the intelligence problem being answered, assessments are supported in two ways: quantitative data and qualitative analysis.

(1) Quantitative data is meaningful, accurate data that describes or measures the quantity produced or accumulated regarding an intelligence problem and is used to

determine the accomplishment of the assigned task. For example, quantitative data may mean the number of targets collected during a mission or the number of reports generated by a PED node. Quantitative data is usually represented by numbers or metrics; in other words, something counted.

(2) Qualitative analysis is the process used to determine the content, quality, or relevance of ISR activities compared to meeting ISR mission objectives. Fundamentally, qualitative analysis answers the "so what?" question about the end result of ISR activities. Qualitative analysis begins with a set of defined ISR mission objectives directly related to answering the intelligence problem.

c. **Assessments Measures.** Assessments measures are the rulers by which performance, efficiency, and effectiveness are measured.

(1) MOPs are used to measure task accomplishment by evaluating if the ISR activities met a measurable standard. In other words, "Was the task performed within a certain standard?" MOPs give an indication of the extent of progress in execution of the plan. MOPs should demonstrate particular characteristics. They are tied to tasks and task assessment; therefore, they should be appropriate to the assigned task or set of related tasks. They should be measurable and are generally focused on the immediate results of tactical actions. They are designed to answer whether a task or related set of tasks was conducted or conducted successfully, whether it/they need to be conducted again, whether the tasked organizations are "doing things right."

(2) MOEs help determine how well the mission is being accomplished. While MOEs involve a component of subjective evaluation on the basis of objective data, MOEs should be based on observable and measurable indicators. Indicators provide the evidence that a certain condition exists or certain results have or have not been attained. Taken together, MOPs and MOEs help decision makers determine whether progress is being made in meeting IRs.

(3) If functions associated with ISR activities are not being performed well enough and the mission is not being accomplished, then the performance of functions should be improved. If functions are being performed well, but the mission is not being accomplished, then a decision is required about whether to wait to draw further conclusions as to mission effectiveness, change actions, raise MOP standards, or lower the expectations for MOEs.

(4) If the functions are not being performed well, but the mission is effective, then there is likely an error in the measure of either performance or effectiveness.

(5) The goal is to meet mission objectives. Assessing ISR activities using MOPs and MOEs should be documented and shared for the purpose of improving the delivery of meaningful and relevant intelligence to requestors.

d. **Types of Assessments.** There are two types of assessments.

(1) **Formative assessments** determine how well an ISR activity was performed and what can be done to improve the next mission. In other words, formative assessments are ongoing assessments that occur after each mission to fine tune requirements for the next mission. Formative assessments answer the following questions.

(a) Did the ISR capabilities perform within technical standards?

(b) What was the volume of requirements collected during the mission?

(c) Were mission objectives met?

(d) How did this mission contribute to answering the intelligence problem?

(e) Do the mission objectives need to be adjusted for the next mission?

(f) Is a different capability needed to meet mission objectives?

(g) If an objective was partially met, what is required for the objective to be fully met?

(h) Do I have the right mix of capabilities to meet mission objectives?

(i) Were there other capabilities with which to cross cue?

(j) What level and extent of interaction was there between intelligence problem owners, collectors, and PED nodes?

(k) What feedback was provided from the supported unit?

(2) **Summative assessments** summarize the overall contribution of ISR activities in meeting mission objectives and answering intelligence problems during a specified period. Summative assessments are accomplished at specified periods such as 30-, 60-, and 90-days for deployments of new capability being introduced into a theater of operations. They may also be accomplished at other intervals such as monthly, bimonthly, quarterly, and annually depending on commander's guidance and mission needs. For example, summative assessments are accomplished bimonthly to meet mission approval requests IAW CJCSI 3250.01, *(U) Policy Guidance for Intelligence, Surveillance, and Reconnaissance and Sensitive Reconnaissance Operations*, or they may be accomplished because of contentious issues related to the allocation of ISR capabilities between CCMDs. Summative assessments answer the following questions:

(a) Overall, how well were mission objectives met?

(b) How well did ISR activities answer intelligence problems?

(c) To what extent was the right mix of ISR capabilities employed?

(d) To what extent were ISR assets available to accomplish missions?

(e) Were there problems with platform or sensor performance?

(f) To what extent did PED support ISR activities?

(g) What volume of requirements was met?

(h) Were the outcomes expected by the command from ISR activities met during the period?

(i) What are recommended improvements for performance, efficiency, and effectiveness in accomplishing mission objectives?

(3) **Numerical Scoring.** The purpose of numerical scoring within ISR assessments is to compare performance over time and to determine if steps to improve performance are moving in a positive or negative direction. Some approaches to scoring include:

(a) **Objectives-Based Scoring.** Scoring is based on an analytical assessment of whether ISR met objectives or not. Numerical scores are straightforward, such as

1. Objective not met = 0.

2. Objective partially met = 1.

3. Objective fully met = 2.

(b) **Assessments Scorecard.** An assessments scorecard allows a higher fidelity of scoring based on the extent to which mission objectives are met. Most scorecards are divided into MOPs and MOEs. Example scorecards are depicted in Figures B-1 and B-2.

(c) Once the numerical score is derived from observations of platform and sensor performance, it should be placed into context, such as how well the capability answered the intelligence problem. By scoring each phase of the intelligence process, specific areas of improvement can be identified and tracked. Figure B-3 is a graphical depiction of performance scoring of ISR in the context of the intelligence cycle.

e. **Mitigation Strategies**

(1) ISR assessments of performance, efficiency, and effectiveness help determine when mitigation strategies should be developed to overcome gaps and shortfalls. Developing a mitigation strategy involves:

(a) Identifying the root cause of poor ISR performance.

(b) Reviewing the intelligence problem to ensure it is properly stated and that it facilitates the development of clearly stated mission objectives.

Performance Assessments Scorecard Example

Performance Assessments Scorecard						
Measure of Performance	Not Assessed	Completely Ineffective	Mostly Ineffective	Somewhat Effective	Mostly Effective	Completely Effective
Performance: At what quantity level is this intelligence/ capability fulfilling tasking?	not applicable	Asset is performing at an unsatisfactory level or way below its technical specifications; meets less than 20% of collection hours as compared to tasked hours.	Asset is performing sub-par and is not meeting expected capabilities; meets between 20-39% of expected collection hours as compared to tasked hours.	Asset is performing adequately with only minor issues that hamper performance; meets between 40-59% of expected collection hours as compared to task hours.	Asset is performing at near optimal level; meets between 60-79% of expected collection hours as compared to task hours.	Asset is performing flawlessly; meets over 80% of expected collection hours as compared to task hours.
Numerical Score:	not applicable	0-19%	20-39%	40-59%	60-79%	80-100%

Figure B-1. Performance Assessments Scorecard Example

(c) Refining MOPs, MOEs, and MOE indicators based on the refined intelligence problem.

(d) Determining alternative means of collecting data in lieu of the capability that performed poorly.

(e) In the absence of clear indicators of activity or in the case of denial and deception, thinking about other pointers to activity. For example, if traditional indicators of a deployment are denied to us, then an alternative indicator of a deployment may be changes in resupply activity, predeployment training, predeployment leave periods, or posts in social media.

(f) Submitting requirements to collect nontraditional indicators.

(g) Identifying PED and analytical requirements associated with mitigation strategies.

(h) Gathering performance data to assess the mitigation strategies.

(i) Assessing whether the mitigation strategy is working.

f. **Determination.** The goal of ISR assessments is to determine the intelligence value gained from ISR activities. Assessments provide lessons learned that can improve ISR performance and avoid waste of resources, time, and PED capacity.

Effectiveness Assessments Scorecard Example

Effectiveness Assessments Scorecard						
Measure of Effectiveness	Not Assessed	Completely Ineffective	Mostly Ineffective	Somewhat Effective	Mostly Effective	Completely Effective
Capability: At what extent can this intelligence/ capability satisfy the specific mission objective?	not applicable	Asset has absolutely no or very limited ability to further the understanding of PIRs.	Asset has the ability to make modest progress toward satisfying mission objectives.	Asset has a moderate ability to further understanding of PIRs or make adequate progress toward satisfying mission objectives.	Asset has the ability to substantially further understanding of PIRs or satisfy mission objectives.	Asset has the ability to enable or facilitate the complete satisfaction of mission objectives.
Capacity: What is the capacity (quantity level of allocation/sourcing) of this intelligence/ capability to satisfy the mission objective?	not applicable	Wrong job for asset or the platform sensor is so under-resourced as to limit any further understanding of PIRs or progress toward satisfaction of mission objectives.	Platform and sensor limitations result in indirect understanding of PIRs or limit progress toward satisfying mission objectives.	Platform and sensor are sufficiently equipped and resourced in a manner that the asset can make adequate progress toward satisfying mission objectives.	Platform and sensor are equipped to substantially further understanding of PIRs or make significant progress toward satisfying mission objectives.	Platform and sensor are provided in quantities sufficient to answer PIRs or to completely satisfy mission objectives.
PED: To what extent can this intelligence/ capability be fully analyzed, exploited, and disseminated to satisfy the specific mission objective?	not applicable	Assets for processing, analysis, exploitation, and dissemination are unable or have very limited ability to increase the understanding of PIRs or to make progress toward satisfaction of mission objectives and the delivery of the required products to the requestor.	Assets for processing, analysis, exploitation, and dissemination are too limited or under-equipped to significantly contribute to increasing the understanding of PIRs or can make only modest progress toward satisfying mission objectives.	Assets for processing, analysis, exploitation, and dissemination are able to generate analysis products that further the understanding of PIRs or that make adequate progress toward satisfying mission objectives without too significant a delay.	Assets for processing, analysis, exploitation, and dissemination are able to substantially further the understanding of PIRs and can make fairly quick progress toward satisfying mission objectives.	Assets for processing, analysis, exploitation, and dissemination are fully available, engaged, and able to facilitate the complete satisfaction of mission objectives.
Performance: At what quality level is the intelligence/ capability delivering usable products to satisfy mission objectives?	not applicable	Asset performs at an unsatisfactory level or way below its advertised capabilities and has absolutely no ability to further the understanding of PIRs and makes no progress toward satisfaction of mission objectives.	Asset performance is weak, under-delivering with regard to known capabilities, minimally or indirectly furthers understanding of PIRs or only makes modest progress toward satisfying mission objectives.	Asset is making adequate progress toward further understanding of PIRs or satisfying mission objectives with only minor issues hampering performance.	Asset performs at or near optimal levels, making extensive gains in understanding PIRs or almost completely satisfying the mission objectives.	Asset performs flawlessly and permits complete understanding of PIRs, thus completely satisfying mission objectives.
Numerical Score:	not applicable	0	1	2	3	4

Legend

PED processing, exploitation, and dissemination

PIR priority intelligence requirement

Figure B-2. Effectiveness Assessments Scorecard Example

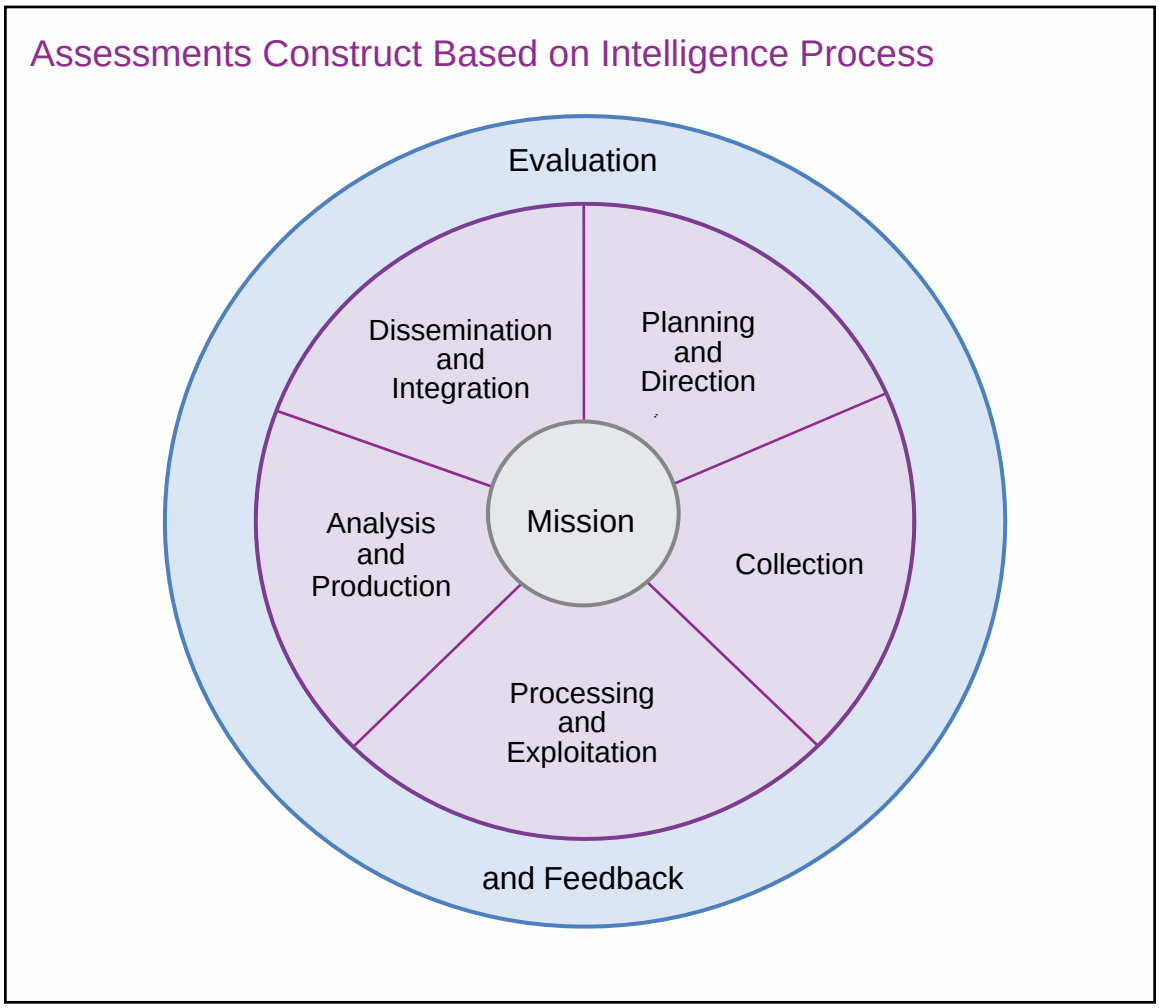


Figure B-3. Assessments Construct Based on Intelligence Process

Intentionally Blank

APPENDIX C
DOCUMENT AND MEDIA EXPLOITATION

1. General

DOMEX is a CCMD responsibility enabled by CSA and US Service support. The CCMD should include resources for DOMEX capabilities in its planning, programming, and budgeting processes IAW DODD 3300.03, *DOD Document and Media Exploitation (DOMEX)*, supported by the DIA through the National Media Exploitation Center (NMEC). DIA staffs and operates theater JDECs and provides other support as needed IAW Intelligence Community Directive (ICD) 302, *Document and Media Exploitation.*

a. DOMEX is the processing, translation, analysis, and dissemination of collected hard copy documents and electronic media that are under the USG's physical control and are not publicly available. This includes the handling of documents and media during their collection, initial review, inventory, and input to a database. DOMEX materials include any information storage media and the means by which it was created (e.g., written, mechanical, chemical, electronic, optical, or magnetic form). A document is any recorded information regardless of its physical form or characteristics, which contains information to support a range of government and military activities including target development, force protection, intelligence collection, watch listing, liaison with foreign partners, interrogation, and criminal investigations. Media is any object on which data can be stored magnetically, optically, chemically, mechanically, electronically, or digitally.

b. DOMEX may provide information on the strategies, plans, operations, activities, tactics, weapons, personnel, contacts, finances, and logistics of adversaries on the battlefield, terrorists, and criminal networks. DOMEX supports multiple processes, such intelligence and information generated for future targeting and biometric and forensic processes supporting the legitimate prosecution of individuals associated to the exploited materials. The forensic and biometrics exploitation of captured or acquired documents and media also enables the development of FEI or BEI data and products to support urgent information needs and operational planning. Both FEI and BEI can support local or international criminal prosecution, which can support the credibility of a prosecuting government or international body.

2. Function

As the national IC center for DOMEX, the NMEC advances the IC's collective capabilities on behalf of the DNI and the defense intelligence enterprise. The NMEC develops training, tradecraft, tools, and technology to integrate IC and DOD DOMEX policies, standards, and procedures. The NMEC provides time-sensitive DOMEX to support the IC, law enforcement, and homeland security requirements consistent with the protection of sources and methods. IAW ICD 302, *Document and Media Exploitation*, NMEC receives all DOD captured or acquired media for databasing and archiving purposes.

a. DOMEX is both a CCMD and IC responsibility. The Services conduct tactical DOMEX with organic assets in support of tactical forces. The NMEC provides national/theater support through the JDEC and other mechanisms, as required.

b. DOMEX organizations provide services to rapidly process, exploit, and disseminate all acquired and seized documents and media from strategic/national through tactical/local levels across the intelligence, CI, military, and law enforcement communities. Forward-deployed DOMEX locations, including the JDEC and Service DOMEX organizations, conduct exploitation activities according to their capabilities. They collaborate in order to share work, maintain accountability and chain of custody, and ensure all captured and acquired documents and media are sent to the central repository at the NMEC. Specific DOMEX organizations and entities include:

(1) **DOMEX Senior Staff Organization.** This organization functions as part of the theater commander's J-2 staff to coordinate and synchronize theater DOMEX operations.

(2) **JDEC.** This is a theater exploitation center deployed by DIA to provide dedicated DOMEX support to a CCDR during contingency operations planning and execution. The JDEC may be under the OPCON of the CCDR or in direct support of the CCDR and under the staff supervision of the CCMD J-2. It receives documents and media from capturing units and other customers and conducts the initial preparation, screening, digitization, translation, and reporting on raw and derived DOMEX data. The JDEC also serves as the theater clearinghouse for images of captured and acquired documents, providing reachback to national DOMEX assets and ensuring all exploited media is uploaded to national repositories. The JDEC can also deploy teams in theater to support operational requirements for limited durations. The size and composition of the JDEC depend on mission requirements. Although the NMEC provides key personnel and mission equipment for the JDEC, the Services or component commands, CI organizations, and other intelligence and law enforcement organizations provide augmentation in support of mission requirements.

(3) **Service-Component-Level DOMEX Organizations.** These organizations conduct initial triage, evidence processing, and tactical exploitation of documents captured by US forces. Documents of strategic or operational value are expeditiously transferred to the JDEC for exploitation and inclusion in databases accessible to the IC.

3. Location

The JDEC and other DOMEX organizations may be adjacent to the joint strategic exploitation center, the JIDC, or the JCMEC to provide mutual support and concurrent exploitation of captured enemy personnel and equipment.

4. Processing

Military forces and individual agencies collect media of various types, classify that media as appropriate, and deliver the media to NMEC, one of its exploitation centers, or organic DOMEX organizations for exploitation. The one exception to this policy is

EPW/detainee property ("pocket litter") that remains with the detainee. When possible, the JDEC and Service DOMEX organizations provide direct support to the JIDC and other strategic and theater EPW holding areas in exploiting detainee property.

a. The handling and classification of captured and acquired media is based on sensitivity, means of acquisition, and authorities. The supporting intelligence staff is the data owner and determines classification and dissemination controls. As a general rule, captured and acquired documents and media are considered unclassified for official use only unless they originate in the US and/or an allied nation and are marked as classified. Supporting intelligence staffs may classify documents and media to protect sources and methods or ongoing operations; however, such classification should be kept to the lowest level possible. Consider foreign disclosure of all triaged and processed evidence or documents before sharing information with partners or authorities for prosecuting captured individuals. Documents that bear foreign classification markings are handled according to US classification standards regarding circumstances of acquisition, regardless of their original foreign classification.

b. Acquiring units should protect material in its captured or acquired form and document and report the capturing unit, date, time, place (preferably grid coordinates), circumstances of capture, and attribution (to whom the documents and devices belong by individual whenever possible). This information and chain of custody documentation should be forwarded with the original items to the nearest DOMEX location. Only qualified personnel should attempt to exploit media.

c. DOMEX personnel receive and account for arriving documents and media. They ensure acquiring units report all critical data and accountability and chain of custody are strictly maintained. DOMEX personnel should coordinate with consumers (i.e., commanders, subordinate leaders, and analysts) to ensure a mutual understanding of consumers' requirements, such as key information sought from the collection, classification and dissemination guidance, and priority of processing. Once the transfer of custody has been executed, DOMEX personnel assign a batch number to catalog a group of documents and media from a single location, target, or detainee. Material should be segregated and tracked by batch or collection throughout the exploitation process.

d. DOMEX organizations maintain and safeguard all captured documents and media. Original documents should never be altered, marked upon, or separated from the batch to which they belong. Physical security requires restricting facility access to personnel involved in the DOMEX process. When at all possible, DOMEX facilities should be fire-protected, have humidity and temperature control systems to maintain the temperature between 55 and 85 degrees Fahrenheit, and implement dust control measures to prevent damage to the equipment. Once exploitation is complete, documents should be moved to a storage facility for long-term storage, returned to the capturing unit, or disposed of as directed by the supported command. Documents designated for destruction should be handled in the same manner prescribed for US classified documents to preclude compromise of US and PN or multinational interests.

5. Triage and Screening

Triage and screening of documents and digital media is a key step of the DOMEX process. During this step, DOMEX technical officers, linguists, and analysts exploit digital devices and documents to identify content of potential intelligence value and to prioritize individual documents and items of media for translation, special handling, or advanced exploitation. The focus of the triage and screening process is to identify actionable intelligence and information in response to the commander's PIRs.

6. Digitizing and Imaging

a. DOMEX organizations digitize documents and media into a searchable theater exploitation database. This is done to create working copies and to allow for the electronic transfer of exploited material to DOMEX repositories. Documents are either scanned or photographed to create a digital record. Media is digitized into an uncompressed format to obtain the highest quality copy. Only the imaged copies of electronic media are subject to additional forensic examination on a stand-alone system. This is done to preserve the integrity of the original media and to guard against virus or malware contamination of communications networks.

b. The NMEC has two centralized national DOMEX repositories. The national Harmony database serves as the repository for exploited documents, files, and reports on DOMEX findings. The central DOMEX repository for forensic images of captured or acquired media is maintained and backed up by the NMEC. This database is the archive of complete media and device images, which is available to analysts across the IC.

7. Foreign Language and Content Exploitation

There are three levels of document translation: full, summary, and gist. The method and level of translation is determined by the content, source, and assigned priority of a given document or item and the availability of DOMEX resources and personnel. Where feasible, machine translation software may facilitate keyword searches to enhance the capabilities of analysts and linguists to further exploit the document. A full translation is a complete and exact translation of a document. A summary translation is an abbreviated translation, which captures all information of intelligence value found in the document. A gist is an abbreviated summary of the key elements of the document including subject, author, and entities. All translation records should provide the metadata for hard copy and digital files. All documents and items of potential intelligence value should receive at least a gist translation.

8. Reporting and Dissemination

DOMEX organizations report significant information to the supported CCDR through tactical intelligence reports, or spot reports, and to the IC through IIRs. Each organization determines which information meets the threshold for spot report generation and whether an IIR should be submitted. Document metadata records, digitized original documents, and associated translations and reporting are uploaded to the NMEC to be disseminated through the national Harmony database. The exploited source and

associated reporting are linked together within the Harmony database for future analysis. All forensic images collected are transferred to NMEC for inclusion in the central DOMEX repository for IC analysts to conduct additional evaluations of the data. The NMEC disseminates gists; translations; triage feedback reports; instant feedback reports; technical exploitation reports; and other DOMEX-derived, serialized reports and products. When possible, a theater exploitation database may be used to allow PN access to releasable documents.

Intentionally Blank

APPENDIX D
TARGET INTELLIGENCE

1. Overview

Target intelligence is all-source intelligence that reveals vulnerabilities in adversary target systems and targets, describes a target's characterization and location, indicates a target's vulnerabilities and relative importance to the adversary, and documents the results of joint fires on targets and target systems. Target intelligence is one of eight intelligence production categories, and includes all target types and supports both lethal and nonlethal fires. Target intelligence production is the conversion of processed or exploited information into target intelligence through analysis and preparation of products in support of known or anticipated user requirements (e.g., target system analysis [TSA], target folders, target lists, and targeting assessment). Intelligence support to targeting is the dissemination and integration of all-source intelligence into the user's decision-making and planning processes (e.g., joint targeting cycle and JPP).

2. Target Intelligence Production

The joint force produces or manages the production of all target intelligence within its operational area. Target intelligence production responsibilities can be inherent or explicit.

a. **Inherent.** When assigned an operational area and military end states, joint forces have inherent target intelligence production responsibilities. Joint forces leverage internal resources (assigned and allocated target intelligence analysts) and external resources (supporting organizations) to fulfill target intelligence production responsibilities.

(1) Geographic CCMDs, which are assigned AORs and objectives through the GEF and Joint Strategic Capabilities Plan, produce target intelligence related to defeating the identified adversaries within their AOR.

(2) When unified commands establish subordinate unified commands or JTFs and give those subordinate joint forces an operational area and objectives to achieve, those subordinate joint organizations have inherent target intelligence production responsibilities. If the subordinate joint force (and its subordinate organizations) lacks the target intelligence production capacity to fulfill these responsibilities, the parent command must fulfill target intelligence production responsibilities while working to enable the subordinate joint force to become self-sufficient.

(3) Joint forces with inherent target intelligence production responsibilities may task subordinate organizations with explicit target intelligence production responsibilities.

b. **Explicit.** Joint forces may require subordinate or partner organizations to produce target intelligence within an organization's expertise. Joint forces are required to document target intelligence production responsibilities and tasks in published plans and

orders (e.g., annex B appendix 4). CSAs, Services, Service components, and functional components have responsibilities to support joint forces with target intelligence consistent with their mission, expertise, and organizational relationship with the supported joint force. While these organizations may be explicitly tasked by supported joint forces to produce target intelligence within their areas of expertise, the joint force is still responsible for ensuring the target intelligence produced meets the JFC's requirements.

c. Joint forces fulfill inherent target intelligence production responsibilities through production (internal resources), delegation (assigned, attached, and supporting organizations), and federation (partner organizations). Joint forces oversee and manage delegated and federated target intelligence to ensure the resultant products meet requirements.

d. At every level of joint force organization, target intelligence work centers produce finished intelligence for decision makers and provide deliverables to operations work centers for non-intelligence processes (see Figure D-1).

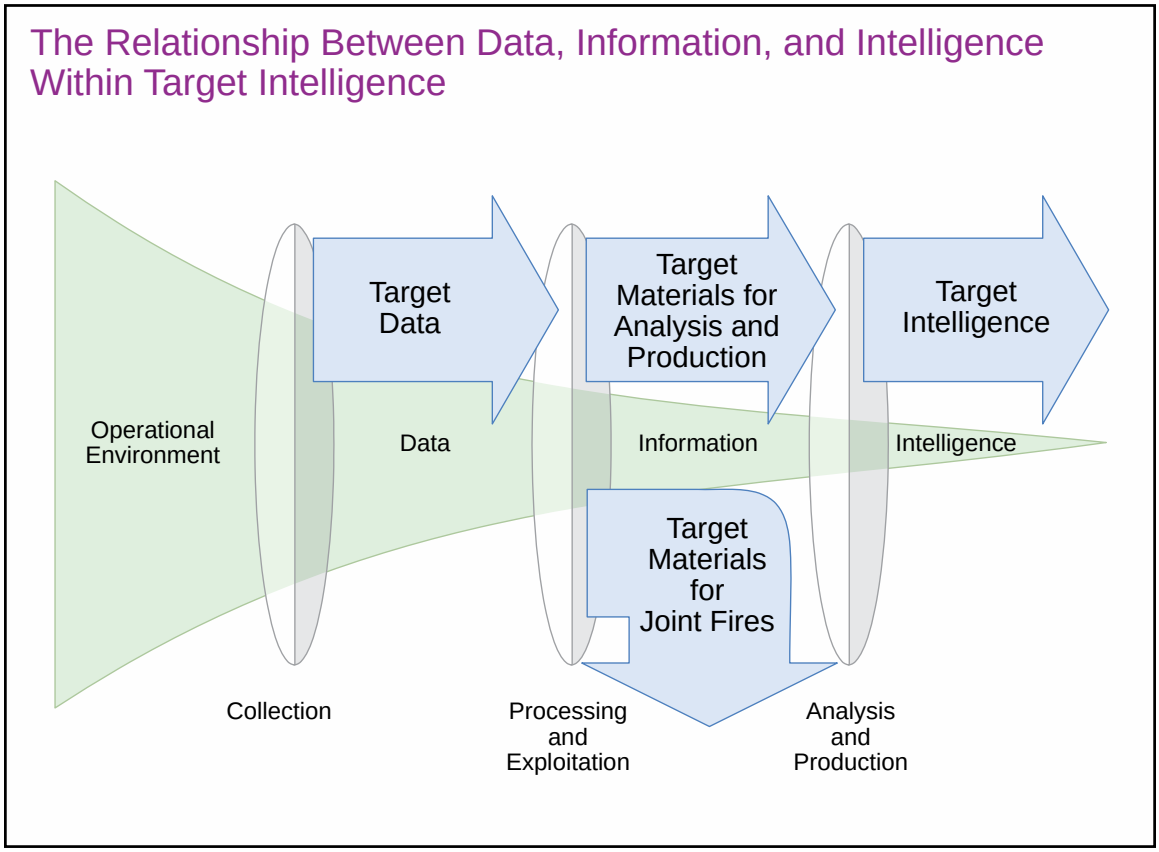


Figure D-1. The Relationship Between Data, Information, and Intelligence Within Target Intelligence

3. Target Intelligence and the Joint Targeting Cycle

a. Target intelligence products and TM for joint fires are located throughout the joint targeting cycle.

(1) Phase 2: TSA, ETFs, some target lists.

(2) Phase 3: Target value analysis, TM for joint fires.

(3) Phase 5: Any TM depicting the location of a non-facility target.

(4) Phase 6: BDA, TM for joint fires, RR.

b. Targeting systematically analyzes and prioritizes targets and matches appropriate lethal and nonlethal actions to those targets to create specific desired effects that achieve the JFC's objectives, accounting for operational requirements, capabilities, and the results of previous assessments. Thus, target intelligence is a key component of joint targeting.

4. Target Data, Target Materials, and Target Intelligence

a. Target intelligence shares the same relationship with data, information, and intelligence as all other types of intelligence. Within the context of target intelligence, data is called "target data," information can be called target information but is most often referred to as TM, and intelligence is called "target intelligence." TM are either the building blocks of target intelligence products or inputs into joint fires processes. Target intelligence results in four target intelligence, products and various TM for joint fires.

b. **TSA.** A TSA is an all-source examination of potential target systems to determine relevance to stated objectives, military importance, and priority of attack. The documentation of the hierarchical and functional relationships of the components and entities that give an adversary a particular capability to wage war. TSAs include (not all-inclusive): target strategies, critical factors analysis, high-value targets, and high-payoff targets.

See JP 3-60, Joint Targeting, *for more information on TSA.*

c. **ETF.** An online repository containing TM and related information prepared for planning and executing action against a specific target. ETFs include (not all inclusive) unique identifiers, target graphics, vetting and validation results, target list assignments, precision points, and collateral damage estimates. ETFs include input from operations, plans, and legal. However, an ETF that contains the TM required to meet intermediate target development standards per CJCSI 3370.01, *Target Development Standards,* is a target intelligence product.

d. **Target List.** A particular grouping of joint targets that are judged by appropriate authority or decision maker to meet specified requirements of law of war, doctrine, policy, plans, operations, regulations, intelligence accuracy, commander's guidance and/or intent. Target lists produced and maintained for intelligence purposes by target

intelligence analysis (candidate target list, joint target list, restricted target list) are target intelligence products, while target lists produced and maintained for operational reasons by joint fires personnel (target nomination list and joint integrated prioritized target list) are not target intelligence products.

e. **BDA.** The assessment of target damage or effect resulting from the application of lethal or nonlethal military force against a target. BDA is composed of physical damage/change assessment, functional damage/change assessment, and target system assessment, typically taking a three-phased approach to proceed from a micro-level examination of the damage or effect inflicted on a specific target element, to ultimately arriving at macro-level conclusions regarding the functional outcomes created in the target system. The three-step analytical process (physical damage/change assessment, functional damage assessment, target system assessment) is reported via a three-phased BDA reporting process: phase 1, BDA initial target assessment; phase 2, BDA supplemental target assessment; and phase 3, BDA target system assessment.

See JP 3-60, Joint Targeting, *for more information on BDA.*

5. Target Materials for Joint Fires

a. **Target vulnerability analysis** includes building an exhaustive list of target vulnerabilities that, if engaged, would result in a reduction in the target's ability to perform its function. Joint fires personnel combine target vulnerabilities with blue force capabilities to form asset-target interactions.

b. **Target imagery analysis for weaponeering** includes the base image and the construction type of a given facility target. Joint fires personnel use the input to derive the optimum blue force munition to use against a facility target.

c. **Target imagery analysis for CDE** includes the base image of a facility target and, when required, the construction type of selected surrounding facilities. Joint fires personnel use the input to conduct the CDE methodology.

d. **Target imagery analysis for collateral damage assessment** includes the base image of a given facility target and, when required, the construction type of selected surrounding facilities. Joint fires personnel use the input to assess how much collateral damage was inflicted by the engagement of a given facility target.

e. **Target imagery analysis for MEA** includes the base image of a given facility target and location and measurement of munition impact craters. Joint fires personnel use the input to assess the difference between where a munition should have landed and where it actually landed and what errors, if any, caused the difference.

f. **RR** occurs in phase 6 of the joint targeting cycle, and is an assessment, derived from the results of BDA and MEA, providing the commander systematic advice on reattack of a target. RR represents the intelligence directorate's opinion on whether a particular target requires another target engagement. Joint fires personnel use the input in their reattack decision.

6. Target Intelligence and Intelligence Support to Targeting

Target intelligence is a subset of intelligence support to targeting. While target intelligence is a discrete set of products and TM, intelligence professionals are also responsible for ensuring those products are integrated into the joint targeting cycle. Therefore, intelligence support to targeting is target intelligence production plus the coordinating actions required to integrate target intelligence into the joint targeting cycle.

Intentionally Blank

APPENDIX E
SECURITY OF CLASSIFIED MATERIAL

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 compromises of classified and controlled unclassified information, 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 operations involving multinational forces, which complicates dissemination and releasability procedures. In all environments, the J-2 must consider and assess such issues as 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.

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. 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 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).

b. CCDRs can grant interim clearances, administratively withdraw clearances, and grant or deny access to classified information per the guidelines contained in DOD 5200.2-R, *Personnel Security Program.* The Services' senior officers of the intelligence community (SOICs) or their designees may grant SCI access for their respective Military Departments. The Director, DIA, is responsible for OSD, Joint Staff, the DOD agencies, and DOD field activities (less NSA/CSS, NGA, and NRO).

3. Sensitive Compartmented Information Facility

Before SCI can be handled, processed, or stored, a SCIF must be accredited based on established physical security guidelines under ICD/Intelligence Community Standard

(ICS) 705 Series to include Technical Specifications for construction and management of SCIFs and Department of Defense Manual (DODM) 5105.21, Volumes 1-3, *Sensitive Compartmented Information (SCI) Administrative Security Manual.* The special security officer (SSO) is the POC for information on accreditation authorities and SCIF physical security guidelines.

a. **Establishing and Accrediting a Temporary SCIF**

(1) A SCIF at any level of accreditation may be established and granted temporary accreditation by Service cognizant security authority, their designee, or DOD component SIOs in support of tactical contingency and field training operations.

(2) The SOIC may approve a temporary sensitive compartmented information facility (TSCIF) for up to one year. The approving authority for the TSCIF will assign the appropriate identification number. There are no specific physical requirements for such a TSCIF, although sound attenuation problems should be addressed, the TSCIF should be staffed around-the-clock when operational, and appropriate guards should monitor and/or patrol the area. IAW DODM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*, extension beyond the one-year period must be justified in writing to DIA.

(3) A TSCIF is a military field operation established during crisis, contingency, or exercise. The local approving authority may require use of a local tactical deployment checklist. The element authorizing establishment of a tactical TSCIF notifies the accreditation authority and DIA by message.

(4) A TSCIF may be operated within a selected structure for the duration of an exercise.

(5) A temporary secure working area (TSWA) is a temporarily accredited facility used no more than 40 hours per month and no longer than 12 months in the same location for handling or discussing SCI. SIOs may approve TSWAs for all levels of SCI. SIOs 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.

(6) A shipboard temporary 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 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 is 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 TSCIF IAW ICD/ICS 705 Series.

b. **TSCIF Security.** Although security is necessary for the integrity of a TSCIF, 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 information. 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 US citizen(s). The J-2, in coordination with the SSO, should ensure constant oversight of nonintelligence elements residing in the SCIF to ensure there will be no compromise of operational matters.

4. Sanitizing and/or Releasing Intelligence

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 US. 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 NDP Committee as

exceptions to policy, a balance is sought between US national interests and the security of the classified information.

a. NDP-1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*, governs how the US releases military information to foreign governments and international organizations and establishes eligibility criteria to receive releasable information.

b. An SSO can provide more detailed information on SCI policy and procedures, and the DIA senior representative assigned to the cognizant CCMD can help to seek exemptions to security policy from national agencies. The CCDR is responsible for the release of intelligence and should request that intelligence producers tailor their product so as to minimize the use of caveats.

c. J-2s should consider the following when determining whether to release classified information:

(1) Determine recipient country's eligibility to receive military intelligence. If the country is not eligible yet meets the conditions listed as follow, a request for exemption to NDP-1 can be made through the CCMD's FDO.

(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.

(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.

d. Key points on release of classified material are listed in Figure E-1.

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 the risks posed during processing are outweighed by the gain. Specifically, this means adequate security of contractor and DOD (less NSA/CSS) automated information systems and the security of

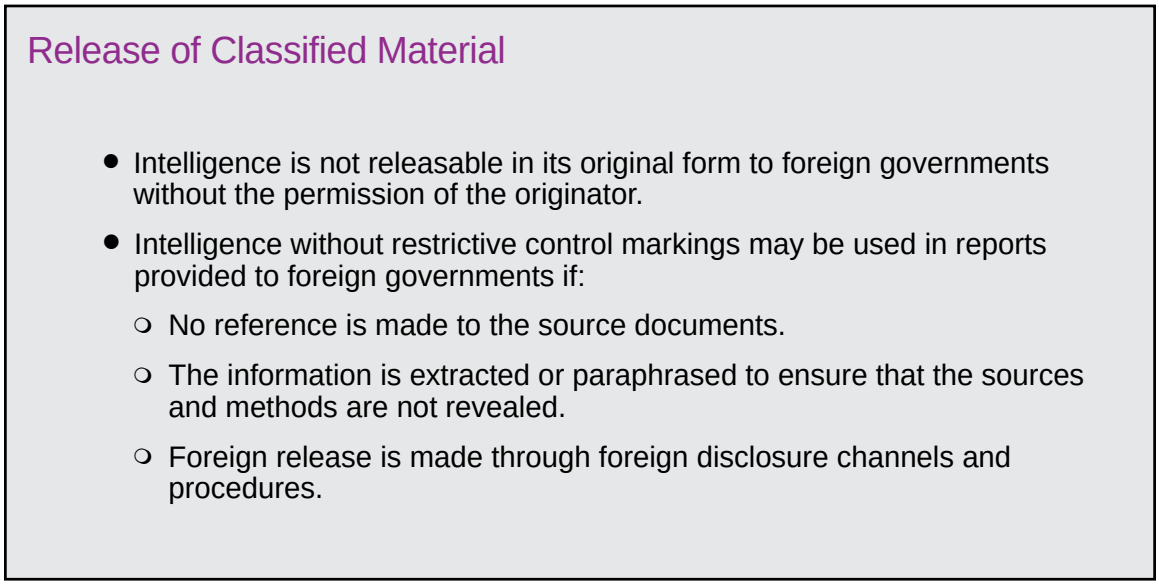


Figure E-1. Release of Classified Material

systems (networks) that store, process, and/or transmit sensitive foreign intelligence information are under the cognizance of the Director, DIA. DIA manages a cybersecurity program for DOD non-cryptographic SCI systems, including DOD Intelligence Information System and JWICS.

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 systems to be used during the operation, as well as planned interconnectivity. DIA works with planners to balance security requirements with operational requirements.

Intentionally Blank

APPENDIX F
JOINT EXPLOITATION SUPPORT TO INTELLIGENCE

1. Introduction

a. Joint exploitation is a methodical, integrated, and collaborative capability used to process information, materiel, and personnel to support CCIR and the planning process. Joint exploitation requires a coordinated and synchronized approach among exploitation stakeholders that includes the Services, industry, academia, international partners, and the whole-of-government.

b. The Services, US Special Operations Command, CSAs, US interagency partners, and multinational partners have developed unique information, materiel, and other exploitation capabilities. These capabilities exploit and process collected data that informs or can be utilized by the IC and can be used by operational commanders. During joint operations, exploitation capabilities may be task-organized to form a tailored support package that satisfies a JFC's forward-deployed technical, forensic, and scientific intelligence and information requirements. A joint exploitation capability is formed when forward-deployed, task-organized exploitation support packages are combined with out-of-theater exploitation capabilities. Collection and exploitation capabilities should deploy early during operations to assist in identifying potential threats, prevent tactical surprise, and to stay abreast of evolving technologies used by enemy forces.

c. Figure F-1 illustrates how joint exploitation informs planning by supporting activities such as force protection, component and materiel sourcing, signature characterization, targeting, support to prosecution, support to special activities, and support to research, development, testing, and engineering.

d. For the purposes of this appendix, these terms are prevalent and used thusly:

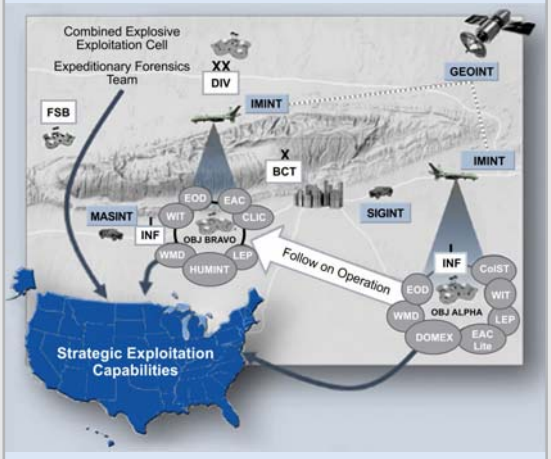
(1) "Information" is all data to include open-source, imagery, geospatial, foreign signals, and scientific data.

(2) "Materiel" is all physical items and equipment that may be of intelligence value.

2. The Joint Exploitation Enterprise

a. Exploitation occurs across all three levels of warfare. It begins by collecting/capturing information, materiel, and/or personnel and continues throughout the tactical, operational, and strategic levels with continuous feedback loops. Exploitation activities may require extensive coordination and collaboration across the multiple intelligence disciplines (CI, GEOINT, HUMINT, MASINT, OSINT, SIGINT, and TECHINT); complementary intelligence applications such as BEI, FEI, DOMEX, and I2; and operational functions (see Figure F-2). During processing and exploitation, raw data is converted into forms/products that can be readily used by commanders, decision makers at all levels, intelligence analysts, and other consumers.

Joint Exploitation

Threats	Expeditionary Exploitation	Outcomes
Defense Intelligence Agency Conventional • Automated Systems • Documents and Media • C&E Equipment • Medical Materiel • Mobility Systems • Munitions • Weapons Defense Threat Reduction Agency Unconventional • Chemical • Biological • Radiological • Nuclear • IEDs • Modified Munitions and Weapons	Collect, Exploit, Analyze DOD Exploitation Capabilities  Organized Under a Joint Task Force with Reachback	• Force Protection • Targeting • Signature Characterization • Component and Material Sourcing • Support to Prosecution • Support to RDT&E • Support to Special Activities

Joint exploitation may be conducted simultaneously at all three levels of warfare. While DIA primarily addresses conventional threats and DTRA primarily addresses unconventional threats, they and other CSAs may address threats in both areas.

Legend

BCT	brigade combat team	GEOINT	geospatial intelligence
C&E	collection and exploitation	HUMINT	human intelligence
CLIC	company level intelligence cell	IED	improvised explosive device
CoIST	company intelligence support team	IMINT	imagery intelligence
CSA	combat support agency	INF	infantry
DIA	Defense Intelligence Agency	LEP	law enforcement professional program
DIV	division	MASINT	measurement and signature intelligence
DOD	Department of Defense	OBJ	objective
DOMEX	document and media exploitation	RDT&E	research, development, test, and evaluation
DTRA	Defense Threat Reduction Agency	SIGINT	signals intelligence
EAC	echelons above corps (Army)	WIT	weapons intelligence team
EOD	explosive ordnance disposal	WMD	weapons of mass destruction
FSB	forward support battalion		

Figure F-1. Joint Exploitation

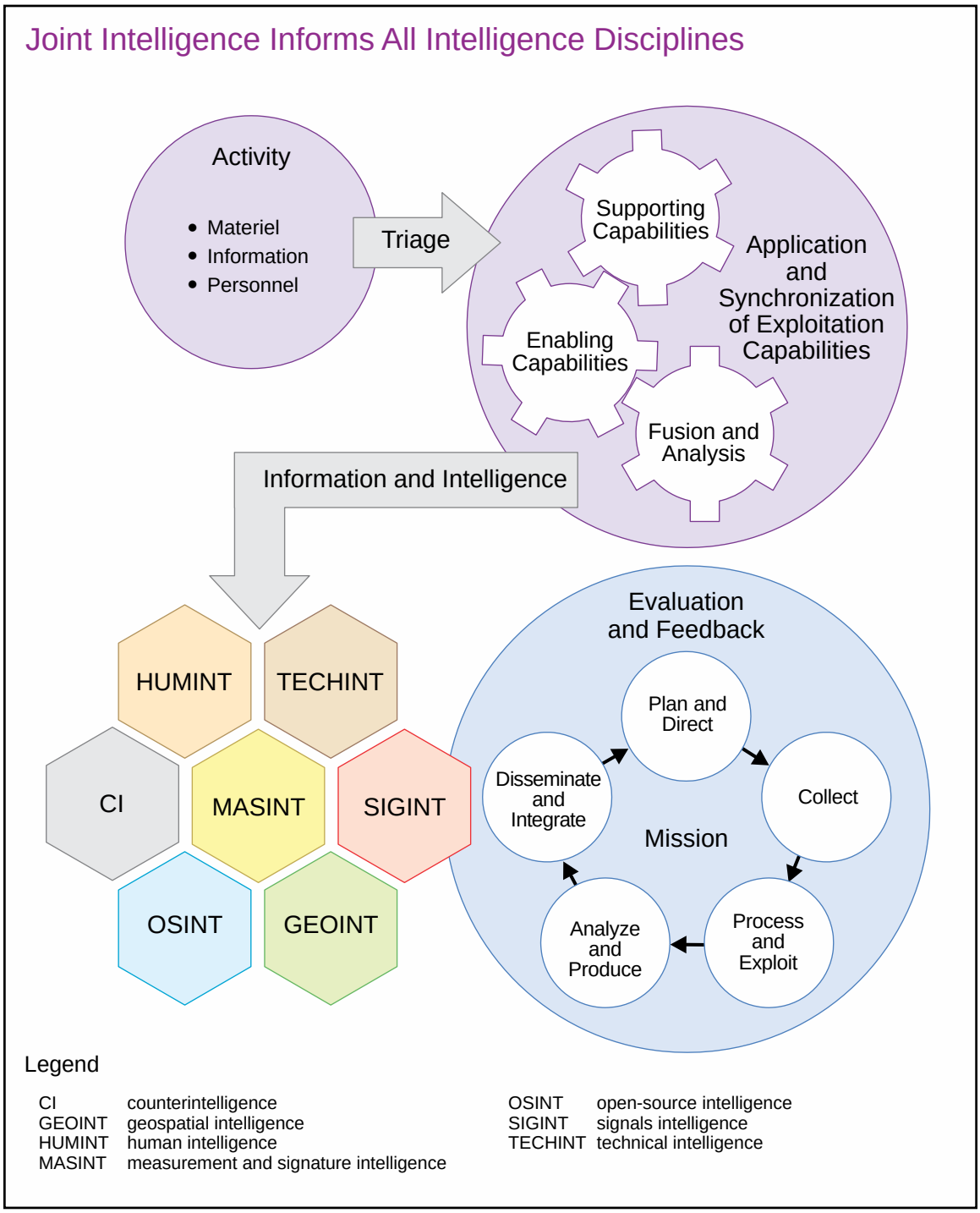


Figure F-2. Joint Intelligence Informs All Intelligence Disciplines

b. Field/tactical exploitation involves actions to gather, preserve, document, and manage information, material, and personnel taken from the battlefield or an incident site. Tactical exploitation can be conducted by specialized units (explosive ordnance disposal, SOF, etc.), but may also be conducted by conventional force units that have proper training and are task-organized (site exploitation teams, maritime visit, board, search, and

seizure teams, etc.). Tactical exploitation determines information and intelligence of immediate tactical value, and screens and prioritizes information, materiel, and POI for further exploitation.

(1) Tactical exploitation delivers timely and credible information about enemy information, material, and personnel capabilities and informs planning activities related to the operation. Limited field exploitation of collected material occurs to meet the immediate needs of tactical units or other vested parties. Recovered information and materiel may be delivered to more capable theater exploitation facilities. These activities may also provide actionable information and intelligence, which may result in retasking of collection and exploitation capabilities and follow on operations.

(2) Field/tactical collection assets conduct systematic searches at the point of collection; recognize information and material of value (e.g., weapon systems, computers and media storage devices, documents, biological materials, firearms, explosives, IED components, drugs, biometrics [Figure F-3]); and adequately document the site using photography, video, and sketching.

c. Theater/operational exploitation combines the outputs of tactical exploitation with operational exploitation results and all-source analysis. Operational exploitation and analysis is conducted by expeditionary exploitation facilities and provides detailed technical, forensic, and scientific analysis of captured information and materiel. Information derived from operational exploitation and analysis informs the intelligence process to provide intelligence to the commander and staff, enhancing the operational and strategic advantage.

d. Out-of-theater/strategic exploitation is conducted at the national level by highly specialized forensic, scientific, and technological laboratories, facilities, and intelligence organizations. Strategic exploitation delivers full-spectrum exploitation and intelligence analysis to support strategic objectives. This level of exploitation employs advanced techniques, equipment, and scientific capabilities to fully understand the nature of the threat by providing in-depth technical, forensic, and intelligence analysis. National-level capabilities operate according to rigorous processes following accredited standards. They utilize sophisticated equipment that is not easily deployable and link exploitation information and related intelligence drawn from tactical through strategic exploitation processes. From full-spectrum exploitation of threats through the production of finished intelligence products, strategic exploitation provides specialized, synchronized support to inform operational and strategic decisions.

3. Planning Considerations

a. Exploitation supports the full range of military operations and should be addressed early in and throughout deliberate and crisis action planning. A wide variety of exploitation capabilities are available to support forward-deployed forces. Deployable exploitation resources are generally scalable and can make extensive use of reachback to provide analytical support. Evaluation based on a systems perspective shall serve as a basis to determine the size and mix of capabilities that will be required to support initial

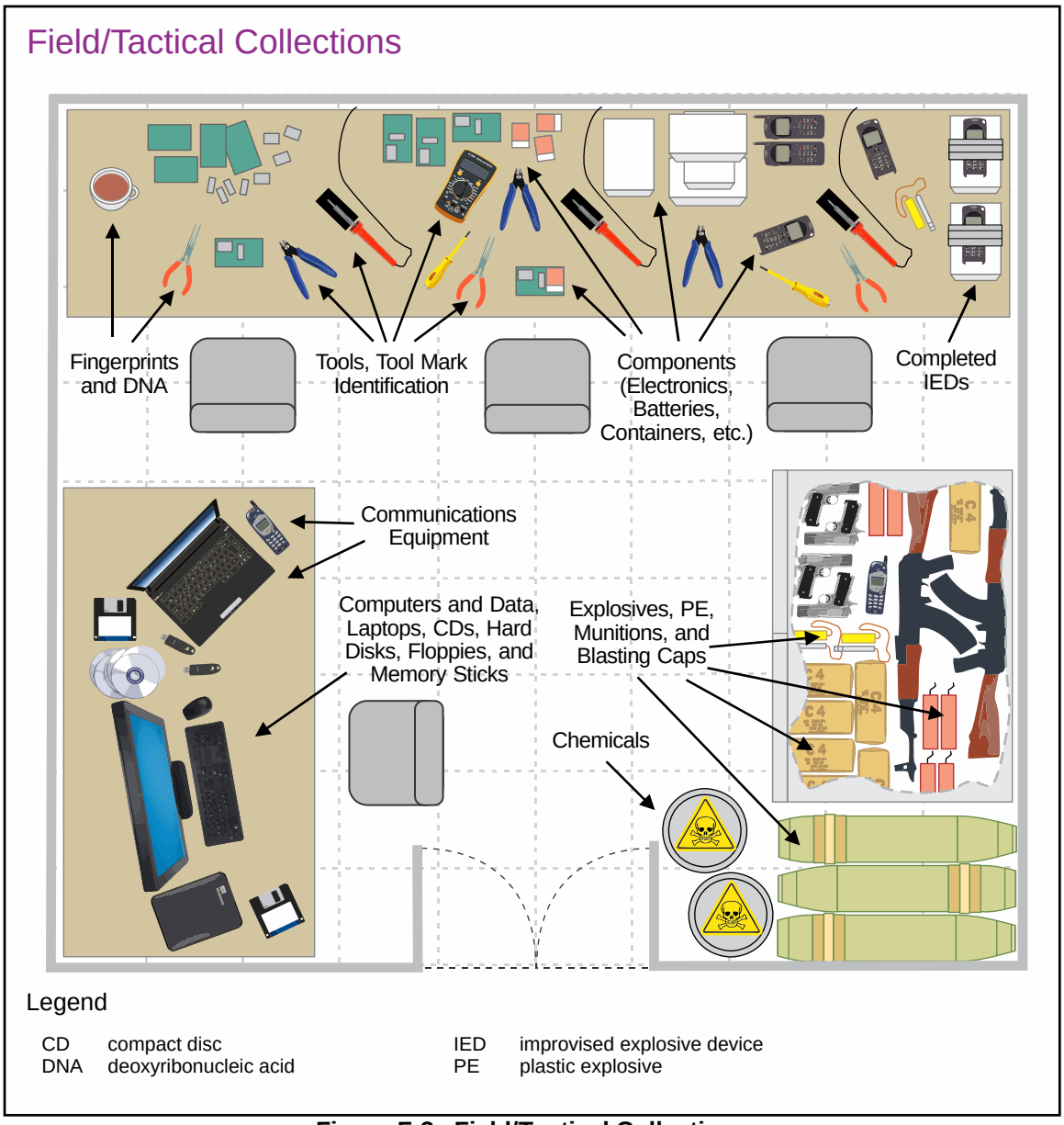


Figure F-3. Field/Tactical Collections

operations. For further explanation, see JP 2-0, *Joint Intelligence.* Mission analysis should consider required exploitation capabilities and other related functions such as reachback and support by CSAs.

b. Managing exploitation capabilities may initially be the responsibility of the J-2 and J-3 and special staff sections. Augmentation of the J-2 may be required to facilitate coordination and synchronization of disparate exploitation capabilities that support the JFC's information requirements and planning. The CCDR/JFC may choose to establish a joint force exploitation staff element (J-2E), in coordination with the J-3, to develop policies and procedures and to plan, coordinate, and synchronize joint exploitation activities that ensure unity of effort among military, intelligence, law enforcement, multinational, host nation/PN, and reachback providers. The J-2E makes sure a

AFGHANISTAN AND PAKISTAN 2011 EXPLOITATION

In late 2011, as part of explosive ordnance disposal (EOD) operations in Afghanistan, a cache of improvised antipersonnel devices was recovered and forwarded to the combined explosive exploitation cell (CEXC) for theater/operational processing. Technical and forensic exploitation revealed unintelligible manufacturer markings and identifiable latent fingerprints, which linked the cache to other improvised explosive device incidents. A subsample of the components was forwarded to Federal Bureau of Investigation's (FBI's) Terrorist Explosive Device Analytical Center (TEDAC) for out-of-theater/strategic exploitation. TEDAC, with support from the Department of the Army, further exploited the components using more sophisticated forensic disciplines including latent prints, forensic imaging, questioned documents, tool marks, and chemistry.

At the same time, an EOD unit in theater, Combined Joint Task Force Paladin and Naval Surface Warfare Center Indian Head Explosive Ordinance Disposal Technology Division, collaborated to identify Afghanistan and Pakistan (AFPAK) 2011 components, mine nomenclature, and develop render safe procedures. Results from TEDAC were shared with the National Media Exploitation Center for further examination. Additional strategic exploitation conducted by research scientists at the US Military Academy encouraged the development and production of specification-grade AFPAK 2011 surrogates by Picatinny Arsenal for post blast analysis by the Army's Adaptive Counter-Improvised Explosive Device/Explosive Ordnance Disposal Solution Division and the FBI's Explosive Unit. Completed in less than three months, the exploitation process yielded the identification of the production source of the mine components. Information gained from these exploitative processes was shared across the intelligence community and other government organizations, resulting in decisions and actions of strategic importance.

Exploitation of the AFPAK 2011 is one example of how interservice and interagency collaboration influences the military decision-making process. Expertise is collaborative throughout the range of military operations and levels of warfare. Used effectively, exploitation can be useful in influencing friendly force adaptations in response to enemy tactics, techniques, and procedures. In the case of the AFPAK 2011, the information obtained from all levels of exploitation influenced research and development, enhanced targeting, improved training, influenced explosive testing/post-blast analysis, established new render safe procedures, and federal requirements for developing new equipment.

Various Sources

centralized theater coordinating authority exists to integrate and synchronize collection, exploitation, and analysis in support of the JFC. Should the operation expand in size or intensity, the JFC may choose to establish an exploitation task force to manage exploitation activities in support of the joint force.

c. There may be significant logistics requirements necessary to support joint exploitation activities. This may include the timely and safe storage and transportation of materiel and custody of personnel. Consideration must also be given to transporting hazardous materials and to maintaining the chain of custody to maintain the integrity of exploited materiel, both in and outside of the operational area.

d. There may also be significant IT and communications requirements to support joint exploitation activities. This may include standardizing data management, providing access to the appropriate communications and C2 networks, and ensuring interoperability across exploitation and analysis providers and users.

Intentionally Blank

APPENDIX G
REFERENCES

The development of JP 2-01 is based upon the following primary references.

1. General

a. National Security Act of 1947.

b. Title 10, United States Code.

c. Title 50, United States Code.

d. *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004.*

e. *The National Security Strategy of the United States.*

f. *The National Military Strategy.*

g. *National Strategy to Combat Weapons of Mass Destruction.*

h. *National Strategy for Homeland Security.*

i. *National Strategy for Combating Terrorism.*

j. *National Intelligence Strategy.*

k. *Defense Intelligence Strategy.*

l. EO 12333, *United States Intelligence Activities*, as amended.

m. EO 12958, *Classified National Security Information.*

n. NDP-1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations.*

o. ICD 302, *Document and Media Exploitation.*

p. ICD 403/401.1, *Intelligence Disclosure Policy.*

q. ICD 705, *Sensitive Compartmented Information Facilities.*

r. ICS 705-1, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities.*

s. ICS 705-2, *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information.*

2. Department of Defense Publications

a. DODD 3000.06, *Combat Support Agencies (CSAs).*

b. DODD 3000.07, *Irregular Warfare (IW).*

c. DODD 3300.03, *DOD Document and Media Exploitation (DOMEX).*

d. DODD 3600.01, *Information Operations (IO).*

e. DODD 5100.01, *Functions of the Department of Defense and Its Major Components.*

f. DODD 5100.03, *Support of the Headquarters of Combatant and Subordinate Unified Commands.*

g. DODD 5100.20, *National Security Agency/Central Security Service (NSA/CSS).*

h. DODD 5105.21, *Defense Intelligence Agency (DIA).*

i. DODD 5105.60, *National Geospatial-Intelligence Agency (NGA).*

j. DODD 5143.01, *Undersecretary of Defense for Intelligence (USD[I]).*

k. DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense.*

l. DODD 5205.12, *Military Intelligence Program (MIP).*

m. DODD 5205.14, *DOD Counter Threat Finance (CTF) Policy.*

n. DODD S-5210.36, *Provision of DOD Sensitive Support to DOD Components and Other Departments and Agencies of the US Government (U).*

o. DODD 5240.01, *DOD Intelligence Activities.*

p. DODD 5240.02, *Counterintelligence (CI).*

q. DODI O-3115.07, *Signals Intelligence (SIGINT).*

r. DODI 3115.10E, *Intelligence Support to Personnel Recovery.*

s. DODI S-5205.01, *DOD Foreign Military Intelligence Collection Activities (FORMICA)(U).*

t. DODI 5240.10, *Counterintelligence (CI) in the Combatant Commands and Other DOD Components.*

u. DODI 6420.01, *National Center for Medical Intelligence (NMCI).*

v. DODI 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DOD.*

w. DODM 5105.21, Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security.*

x. DODM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security.*

y. DODM 5105.21, Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities.*

z. DOD 5200.2-R, *Personnel Security Program.*

3. Chairman of the Joint Chiefs of Staff Publications

a. JP 1, *Doctrine for the Armed Forces of the United States.*

b. JP 1-0, *Joint Personnel Support.*

c. JP 2-0, *Joint Intelligence.*

d. JP 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations.*

e. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment.*

f. JP 2-03, *Geospatial Intelligence in Joint Operations.*

g. JP 3-0, *Joint Operations.*

h. JP 3-05, *Special Operations.*

i. JP 3-06, *Joint Urban Operations.*

j. JP 3-08, *Interorganizational Cooperation.*

k. JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments.*

l. JP 3-12, *Cyberspace Operations.*

m. JP 3-13, *Information Operations.*

n. JP 3-13.2, *Military Information Support Operations.*

o. JP 3-16, *Multinational Operations.*

p. JP 3-24, *Counterinsurgency*.

q. JP 3-27, *Homeland Defense*.

r. JP 3-28, *Defense Support of Civil Authorities.*

s. JP 3-29, *Foreign Humanitarian Assistance.*

t. JP 3-33, *Joint Task Force Headquarters.*

u. JP 3-40, *Countering Weapons of Mass Destruction.*

v. JP 3-50, *Personnel Recovery.*

w. JP 3-57, *Civil-Military Operations.*

x. JP 3-59, *Meteorological and Oceanographic Operations.*

y. JP 3-60, *Joint Targeting.*

z. JP 5-0, *Joint Planning.*

aa. JP 6-0, *Joint Communications System.*

bb. CJCSI 1301.01F, *Joint Individual Augmentation Procedures.*

cc. CJCSI 3110.01J, *(U) 2015 Joint Strategic Capabilities Plan (JSCP).*

dd. CJCSI 3110.02H, *Intelligence Planning, Objectives, Guidance, and Tasks.*

ee. CJCSI 3150.25F, *Joint Lessons Learned Program.*

ff. CJCSI 3250.01E, *(U) Policy Guidance for Intelligence, Surveillance, and Reconnaissance and Sensitive Reconnaissance Operations.*

gg. CJCSI 3340.02B, *Joint Enterprise Integration of Warfighter Intelligence.*

hh. CJCSI 3370.01A, *Target Development Standards.*

ii. CJCSI 3505.01B, *Target Coordinate Mensuration Certification and Program Accreditation.*

jj. CJCSI 5120.02D, *Joint Doctrine Development System.*

kk. CJCSI 5221.01D, *Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations.*

ll. CJCSM 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance.*

mm. CJCSM 3150.25A, *Joint Lessons Learned Program.*

nn. CJCSM 3314.01A, *Intelligence Planning.*

Intentionally Blank

APPENDIX H
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff J-7, Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 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, *Joint and National Intelligence Support to Military Operations*, 05 January 2012.

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: Deputy Director, Joint Education and Doctrine (DD JED), Attn: Joint Doctrine Division, 7000 Joint Staff (J-7), Washington, DC, 20318-7000 or email:js.pentagon.j7.list.dd-je-d-jdd-all@mail.mil.

b. Routine changes should be submitted electronically to the Deputy Director, Joint Education and Doctrine, Joint Doctrine Analysis Division and info the lead agent and the Director for Joint Force Development, J-7/JED.

c. When a Joint Staff directorate submits a proposal to the CJCS 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 Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Lessons Learned

The Joint Lessons Learned Program (JLLP) primary objective is to enhance joint force readiness and effectiveness by contributing to improvements in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. The Joint Lessons Learned Information System (JLLIS) is the DOD system of record for lessons learned and facilitates the collection, tracking, management, sharing, collaborative resolution, and dissemination of lessons learned to improve the development and readiness of the joint force. The JLLP integrates with joint doctrine

through the joint doctrine development process by providing lessons and lessons learned derived from operations, events, and exercises. As these inputs are incorporated into joint doctrine, they become institutionalized for future use, a major goal of the JLLP. Lessons and lessons learned are routinely sought and incorporated into draft JPs throughout formal staffing of the development process. The JLLIS Website can be found at https://www.jllis.mil or http://www.jllis.smil.mil.

6. Distribution of Publications

Local reproduction is authorized, and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be IAW DOD Manual 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification*, and DOD Manual 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information.*

7. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS Joint Electronic Library Plus (JEL+) at https://jdeis.js.mil/jdeis/index.jsp (NIPRNET) and http://jdeis.js.smil.mil/jdeis/index.jsp (SIPRNET), and on the JEL at http://www.dtic.mil/doctrine.

b. Only approved JPs are releasable outside the combatant commands, Services, and Joint Staff. Defense attachés may request classified JPs by sending written requests to Defense Intelligence Agency (DIA)/IE-3, 200 MacDill Blvd., Joint Base Anacostia-Bolling, Washington, DC 20340-5100.

c. JEL CD-ROM. Upon request of a joint doctrine development community member, the Joint Staff J-7 will produce and deliver one CD-ROM with current JPs. This JEL CD-ROM will be updated not less than semi-annually and when received can be locally reproduced for use within the combatant commands, Services, and combat support agencies.

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

AF	Air Force
AF/A2	Deputy Chief of Staff of the Air Force for Intelligence, Surveillance, and Reconnaissance
AGILE	Advanced Global Intelligence Learning Environment
AOR	area of responsibility
APEX	Adaptive Planning and Execution
BDA	battle damage assessment
BEI	biometrics-enabled intelligence
BEWL	biometric-enabled watchlist
BIA	behavioral influences analysis
BICES	battlefield information collection and exploitation system (NATO)
C2	command and control
CA	combat assessment
CAT	crisis action team
CBRN	chemical, biological, radiological, and nuclear
CCDR	combatant commander
CCIR	commander's critical information requirement
CCMD	combatant command
CDE	collateral damage estimation
CENTRIXS	Combined Enterprise Regional Information Exchange System
CHCSS	Chief, Central Security Service
CI	counterintelligence
CIA	Central Intelligence Agency
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
CO	cyberspace operations
COA	course of action
COG	center of gravity
COLISEUM	community on-line intelligence system for end-users and managers
COM	collection operations management
CONOPS	concept of operations
COP	common operational picture
CRM	collection requirements management
CRMx	collection requirements matrix

CSA	combat support agency
CSG	cryptologic services group
DCGS	distributed common ground/surface system
DCM	defense collection manager
DCME	Defense Collection Management Enterprise
DCO	defense coordinating officer
DEA	Drug Enforcement Administration (DOJ)
DHS	Department of Homeland Security
DI	Defense Intelligence Agency (DIA) Directorate for Analysis
DIA	Defense Intelligence Agency
DIAP	Defense Intelligence Analysis Program
DIO	defense intelligence officer
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODIN	Department of Defense information network
DODM	Department of Defense manual
DOMEX	document and media exploitation
DOS	Department of State
DPM	dissemination program manager
DSCA	defense support of civil authorities
DSE	direct support element
DTA	dynamic threat assessment
EEI	essential element of information
ELINT	electronic intelligence
EO	executive order
EPW	enemy prisoner of war
ETF	electronic target folder
F3EAD	find, fix, finish, exploit, analyze, and disseminate
FADM	force allocation decision matrix
FBI	Federal Bureau of Investigation (DOJ)
FDO	foreign disclosure officer
FEI	forensic-enabled intelligence
FEMA	Federal Emergency Management Agency (DHS)
FFIR	friendly force information requirement
FISINT	foreign instrumentation signals intelligence
FSP	functional support plan
G-2	Army Deputy Chief of Staff for Intelligence

GCC	geographic combatant commander
GCCS	Global Command and Control System
GCCS-I3	Global Command and Control System-Integrated Imagery and Intelligence
GEF	Guidance for Employment of the Force
GEOINT	geospatial intelligence
GFM	global force management
GFMAP	Global Force Management Allocation Plan
GI&S	geospatial information and services
GMI	general military intelligence
HD	homeland defense
HQ	headquarters
HQMC	Headquarters, Marine Corps
HSIN	Homeland Security Information Network (DHS)
HUMINT	human intelligence
I2	identity intelligence
I2SP	identity intelligence support packet
IAA	incident awareness and assessment
IAW	in accordance with
IBS	integrated broadcast service
IC	intelligence community
ICC	Intelligence Coordination Center (USCG)
ICD	intelligence community directive
ICS	intelligence community standard
IED	improvised explosive device
IIR	intelligence information report
IMINT	imagery intelligence
INSCOM	United States Army Intelligence and Security Command
IO	information operations
IOII	information operations intelligence integration
IP	intelligence planning
IR	intelligence requirement
IRC	information-related capability
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
ITF	intelligence task force (DIA)
IWG	intelligence working group
J-2	intelligence directorate of a joint staff
J-2E	joint force exploitation staff element
J-2X	joint force counterintelligence and human intelligence 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	communications system directorate of a joint staff
JCMB	joint collection management board
JCMEC	joint captured materiel exploitation center
JCRM	Joint Capabilities Requirements Manager
JCS	Joint Chiefs of Staff
JCSE	Joint Communications Support Element (USTRANSCOM)
JDEC	joint document exploitation center
JDISS	joint deployable intelligence support system
JFC	joint force commander
JFO	joint field office
JIDC	joint interrogation and debriefing center
JIOC	joint intelligence operations center
JIPCL	joint integrated prioritized collection list
JIPOE	joint intelligence preparation of the operational environment
JISE	joint intelligence support element
JMICS	Joint Worldwide Intelligence Communications System mobile integrated communications system
JOC	joint operations center
JP	joint publication
JPP	joint planning process
JTF	joint task force
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LFA	lead federal agency
LNO	liaison officer
LOC	line of communications
LOE	line of effort
LTIOV	latest time information is of value
MASINT	measurement and signature intelligence
MASLO	measurement and signature intelligence liaison officer
MCIA	Marine Corps Intelligence Activity
MCISRE	Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise
MEA	munitions effectiveness assessment
METOC	meteorological and oceanographic
MIDB	modernized integrated database
MIP	military intelligence program
MOE	measure of effectiveness
MOP	measure of performance

NATO	North Atlantic Treaty Organization
NCR	National Security Agency/Central Security Service representative
NDP	national disclosure policy
NG	National Guard
NGA	National Geospatial-Intelligence Agency
NG JFHQ-State	National Guard joint force headquarters-state
NGO	nongovernmental organization
NICC	National Intelligence Coordination Center
NIM	national intelligence manager
NIP	National Intelligence Program
NIPF	National Intelligence Priorities Framework
NIPRNET	Non-classified Internet Protocol Router Network
NISP	national intelligence support plan
NJOIC	National Joint Operations and Intelligence Center
NMEC	National Media Exploitation Center
NMO	National Measurement and Signature Intelligence Office
NOC	National Operations Center (DHS)
NRO	National Reconnaissance Office
NRT	near real time
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
NST	National Geospatial-Intelligence Agency support team
OB	order of battle
ODNI	Office of the Director of National Intelligence
OE	operational environment
ONI	Office of Naval Intelligence
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
PED	processing, exploitation, and dissemination
PIR	priority intelligence requirement
PN	partner nation
POC	point of contact
POI	person of interest
PR	production requirement
PRMx	production requirements matrix
RFF	request for forces
RFI	request for information
RFS	request for sourcing

RR	reattack recommendation
S&T	scientific and technical
S&TI	scientific and technical intelligence
SCA	sociocultural analysis
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SecDef	Secretary of Defense
SIC	supporting intelligence center
SIGINT	signals intelligence
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
SSO	special security officer
TECHINT	technical intelligence
TENCAP	tactical exploitation of national capabilities program
TFCICA	task force counterintelligence coordinating authority
TIA	theater intelligence assessment
TIM	toxic industrial material
TM	target materials
TSA	target system analysis
TSCIF	temporary sensitive compartmented information facility
TSWA	temporary secure working area
UN	United Nations
US BICES	United States Battlefield Information Collection and Exploitation System
US BICES-X	United States Battlefield Information Collection and Exploitation System Extended
USCENTCOM	United States Central Command
USCG	United States Coast Guard
USCS	United States Cryptologic System
USCYBERCOM	United States Cyber Command
USD(I)	Under Secretary of Defense for Intelligence
USFK	United States Forces, Korea
USG	United States Government
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSTRATCOM	United States Strategic Command
VTC	video teleconferencing
WAN	wide-area network

WMD	weapons of mass destruction
WTI	weapons technical intelligence

PART II—TERMS AND DEFINITIONS

access to classified information. None. (Approved for removal from the DOD Dictionary.)

agency. In intelligence usage, an organization or individual that collects and/or processes information. Also called **collection agency.** (Approved for incorporation into the DOD Dictionary.)

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. (DOD Dictionary. SOURCE: JP 2-01)

arms control agreement. None. (Approved for removal from the DOD Dictionary.)

basic encyclopedia. A compilation of identified installations and physical areas of potential significance as objectives for attack. Also called **BE.** (DOD Dictionary. SOURCE: JP 2-01)

collection. In intelligence usage, the acquisition of information and the provision of this information to processing elements. (DOD Dictionary. SOURCE: JP 2-01)

collection agency. Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (DOD Dictionary. SOURCE: JP 2-01)

collection asset. A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (DOD Dictionary. SOURCE: JP 2-01)

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.** (DOD Dictionary. SOURCE: JP 2-01)

collection requirements matrix. A worksheet that compiles collection requirements to inform the initial integrated collection planning efforts and links priority intelligence requirements, their associated essential elements of information, and related indicators to supporting specific information requirements. Also called **CRMx.** (Approved for inclusion in the DOD Dictionary.)

collection resource. A collection system, platform, or capability that is not supporting, assigned, or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. (Approved for incorporation into the DOD Dictionary.)

combat information. Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the

situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (DOD Dictionary. SOURCE: JP 2-01)

consumer. A person or agency that uses information or intelligence produced by either its own staff or other agencies. (Approved for incorporation into the DOD Dictionary.)

control. 1. Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (JP 1) 2. In mapping, charting, and photogrammetry, a collective term for a system of marks or objects on the Earth or on a map or a photograph, whose positions or elevations (or both) have been or will be determined. (JP 2-03) 3. Physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. (JP 3-0) 4. In intelligence usage, an indicator governing the distribution and use of documents, information, or material. (JP 2-01) (Approved for incorporation into the DOD Dictionary.)

courier. A messenger (usually a commissioned or warrant officer) responsible for the secure physical transmission and delivery of documents and material. (DOD Dictionary. SOURCE: JP 2-01)

dissemination. In intelligence usage, the delivery of intelligence to users in a suitable form. (Approved for replacement of "dissemination and integration" and its definition in the DOD Dictionary.)

evaluation. In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (DOD Dictionary. SOURCE: JP 2-01)

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. (DOD Dictionary. SOURCE: JP 2-01)

foreign instrumentation signals intelligence. A subcategory of signals intelligence consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-United States aerospace, surface, and subsurface systems. Also called **FISINT.** (Approved for incorporation into the DOD Dictionary.)

formerly restricted data. None. (Approved for removal from the DOD Dictionary.)

information report. A report used to forward raw information collected to fulfill intelligence requirements. (Approved for incorporation into the DOD Dictionary.)

integration. 1. In force protection, the synchronized transfer of units into an operational commander's force prior to mission execution. (JP 1) 2. The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 1) 3. In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or the process by which several

photographic images are combined into a single image. (JP 1) 4. In intelligence usage, the application of the intelligence to appropriate missions, tasks, and functions. (JP 2-01) (Approved for incorporation into the DOD Dictionary.)

intelligence annex. None. (Approved for removal from the DOD Dictionary.)

intelligence database. None. (Approved for removal from the DOD Dictionary.)

intelligence federation. An agreement in which a combatant command joint intelligence operations center receives intelligence support from other joint intelligence centers, Service intelligence organizations, reserve organizations, and national agencies. (Approved for incorporation into the DOD Dictionary.)

intelligence mission management. A systematic process by an intelligence staff to proactively and continuously formulate and revise command intelligence requirements and track the resulting information through the processing, exploitation, and dissemination process to satisfy user requirements. Also called **IMM.** (Approved for incorporation into the DOD Dictionary.)

intelligence operations. The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. (DOD Dictionary. SOURCE: JP 2-01)

intelligence process. The process by which information is converted into intelligence and made available to users, consisting of the six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (DOD Dictionary. SOURCE: JP 2-01)

intelligence-related activities. None. (Approved for removal from the DOD Dictionary.)

intelligence report. A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. (DOD Dictionary. SOURCE: JP 2-01)

intelligence, surveillance, and reconnaissance. 1. An integrated operations and intelligence 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. 2. The organizations or assets conducting such activities. Also called **ISR.** (Approved for incorporation into the DOD Dictionary.)

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 retasking and time-sensitive decision making. Also called **ISR visualization.** (DOD Dictionary. SOURCE: JP 2-01)

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. (DOD Dictionary. SOURCE: JP 2-01)

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. (DOD Dictionary. SOURCE: JP 2-01)

joint captured materiel exploitation center. An element responsible for deriving intelligence information from captured enemy materiel. It is normally subordinate to the intelligence directorate of a joint staff. Also called **JCMEC.** (DOD Dictionary. SOURCE: JP 2-01)

joint document exploitation center. An element, normally subordinate to the intelligence directorate of a joint staff, responsible for deriving intelligence information from captured documents including all forms of electronic data and other forms of stored textual and graphic information. Also called **JDEC.** (Approved for incorporation into the DOD Dictionary.)

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 enemy and adversary situation. Also called **JISE.** (Approved for incorporation into the DOD Dictionary.)

joint interrogation operations. 1. Activities conducted by a joint or interagency organization to extract information for intelligence purposes from detainees. 2. Activities conducted in support of law enforcement efforts to adjudicate enemy combatants who are believed to have committed crimes against United States persons or property. Also called **JIO.** (Approved for incorporation into the DOD Dictionary.)

Measurement and Signature Intelligence Requirements System. A system for the management of theater and national measurement and signature intelligence collection requirements, providing automated tools for users in support of submission, review, and validation of measurement and signature intelligence nominations of requirements to be tasked for national and Department of Defense measurement and signature intelligence collection, production, and exploitation resources. Also called **MRS.** (DOD Dictionary. SOURCE: JP 2-01)

medical intelligence. That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that 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.** (DOD Dictionary. SOURCE: JP 2-01)

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. Also called **MIDB.** (DOD Dictionary. SOURCE: JP 2-01)

munitions effectiveness 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. Also called **MEA.** (Approved for incorporation into the DOD Dictionary.)

national intelligence. All intelligence that pertains to more than one agency and involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security. (Approved for incorporation into the DOD Dictionary.)

national intelligence estimate. None. (Approved for removal from the DOD Dictionary.)

originator. The command by whose authority a message is sent, which includes the responsibility for the functions of the drafter and the releasing officer. (DOD Dictionary. SOURCE: JP 2-01)

personnel security investigation. None. (Approved for removal from the DOD Dictionary.)

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. (DOD Dictionary. SOURCE: JP 2-01)

priority intelligence requirement. An intelligence requirement that the commander and staff need to understand the threat and other aspects of the operational environment. Also called **PIR.** (Approved for incorporation into the DOD Dictionary.)

processing and exploitation. In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (DOD Dictionary. SOURCE: JP 2-01)

production requirements matrix. A compilation of prioritized combatant command all-source intelligence analysis and production requirements that support all phases of a plan. Also called **PRMx.** (Approved for inclusion in the DOD Dictionary.

requirements management system. None. (Approved for removal from the DOD Dictionary.

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.** (DOD Dictionary. SOURCE: JP 2-01)

sensitive. An agency, installation, person, position, document, material, or activity requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. (DOD Dictionary. SOURCE: JP 2-01)

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. Also called **SCI.** (Approved for incorporation into the DOD Dictionary.

sensitive compartmented information facility. An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed, where procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular sensitive compartmented information authorized for use or storage within the sensitive compartmented information facility. Also called **SCIF.** (DOD Dictionary. SOURCE: JP 2-01)

short title. None. (Approved for removal from the DOD Dictionary.)

signals intelligence operational control. None. (Approved for removal from the DOD Dictionary.)

signals intelligence operational tasking authority. A military commander's authority to operationally direct and levy signals intelligence requirements on designated signals intelligence resources; includes authority to deploy and redeploy all or part of the signals intelligence resources for which signals intelligence operational tasking authority has been delegated. Also called **SOTA.** (DOD Dictionary. SOURCE: JP 2-01)

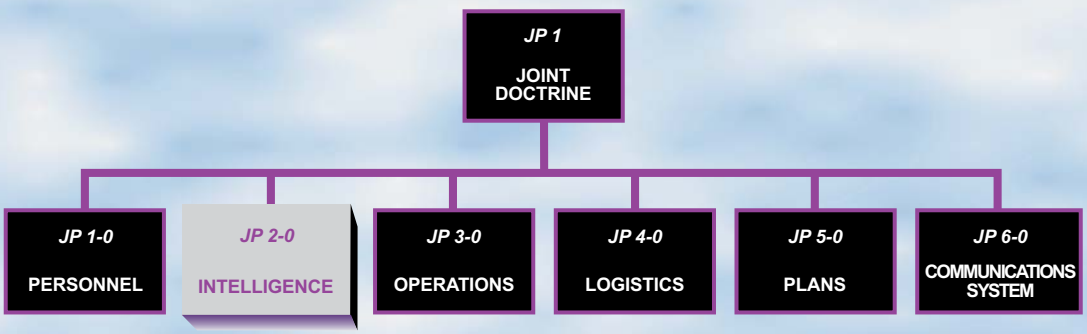
source. 1. A person, thing, or activity from which information is obtained. 2. In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. 3. In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. (DOD Dictionary. SOURCE: JP 2-01)

tactical exploitation of national capabilities. Congressionally mandated program to improve the combat effectiveness of the Services through more effective military use of national programs. Also called **TENCAP.** (DOD Dictionary. SOURCE: JP 2-01)

threat warning. The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (DOD Dictionary. SOURCE: JP 2-01)

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. (JP 2-01) 2. A part of target development that ensures all vetted targets meet the objectives and criteria outlined in the commander's guidance and ensures compliance with the law of war and rules of engagement. (JP 3-60) 3. 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. (JP 3-35) 4. Execution procedure whereby all the information records in a time-phased force and deployment data are confirmed error free and accurately reflect the current status, attributes, and availability of units and requirements. (DOD Dictionary. SOURCE: JP 3-35)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



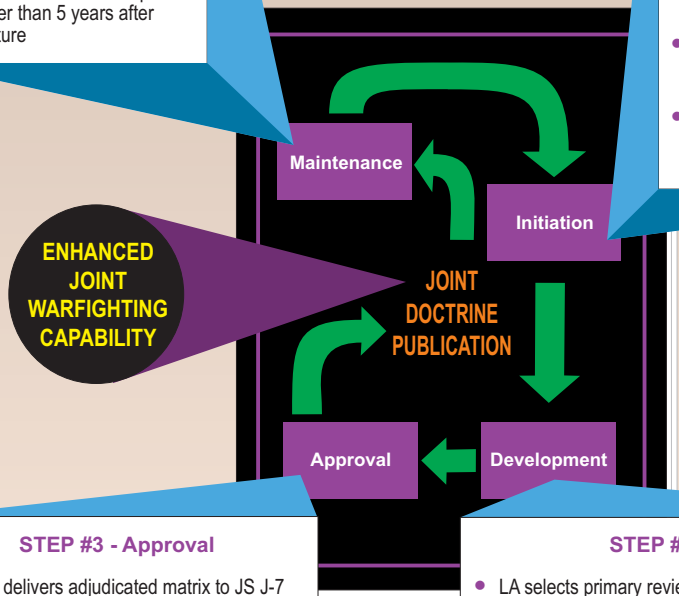
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 2-01** is in the **Intelligence** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

STEP #4 - Maintenance

- JP published and continuously assessed by users
- Formal assessment begins 24-27 months following publication
- Revision begins 3.5 years after publication
- Each JP revision is completed no later than 5 years after signature

STEP #1 - Initiation

- Joint doctrine development community (JDDC) submission to fill extant operational void
- Joint Staff (JS) J-7 conducts front-end analysis
- Joint Doctrine Planning Conference validation
- Program directive (PD) development and staffing/joint working group
- PD includes scope, references, outline, milestones, and draft authorship
- JS J-7 approves and releases PD to lead agent (LA) (Service, combatant command, JS directorate)



STEP #3 - Approval

- JSDS delivers adjudicated matrix to JS J-7
- JS J-7 prepares publication for signature
- JSDS prepares JS staffing package
- JSDS staffs the publication via JSAP for signature

STEP #2 - Development

- LA selects primary review authority (PRA) to develop the first draft (FD)
- PRA develops FD for staffing with JDDC
- FD comment matrix adjudication
- JS J-7 produces the final coordination (FC) draft, staffs to JDDC and JS via Joint Staff Action Processing (JSAP) system
- Joint Staff doctrine sponsor (JSDS) adjudicates FC comment matrix
- FC joint working group


JOINT
CHIEFS OF STAFF