Joint Publication 2-0

Joint Intelligence

26 May 2022
Incorporating Change 1
05 July 2024

PREFACE

1. Scope

This publication is the keystone document for joint intelligence. It provides the doctrinal foundation and fundamental principles that guide joint and national intelligence products, services, and assessments and support to joint 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 of the United States 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, combatant commands, subordinate unified commands, joint task forces, subordinate components of these commands, the Services, the National Guard Bureau, and combat support agencies.

b. This doctrine constitutes official advice concerning the enclosed subject matter; however, the judgment of the commander is paramount in all situations.

c. 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 United States, commanders should evaluate and follow the multinational command's doctrine and procedures where applicable and consistent with United States law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

STUART B. MUNSCH
Vice Admiral, United States Navy
Director, Joint Force Development

SUMMARY OF CHANGES
CHANGE 1 TO JOINT PUBLICATION 2-0
DATED 26 MAY 2022

- **Joint intelligence preparation of the operational environment content includes analysis of the civilian environment.**

- **Incorporates content to mitigate cognitive bias.**

- **Updates description of red team including assessment of the civilian environment.**

- **Simultaneously revises Joint Publication (JP) 2-0, *Joint Intelligence,* and consolidates the entire JP 2-0 series.**

- **Aligns content and maintains consistency with JP 3-0, *Joint Campaigns and Operations*, and JP 5-0, *Joint Planning*.**

- **Clarifies the distinction between estimative intelligence and information.**

- **Provides an update on intelligence organizations, responsibilities, and procedures.**

- **Updates and expands descriptions of the intelligence disciplines.**

- **Revises intelligence support to military operations across the competition continuum.**

- **Adds a classified appendix on the counterintelligence and human intelligence discipline and related Department of Defense (DoD) cover program.**

- **Adds discussions of a common operating picture and common intelligence picture.**

- **Includes analytical confidence levels based on Intelligence Community Directive 203, *Analytic Standards.***

- **Clarifies target intelligence as a subset of intelligence support to joint targeting.**

- **Includes a concise Joint Staff J-2 [Intelligence Directorate] planning checklist.**

- **Adds the Defense Intelligence Agency’s campaign intelligence estimate and how this product supports the joint planning process.**

- **Includes a description of collection orchestration as a component of DoD collection management.**

- **Revises the description of warning intelligence, based on DoD Instruction 3115.16, *The Defense Warning Network.***

- **Revises intelligence planning and assessment based on Chairman of the Joint Chiefs of Staff Instruction 3110.02, *Intelligence Supplement to the Joint Strategic Campaign Plan.***

TABLE OF CONTENTS

APPENDIX

GLOSSARY

FIGURE

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses the nature and role of intelligence in joint operations**
- **Describes roles and responsibilities of joint intelligence**
- **Presents the principles of joint intelligence**
- **Describes intelligence organizations, responsibilities, and procedures**
- **Discusses the joint intelligence process**
- **Discusses intelligence planning and assessment**

The Nature and Role of Intelligence

Introduction

Joint and national intelligence supports military operations across the competition continuum by providing information, operational intelligence, finished intelligence products, and joint targeting information to the combatant command (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 enemy's composition, disposition, strategy, tactics, intent, objectives, strengths, weaknesses, values, capabilities, and critical vulnerabilities. Intelligence also contributes heavily to understanding the operational environment (OE) through its physical, informational, and human aspects. The intelligence process is comprised of a variety of interrelated intelligence activities: planning and direction, tasking and collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback.

Roles and Responsibilities of Joint Intelligence

Role. The primary role of joint intelligence is to provide information, assessments, and estimates to the Chairman of the Joint Chiefs of Staff (CJCS), combatant commanders (CCDRs), subordinate commanders, and their staffs to support situational understanding and enable decision making.

Responsibilities

Inform the Commander. Intelligence directly supports the joint force commander (JFC) in planning, executing, and assessing the impact of campaigns and operations.

Describe the OE. Present the OE as a confluence of the conditions, circumstances, and influences that affect the behavior of relevant actors and employment of friendly, neutral, and enemy forces.

Identify, Define, and Nominate Objectives. All aspects of military planning are dependent on the determination of clearly defined, achievable, and measurable objectives.

Support the Planning and Execution of Campaigns and Joint Operations. Commanders and staffs at all levels require intelligence to plan, direct, conduct, and assess operations.

Counter Enemy Deception and Surprise. Joint force vulnerability to enemy denial and deception is determined, in large part, by the enemy's efforts to deny and deceive collection efforts.

Support Friendly Deception Efforts. Altering the perception of an enemy—to mislead or delude—helps achieve security and surprise.

Assess the Effectiveness of Operations. Intelligence helps evaluate military operations by objectively assessing their impact on the enemy, adversary, and other relevant aspects of the OE with respect to the JFC's intent and objectives.

Principles of Joint Intelligence

The following principles of joint intelligence are appropriate across the competition continuum:

- **Perspective**—Think Like the Identified Threat.
- **Synchronization**—Synchronize Intelligence with Plans and Operations.
- **Integrity**—Remain Intellectually Honest.
- **Unity of Effort**—Cooperate to Achieve a Common Objective.
- **Prioritization**—Prioritize Requirements Based on Commander's Guidance.

- **Excellence**—Strive to Achieve the Highest Standards of Quality.

Assessment of Risk in Predicting Threat Intentions. Although intelligence should identify and assess the full range of threat capabilities, it is most useful when it focuses on the future and intent of the threat and relevant actors.

Intelligence and the Levels of Warfare

Joint Publication 1, Volume 1, *Joint Warfighting,* discusses three levels of warfare: strategic, operational, and tactical.

Strategic intelligence is the process and product of developing the context, knowledge, and understanding of the strategic environment required to support United States (US) national security policy and planning decisions.

Operational intelligence focuses on answering the commander's priority intelligence requirements (PIRs) to support the commander and staff in assessing the effectiveness of campaigns and subordinate operations; monitoring assumptions; maintaining situational awareness (SA) of adversary and/or relevant actor military composition, disposition, and intentions; the information environment; and other relevant aspects of the OE.

Tactical intelligence is used by commanders, planners, and operators for planning and conducting a broad range of tactical activities supporting integrated operations.

Globally Integrated Operations

Actions taken in one CCMD area of responsibility (AOR) or functional responsibility can create unintended escalatory effects in other AORs. Intelligence should provide CCDRs awareness of the complex relationships associated with this global landscape to enable a globally integrated approach in support of strategic and operational objectives.

Competition Continuum

Rather than a world either at peace or at war, the competition continuum describes a world of enduring competition conducted through a mixture of cooperation, adversarial competition below armed conflict, and armed conflict or war.

Intelligence Organizations, Responsibilities, and Procedures

Introduction

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 advantage throughout the OE, enabling the successful conduct of operations.

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

Joint Intelligence

Joint Staff, Directorate for Intelligence

The Joint Staff J-2 [Intelligence Directorate] is under the authority, direction, and control of the CJCS and is resourced by the Defense Intelligence Agency (DIA). It provides all-source intelligence and intelligence staff support to the Secretary of Defense (SecDef), the CJCS, other Joint Staff directorates, CCMDs, and the Services.

Combatant Command Intelligence Organizations and Responsibilities

The **CCMD J-2** coordinates the intelligence structure and architecture, recommends and manages appropriate command relationships for intelligence assets, and supervises the production and dissemination of appropriate intelligence products while supporting the staff in developing strategy and planning operations and campaigns.

CCMD JIOC. Each CCMD and some subordinate unified commands have assigned JIOCs to integrate intelligence capabilities in support of the CCMD's mission.

Subordinate Joint Force Intelligence Organizations and Responsibilities

To accomplish the assigned mission, the subordinate joint force J-2 uses a combination of the following elements:

- **JISE.** At the joint task force (JTF) level, a JISE is normally established.

- **Operational-Level JIOC.** Alternatively, in a particularly large or protracted campaign, the commander, JTF, may decide to employ an operational-level JIOC.
- **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 counterintelligence (CI) by combining the HUMINT operations cell, the CI coordinating authority, a CI/HUMINT analysis and requirements cell, and an operations support element.
- **Geospatial Intelligence (GEOINT) Cell.** The JFC may establish a GEOINT cell to manage the tasks, actions, and events required to collect, analyze, and provide imagery, imagery intelligence, and geospatial information necessary to tactical navigation and joint targeting.
- **Sociocultural Analysis (SCA) Cell.** The JFC may establish an SCA cell to manage the tasks, actions, and events required to collect, analyze, and provide finished intelligence necessary to develop understanding and SA of the human aspects of the OE.
- **National Intelligence Agency Support.** The JFC, at the recommendation of the J-2, may request that national-level intelligence community (IC) analysts or subject matter experts deploy to support a JISE or operational-level JIOC.

National Intelligence Overview

The IC 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 Office of the Director of National Intelligence (ODNI) and 17 additional member organizations.

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 threats, events, and other worldwide intelligence requirements (IRs). The national intelligence organizations routinely provide support to the JFC while continuing to support national decision makers.

Department of Defense Intelligence and Combat Support Agency Organizations and Responsibilities

Under Secretary of Defense for Intelligence and Security (USD[I&S]). USD(I&S) serves as the principal staff assistant to SecDef and the Deputy Secretary of Defense regarding intelligence, CI, security, sensitive activities, and other intelligence-related matters.

Assistant to the Secretary of Defense for Intelligence Oversight (ATSD[IO]). ATSD(IO) is responsible for ensuring intelligence oversight policies and regulations are carried out by Department of Defense (DoD) organizations that perform intelligence functions in accordance with (IAW) Department of Defense Directive (DoDD) 5148.13, *Intelligence Oversight.*

National Joint Operations and Intelligence Center (NJOIC). The NJOIC is an integrated Joint Staff J-2/Joint Staff J-3 [Operations Directorate]/Joint Staff J-5 [Plans Directorate] element that continuously monitors the global situation and provides the CJCS and SecDef a DoD planning and crisis response capability.

DIA. DIA is an intelligence CSA under SecDef and a member of the national IC. The Director, DIA, reports to SecDef through the USD(I&S).

National Security Agency/Central Security Service (NSA/CSS). NSA/CSS provides signals intelligence and ensures the protection of national security systems. The National Security Agency is an intelligence CSA dual-tasked as a member of the national IC under the Director of National Intelligence (DNI).

National Geospatial-Intelligence Agency (NGA). NGA is a CSA and an element of the IC and is subject to the oversight of both SecDef and DNI.

National Reconnaissance Office (NRO). The NRO is a DoD agency and a member of the national IC. The Director, NRO, reports to both the DNI and SecDef.

Service Intelligence Organizations. The Service Chiefs 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 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.

ODNI is led by DNI and comprises several components, including the National Counterterrorism Center, the National Counterproliferation Center, the National Counterintelligence Executive, and the National Intelligence Council.

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

The **Federal Bureau of Investigation (FBI)**, as a member of the Department of Justice, 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 **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 Energy** analyzes foreign information that is relevant to US energy policies and nonproliferation issues to identify and mitigate threats to US national security and the Department of Energy enterprise.

The **Department of Homeland Security** 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's** Intelligence Coordination Center and maritime intelligence fusion centers operate under the direction of the Assistant Commandant for Intelligence.

The **Drug Enforcement Administration** is responsible for the collection, analysis, and dissemination of drug-related intelligence.

Joint and National Intelligence Support Forums

CCMD JIOCs. The CCMD JIOC is the first stop for CCMD staff, Service component commands, and subordinate joint force headquarters (HQ) IRs. For non-time-sensitive requirements, JIOCs receive requests for information (RFIs) from subordinate intelligence organizations through the community on-line intelligence system for end-users and managers (COLISEUM).

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.

DIA. DIA maintains senior representatives at each of the CCMDs; United States Forces, Korea; Supreme Headquarters Allied Powers Europe; and North Atlantic Treaty Organization (NATO) HQ.

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.

NGA Representatives. NGA provides representatives to the CCMDs, Services, and CSAs in the form of NGA support teams composed of staff officers, imagery analysts, and geospatial analysts.

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.

National Intelligence Support. National intelligence agencies can provide support to commanders during crisis or contingency operations.

Interoperability of Intelligence Systems and Processes

The Defense Intelligence and Security Enterprise is supported by a diverse array of capabilities providing documented processes and organizational structure, as well as information technology strategy, systems, networks, databases, and applications. These capabilities originate from the Services, CCMDs, and CSAs and are interoperable with diverse mission partners. The combination of these intelligence information capabilities, associated processes, and personnel enables the collection, processing, storage, dissemination, and management of information to joint and partner forces and support personnel.

Intelligence and the Department of Defense Information Network

The Department of Defense information network (DoDIN) enables intelligence and operations information and schematics to provide a common operational picture (COP) that facilitates interoperability between Service information systems and provides assured, secure, and tailorable information on demand to all appropriate users. DIA establishes DoD-wide intelligence priorities to achieve interoperability among the tactical, theater, and national intelligence systems and their respective communications systems at each level.

Interagency, International, and Multinational Intelligence Sharing

Principles for Multinational Intelligence Sharing

In most multinational operations, the JFC shares intelligence with foreign military forces and coordinates receiving intelligence from those forces. Intelligence efforts should complement and take into consideration the intelligence system's strengths, limitations, and each nation's unique and valuable capabilities. In some multinational operations or campaigns, JFCs can use existing international standardization agreements (e.g., NATO) as a basis for establishing rules and policies for conducting joint intelligence operations. Since each multinational operation is unique, such agreements may have to be modified or amended based on the situation. The joint force should consider releasability of information to allies (e.g., NATO) and trusted and vetted partner nations (PNs) as this approach facilitates expedited information sharing.

Multinational Intelligence Collaboration

Typically, in a multinational operation, allied military intelligence counterparts may locate or co-locate around the JTF HQ in the form of national intelligence cells and may contribute to the multinational intelligence fusion cell that develops the combined intelligence picture. The JTF/J-2 should establish good working relationships with multinational partners to encourage a shared view of the OE and their contributions to the combined intelligence picture. Allied nations also bring valuable intelligence contributions and can often provide niche capabilities in support of the overall JTF mission.

Synchronization of International Efforts

Synchronizing United States Government departments and agencies with joint or multinational military operations, international organizations, nongovernmental organizations, and contractors enables US forces to gain access to specialized knowledge or insight and understanding that these organizations possess.

Interorganizational Intelligence Collaboration

The role of DoD intelligence elements in an operation involving interagency partners is dictated by the nature of the support relationship. DoD intelligence organizations should expect to operate alongside interagency partners as needed to conduct authorized intelligence functions in support of operations conducted in the homeland IAW Executive Order 12333, *United States Intelligence Activities;* DoDD 5240.01, *DoD Intelligence Activities;* and DoD Manual 5240.1, *Procedures Governing the Conduct of DoD Intelligence Activities.*

The Joint Intelligence Process

Introduction

The joint intelligence process consists of six interrelated categories of intelligence operations characterized by broad activities conducted by intelligence staffs and organizations for the purpose of providing commanders and national-level decision makers with relevant and timely intelligence. The six categories of intelligence operations include planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback.

The Intelligence Process

The intelligence process describes how the various types of intelligence activities 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 activities and their interrelationships.

Joint Intelligence Preparation of the Operational Environment (JIPOE). JIPOE is the analytical process joint intelligence organizations use to produce intelligence assessments, estimates, and other intelligence products in support of the JFC's decision-making process.

Planning and Direction

Overview

The planning and direction portion of joint intelligence operations occurs continuously as the intelligence component of a command's planning effort across the competition continuum.

Intelligence Requirements and Information Requirements Planning

CCMD- and JTF-level intelligence planners lead intelligence planning (IP) teams to define, recommend the priority of, and analyze/decompose IRs. They participate in planning and decision-making processes to receive guidance and help focus the intelligence effort.

Intelligence Planning

As the intelligence component of the joint planning process (JPP), IP provides a methodology to coordinate, integrate, and synchronize all available intelligence capabilities to meet the commander's IRs for joint planning, execution, and assessment. It ensures the intelligence system is focused on providing the commander with the intelligence required to make timely, informed decisions that lead to desired effects and achieve operational objectives.

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.*

Requesting National Intelligence

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 should be prepared and submitted.

Collection Management

Principles of Collection Management. If, during the conduct of operations, it is determined that an RFI must be converted into a collection requirement (CR), a nomination for collection is submitted and collection management begins. Collection management is the process of converting intelligence-related information requirements into CRs, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. Anchored on the appropriate collection management authority, collection management is composed of two functions, collection requirements management and collection operations management, and requires collection orchestration.

Collection

Overview of Theater-Level and Below Collection

Collection operations acquire raw data and information about relevant aspects of the OE and provide that information to intelligence processing and exploitation elements.

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 is requested and coordinated through the chain of command of the unit that directs and controls them.

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

Collection Assets and Resources

Collection assets and resources can be categorized by three types: technical collection (not to be confused with technical intelligence [TECHINT]), human-based collection, and a combination of technical and human-based collection.

Measurement and Signature Intelligence

Measurement and signature intelligence (MASINT) provides technically derived intelligence to detect, locate, and describe the specific characteristics of targets. As an integral part of the all-source collection effort, MASINT can provide unique and complementary information to satisfy the information requirements of commanders.

Technical Intelligence

TECHINT is derived from the exploitation of foreign materiel, collected exploitable material, and scientific information. TECHINT begins with the acquisition or recovery of a foreign piece of equipment or foreign scientific/technological information.

Counterintelligence

CI is conducted to identify, deceive, exploit, disrupt, or protect against espionage, sabotage, assassinations, or other intelligence activities conducted by organizations or persons on behalf of foreign powers or international terrorist organizations.

Analysis and Production

Overview

Intelligence is produced through the integration, evaluation, analysis, and interpretation of information from a single source or from multiple sources. Intelligence results from analysis and production, which is accomplished in response to expressed and anticipated user requirements.

Conversion of Information into Intelligence

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 production requirements (PRs).

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.

Databases and Virtual Knowledge Bases

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.

All-Source Product Categories

Intelligence products are generally placed in one of eight all-source production categories: warning intelligence, current intelligence, general military intelligence, target intelligence, scientific and technical intelligence, CI, estimative intelligence, and identity intelligence. The categories are distinguished from each other primarily by the purpose for which the intelligence is produced. The categories can and do overlap, and some of the same intelligence and information can be found and used by analysts in each of the categories.

Support to Operational Commanders

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 Responsibilities

Production centers at all levels are assigned clearly delineated areas of analytical responsibility. 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.

Request Production 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, target materials, 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 Defense Intelligence Analysis Program procedures for registration and assignment of RFIs and subsequent tracking of the RFIs.

Prioritizing Requirements

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.

Dissemination and Integration

Overview

Intelligence support to command and control (C2) is the primary vehicle for integrating intelligence and operations. Intelligence support to C2 encompasses intelligence systems; networks; functions; activities; personnel; processes; tactics, techniques, and procedures; data; and products that support C2 via a common intelligence picture (CIP). Together, the COP and its CIP deliver the SA necessary to enable information advantage, promote unity of effort, and enable decisive combat advantage.

Dissemination Methods

Digital dissemination has become the predominant method of communicating finished intelligence products to the consumer. Most 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.

Hard Copy Dissemination. 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.

Integration of Intelligence and Operations

Information advantage requires the timely integration of intelligence and meteorological and oceanographic (METOC) information 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 continuous integration of intelligence, METOC information, and operations allows commanders and all operational planners access to the most current information available, thereby optimizing intelligence and METOC support to C2 and planning. The combined COP and CIP is the nexus of intelligence and operations integration.

Evaluation and Feedback

Overview

Intelligence personnel should assess the execution of the intelligence tasks they perform and gauge their impacts. Evaluation and feedback require a collaborative dialogue between intelligence planners, collection managers, collectors, single and all-source analysts, and intelligence systems architects to identify deficiencies within the intelligence process.

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.

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.

Assessment

Information gathered during evaluation and feedback may inform broader assessments of the intelligence joint function. Assessments provide leaders with the information to make decisions about reprioritization of IRs, shifts in collection emphasis, changes to analytic levels of effort, reallocation of available intelligence assets, training of intelligence personnel, and the development of new intelligence capabilities.

Intelligence Planning and Assessment

Intelligence Planning

Overview

The planning of joint operations is accomplished through the JPP. The IP process is conducted by the organizations within the DoD component of the IC. IP is the structured integration and management support to the Joint Strategic Planning System (JSPS) and JPP and is executed through an established methodology to coordinate and integrate available Defense Intelligence and Security Enterprise capabilities in support of CJCS direction and the problem set's coordinating authority or lead CCDR's plans or orders. IP involves planning and directing DoD intelligence operations and collaboration with interagency partners and IC, allied, and PN intelligence organizations to achieve integrated intelligence support during execution of contingency and campaign plans to align with objectives of an operation.

Joint Planning

Joint planning consists of four functions (strategic guidance, concept development, plan development, and plan assessment), the JPP, and an operational design methodology.

During the JPP, CCMD J-2s lead development of annex B (Intelligence). Annex B is the intelligence annex to a plan or order that provides detailed information on the threat 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.

The Intelligence Planning Process

Intelligence Planning Activities

IP activities are generally organized along two distinct lines: providing intelligence to joint planning and planning intelligence operations.

Providing Intelligence to Joint Planning. IP activities supporting the JSPS include the production of intelligence assessments and estimates of enemy intentions, capabilities, and courses of action (COAs). Specific intelligence outputs of the JSPS are the DIA-produced dynamic threat assessment (DTA), or xcampaign intelligence estimate (xCIE), and the development of tailored products from the CCMD's JIPOE process that culminate in the production and maintenance of the intelligence estimate.

Planning Intelligence Operations through the JPP. IP activities in the JPP include identifying information gaps, prioritizing IRs, developing federated production and integrated collection plans, and assessing intelligence capabilities for the purpose of identifying shortfalls and mitigation strategies.

Intelligence Planning Activities During Strategic Guidance

IP Activities Providing Intelligence to Joint Planning

- DIA will validate, update, or produce a DTA or an xCIE.
- At the CCMD level and below, intelligence planners orchestrate the command's continuous JIPOE effort for analysts to provide a baseline assessment of the OE, enemy capabilities, objectives and associated centers of gravity, critical capabilities, critical requirements, critical vulnerabilities, and COAs and related decisive points.

IP Activities While Planning Intelligence Operations

- Intelligence planners assemble an intelligence planning team (IPT) or similar community of interest with all-source analysts and collection strategists as its core members.
- The IPT develops an IP timeline that is synchronized with the command's planning timeline.
- To generate the J-2 staff estimate, the IPT, in coordination with representatives from Service components and subordinate joint force commands, identifies and analyzes all intelligence capabilities of assigned forces available to support the execution of the plan.
- The IPT evaluates current theater collection and production postures to identify available assets that may need to be redirected to support the planning effort or the execution of the plan under consideration.
- Based on the list of all available intelligence capabilities, the IPT drafts and submits the initial J-2 staff estimate to the joint planning group (JPG) to support the command's overall force structure analysis.
- Considering all of the identified intelligence gaps relevant to the planning effort and recognizing the uncertainties in analytical conclusions, intelligence planners, in collaboration with the JPG, may nominate additional planning assumptions and initial PIRs for validation during the current planning cycle.

Intelligence Planning Activities During Concept Development

IP Activities Providing Intelligence to Joint Planning

- Intelligence planners evaluate JIPOE products to be disseminated to the JPG. The intelligence planner or the analyst presents these products to the JPG IAW the established planning timeline.
- Intelligence planners coordinate personnel to participate in COA analysis and wargaming.

IP Activities While Planning Intelligence Operations

- During COA development, intelligence planners consider how theater intelligence assets and external intelligence resources could be employed to support the execution of the plan.

- The intelligence planner revises the J-2 staff estimate capturing additional factors, unique to each of the proposed friendly COAs, which may limit the employment of intelligence capabilities.
- The intelligence planner consolidates final PIR nominations from across the staff and drafts PIRs as required to support CCDR decisions.
- Following COA approval, the intelligence planner, in collaboration with the IPT, develops essential elements of information (EEIs) and associated indicators required to satisfy the PIR.
- Coordinate with CCMD geospatial information and services (GI&S) personnel to identify GI&S support necessary for selected COA.
- Based on IRs (to include PIRs), information requirements (to include EEIs), their associated indicators, and anticipated specific information requirements, the IPT then generates a matrix of anticipated PRs to guide the development of federated production plans and a matrix of anticipated CRs to guide the development of integrated collection plans.
- The Joint Staff J-2, in coordination with the CCMD J-2, determines when a national intelligence support plan is required for each integrated contingency plan and will task development based on all of the CCMD J-2 staff estimates.

Intelligence Planning Activities During Plan Development

IP Activities Providing Intelligence to Joint Planning

- The JIOC's analytical cell completes the intelligence estimate.

IP Activities While Planning Intelligence Operations

- Intelligence planners develop the base annex B (Intelligence), which outlines the intelligence mission; concept of intelligence operations; PIRs; and guidance for how collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback will be performed during execution.
- Intelligence planners evaluate whether targeting is necessary to accomplish the operation. If so, the IPT facilitates target systems analysis, target development, and target list management.

- Intelligence planners collaborate with discipline-specific managers and other subject matter experts to develop required functional appendices to annex B (Intelligence)

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.

Plan Assessment and Execution

Intelligence Support to Plan Assessment and Decision Making

Continual and timely assessments are essential to measure progress of the joint force toward achieving objectives. Commanders continuously assess the OE and the progress of their operations and campaigns and then compare them to their initial vision and intent.

Assessment actions and measures help commanders adjust operations and align future operations strategic- and operational-level assessment efforts concentrate on broad tasks, effects, objectives, and progress toward the end state, while tactical-level assessment focuses on specific task accomplishment. Normally, the joint force J-2 assists the J-3 [operations directorate of a joint staff] or J-5 [plans directorate of a joint staff] in coordinating assessment activities.

The assessment process is continuous and linked to the commander's critical information requirement process by the commander's need for timely information and recommendations to make decisions throughout the operation or campaign.

Intelligence and the Assessment Process

The assessment process uses measures of performance (MOPs) to evaluate task performance at all levels of warfare and measures of effectiveness (MOEs) to determine progress of operations toward achieving objectives. MOPs are used to measure task accomplishment and answer the questions "was the action taken, were the tasks completed to standard?" to produce the desired effect. MOEs are used at the strategic-, operational-, and tactical-level intelligence staffs to assess changes in the threat's behavior, capabilities, or the OE. MOEs help answer questions like: "are we doing the right things, are our actions producing the desired effects, or are alternative actions required?"

Intelligence Support to Strategic and Operational-Level Assessment

Strategic- and operational-level assessment efforts concentrate on broad tasks, effects, and progress toward objectives. Continuous assessment helps the JFC and joint force component commanders determine if the joint force is "doing the right things" to achieve objectives, not just "doing things right," and if executing the correct actions are creating the required effects against the adversary or enemy.

Tactical-Level Assessment

The results of tactical tasks are often physical in nature but can also reflect the impact on specific functions and systems. Tactical-level assessment may include assessing progress by geographic phase lines; neutralization of enemy forces; control of key terrain, people, or resources; and security or reconstruction tasks.

Intelligence Support to Joint Operations Across the Competition Continuum

General

Intelligence support is crucial to all aspects of military operations across the competition continuum because it identifies changes in the strategic and operational environment that may reveal opportunities or signal an emerging crisis.

Global Campaign Plans

A prerequisite to preparing a long-term campaign is the development of a strategic estimate containing factors and trends that influence the CCDRs' AORs. This estimate informs the relationship between ends, ways, means, and risks involved in the conduct of CJCS Instruction 3110.01, *(U) 2018 Joint Strategic Capabilities Plan (JSCP)*-directed global campaign plans. Intelligence activities support the CCDRs' strategic estimates.

Intelligence liaison and the establishment of intelligence-sharing arrangements with multinational partners are critical aspects of global campaign execution. Whenever possible, and in coordination with the responsible ODNI representative, JFCs should coordinate with PNs by ensuring the participation of US personnel in mutual intelligence training; temporary exchanges of intelligence personnel; federated intelligence arrangements; and the integration and exercise of intelligence, surveillance, and reconnaissance support architectures.

Crisis and Contingency Response

If an evolving situation exceeds the scope of the global campaign, the joint force senior leadership will begin to organize around the problem through a more comprehensive analysis. Intelligence informs senior joint leadership, to include the likely supported and supporting commanders, enabling them to diagnose all the situational factors, range of possible outcomes, likely long-term consequences, and begin to form a globally integrated approach of all the joint force capabilities. The IC updates intelligence estimates based on changes resulting from operation and campaign activities.

Intelligence During Stabilization and Transitions

Campaign requirements for support to stabilization can occur anywhere along the competition continuum and be unassociated with armed conflict. However, the particular demands of the transition from armed conflict to the new competition are complex and can require continued significant military involvement, to include some combat operations for years. As commanders make progress, military forces may increase their focus on supporting the efforts of host-nation authorities, but achieving and maintaining the strategic objectives is the priority.

CONCLUSION

This publication is the keystone document for joint intelligence. It provides the doctrinal foundation and fundamental principles that guide joint and national intelligence products, services, and assessments and support to joint operations.

CHAPTER I
THE NATURE AND ROLE OF INTELLIGENCE

> *"By 'intelligence' we mean every sort of information about the enemy and his country—the basis, in short, of our own plans and operations."*
>
> **Carl von Clausewitz**
> ***On War*, 1832**

1. Introduction

Joint and national intelligence supports military operations across the competition continuum by providing information, operational intelligence, finished intelligence products, and joint targeting information to the combatant command (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 enemy's composition, disposition, strategy, tactics, intent, objectives, strengths, weaknesses, values, capabilities, and critical vulnerabilities. Intelligence also contributes heavily to understanding the operational environment (OE) through its physical, informational, and human aspects. The intelligence process is comprised of a variety of interrelated intelligence activities: planning and direction, tasking and collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback (see Figure I-1). These intelligence activities should focus on the commander's mission and support the commander's decision-making process.

a. The management and integration of intelligence into military operations are inherent responsibilities of command. These responsibilities are performed at every echelon of command during all military operations and performed continuously in support of military campaigns and operations. Intelligence enables joint force and component commanders and their staffs access to critical information that characterizes the OE—the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. The OE consists of the physical domains of air, land, maritime, and space; the information environment (IE) (which includes cyberspace); and the electromagnetic OE. This includes a wide range of issues relating to friendly, neutral, adversary, and enemy forces and the civilian populace, including information concerning weather, terrain, and cultural influences. A critical function of intelligence is to identify the relevant actors in the OE. This includes the individuals, groups, populations, or automated systems whose capabilities or behaviors can affect the success of a particular campaign, operation, or tactical action. Through analysis, this mass of information is distilled into intelligence to support a predictive estimate of the situation that describes the capabilities and intentions of all threats within the OE. The estimative nature of intelligence distinguishes it from the mass of other information available to the commander.

For a detailed discussion of the intelligence process, see Chapter III, "The Joint Intelligence Process."

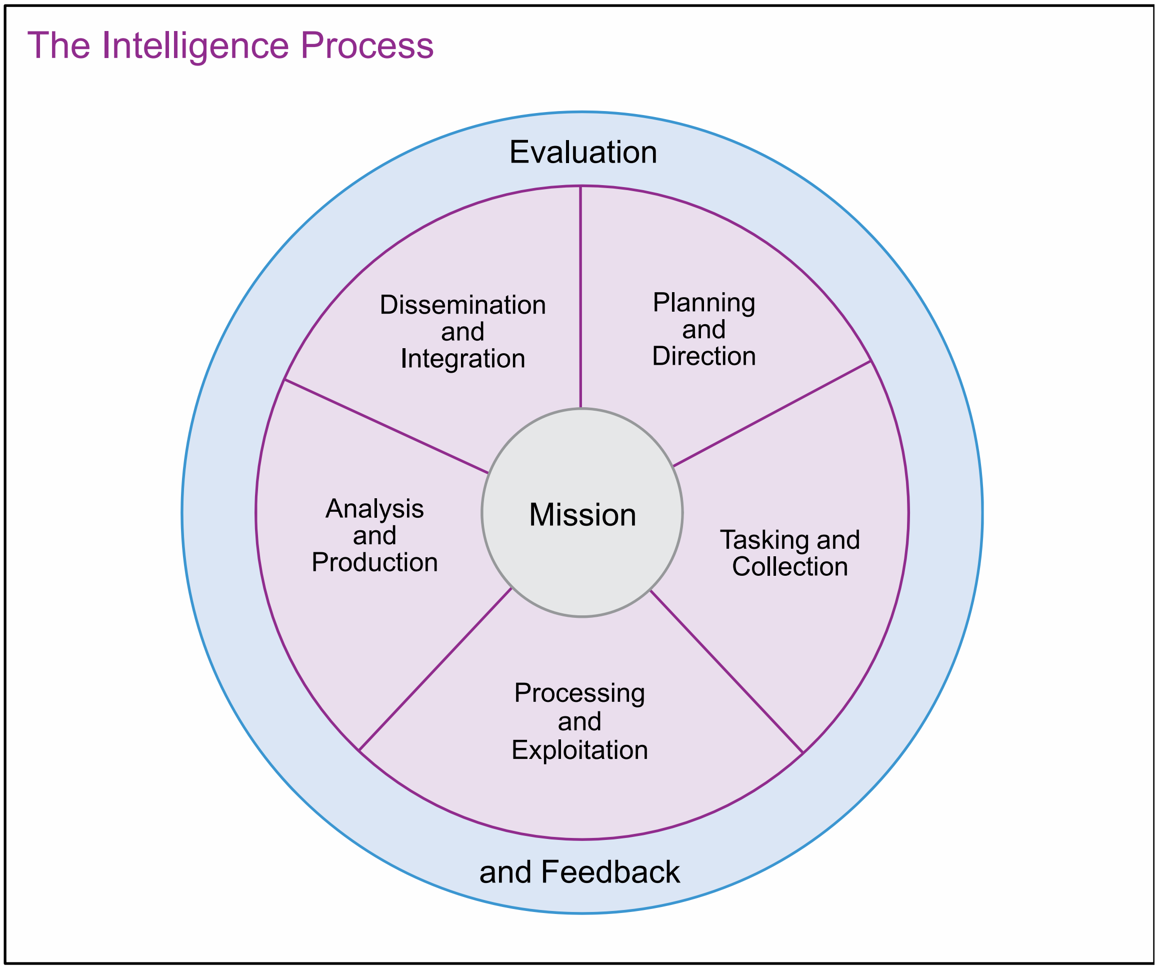


Figure I-1. The Intelligence Process

b. Intelligence is of greatest value when it contributes to the commander's decision-making process by providing insight into future conditions or situations. While raw data by itself can be useful, when collected information is processed, integrated, evaluated, and exploited, it gains greater utility. The foundation of the process that produces intelligence is built by analysts relating or comparing information against other information or existing intelligence and drawing new conclusions. The relationship between data, information, and intelligence is graphically depicted in Figure I-2. Ultimately, intelligence has three critical features that distinguish it from information. First, intelligence fuses (or integrates) and evaluates information from multiple sources to provide the most accurate assessment possible of the current state of the OE. Second, from current assessments, intelligence draws predictive estimates of the full range of potential alternative future states of the OE. Third, to inform decisions regarding the adoption of friendly courses of action (COAs), intelligence illuminates how the OE may react to different friendly options under consideration.

WHAT IS INFORMATION?

Information is data in context to which an observer assigns meaning. Data useful to characterizing the environment contribute to information.

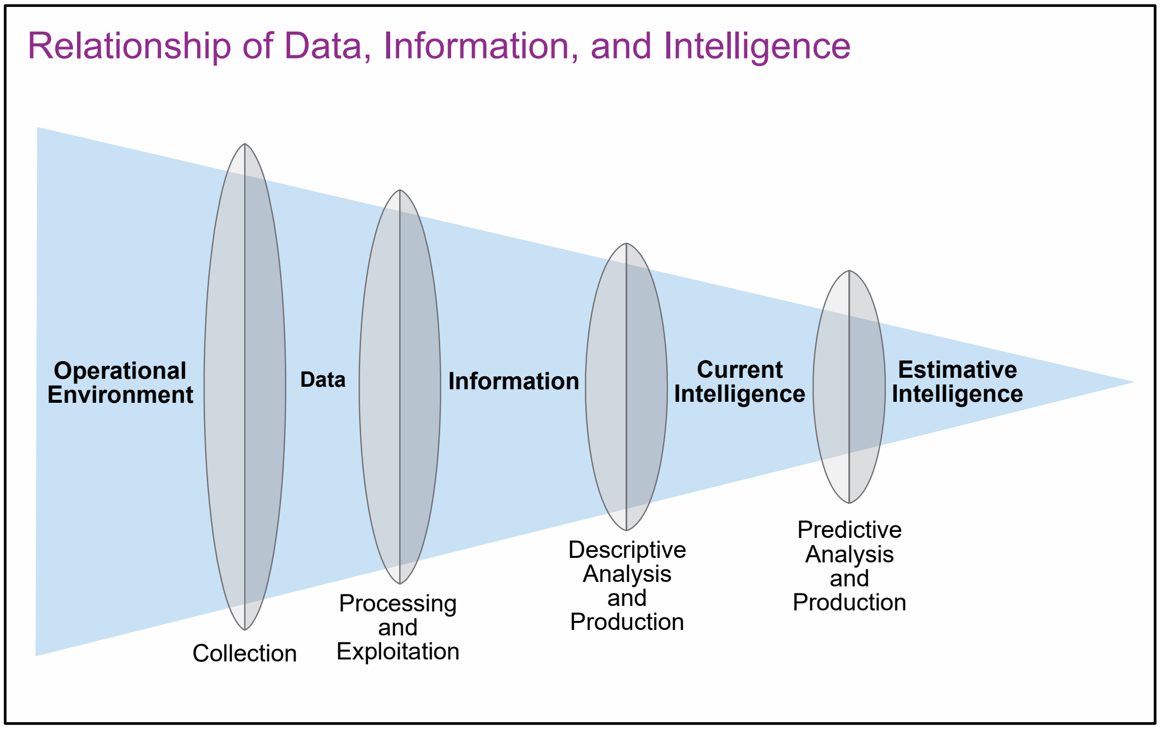

Relationship of Data, Information, and Intelligence
Operational Environment
Data
Information
Current Intelligence
Estimative Intelligence
Collection
Processing and Exploitation
Descriptive Analysis and Production
Predictive Analysis and Production

Figure I-2. Relationship of Data, Information, and Intelligence

c. Intelligence supports all the instruments of national power. Within the military instrument of national power, intelligence is one of the joint functions—related capabilities and activities grouped together to help the joint force commanders (JFCs) integrate, synchronize, and direct joint operations—along with command and control (C2), information, fires, movement and maneuver, protection, and sustainment. Intelligence serves as a critical enabler to all joint functions by continuously providing commanders and their staffs a holistic appreciation of the OE to inform operational design and planning, future intelligence estimates against which to plan joint military operations, and current intelligence to assess the impacts of those operations in relation to desired effects and objectives. Intelligence provides the commander a variety of assessments and estimates that facilitate understanding the OE. Assessments are situational. For example, some assessments will be threat-based, providing an analysis of threat capabilities and dispositions; others are population-based, providing the commander an analysis of sociocultural factors; and still others may be based on specific physical and nonphysical aspects of the OE. Through timely, accurate, and relevant intelligence estimates, commanders gain a temporal decision advantage in the OE by understanding a threat's decision-making cycle and anticipating and countering the threat's operations, intentions, and the full range of alternative futures in relative order of probability. Thus, intelligence estimates give commanders and their staffs the time needed to assess risks, develop plans, and direct the execution of effective military operations before the opportunity to do so expires.

d. Intelligence is not an exact science. As intelligence analysts assess the OE, there is some degree of uncertainty. This uncertainty is a factor for the commander and staff as they plan and execute operations. Intelligence, as the synthesis of quantitative analysis and qualitative judgment, is subject to competing interpretation. It is, therefore, important that intelligence analysts communicate the degree of confidence they have in their analytic conclusions. Analytic confidence helps intelligence consumers to decide how much weight to place on intelligence assessments when making a decision. One methodology intelligence personnel may use to assign a confidence level to their analytic conclusions or intelligence assessments is discussed in Appendix A, "Analytic Standards."

e. Intelligence includes the organizations, capabilities, and processes used in the tasking, collection, processing, analysis, exploitation, and reporting of single-source intelligence, as well as information from intelligence, surveillance, and reconnaissance (ISR) assets, and the analysis, production, and dissemination of all-source finished intelligence. To increase the operational relevance of intelligence, intelligence planners and managers anticipate consumer needs. Thus, an assessment of whether intelligence is effective or influential not only depends on the intelligence organizations, processes, and products but also examines users' intelligence needs. The intelligence staff supports users by evaluating and tailoring the language of their intelligence requirements (IRs). Explicit user requirements identified and properly communicated to intelligence organizations initiate the appropriate intelligence activities. Intelligence products provide users with information collected and analyzed based on their requirements. Intelligence is a continuous activity or cycle that is a planned and coordinated process to synchronize activities to gather information, target adversaries, the enemy, other relevant actors, and support OE analysis and operational awareness.

"(5) The terms "national intelligence" and "intelligence related to national security" refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that—

(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and

(B) that involves—

(i) threats to the United States, its people, property, or interests;

(ii) the development, proliferation, or use of weapons of mass destruction; or

(iii) any other matter bearing on United States national or homeland security."

Source: Title 50, United States Code, Section 3003

2. Roles and Responsibilities of Joint Intelligence

a. **Role.** The primary role of joint intelligence is to provide information, assessments, and estimates to the Chairman of the Joint Chiefs of Staff (CJCS), combatant commanders (CCDRs), subordinate commanders, and their staffs to support situational understanding and enable decision making (see Figure I-3). Intelligence constitutes one of seven joint

Role and Responsibilities of Joint Intelligence

Role:

Provide information, assessments, and estimates to commanders and their staffs to support situational understanding and enable decision advantage.

Responsibilities:

- Support the planning of operations
  - Describe the operational environment (OE)
  - Provide estimates of adversary capabilities, intentions, and courses of action
  - Analyze target systems and identify their vulnerabilities
  - Identify, define, and nominate objectives
- Support the execution of operations
  - Monitor the OE
  - Provide warnings
  - Enable physical and nonphysical engagements against designated targets
- Assess the effectiveness of operations
  - Perform battle damage assessment
  - Measure changes to adversary capabilities, system behavior, and the OE

Figure I-3. Role and Responsibilities of Joint Intelligence

functions. Other joint functions include C2, information, fires, movement and maneuver, protection, and sustainment.

b. **Responsibilities**

(1) **Inform the Commander.** Intelligence directly supports the JFC in planning, executing, and assessing the impact of campaigns and operations. The intelligence directorate of a joint staff (J-2) analyzes the threat and other relevant aspects of the OE and produces assessments on a continuing basis to support the commander in creating and/or exploiting opportunities to accomplish friendly force objectives. For example, to maintain the initiative, the JFC will seek to understand and potentially influence the threat's decision-making process (e.g., the JFC will seek the latest intelligence that will enable friendly forces to take effective action faster than the threat). The J-2 should assess the characteristics of the threat's decision-making process and identify weaknesses that may be exploited. The J-2 should disseminate intelligence in a timely manner to the JFC, staff, and components.

(2) **Describe the OE.** Present the OE as a confluence of the conditions, circumstances, and influences that affect the behavior of relevant actors and employment of friendly, neutral, and enemy forces. Describing this OE to the commander and staff affects the commander's COA assessment, as well as future operations.

(3) **Identify, Define, and Nominate Objectives.** All aspects of military planning are dependent on the determination of clearly defined, achievable, and measurable objectives. When identifying and nominating objectives, the J-2 should understand the

command's responsibilities; the JFC's mission and intent; means available, including host-nation and multinational forces, interagency partners, nongovernmental organizations (NGOs), and international organizations; the threat; weather impacts; and characteristics of the operational area. Many objectives, especially in strategic competition, can be expressed in terms of the desired behavior and decision-making process of relevant actors. Intelligence should increase the commander's understanding of the relevant actors' self-perceived interests, goals, influencers, vulnerabilities, and opportunities, to include the enemy's probable intentions, objectives, most likely and most dangerous COAs, strengths, and critical capabilities. Thus, the J-2 has a critical perspective on identification of objectives, requirements, and centers of gravity (COGs). Once objectives are approved by the commander, the J-2 continuously reviews them with respect to the threat and the changing situation to determine whether they remain relevant to the commander's intent.

(4) **Support the Planning and Execution of Campaigns and Joint Operations.** Commanders and staffs at all levels require intelligence to plan, direct, conduct, and assess operations. This intelligence is crucial to commanders, staffs, and components in identifying and selecting specific objectives and targets, associating them with desired effects, and determining the means to accomplish the JFC's overall mission. The J-2 participates in the development of campaign and contingency plans. The J-2 supports the execution of the plan with the strategic, operational, and tactical intelligence needed to sustain the operation.

(5) **Counter Enemy Deception and Surprise.** Joint force vulnerability to enemy denial and deception is determined, in large part, by the enemy's efforts to deny and deceive collection efforts. Intelligence analysts should remain sensitive to the possibility that they are being deceived and should consider all possible enemy capabilities and intentions. Similarly, analytical approaches that emphasize anomalies characterized by a lack of activity (e.g., absence of seasonal training, important persons missing from ceremonial events) are particularly valuable. To counter enemy deception efforts, intelligence analysts confirm their analysis using multiple analytical methods and processes (e.g., use of red teams, devil's advocates, alternative hypotheses).

(6) **Support Friendly Deception Efforts.** Altering the perception of an enemy—to mislead or delude—helps achieve security and surprise. Intelligence and counterintelligence (CI) support effective friendly planning efforts through sociocultural analysis (SCA) of enemy leadership characteristics. The J-2 also assesses how the enemy is reacting to the friendly deception effort. Identifying deception objectives to complement operational objectives should be an interactive process, which is aided by the use of a red team or red cell.

(7) **Assess the Effectiveness of Operations.** Intelligence helps evaluate military operations by objectively assessing their impact on the enemy, adversary, and other relevant aspects of the OE with respect to the JFC's intent and objectives. Intelligence should assist JFCs in determining if operations are producing desired or undesired effects, when objectives have been achieved, and when unforeseen opportunities can be exploited or require a change in planned operations.

3. Principles of Joint Intelligence

a. Intelligence theory and operational experience combine to establish fundamental principles that are intended to contribute to effective and successful joint intelligence activities. The following principles of joint intelligence are appropriate across the competition continuum (see Figure I-4).

(1) **Perspective—Think Like the Identified Threat.** Intelligence analysts must strive to understand all relevant aspects of the OE. This understanding must include not only the threat's disposition but also the sociocultural nuances of relevant actors. One analytic technique is to assess all proposed actions from the following perspective: "How will the threat likely perceive this action, and what are the threat's probable responses?" Analysts must remember that, even if a threat or other relevant actor is performing an action that seems irrational from a United States (US) perspective, the threat or other relevant actor has a logical reason for its actions from its standpoint. Analysts must place themselves in the other's viewpoint and endeavor to not only understand their goals and biases but the reasons that those goals and biases exist.

(a) The ability to think like the adversary or other relevant actor is predicated on a detailed understanding of their perception of issues, goals, influencers, vulnerabilities, and opportunities. These manifest in the form of motivations, objectives, strategy, intentions, capabilities, methods of operation, vulnerabilities, sense of value and loss, and the effects they have on their own assessment of risk. The J-2 should understand the social systems and cultures of and relevant actors in the OE. The ability of intelligence analysts to understand sociocultural factors is of particular value when wargaming various COAs and determining high-value individuals and high-value targets (HVTs).

(b) Understanding an adversary or relevant actor's decision-making process and how those processes may adapt to changes in the environment should be an integral

Principles of Joint Intelligence

- Perspective (Think like the threat.)
- Synchronization (Synchronize intelligence with plans and operations.)
- Integrity (Remain intellectually honest and aware of biases.)
- Unity of Effort (Cooperate to achieve a common objective.)
- Prioritization (Prioritize requirements based on commander's guidance.)
- Excellence (Strive to achieve the highest standards of quality.)
- Assessment of Risk (Accept the risk of anticipating the threat's intentions.)
- Agility (Remain flexible and adapt to changing situations.)
- Collaboration (Leverage expertise of diverse analytic resources.)
- Fusion (Exploit all sources of information and intelligence.)

Figure I-4. Principles of Joint Intelligence

part of a continuing interaction of the intelligence staff with the JFC, other staff elements, interagency, and multinational partners.

(2) **Synchronization—Synchronize Intelligence with Plans and Operations.** Intelligence should be synchronized with plans and operations to provide timely answers to IRs and influence the decision they are intended to support. Intelligence synchronization requires all intelligence sources and methods be applied in concert with the operation plan (OPLAN) and operation order (OPORD). OPLAN and OPORD requirements, therefore, constitute the principal driving forces that dictate the timing and sequencing of intelligence operations. Intelligence planning (IP) and direction, collection, processing and exploitation, analysis and production, and dissemination should all be accomplished with sufficient lead time to permit the integration of the intelligence product in operational decision making and plan execution. Intelligence evaluation and feedback from commanders, operators, and intelligence personnel must also be timely to keep intelligence operations focused to support the commander's plan and intent. Effective synchronization results in the maximum use of all intelligence at a time and place to make the greatest contribution to the mission.

(a) The most common error in attempting to synchronize intelligence with plans and operations is the failure to build sufficient lead time for intelligence production, baseline operation assessment, and operational decision making. To ensure the usefulness and relevancy of intelligence, the JFC, operations directorate of a joint staff (J-3), and the plans directorate of a joint staff (J-5), in collaboration with the J-2, should establish a suspense or specify a timeframe during which each IR must be answered to support planning, decision making, and execution. Likewise, the J-2 should provide sufficient lead time for the collection, processing, analysis, and dissemination of the requisite intelligence to meet the commander's specified deadline. To facilitate synchronization, the J-2 should be involved as early as possible in planning and play an active role during the wargaming and analysis of all COAs and plans.

(b) The commander drives the intelligence synchronization effort by determining the friendly COA, priority intelligence requirements (PIRs), and points in time and space (decision points) where critical events and activity would necessitate a command decision. Decision points may be identified on an event template developed during the joint intelligence preparation of the operational environment (JIPOE) process. The event template provides the operational context for PIR development, optimized collection planning, and the formulation of an intelligence synchronization matrix (ISM). The event template evolves into the decision support template during COA analysis.

(3) **Integrity—Remain Intellectually Honest.** Intellectual integrity, objectivity, and moral courage are the hallmarks of the intelligence profession. They are the cardinal elements in intelligence analysis and reporting, as well as the foundation on which credibility with the intelligence customer is built. Integrity and objectivity require adherence to facts and truthfulness with which those facts are interpreted and presented. Moral courage is required to remain intellectually honest and to resist the pressure to reach intelligence conclusions that support predetermined assumptions despite an analysis of relevant facts. The methodology, production, and use of intelligence should not be directed

or manipulated to conform to a desired result; institutional position; preconceptions of a situation or a threat; or predetermined objective, operation, or method of operations. Intelligence analysts should take active measures to recognize and avoid cognitive biases that affect their analysis.

(a) Intelligence analysts continuously guard against cognitive biases common to intelligence (e.g., anchoring bias, confirmation bias, mirror imaging, availability bias, and interpretation bias). Intelligence analysts should constantly seek to mitigate biases by continuously reviewing and, where necessary, revising available information, taking into account all new information and comparing it with what is already known. Intelligence professionals should admit to analytic misjudgments and exhibit the courage to change or adjust previously stated assessments when warranted by new information. Intelligence analysts should avoid "group think," a mode of thinking that occurs when group members strive for agreement without examining alternatives. Indicators of group think include assessments that discourage creativity, have no individual responsibility or uncritical acceptance, or are unanimous.

(b) The same integrity and analytic process extends to reporting what is not known. Intelligence professionals should avoid the temptation to make assessments appear more definitive than the facts warrant. Intellectual integrity requires the intelligence professional to distinguish conclusions grounded in fact from extrapolations or extensions of the fact. The commander should not be left with uncertainty regarding what is fact, what is opinion, and what is unknown.

(4) **Unity of Effort—Cooperate to Achieve a Common Objective.** Unity of effort is facilitated by centralized planning and direction and decentralized execution of intelligence operations, which enables JFCs to apply available collection capabilities and processing, exploitation, and dissemination (PED) systems efficiently and effectively. It optimizes intelligence operations by reducing unnecessary redundancy and duplication in intelligence collection and production. Unity of effort requires intelligence operations, functions, and systems that are coordinated, synchronized, integrated, and interoperable. Intelligence organizations (joint, national, and multinational) operating in a JFC's operational area should have a clear understanding and common acceptance of the commander's desired effects and objectives. Understanding the commander's desired effects and objectives is particularly important when employing distributed, reachback, and federated capabilities, many of which are not located in a JFC's operational area.

(a) Organic and attached intelligence assets operating in the JFC's operational area, as well as national and theater intelligence resources allocated to support that force, should be integrated into an interoperable architecture so that appropriate elements have access to required intelligence. This approach enables the JFC and J-2 to effectively manage intelligence activities to meet the joint force's IRs. The seamless provision of joint intelligence support to operational forces as they deploy from one theater to another is particularly important. To effectively plan and execute unit missions, deploying intelligence personnel must know the supported commander's concept of intelligence operations, intelligence architecture, estimate of the situation, map standards, and other specific requirements. This information should be disseminated in a timely manner to deploying forces in a standardized format by intelligence producers.

(b) Achieving unity of effort is most challenging during the coordination of multinational operations or when supporting another lead federal agency (LFA). Unity of effort requires an atmosphere of trust and cooperation. It also requires understanding the partner nations' (PNs') requirements, perceptions, and intelligence policies and procedures. Unity of effort should maximize the intelligence support provided to the JFC, while simultaneously facilitating information sharing among other appropriate commanders, staffs, and partners or coordinating with the multinational force.

(5) **Prioritization—Prioritize Requirements Based on Commander's Guidance.** Intelligence consumers drive the intelligence prioritization effort by identifying their intelligence needs and the relative importance of those needs. J-2s advise and assist in this effort by recommending intelligence priorities based on the commander's guidance and operational needs. At all levels, the commander's identification of intelligence needs determines prioritization.

(a) Because operational needs for intelligence often exceed intelligence capabilities and capacity, prioritizing limited intelligence resources supporting the OPLAN's or OPORD's objectives is an important aspect of the IP process. Prioritization is a mechanism for addressing requirements and effectively managing risk by identifying the most important decision and applying available resources against providing the intelligence to support that decision. Implicit in prioritization is the realization that some IRs are more important than others and that some lower-priority requirements might not be accomplished due to resource limitations. Effective prioritization depends upon active cooperation and coordination between intelligence producers and intelligence consumers.

(b) An agreed upon prioritization framework provides the basis for optimizing the allocation of national intelligence resources among CCMDs, as well as optimizing the CCMD collection and PED resources of subordinate forces. Global force management (GFM) processes determine the allocation of collection and associated PED resources across the CCMDs based upon the prioritization provided by the Secretary of Defense (SecDef). The allocation of national intelligence resources is based upon the National Intelligence Priorities Framework (NIPF) established by the Director of National Intelligence (DNI). The integrated Department of Defense (DoD) intelligence priorities, managed by the Under Secretary of Defense for Intelligence and Security (USD[I&S]), are used to prioritize DoD efforts and serve as the consolidated DoD input to the NIPF. Without clear prioritization and understanding of risk at all levels, competition for ISR resources not only reduces what intelligence could provide, it also inhibits full cooperation among organizations by making them see themselves as competitors rather than teammates.

(6) **Excellence—Strive to Achieve the Highest Standards of Quality.** Producers of intelligence should constantly strive to achieve excellence in their products. The quality of intelligence products is paramount to the intelligence professional's ability to achieve and maintain credibility with intelligence consumers. The attributes of

intelligence product excellence are objectives for intelligence activities supporting joint operations and standards against which the quality of intelligence products should be continuously evaluated. To achieve the highest standards of excellence, intelligence products must be anticipatory, timely, accurate, usable, complete, relevant, objective, and discoverable.

(a) **Anticipatory.** Intelligence must anticipate the informational needs of the commander and joint force staff to provide a solid foundation for operational planning and decision making. Anticipating the JFC's intelligence needs requires the intelligence staff to identify and fully understand the command's current and potential missions, the commander's intent, relevant aspects of the OE, and possible friendly and threat COAs. Most importantly, anticipation requires the aggressive involvement of intelligence in operation planning at the earliest time possible.

(b) **Timely.** Intelligence should be disseminated and made available to commanders in a usable format in a timely manner, enabling the commander to anticipate events in the operational area. In turn, this enables the commander to time operations for maximum effectiveness and to avoid being surprised. A balance between producing complete intelligence products and disseminating those products in a timely manner is therefore critical. If the intelligence product is incomplete, this should be noted in the product and addressed at a later time.

(c) **Accurate.** Intelligence must be analytically correct, portray the situation correctly when examined in hindsight, and provide an understanding of the OE based on the rational evaluation of available information. This evaluation should determine the possibility of an enemy's denial and deception effort. The accuracy of intelligence products may be enhanced by placing proportionally greater emphasis on information reported by the most reliable sources. The reliability of a source needs to be validated through a feedback process in which past data received from a source is compared with subsequent events or information confirming the source's accuracy.

(d) **Usable.** Intelligence must be tailored to the commander's specific needs and provided in an appropriate format for dissemination. Providing useful intelligence requires its producers to understand the decisions facing the commander, the relevance and impact of intelligence on those decisions, and how to deliver the intelligence to the commander in context so that it balances efficiency and effectiveness. Commanders must be able to quickly apply intelligence to the task and may not have sufficient time to analyze complex intelligence reports.

(e) **Complete.** Complete intelligence answers the commander's questions about the enemy and other aspects of the OE to the extent possible and informs the commander of significant intelligence gaps. To be complete, intelligence needs to not only identify and describe relevant aspects of the OE impacting mission accomplishment but also offer alternative analysis. Complete intelligence identifies and informs the commander of all major COAs that are available to the enemy and assesses which COAs are most likely and most dangerous. The intelligence staff should remain focused on the commander's PIRs. Intelligence organizations should anticipate and respond to the commander's existing and contingent IRs by evaluating the intelligence process input and output surrounding the mission.

(f) **Relevant.** Intelligence must be relevant to the planning and execution of the operation at hand and aid the commander in the accomplishment of the mission. It must contribute to the commander's understanding of the enemy and other significant aspects of the OE. To ensure intelligence remains relevant, the J-2 staff needs to remain cognizant of the commander's intent and understanding of how the operational concept creates desired effects to achieve the operational objectives. The J-2 staff also updates requirements as the friendly mission or the enemy situation changes.

(g) **Objective.** Due to the decisive and consequential impact of intelligence on operations, and the reliance on intelligence for planning and operations decisions, it is important for the J-2 to maintain objectivity and independence when developing assessments. When informing the commander, joint intelligence analysts should be vigilant in guarding against biases that shade, slant, or frame assessments that favor the commander's chosen COA or that bolster the commander's preconceived notions. In particular, intelligence should recognize each enemy as unique and avoid mirror imaging (the analysts' assumption that the threat being studied think like the analysts themselves) while realizing the possible bias involved in their assessment. For example, current intelligence and warning intelligence estimates may assess the same indicators differently. Red teams can be used to check analytical judgments and intelligence assessments to ensure assumptions about the enemy are sound and to help minimize bias.

(h) **Discoverable.** Intelligence must be readily accessible to the commander. Availability is a function of not only timeliness and usability but also appropriate security classification, interoperability, connectivity, and data formatting. Intelligence producers should strive to provide information at the appropriate level of classification but with the least restrictive releasability caveats possible, thereby maximizing the consumers' access, while protecting sources of information and methods of collection. Consideration must also be given to the perishability of the information when making classification and releasability decisions that may impact coalition planning and operations.

(7) **Assessment of Risk in Predicting Threat Intentions.** Although intelligence should identify and assess the full range of threat capabilities, it is most useful when it focuses on the future and intent of the threat and relevant actors. JFCs require and expect timely intelligence estimates that accurately identify threat and relevant actor intentions, support offensive and/or defensive operations, and predict the threat's possible future COAs in sufficient detail as to be actionable. If there is inadequate information upon which to base forecasts, the intelligence staff should inform the commander of this uncertainty.

(a) In conventional analysis, the analyst examines, assesses, and compares information and synthesizes findings into an intelligence product that usually reflects enemy capabilities and vulnerabilities. However, analysis goes beyond the identification of capabilities by forecasting enemy intentions and future COAs. The JIPOE process is the methodology used by joint intelligence organizations for assessing threat intentions and the relative probability of enemy COAs.

(b) Predictive analysis is riskier than capabilities analysis because it deals more extensively with the dynamic characteristics of the OE, a greater range of unknown factors, and possibly enemy deception plans. Therefore, there is a higher probability of producing assessments based on faulty analysis or incorrect assumptions. As a consequence, there may be a tendency among overly cautious intelligence personnel to avoid predictive analysis. However, JFCs need to know enemy intentions and behavior, as well as enemy capabilities to make plans and direct forces. The analyst or J-2 must produce these assessments with all available information and identify risk based on intelligence gaps and/or assumptions. The analyst who successfully performs predictive analysis and accurately assesses enemy intentions and behavior in advance of events performs an invaluable service to the commander and staff.

(c) Intelligence is vulnerable to incomplete information and enemy deception. JFCs should understand that intelligence forecasts are only estimates and that they accept risk in formulating plans based only on the J-2's assessment of the enemy's most probable COA. The J-2 should ensure the JFC is fully aware of all potential enemy COAs and provides an estimate regarding the level of confidence for each COA.

(8) **Agility—Remain Flexible and Adapt to Changing Situations.** Agility is the ability to quickly shift focus and bring to bear the skill sets necessary to address the new problem at hand while simultaneously continuing critical preexisting work. Agility is a key characteristic of the intelligence analyst. Through the preparation and organization for all types of contingencies in advance, analysts develop and maintain the agility needed to respond effectively to any future contingency. Intelligence structures, methodologies, databases, products, and personnel should be sufficiently agile and flexible to meet changing operational situations, requirements, priorities, and opportunities. Whether due to military contingencies or diplomatic challenges, sudden changes in the OE and requirements of intelligence consumers may allow little reaction and recovery time. Maintaining responsiveness under such circumstances requires considerable vigilance and foresight. Intelligence professionals anticipate not only the future decisions of enemies but of intelligence consumers as well.

(a) Building agility is fundamentally a long-term project that requires a principled commitment on the part of JFCs and an accurate vision of future requirements. Agility is built only by continuous preparation. Intelligence organization staffs should have an appropriate mix of skills and personal characteristics that enable them to quickly adapt to, and remain responsive in, a changing OE. Intelligence activities employ modularized automated data handling and communications systems that are capable of responding to changing circumstances, facilitating survivability and reliability, and enabling the seamless delivery of intelligence products to consumers regardless of the conditions in the OE.

(b) Intelligence managers should continuously assess what must be done to support potential requirements, monitor changes in the OE, and adjust resources accordingly. Agility requires anticipation and readiness, and intelligence organizations should be staffed, equipped, and organized for flexible responses to changing conditions in the OE.

(c) Due to complexity and change, commanders should be comfortable in the recognition that they will never know everything about the given OE and will never be able to fully define its problems. As such, many of the problems in the OE may not have solutions. Success in complex OEs may require innovation and rapid, iterative adaptation based on assessment of results from activities and changes in the OE. To that end, the commander empowers organizational learning and develops methods to determine whether modifying the operational approach is necessary during the course of an operation or campaign. This requires assessment and reflection that challenge understanding of the existing problem and the relevance of actions addressing that problem.

(9) **Collaboration—Leverage Expertise of Diverse Analytic Resources.** By its nature, intelligence is imperfect (e.g., everything cannot be known, analysis is vulnerable to deception, and information is open to alternative interpretations). The best way to achieve a higher degree of fidelity is to consult with and solicit the opinions of other analysts.

(a) Invaluable expertise on a diverse range of topics resides in governmental and nongovernmental centers of excellence. PNs can offer unique perspectives and may be able to provide the capabilities that are needed to address intelligence challenges. Without collaboration, intelligence products and reports end up being one-dimensional and thus less comprehensive.

(b) Intelligence collaboration relies on unhindered access to, and sharing of, all relevant information and can take many forms, such as competitive analysis, brainstorming, and federation. The collaborative sharing of information should not be confused with interorganizational document coordination; collaboration is informal information sharing among individuals, while document coordination is a formal staff process in which official organizational positions are obtained or confirmed. Competitive analysis (in which multiple teams use different or competing hypotheses to analyze the same intelligence problem) is useful if sufficient resources are available. In competitive analysis, it is imperative that each team have access to the same information. If resources are not available to conduct a competitive analysis, analysts should collaborate with their counterparts to gain different perspectives and formulate multiple hypotheses. Collaboration on complex intelligence problems may benefit from a federated approach in which different organizations may assume responsibility for subtopics within the larger problem. The J-2 considers all opinions and views obtained through collaboration in the preparation of the joint force's intelligence products.

(c) Discourse and leveraging dialogue and collaboration with partners is especially critical when addressing complex problems or OEs. Partners, including interagency, international, and local, can be sources of additional information on the problem or OE and can provide differing perspectives, which can broaden understanding and challenge institutional biases. Local actors are typically well suited to detect and understand changes in the OE, and their input can be instrumental for assessment. Red teaming can also be a means to improve understanding by challenging assumptions.

(10) **Fusion—Integrate All Sources of Information and Intelligence.** Fusion is a deliberate and consistent process of collecting and examining information from all available sources and intelligence disciplines to derive as complete an assessment as possible. It draws on the complementary strengths of all intelligence disciplines and relies on an all-source approach to intelligence collection and analysis. The JFC or J-2 might establish a specific staff organization to conduct fusion analysis.

For more information on intelligence disciplines, see Appendix B, "Intelligence Disciplines."

(a) Fusion relies on collection and analysis efforts that optimize the strengths and minimize the weaknesses of different intelligence disciplines. Information is sought from the widest possible range of sources to avoid any bias that can result from relying on a single source of information and to improve the accuracy and completeness of intelligence. The collection of information from multiple sources is essential to countering the enemy's operations security (OPSEC) and deception operations. The operations of all collection sources should be synchronized and coordinated to enable cross-cueing and tipping among collectors. JFCs should develop methods to improve their own and staff's knowledge of the OE. This requires improving the integration of civil information into the planning and operational processes, then sharing that information with external partners to enhance relationships and operational effectiveness.

(b) All-source, fused intelligence results in a finished intelligence product that provides the most accurate and complete description of what is known about any given topic. While the level of detail in single-source reports may be sufficient to meet narrowly defined customer needs, fused reports are essential to gain an in-depth understanding. Because the enemy will engage in deception efforts, analysts should guard against placing unquestioned trust in a single-source intelligence report. However, if such information is disseminated to meet timeliness criteria, or if no supporting data is available, they disclose the single-source nature of the reporting to the consumers. If the intelligence report does not include supporting data and information from multiple sources, the analysts should inform consumers that the intelligence report is based solely on single-source information.

b. Today's complex world presents a variety of intelligence challenges. Globalization, return to great power competition, and technological advancements enable more threats to challenge the security of the United States and its allies. Interstate strategic competition, not terrorism, is now the primary concern in US national security. Intelligence organizations should be prepared to respond to numerous requirements in a wide variety of situations across the competition continuum. 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.

4. Intelligence and the Levels of Warfare

a. **Levels of Warfare.** Joint Publication (JP) 1, Volume 1, *Joint Warfighting,* discusses three levels of warfare: strategic, operational, and tactical. Figure I-5 shows how intelligence operations support each level of warfare. The levels clarify links between strategic objectives, operational objectives, effects, and tactical actions and enable commanders to visualize a logical flow of operations, resource allocation, and tasks. It also focuses the JFC's staff on the appropriate time horizons. All levels of warfare have corresponding levels of intelligence activities. The construct of strategic, operational, and tactical levels of intelligence helps commanders and their J-2s visualize the flow of intelligence from one level to another. This construct facilitates the allocation of required collection, analytical, and dissemination resources and permits the assignment of appropriate intelligence tasks to national, theater, component, and supporting intelligence elements.

b. **Strategic Intelligence**

(1) National strategic intelligence is produced for the President, the National Security Council (NSC), Congress, SecDef, senior military leaders, CCDRs, and other United States Government (USG) departments and agencies. Strategic intelligence is the process and product of developing the context, knowledge, and understanding of the strategic environment required to support US national security policy and planning decisions. It is used to develop national strategy and policy, monitor the international and global situation, prepare military plans, determine major weapon systems and force

Levels of Intelligence

Strategic

Senior Military and Civilian Leaders
Combatant Commanders

- Assist in developing national strategy and policy.
- Monitor the international or global situation.
- Assist in developing military plans.
- Assist in determining major weapon systems and force structure requirements.
- Support the conduct of strategic operations.

Operational

Combatant Commanders, Subordinate Joint Force Commanders,
and Component Commanders

- Focus on military capabilities and intentions of enemies and adversaries.
- Analyze the operational environment.
- Identify enemy and adversary centers of gravity and critical vulnerabilities.
- Monitor events in the commander's area of interest.
- Support the planning and conduct of joint campaigns and operations.

Tactical

Commanders

- Support planning and the execution of battles, engagements, and other joint force activities.
- Provide commanders with information on imminent threats to their forces and changes in the operational environment.

Figure I-5. Levels of Intelligence

structure requirements, and support assessment of ongoing strategic activities. Strategic intelligence enables the production of strategic estimates, strategies, plans, and assessments, to accomplish missions assigned by higher authorities. Strategic intelligence enables national leadership to determine potential options using the nonmilitary instruments of national power (diplomatic, informational, and economic) based on estimates of the opposing force or the threat's reaction to US actions.

(2) Theater strategic intelligence supports joint planning and campaigning across the competition continuum by assessing the current situation and estimating future capabilities and intentions of threats that could affect the national security of the United States or allied interests.

c. **Operational Intelligence**

(1) Operational intelligence is primarily used by CCDRs, subordinate JFCs, and their component commanders. Operational intelligence focuses on answering the commander's PIRs to support the commander and staff in assessing the effectiveness of campaigns and subordinate operations; monitoring assumptions; maintaining situational awareness (SA) of adversary and/or relevant actor military composition, disposition, and intentions; the IE; and other relevant aspects of the OE. Operational intelligence helps commanders keep abreast of events within their area of interest (AOI) and helps them better understand the threat in the OE when deciding to remain with or shift operations. This drives the time horizon of intelligence to focus on the adversary's future intent so that the commander is making decisions within the adversary's decision cycle.

(2) Operational intelligence is increasingly concerned with stabilization activities across the competition continuum and has a greater focus on political, military, economic, social, information, and infrastructure systems and network (friendly, neutral, and threat) factors, which are important to global campaign plan (GCP) and combatant command campaign plan (CCP) execution of operations, activities, and investments. It also assists commanders in assessing and evaluating actions and possible implications associated with noncombat operations such as security assistance and foreign humanitarian assistance.

d. **Tactical Intelligence**

(1) Tactical intelligence is used by commanders, planners, and operators for planning and conducting a broad range of tactical activities supporting integrated operations. Relevant, accurate, and timely tactical intelligence enables tactical units to achieve positional and informational advantage over their threats. Determining the precise location of the friendly forces and relevant actors, tracking the target, and selecting the appropriate capabilities to create the desired effects are essential for success during mission execution. In addition, a key element of tactical intelligence is post-strike combat assessment (CA), which is used by commanders and planners to determine the need to dynamically retask assets to restrike identified targets.

(2) Tactical intelligence addresses the threat in the OE and across the competition continuum. Tactical intelligence identifies and assesses the threat's capabilities, intentions,

and vulnerabilities, as well as describes the physical environment. Tactical intelligence seeks to identify when, where, and in what strength the adversary will conduct tactical operations.

5. Globally Integrated Operations

a. The current global environment requires a globally integrated approach to operations. Actions taken in one CCMD area of responsibility (AOR) or functional responsibility can create unintended escalatory effects in other AORs. Intelligence should provide CCDRs awareness of the complex relationships associated with this global landscape to enable a globally integrated approach in support of strategic and operational objectives.

b. Inclusion of appropriate interagency partners, other international organizations, and PNs early in the planning process enhances the ability of the JFC to adequately include and deconflict activities to preserve resources and maximize the effectiveness of actions. Sharing information must be integrated at initiation of planning considerations to build effective C2 and assigning/requesting resources to address specific lines of effort (LOEs), as well as addressing issues at a level of classification accessible to all involved. By including different partners' inputs and requesting assistance/coordination early in the process, CCDRs have a more comprehensive and varied array of options at their disposal to create desired global effects.

For more information, see JP 1, Volume 1, Joint Warfighting.

6. Competition Continuum

a. Rather than a world either at peace or at war, the competition continuum describes a world of enduring competition conducted through a mixture of cooperation, adversarial competition below armed conflict (from this point forward "competition" will be used in this publication), and armed conflict or war. These descriptors refer to the relationship between the United States and another strategic relevant actor (state or non-state) in relation to a set of specific policy objectives. In practice, competition with a major adversary is often indirect, with a more direct focus on a nation, region, or international actor over which the United States and its competitors vie for increased access and influence. The three categories are not always linear; can begin within any of the categories; consist of activities that accelerate, surge, or decrease capabilities; and can occur simultaneously. This allows for simultaneous interaction with the same strategic relevant actor (state or non-state) at various points along the competition continuum. In practice, all instruments of national power should function together as an interrelated and integrated whole to develop key partners, find and develop new partners, build partner networks against adversaries, compete against aggressive adversaries, reduce the risk of escalation to conflict, and support conflict or war.

b. Intelligence plays a critical role to assist commanders in making decisions in military operations across the competition continuum. Intelligence activities continue throughout military operations across the competition continuum, helping commanders monitor foreign states, volatile regions, and transnational issues to identify threats to US interests in time for senior leaders to respond effectively.

c. Deterrence applies across the competition continuum. Deterrence is a human psychological effect and cognitive outcome that occurs within the minds of relevant actors, especially the key leaders and decision makers of adversary states, populations, groups, and networks and is informed by the human aspects of their societies along with their perceptions, motivations, and will. Deterrence of societal and institutional subversion and malign activities will focus on identification, characterization, attribution, and countering (up to and including elimination) of individuals, units, and organizations (relevant actors) involved to disincentivize adversaries from conducting operations, activities, and investments counter to US interests.

d. **Intelligence in Cooperation.** Maintaining a forward presence enables activities such as professional military exchanges, forward basing, and cooperative relationships with multinational partners to enhance US forces' ability to shape potential operations across the competition continuum.

e. **Intelligence in Competition.** Competition exists when two or more state or non-state adversaries have incompatible interests, but neither seeks armed conflict. Competition may include coercive measures, such as exclusion zones, air and maritime interdiction, enforcement of US and international economic sanctions, actions against irregular threats, support to friendly resistance, information activities, cyberspace operations (CO), special operations, and show of force. Countering and coercing an adversary's behavior are challenging. Even with a sound appreciation of an adversary's resolve and ability to resist, coercing behavior is difficult, uncertain, and risky. It is intrinsically more difficult to get an adversary to change its behavior than to maintain and accept the status quo. In changing an adversary's behavior, one barrier to success is that it usually requires the adversary's overt submission. An adversary can resist coercive attempts in imaginative and unexpected ways, even when the JFC has substantial leverage. Intelligence support reduces uncertainty by anticipating the adversary's reactions and counter actions, and what actions will lead to compliance.

f. **Intelligence in Armed Conflict.** For DoD, armed conflict involves two strategic uses of military force—coercion and compellence. Armed conflict varies in intensity and ranges from terrorism, insurgency, and armed resistance to occupation, through crisis response and limited contingency operations to large-scale combat operations.

For more information on the competition continuum, see JP 3-0, Joint Campaigns and Operations.

Intentionally Blank

CHAPTER II
INTELLIGENCE ORGANIZATIONS, RESPONSIBILITIES, AND PROCEDURES

1. Introduction

a. JFCs exercise control over a vast array of assigned, allocated, attached, and contracted intelligence collection and analytic capabilities. Nevertheless, these alone cannot satisfy all the joint force's IRs. The J-2 relies on theater, national, PN, and law enforcement organizations to satisfy the JFC's IRs. The J-2 should understand the organization, procedures, production responsibilities, and expertise resident in the various multinational and national intelligence agencies to integrate their capabilities efficiently.

b. 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 advantage throughout the OE, enabling the successful conduct of operations. The intelligence staff provides the JFC with an understanding of the OE, particularly with regard to the threat's forces, capabilities, and intentions. To ensure timely and accurate intelligence is provided or made available to the JFC, subordinate commands, and components, the intelligence staff performs the following tasks:

(1) Clearly understand and be aware of objectives and associated IRs of their senior and subordinate commands and components.

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

(3) Task and utilize theater, DoD, and national capabilities to address identified shortfalls and gaps.

c. Joint intelligence doctrine describes the roles and relationships of intelligence organizations at the national, combat support agency (CSA), CCMD, and subordinate joint force levels. 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 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 as part of the evaluation and feedback phase of the intelligence process and shared to further maximize intelligence support.

SECTION A. JOINT INTELLIGENCE

2. Joint Staff, Directorate for Intelligence

The Joint Staff J-2 [Intelligence Directorate] is under the authority, direction, and control of the CJCS and is resourced by the Defense Intelligence Agency (DIA). It provides all-source intelligence and intelligence staff support to SecDef, the CJCS, other Joint Staff directorates, CCMDs, and the Services. Additionally, the Joint Staff J-2 represents and advocates CCMD intelligence interests to the Joint Staff, the Office of the Secretary of Defense (OSD), and the Office of the Director of National Intelligence (ODNI). It also serves as the single focal point for intelligence support to national and theater decision makers during crisis situations, 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 intelligence community (IC) coordinator for support to military operations.

3. Combatant Command Intelligence Organizations and Responsibilities

a. **CCMD J-2.** The CCMD J-2 coordinates the intelligence structure and architecture, recommends and manages appropriate command relationships for intelligence assets, and supervises the production and dissemination of appropriate intelligence products while supporting the staff in developing strategy and planning operations and campaigns. The CCMD J-2 also serves as the defense intelligence component head, responsible for all intelligence activities involving US persons or US person information and its appropriate disposition. 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 NGOs. Specifically, the CCMD J-2 should:

(1) 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 CCMD, staff, subordinate component commands, and joint task forces (JTFs).

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

(4) Determine intelligence needs based on mission analysis and commander's planning guidance, recommend the relative priorities of intelligence needs and nominate

PIRs to support the CCDR's decision making, and decompose IRs and PIRs into information requirements and essential elements of information (EEIs) to drive specific collection requirements (CRs) and production requirements (PRs).

(5) Develop and manage optimal collection plans that fully support, and are 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 DoD and national intelligence organizations.

(8) If delegated, assume order of battle (OB) production authority in crisis/conflict for the AOR and delegate responsibilities to federated producers. In conjunction with DIA, produce the enemy's OB in electronic databases (e.g., modernized integrated database [MIDB], Machine-assisted Analytic Rapid-repository System [MARS], or other applicable database).

(9) Coordinate the intelligence effort of subordinate commands.

(10) Assist the J-3 and 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 planning and operations (see JP 3-60, *Joint Targeting,* for more on targeting authorities and responsibilities).

(13) Produce and maintain target intelligence products, which meet the requirements of the commander.

(14) Coordinate and manage the CCMD target development working group to facilitate target intelligence production.

(15) Provide appropriate representation to the joint targeting working group and joint targeting coordination board (JTCB), as well as other associated staff organizations when established.

(16) Support joint planning, J-5 operational planning teams, and J-3 crisis action teams (CATs), as required to ensure intelligence directorate equities are represented.

(17) Exchange relevant information and conduct mission synchronization with elements of cyberspace, electromagnetic warfare, information, space, and special operations forces to provide information and intelligence, tip and cue, and ensure collection coverage among non-intelligence assets, as well as the intelligence disciplines.

Coordination with subject matter experts is critical to situational understanding and target development.

(18) Develop, manage, and synchronize the CCMD's computer mapping system and paper maps for the common operational picture (COP). Ensure J-2 and J-3 staff coordinate blue force and threats and that they are displayed on the COP. Develop a threat picture for the COP.

(19) Manage and control access to classified systems for the CCMD.

(20) Identify changes in the OE that require commander attention or changes to ongoing missions.

b. **CCMD JIOC.** Each CCMD and some subordinate unified commands have assigned JIOCs to integrate intelligence capabilities in support of the CCMD's mission. The CCMD J-2 reserves the right to organize the JIOC to meet the CCDR's requirements. The JIOC may be the focal point for the CCMD's IP, collection management, analysis and production, and target intelligence. 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 intelligence from external DoD and national intelligence organizations, PNs, NGOs, 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 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. There is no standard JIOC organizational structure. Although each JIOC varies depending on CCMD requirements, JIOCs are generally organized around a set of key principles and functions. These include:

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

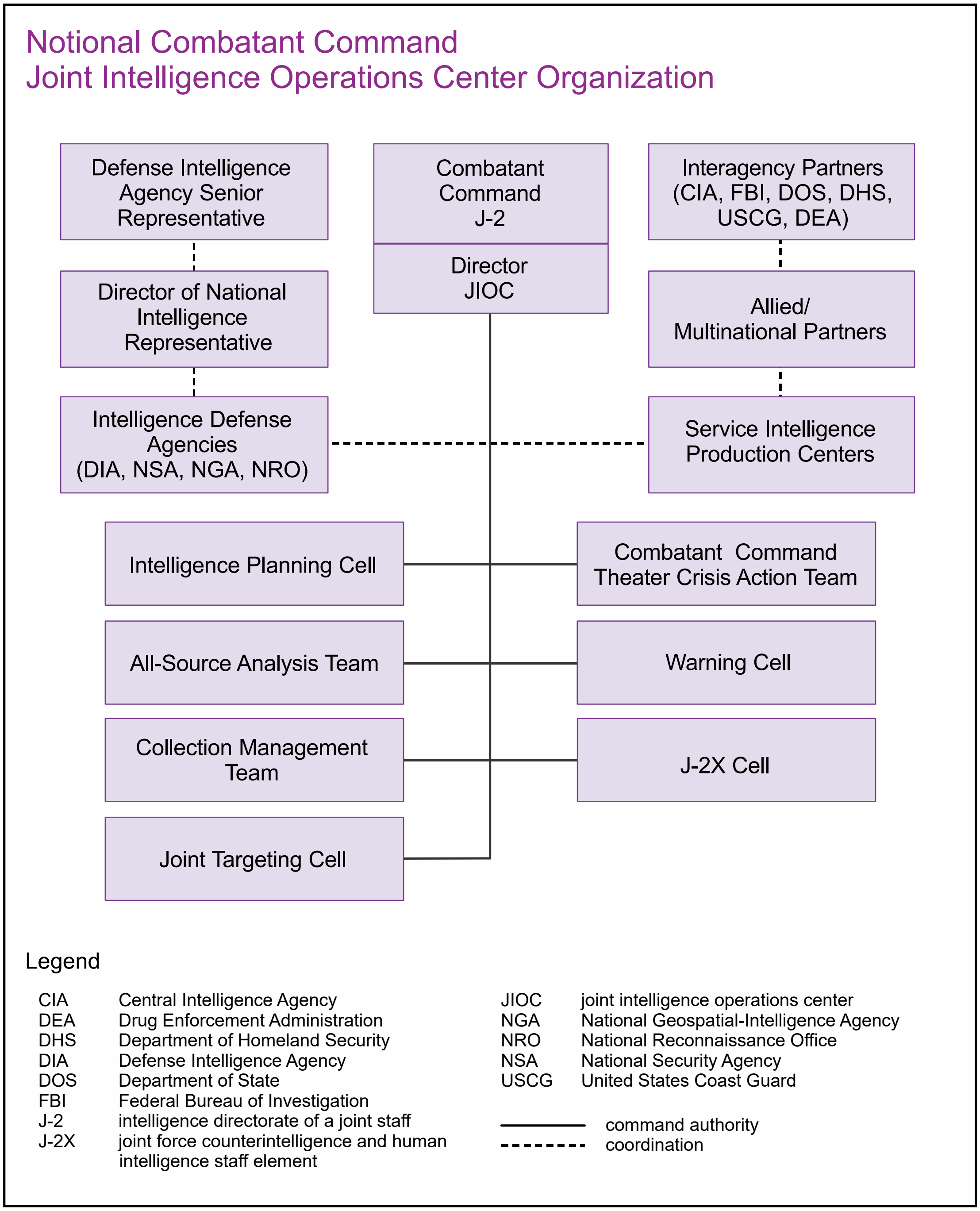
(b) Institutionalize IP as the intelligence component of the planning process.

(c) Improve Reserve Component integration.

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

(e) Facilitate intelligence mission/collection management.

(f) Expand alternative analysis capabilities.


Notional Combatant Command
Joint Intelligence Operations Center Organization
Defense Intelligence Agency Senior Representative
Combatant Command J-2
Director JIOC
Interagency Partners (CIA, FBI, DOS, DHS, USCG, DEA)
Director of National Intelligence Representative
Allied/ Multinational Partners
Intelligence Defense Agencies (DIA, NSA, NGA, NRO)
Service Intelligence Production Centers
Intelligence Planning Cell
Combatant Command Theater Crisis Action Team
All-Source Analysis Team
Warning Cell
Collection Management Team
J-2X Cell
Joint Targeting Cell
Legend
command authority
coordination

CIA	Central Intelligence Agency
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOS	Department of State
FBI	Federal Bureau of Investigation
J-2	intelligence directorate of a joint staff
J-2X	joint force counterintelligence and human intelligence staff element
JIOC	joint intelligence operations center
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
USCG	United States Coast Guard

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

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

(h) Establish a horizontal integration/collaborative information technology (IT) enterprise.

(i) Improve training, education, and readiness.

(j) Integrate national intelligence and CSAs' capabilities.

(k) Produce all-source finished intelligence spanning tactical-operational-strategic levels, and communicate this understanding broadly to enhance a USG fused, synchronized, holistic picture of security issues in the midst of operational activity and campaign plan execution.

(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:

(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 reduce possible knowledge gaps and mitigate intelligence capabilities shortfalls.

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

(d) Maintain and coordinate execution of the CCMD intelligence collection plan with components and 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, to include target system analysis (TSA), electronic target folders (ETFs), target lists, and battle damage assessment (BDA), is being produced by the appropriate echelon within the CCMD organizational structure and, if target intelligence cannot be produced with assigned assets, coordinate target intelligence production requests and requirements with the appropriate Defense Intelligence and Security 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) Conduct JIPOE. Integrate IC analysis with JIOC products in support of subordinate commands and other organizations, and ensure the JIPOE process encompasses a systematic analysis of the OE, including the civilian environment, and is aligned with the JFC's plans and operations. The civilian environment consists of factors within the OE that relate to civilians and their communities, including the civilian population and the personnel, organizations, resources, infrastructure, essential services, and systems on which civilian life depends. Continuously develop and update tailored products to support planning and assessment efforts.

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

(j) Provide intelligence collection and analysis to support the understanding of the effects friendly and adversary actions have on the civilian environment, to inform planning, operations, and targeting.

(3) **Concept of Operations (CONOPS).** CCMD JIOCs use a task-oriented approach with personnel 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, as well as intelligence customers throughout the AOR. 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 capability. The JIOC is organized to facilitate the fusion of information and intelligence received from all available sources. The JIOC coordinates with mission partners, including CCMD and Service component staffs, the defense intelligence component representatives, PNs, and the CCMD's DNI representative to actively task and integrate intelligence from all sources and levels to satisfy command PIRs.

(b) JIOCs plan across the competition continuum. 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 commands and JTFs, and through the Joint Staff J-2, the Defense Intelligence Security 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 OPORDs and fragmentary orders (FRAGORDs) that delegate CMA for subordinate components and JTFs.

(d) A red team exists intellectually and institutionally separate from the JIOC's red cell and conventional analysts. The red team is an organized element comprised of personnel with knowledge of known threats and trained in appropriate concepts and methodologies. The red team is a decision-support organization that can complement problem solving and analytical efforts, and is normally focused on supporting plans, operations, and intelligence. In contrast with the J-2 red cell, which performs threat emulation, the red team reviews key intelligence assessments and OPLAN assumptions to provide alternative analysis and reduce risk. Red teams assess the OE, including the civilian environment, and threats. Red teams assist joint planning by challenging or validating assumptions about the threat and adversary; combating cognitive bias; participating in the wargaming of friendly, threat, and adversary COAs; and devising alternatives.

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 the IC and interagency partners such as the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Department of State (DOS) and country teams, Department of the Treasury, Department of Homeland Security (DHS), Department of Transportation, United States Coast Guard (USCG), and Drug Enforcement Administration (DEA), and other federal partner organizations, to ensure a whole-of-government approach. In accordance with (IAW) CCPs, CCMD JIOCs establish intelligence exchange relationships with multinational partners to ascertain their potential and willingness to contribute to a combined intelligence effort.

(f) The JIOC fully participates, whenever possible, in national-level discussions of AOR security issues, coordinating and drafting products, up to and including National Intelligence Council products, ensuring operational and tactical perspectives are represented through the unique expertise and access of JIOC analysts. This happens informally and unevenly; it is tremendously helpful to national agencies to be able to get fresh perspectives in their deliberations.

4. 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 SA to the commander, joint task force (CJTF); 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) Directs production of JTF JIPOE products by the CCMD JIOC. Integrate separate intelligence preparation of the operational area efforts into JIPOE products to better support JTF intelligence assessments.

(5) Provide threat warnings to the CJTF, battle staff, component units, and multinational forces.

(6) Provide target intelligence as necessary.

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

(a) JTCB.

(b) JCMB.

(c) Information cell.

(d) Joint personnel recovery center.

(e) J-3.

(f) Joint planning group (JPG).

(g) Geospatial intelligence (GEOINT) cell.

(h) Red team.

(i) JIPOE coordination cell.

(j) Public affairs.

(k) Special technical operations representative.

(l) Prisoner of war and detainee operations.

(m) CO-integrated planning element.

(n) United States Space Command liaison element.

(o) OPSEC cell.

(p) Military deception cell.

(q) Joint electromagnetic spectrum operations cell (JEMSOC).

(r) Missile and space all-source analysis cell.

(s) Joint force counterintelligence and human intelligence staff element (J-2X).

(t) Civilian harm assessment cell.

(u) Civilian environment team.

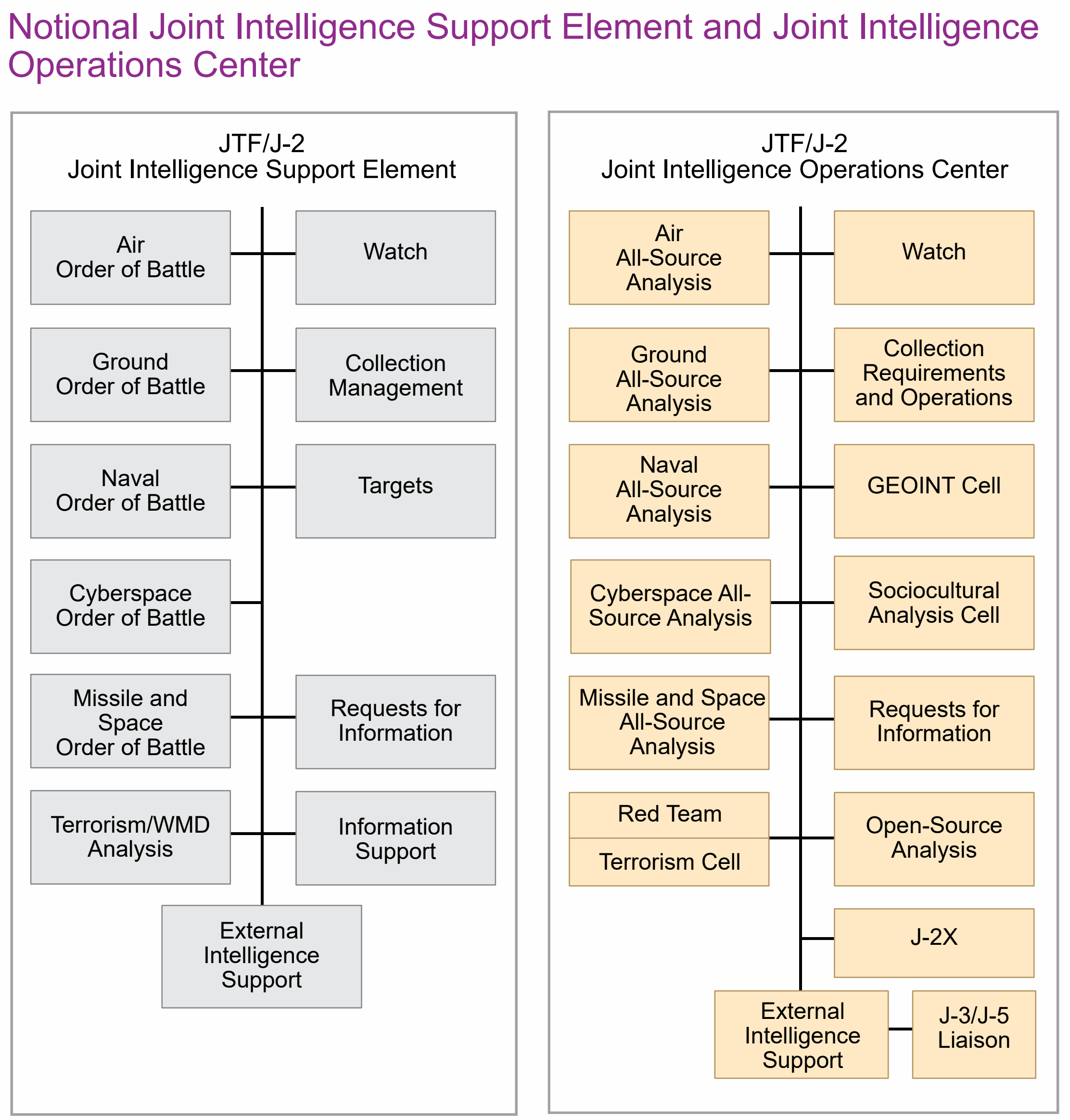
Appendix H, "Intelligence Directorate of a Joint Staff Planning Checklist," contains a detailed list and generic descriptions of joint force J-2 tasks and responsibilities.

b. To accomplish the assigned mission, the subordinate joint force J-2 uses a combination of the following elements:

(1) **JISE.** 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 a continuous analytical capability and with tailored intelligence products and services. Capabilities of the JISE may include OB analysis, collection management, target intelligence, analysis of the IE, warning intelligence, and a request for information (RFI) desk.

(2) **Operational-Level JIOC.** Alternatively, in a particularly large or protracted campaign, the CJTF 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) **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 CI coordinating authority, a CI/HUMINT analysis and requirements cell, and an operations support element. The operations support element provides services of common concern to the HUMINT operations cell and CI coordinating authority, such as report and source administration, linguistic support, and polygraph support. As the JFC's tasking authority for HUMINT and CI collection, the J-2X manages,


Notional Joint Intelligence Support Element and Joint Intelligence Operations Center
JTF/J-2
Joint Intelligence Support Element
Air Order of Battle
Watch
Ground Order of Battle
Collection Management
Naval Order of Battle
Targets
Cyberspace Order of Battle
Missile and Space Order of Battle
Requests for Information
Terrorism/WMD Analysis
Information Support
External Intelligence Support
JTF/J-2
Joint Intelligence Operations Center
Air All-Source Analysis
Watch
Ground All-Source Analysis
Collection Requirements and Operations
Naval All-Source Analysis
GEOINT Cell
Cyberspace All-Source Analysis
Sociocultural Analysis Cell
Missile and Space All-Source Analysis
Requests for Information
Red Team
Terrorism Cell
Open-Source Analysis
J-2X
External Intelligence Support
J-3/J-5 Liaison

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

coordinates, and deconflicts all assigned, attached, and allocated HUMINT and CI collection capabilities within the operational area. The J-2X maintains the command source registry, deconflicts source matters, and performs liaison functions with external organizations. It is imperative that a secure communications/systems architecture be established for the J-2X that is compatible with component HUMINT elements and other intelligence organizations. The J-2X should be located in a sensitive compartmented information facility (SCIF).

Additional information on the J-2X organization and responsibilities can be found in classified Appendix C, "(U) Classified Appendix on Joint Intelligence (Counterintelligence and Human Intelligence/Department of Defense Cover)."

(4) **GEOINT Cell.** The JFC may establish a GEOINT cell to manage the tasks, actions, and events required to collect, analyze, and provide imagery, imagery intelligence (IMINT), and geospatial information (GI) necessary to tactical navigation and joint targeting. The cell enhances the joint force's COP for SA and decision making by exercising National Geospatial-Intelligence Agency (NGA) and National Reconnaissance Office (NRO) processes, tasking capabilities, and coordination with subject matter experts. Optimally, the core GEOINT cell consists of a GEOINT officer, an imagery collection and production manager, and a geospatial collection and production manager. GEOINT support includes imagery, IMINT, and geospatial information and services (GI&S). GI&S includes tools that enable users to access and manipulate data.

For more information on GEOINT, see the National System for Geospatial Intelligence Publication 1.0, Geospatial Intelligence (GEOINT) Basic Doctrine.

(5) **SCA Cell.** The JFC may establish a SCA cell to manage the tasks, actions, and events required to collect, analyze, and provide finished intelligence necessary to develop understanding and SA of the human aspects of the OE. SCA fuses intelligence from all of the intelligence disciplines to inform its work. The resulting intelligence will provide context for the JFC's decision making. The SCA cell will also enhance the joint force's COP for SA. Composition of the SCA cell will depend on the composition, complexity, and populations of various relevant actors in the OE. Resource constraints may force cross-cultural vice culture-specific expertise based organizational solutions.

(6) **National Intelligence Agency Support.** The JFC, at the recommendation of the J-2, may request that national-level 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 including target automation systems.

(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 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 electromagnetic OB processes.

(12) Provide BDA 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) Support CCMD J-2 through integrating identity intelligence (I2) activities and process.

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

SECTION B. NATIONAL INTELLIGENCE

5. Overview

a. The IC had its origin in the National Security Act of 1947, amended by the Intelligence Reform and Terrorism Prevention Act of 2004 [short title: IRTPA of 2004], and guided by Executive Order 12333, *United States Intelligence Activities,* as amended. The IC 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 ODNI and 17 additional member organizations.

b. **IC Governance.** The IRTPA of 2004 established the 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 standards for or setting policy for protection of intelligence sources and methods.

c. 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 threats, 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 substantially enhance intelligence support to JFC decision making.

For more information on IP, see Chapter I, "The Nature and Role of 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.

d. Successful support to JFCs by national IC elements and Defense Intelligence and Security Enterprise components that are not national IC elements (e.g., CCMD JIOCs and the Joint Staff J-2) is vital for overall national defense.

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

a. **USD(I&S).** USD(I&S) serves as the principal staff assistant to SecDef and the Deputy Secretary of Defense regarding intelligence, CI, security, sensitive activities, and other intelligence-related matters. USD(I&S) also exercises SecDef's authority, direction, and control over, and oversees the activities of, DIA, the NGA, the National Security Agency/Central Security Service (NSA/CSS), the NRO, and the Defense Counterintelligence and Security Agency and exercises planning, policy, and strategic oversight over all DoD intelligence, CI, and security policy, plans, and programs. The USD(I&S) manages all-source defense intelligence analytical efforts through DIA and the Defense Intelligence Analysis Program (DIAP). On behalf of SecDef, USD(I&S) 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&S) monitors MIP implementation and execution by the Services and the defense intelligence components.

b. **Assistant to the Secretary of Defense for Intelligence Oversight (ATSD[IO]).** ATSD(IO) is responsible for ensuring intelligence oversight policies and regulations are carried out by DoD organizations that perform intelligence functions IAW Department of

Defense Directive (DoDD) 5148.13, *Intelligence Oversight*. DoD intelligence organizations, units, and personnel comply with the United States Constitution, applicable law, and relevant policy during the conduct of authorized intelligence activities. Department of Defense Manual (DoDM) 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities,* applies Executive Order 12333, *United States Intelligence Activities*, as amended, to defense intelligence activities, directs the DoD intelligence oversight program, and serves as the basis for the DoD regulations and instructions that implement intelligence oversight in the Services, CCMDs, and DoD intelligence agencies. National and DoD policy establishes procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of US persons. DoD-authorized intelligence activities are foreign intelligence and CI activities unless otherwise specified.

(1) Commanders and leaders ensure DoD intelligence component personnel are trained on and comply with intelligence oversight requirements. DoD component heads conducting intelligence or intelligence-related activities will develop intelligence oversight implementing guidance and administer an intelligence oversight training program that is tailored to mission requirements. Commanders and leaders should consult with their judge advocate/legal advisor on all intelligence oversight issues.

(2) DoD intelligence components may not investigate US persons or collect or maintain information about them solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. DoD intelligence components are not authorized and will not engage in any intelligence activity for the purpose of affecting the political process in the United States.

(3) DoD intelligence components only collect, retain, and disseminate information concerning US persons in compliance with applicable laws and policy, in particular the procedures specified in DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities.*

(4) Questionable intelligence activities and significant or highly sensitive matters are identified, investigated, and reported IAW DoDD 5148.13, *Intelligence Oversight.* Intelligence and intelligence-related activities reportable to the ATSD(IO) are not limited to those that concern US persons. Senior leaders and policymakers in the Executive Branch and congressional defense and intelligence committees will be notified of events that may erode public trust and confidence in the conduct of DoD intelligence activities.

(5) DoD intelligence support provided to other USG departments and agencies is conducted IAW DoDD 5148.13, *Intelligence Oversight*; DoDD S-5210.36, *(U) Provision of DoD Sensitive Support to DoD Components and other Departments and Agencies of the US Government;* and other applicable guidance, authorities, and directives. Requests for DoD intelligence support to civil authorities and civilian law enforcement agencies may implicate DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*; DoDD 3025.18, *Defense Support of Civil Authorities (DSCA);* and Department of Defense Instruction (DoDI) 3025.21, *Defense*

Support of Civilian Law Enforcement Agencies. Upon receipt of defense support of civil authorities (DSCA) and defense support of civilian law enforcement agency requests, DoD intelligence component legal counsel should be consulted for advice on applicability of the Fourth Amendment to the Constitution; Sections 101-112 of the Foreign Intelligence Surveillance Act of 1978, as amended (Sections 1801-1812 of Title 50, United States Code [USC]); Title 18, USC, Section 831l; Title 10, USC, Chapter 15 (Military Support for Civilian Law Enforcement Agencies); and other potentially applicable authorities and restrictions.

c. **NJOIC**

(1) The NJOIC is an integrated Joint Staff J-2/Joint Staff J-3 [Operations Directorate]/Joint Staff J-5 [Plans Directorate] element that continuously monitors the global situation 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 designated CCMDs; and representatives from each Service intelligence staff element, the intelligence CSAs, and the CIA. To provide intelligence analytical depth, DIA maintains a continuous direct support element at the NJOIC, tailored to the current global situation and operating tempo. The NJOIC also coordinates the intelligence response to immediate crises and contingencies.

(2) The Alert Center is a continuously manned, all-source, multidiscipline intelligence center providing defense intelligence SA, 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, throughout the competition continuum. It provides the infrastructure for the planning, for and management of intelligence working groups (IWGs) and intelligence task forces (ITFs) that provide direct intelligence support during conflicts. If a developing situation escalates into a crisis, the relevant Alert Center regional desk officer is augmented with analytical support and an intelligence cell, IWG, or ITF is formed. This support may range from a few additional analysts in an intelligence cell to a continuously staffed IWG or ITF augmented as required.

(a) **Intelligence Cell or Focus Group.** An intelligence cell or focus group is established based on indications that a threat exists or when other crisis situations arise. The cell or group, typically consisting of Joint Staff J-2 personnel, is formed to respond to the needs of the NJOIC or CCMD JIOCs. The cell monitors and provides an assessment of the developing situation. If the cell or focus group is not continuously manned, extended duty hours or 24-hour operations and augmentation from DIA may be warranted.

(b) **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 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 continuously manned if warranted by the level of crisis.

(c) **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 it may be formed using an IWG as its core. The defense intelligence agencies, CIA, and other 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:

1. Is convened when deemed appropriate by the Joint Staff J-2, usually whenever a 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, or not if the reason for the CAT does not warrant dedicated intelligence support.)

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

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

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

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

6. 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.

7. Coordinates tasking of other USG departments and agencies in support of OSD, the 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 USD(I&S). Director, DIA, also serves as the Defense HUMINT Manager overseeing and coordinating the Defense HUMINT Enterprise. 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. 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, prevent strategic surprise, and support DoD's acquisition and force development process. Through the Deputy Directorate for Global Integration and its subordinate regional and functional centers, DIA facilitates federated intelligence support to military operations in response to intelligence customer requests and requirements. The DIA Directorate for Operations conducts strategic, overt, and clandestine HUMINT operations to provide timely, relevant, and accurate information to defense planners, policy makers, and CCMDs. Additionally, the DIA Directorate for Operations conducts full-spectrum CI operations to exploit and degrade foreign intelligence directed towards US and allied equities. DIA also manages and operates the Joint Worldwide Intelligence Communications System (JWICS) through its Chief Information Office. DIA leads and coordinates measurement and signature intelligence (MASINT) collection, processing, exploitation, and dissemination for DoD. DIA also leads efforts to align intelligence activities and links and synchronizes national, defense, and military intelligence.

(1) **DIA analytical and operational support includes:**

(a) CI and HUMINT.

(b) Combating terrorism.

(c) Counterdrug operations.

(d) CO.

(e) Personnel recovery.

(f) Counterproliferation of weapons of mass destruction (WMD) and associated delivery means.

(g) UN peacekeeping and multinational support.

(h) MASINT.

(i) Noncombatant evacuation operation efforts.

(j) Warning intelligence.

(k) Target intelligence and CA.

(l) Current intelligence.

(m) Collection management.

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

(o) DOMEX.

(p) Counterinsurgency (COIN) support.

(q) Forensic analysis of collected exploitable material (CEM).

(r) IE characterization through the integration of intelligence related to forecasting, identifying vulnerabilities, determining effects, and assessing the IE.

(s) Threat finance intelligence.

(t) Counter-transnational organized crime.

(u) Foreign military OB.

(v) Defense critical infrastructure.

(w) Intelligence analysis and production through open-source intelligence (OSINT) collection, processing, exploitation, reporting, and integration.

(x) Integration of foreign partner intelligence capability.

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

(z) Foreign materiel program.

(aa) Vendor vetting (e.g., supply chain risk management).

(2) **Additional functions of DIA:**

(a) **Collection Management.** DIA serves as the DoD functional manager for analysis and defense intelligence collection to:

1. Manage the Defense Collection Management Enterprise (DCME).

2. Promote coordination, cooperation, information sharing, and cross-service management of collection management within DoD and the IC.

3. Issue collection management guidance, operating procedures, professionalization standards, and IT standards to enhance DCME mission effectiveness.

4. Set priorities for DoD CRs.

5. Develop and implement all-domain, multidiscipline collection strategies that fully integrate national, theater, and special collection capabilities into multidiscipline strategies against national and theater intelligence information needs.

6. Pursue and adopt advanced technology and development of data strategies and analytics to improve the interoperability and effectiveness of multidiscipline collection management tradecraft.

7. Advance collection management training, tradecraft, and certification.

8. Advance DCME governance processes and programs.

9. Strengthen partnerships, collaboration, and interoperability with national IC elements and allies.

(b) **IP.** The DIA Deputy Director of Global Integration supports the CCMD IP process led by the Joint Staff J-2 IP functional manager to develop dynamic threat assessments (DTAs), xcampaign intelligence estimates (xCIEs), and national intelligence support plans (NISPs) to support the development and execution of CCDR plans and orders and assists the CCMDs in evaluating NISP production requirements matrices (PRMxs) and collection requirements matrices (CRMxs).

(c) **Support to CCMD JIOCs and JFCs.** The Director, DIA, develops and recommends to the Joint Staff 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; and, along with the Services, prepares, equips, trains, and deploys military intelligence personnel in support of CCMD or JFC requirements. The DIA's Deputy Director for Global Integration synchronizes intelligence analysis of DIA's regional intelligence centers to support global integration, while illuminating adversary action and capabilities to challenge our adversaries and identifying strategic opportunities. The DIA's Deputy Director for Global Integration provides critical horizontal integration, ensuring efforts of the intelligence integration centers and directorates are prioritized and synchronized, and vertical integration to ensure alignment from the CCMDs to DIA through DoD and the IC.

e. **NSA/CSS.** NSA/CSS provides signals intelligence (SIGINT) and ensures the protection of national security systems. The National Security Agency (NSA) is an intelligence CSA 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 cybersecurity policy and technology implementation support to the CCMD JIOCs through the Central Security Service (comprised of the Service cryptologic components). The Director, National Security Agency/Chief, Central Security Service:

(1) Is a general/flag officer serving concurrently as Commander, United States Cyber Command.

(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—the SIGINT and cybersecurity program activities of the USG.

f. **NGA.** NGA is a CSA and an element of the IC and is subject to the oversight of both SecDef and DNI. NGA provides timely, relevant, and accurate GEOINT to DoD; providing GEOINT for safety of navigation information; preparing and distributing nautical and aeronautical charts, topographic and geomatic maps, books, models, and datasets; designing, developing, operating, and maintaining systems related to the processing and dissemination of GEOINT; and providing GEOINT in support of the objectives of the Armed Forces of the United States. 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, the Director, NGA, develops GEOINT tradecraft standards, develops strategic guidance and procedures, and develops IT architecture and standards. NGA also ensures coordination across intelligence disciplines and IC elements. GEOINT consists of imagery, IMINT, and GI. GEOINT exploitation includes analysis of electro-optical (EO), infrared, and radar imagery; full-motion video; moving target indicators; GI; and spectral, laser infrared, radiometric, polarimetric, spatial, and temporal data. It employs ancillary data, signature information, and fused data products. NGA provides GEOINT analysis to produce tailored, actionable intelligence to support customers across DoD, the IC, and other USG departments and agencies. NGA provides direct support to the CCMD JIOCs and procures and disseminates commercial, remotely sensed imagery for DoD and the IC.

g. **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.

h. **Service Intelligence Organizations.** The Service Chiefs 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**

(a) The Army Deputy Chief of Staff, G-2 [Intelligence], is the principal military adviser to the Secretary of the Army and Chief of Staff of the Army on intelligence and CI; the Army's senior agency official for information, personnel, and industrial security; and the Army's principal foreign disclosure authority. The Deputy Chief of Staff, G-2, is the Army's senior intelligence officer (SIO) and the Army's IC element head, responsible for intelligence plans, programming, and integration with the IC and formulating requests and managing resources for the Army MIP and NIP. The Deputy Chief of Staff, G-2, is responsible for:

1. Providing current and estimative intelligence to Headquarters, Department of the Army; developing the current and future threat environment for the Army; providing oversight, training guidance, and policy review of the Army's Foreign Materiel Program; and providing foreign technical threat intelligence assessments in support of Army acquisition programs, science and technology efforts, and research and development programs.

2. Serving as the Army staff lead for ISR integration issues, including plans, policies, and architectures.

3. Coordinating and providing technical assistance and advice to the Army Secretariat with regard to the development and implementation of Army protection and security policies.

4. Developing policies and programs for Army intelligence and intelligence oversight and planning and supervising the execution of those policies and programs.

(b) 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 brigade combat teams.

(c) The Deputy Chief of Staff, G-2, also exercises staff supervision over the United States Army Intelligence and Security Command (INSCOM). INSCOM conducts and synchronizes worldwide intelligence disciplines and all-source intelligence operations. INSCOM also delivers contract linguist support and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities to support Army, joint, and multinational partners and the IC. INSCOM's functional brigades and groups may provide general support, general support reinforcing, or direct support to theaters through intelligence reach, or they may be force-tailored for deployment to support the joint force.

(2) **United States Air Force (USAF) Intelligence.** The Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance and Cyber Effects Operations (AF/A2/6) is responsible for policy formulation, planning, evaluation, oversight, and leadership of USAF global integrated ISR, electromagnetic warfare, cyberspace, and information capabilities. As the USAF's SIO, the AF/A2/6 is directly responsible to USD(I&S). As head of the USAF IC element, the AF/A2/6 coordinates and advocates for USAF ISR capabilities with the ODNI.

(3) **United States Space Force (USSF) Intelligence**

(a) The Director, USSF ISR [short title: SF/S2] has similar responsibilities as the AF/A2/6. The USSF SF/S2 is directly responsible to USD(I&S) and coordinates USSF ISR capabilities with the ODNI.

(b) The USSF National Space Intelligence Center provides intelligence on foreign space and counterspace capabilities and intent. It performs national and military space operations and evaluates capabilities, performance, limitations, and vulnerabilities of space and counterspace systems and services.

(c) The USSF Space Operations Command is responsible for all intelligence operations and exercises day-to-day responsibility for IRs at the operational to strategic level to meet CCDR objectives.

(4) **Navy Intelligence.** The Director of Naval Intelligence is the Navy's senior official within the defense and intelligence communities regarding intelligence authorities and responsibilities. The Director of Naval Intelligence also serves as the Navy's central liaison for coordination with other Services, joint offices, OSD, ODNI, and national agencies on Navy's ISR and information requirements, capabilities, and resources. The Director of Naval Intelligence is also the Navy's MIP component manager and the NIP resource sponsor. The Naval Intelligence Activity (NIA) is the Navy's functional manager for naval intelligence, tasked with the synchronization of naval intelligence with other elements of the IC. The NIA manages all aspects of the Navy's foreign intelligence-sharing relationships, executes the Navy's international intelligence engagement strategy, and serves as the single Navy element responsible for coordinating and deconflicting CI and HUMINT operations conducted under Navy authorities. The Office of Naval Intelligence is the leading provider of maritime intelligence.

(5) **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; MIP manager; and chief architect of the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise and has OPCON of the Marine Corps Intelligence Activity. This encompasses all aspects of the intelligence function. As such, the Director of Intelligence serves as the Service Intelligence Chief for joint intelligence matters and formulates policy for intelligence and CI.

(b) The Headquarters, United States Marine Corps (HQMC), Deputy Commandant for Information's Information Intelligence Division, is responsible for policy, plans, programming, budgets, and staff supervision of intelligence and supporting activities within the United States Marine Corps. The HQMC Information Intelligence Division supports the Commandant of the Marine Corps in the role as a member of the JCS and represents the Marine Corps in joint and IC matters. The HQMC Information Intelligence Division has Service staff responsibility for GEOINT, SIGINT, HUMINT, MASINT, CI, OSINT, and the tactical exploitation of national capabilities program and ensures there is a single synchronized strategy for the development of the Marine Corps ISR capabilities.

(6) **National Guard (NG) Intelligence Support.** NG incident awareness and assessment (IAA) assets can provide a collection, dissemination, and communications bridge between state/local authorities and DoD agencies. NG IAA assets principally focus on the geographic aspects of the OE that affect all-hazard response operations like terrain, trafficability, lines of communications, hydrology, and damage assessment. NG IAA forces can serve as a liaison between DoD and state/local agencies and provide augmentation and liaison to state and local agencies, as well as serve the needs of DoD for local IAA support. The National Guard Bureau (NGB) 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 NGB J-2 provides intelligence products, policy guidance, training, tools, IAA support, intelligence

oversight, and special security activities to the NG JFHQ-State and NG forces in Title 32, USC, or state active duty status, IAW applicable DoD and Service policies.

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

(7) **Defense Threat Reduction Agency (DTRA).** DTRA is a CSA that enables DoD, the USG, and international partners to counter and deter WMD and emerging threat networks, while supporting the nuclear deterrent. DTRA develops and maintains data and technical tools to conduct analysis on chemical, biological, radiological, or nuclear (CBRN) plume hazard estimations and explosive hazards in support of a commander's collateral damage estimation (CDE) requirements. DTRA's capability encompasses the entire spectrum of CBRN threats and utilizes on-staff subject matter experts, as well as software capabilities, to conduct in-depth, long-range, and time-sensitive plume hazard analyses. DTRA's countering emerging threat network expertise includes, but is not limited to, comprehensive persistent views of networks, pattern analysis, geospatial analysis, network dynamics analysis, social network analysis, complex adaptive systems analysis, products that support JIPOE, and target intelligence, all focused on defining and enabling the commander to have desired effects on networks. DTRA also harnesses, masses, and fuses information, analysis, technology, interagency collaboration, and training support to enable more precise attacks to counter threat networks. DTRA provides analytical support and enemy network information to other USG organizations and multinational partners. DTRA also provides modeling, predictions, assessments, publications, lessons learned, analysis, and other support as required. DTRA provides technical reachback support through the DTRA National Weapons of Mass Destruction Technical Reachback Enterprise, a continuous WMD and CBRN national reachback and SA facility, for all technical analysis support. During CBRN response, DTRA liaises with other technical support providers and the IC to meet support requests.

For additional details on DTRA capabilities, see the DoDD 5105.62, Defense Threat Reduction Agency (DTRA).

7. National Intelligence Community Organizations and Responsibilities

a. The IRTPA of 2004 created the ODNI to improve information sharing, promote a unified and strategic direction for the IC, and ensure integration of effort across the IC. The DNI serves as the principal advisor to the President, 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 DNI work closely with their leadership team 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. ODNI is led by DNI and comprises several components, including the National Counterterrorism Center, the National Counterproliferation Center, the National Counterintelligence Executive, and the National Intelligence Council.

(1) The IRTPA of 2004 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 threat 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 plan strategies to collect the data and to evaluate IC performance in fulfilling assigned tasks. The IRTPA of 2004 also established the Office of the Ombudsman for Analytic Objectivity within the CIA to carry out duties detailed in Title 10, USC, Section 3525.

(2) The ODNI Deputy Director for Intelligence Integration deconflicts national and DoD intelligence activities and enhances 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. The CIA also oversees the Open Source Enterprise. The Director, CIA, serves as the National HUMINT Manager and coordinates, deconflicts, and evaluates clandestine HUMINT operations across the IC. 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. 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. 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 to support both foreign policy and national security with an emphasis on terrorism and foreign law enforcement activities, including proliferation concerns.

d. The **FBI,** as a member of the Department of Justice, 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 (CT) operations conducted in the United States. FBI CI operations overseas are coordinated with the CIA. The FBI shares law enforcement/CI information with appropriate DoD entities and 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, transnational organized crime, and illicit finance.

f. The **Department of Energy** analyzes foreign information that is relevant to US energy policies and nonproliferation issues to identify and mitigate threats to US national security and the Department of Energy enterprise. Seventeen national science and engineering laboratories are under its authority and they help inform national security decision making through scientific and technical (S&T) expertise.

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.

h. The **USCG** is a member of the IC. 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 within the Coast Guard. The ICC provides intelligence to Coast Guard operating units, DHS, and all members of the IC, including DoD and key decision makers at the national level.

i. **DEA** enforces laws and regulations governing narcotics and controlled substances, chemical diversion, and trafficking. It is also the lead agency overseas for counterdrug law enforcement activities and investigations. DEA is responsible for the collection, analysis, and dissemination of drug-related intelligence. DEA's intelligence mission is to collect and produce intelligence in support of the DEA Administrator and other federal, state, and local agencies; establish and maintain close working relationships with all agencies that produce or use narcotics intelligence; increase the efficiency in the reporting, analysis, storage, retrieval, and exchange of such information; and undertake a continuing review of the narcotics intelligence effort to identify and correct deficiencies.

8. Joint and National Intelligence Support Forums

a. **CCMD JIOCs.** The CCMD JIOC is the first stop for CCMD staff, Service component commands, and subordinate joint force headquarters (HQ) IRs. For non-time-sensitive requirements, JIOCs receive RFIs from 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 CRs 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; United States Forces, Korea; Supreme Headquarters Allied Powers Europe; and North Atlantic Treaty Organization (NATO) HQ. The DIA senior representative, as the forward representative of DIA, enhances and expedites the exchange of information between DIA and the supported command. They provide 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. The DIA Directorate of Science and Technology provides DIA senior representatives to the CCMDs in the form of senior science and technology officers (SSTOs) and IT representatives (referred to as chief information officer senior representatives). The SSTO helps expedite science and technology operational support between the DIA Directorate of Science and Technology and the supported CCMD. For example, the SSTO provides technical assistance on MASINT capabilities available to support military operations. Additionally, SSTOs are the means for providing feedback on the commander's operational needs for integration into MASINT-related current operations and future acquisition requirements.

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) **NGA Representatives.** NGA provides representatives to the CCMDs, Services, and CSAs 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 point of contact (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; and coordinates geospatial support.

Annex B (Intelligence). Annex B is the intelligence annex to a campaign or contingency plan or order that assesses the adversary situation, provides a detailed intelligence estimate, establishes priorities, identifies intelligence products, assigns intelligence tasks, requests support from higher echelons, and supporting and collaborating combatant commands, and describes the concept of intelligence procedures.

(2) **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 both 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 *(U) Global Force Management Allocation Plan* and through annex B (Intelligence) to 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.

(2) **Required Support from Supported Commands.** Supporting national intelligence agencies may require infrastructure, transportation, logistic, and communications bandwidth support from the supported command. At a minimum, it requires 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 and relevant meteorological and oceanographic (METOC) data should be available to the J-2 organization, joint METOC personnel/offices, and the JFC.

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

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 Support Branch coordinates the specialized intelligence support provided by various organizations to supported CCMDs to preclude redundancy with any support being provided by federation partners during a crisis.

(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, joint exploitation, forensic-enabled intelligence (FEI), and biometrics-enabled intelligence (BEI) specifically related to COIN, countering improvised explosive devices (IEDs), and threat identification and joint targeting. These capabilities may deploy with other supporting joint force units as requested.

(2) NSA/CSS can provide support teams for crisis response. The teams provide enhanced SA, threat warning, personnel recovery support, and tailored intelligence products as required. During the initial stages of crisis, a CCDR can request the immediate deployment of a support team to provide remote limited access to NSA's 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 daily. 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.

9. Interoperability of Intelligence Systems and Processes

a. The threat environment and evolving security challenges reinforce the need for the joint force to be able to quickly combine capabilities within itself and mission partners throughout the OE (at all levels), across geographic boundaries, and organizational affiliations. Meeting these challenges also requires the ability to utilize global agility, demonstrating flexibility, improving synergy, using flexible/low-signature capabilities, establishing secure communications, and integrated joint and partner ISR capabilities along with other global enabling capabilities.

b. The Defense Intelligence and Security Enterprise is supported by a diverse array of capabilities providing documented processes and organizational structure, as well as IT strategy, systems, networks, databases, and applications. These capabilities originate from the Services, CCMDs, and CSAs and are interoperable with diverse mission partners. The combination of these intelligence information capabilities, associated processes, and personnel enables the collection, processing, storage, dissemination, and management of information to joint and partner forces and support personnel. This set of capabilities includes communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. This collaborative environment supports DoD and IC missions and functions across the competition continuum.

c. Enabling capabilities from the IC and DoD provide an intelligence architecture that requires common standards across a range of technology approaches and across a range of organizational entities from IC agencies to subordinate CCMD organizations, a range of organizational levels from strategic to tactical units, and a range of security domains (networks) from those that are highly classified with highly controlled access to the unclassified, open environment.

d. The Department of Defense information network (DoDIN) supports all military operations by enabling US mission partners to securely and seamlessly share required information. However, multinational information sharing seams and challenges exist, requiring extensive manual cross-domain [network] transfers as information is shifted out of one controlled security domain [network] and injected manually into another. Joint forces must be able to integrate effectively with USG departments and agencies, PN militaries, and indigenous and regional stakeholders. This integration must be scalable, ranging from the ability of an individual unit to utilize the expertise of a nongovernmental partner to multinational operations. A mission partner environment information sharing capability framework has been developed using these criteria to enable assured information exchange among mission partners and consists of a combination of people, systems, policies, procedures, and processes to plan, prepare, and execute operations within a collaborative IE.

10. Intelligence and the Department of Defense Information Network

a. The 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. It includes all communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems and supports all DoD missions and functions. 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. DIA establishes DoD-wide intelligence priorities to achieve interoperability among the tactical, theater, and national intelligence systems and their 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 uses this standard "package," in coordination with DIA, to build a theater intelligence architecture based on the mission, CCDR guidance, and command requirements.

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 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) 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.

(b) 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, Nonclassified Internet Protocol Router Network (NIPRNET), SIPRNET local area network (LAN), SCI LAN workstations, joint deployable intelligence support system (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. 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 enables 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 SA, rapid threat warning, friendly force tracking, combat search and rescue, missile defense, 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 and METOC 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 a 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. **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) **TROJAN SPIRIT II.** Marine Corps forces use the High Bandwidth Special Intelligence-Palletized Terminal and the Expeditionary Command and Control System. The Army and Marine Corps and special operations forces (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 and weather 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.

SECTION C. INTERAGENCY, INTERNATIONAL, AND MULTINATIONAL INTELLIGENCE SHARING

11. Principles for Multinational Intelligence Sharing

a. In most multinational operations, the JFC shares intelligence with foreign military forces and coordinates receiving intelligence from those forces. Intelligence efforts should complement and take into consideration the intelligence system's strengths, limitations, and each nation's unique and valuable capabilities. In some multinational operations or campaigns, JFCs can use existing international standardization agreements (e.g., NATO) as a basis for establishing rules and policies for conducting joint intelligence operations. Since each multinational operation is unique, such agreements may have to be modified or amended based on the situation. The joint force should consider releasability of information to allies (e.g., NATO) and trusted and vetted PNs, as this approach facilitates expedited information sharing. A JFC participating in a multinational force develops the information sharing policy and procedures for that particular operation based on CCDR guidance and national policy as contained in the National Disclosure Policy (NDP)-1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations.* NDP-1 provides policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance. The following general principles provide a starting point for creating the necessary policy and procedures:

(1) **Align with NDP.** CCMD and the joint force foreign disclosure officers (FDOs) require authorization before they share classified military information or national intelligence with a foreign entity. Classified military information, as defined in the National Security Decision Memorandum 119, *Disclosure of Classified US Military Information to Foreign Governments and International Organizations,* is that set of classified information that is under the control or jurisdiction of DoD, its departments or agencies, or is of primary interest to them.

(2) **Maintain Unity of Effort.** Intelligence personnel of each nation need to view the threat from multinational as well as national perspectives. A threat to one element of the multinational force by the common adversary is a threat to all multinational force elements. Success in intelligence sharing requires establishing a trusted partnership with foreign counterparts to counter a common threat and maintain unity of effort.

(3) **Make Adjustments.** There will be differences in intelligence doctrine and procedures among the multinational partners. A key to effective multinational intelligence is readiness, beginning with the highest levels of command, to make the adjustments required to resolve significant differences. Major differences may include how intelligence is provided to the commander (jointly or through individual Services or agencies), procedures for sharing information among intelligence agencies, and the degree of security afforded by different communications systems and procedures. Administrative differences that need to be addressed may include classification levels, personnel security clearance standards, requirements for access to sensitive intelligence, and translation requirements.

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

(5) **Share Necessary Information.** The joint force should share relevant intelligence about the situation and adversary with its multinational partners consistent with respective NDP and JFC guidance. However, information about intelligence sources and methods should not be shared among allies and PNs until approved by the appropriate national-level agency.

(a) To share critical intelligence information with allies and PNs efficiently, US intelligence information should be written for release at the most appropriate classification level and given the fewest possible dissemination restrictions within foreign disclosure guidelines. When information relating to a particular source cannot be shared, the intelligence derived from that source may still be provided to other PNs, so long as the information itself does not compromise the source. The J-2 establishes procedures for separating intelligence from sources and methods. "Writing for release," which is the deliberate process of producing information with the intent and foreknowledge that a final product may be disclosed to mission partners, should be practiced at all levels; any references to sources and methods should only be included below a tear line to maximize the ability to share relevant information with partners. Intelligence production agencies often use a tear line in classified reports to separate compartmented information from intelligence that can be widely disseminated (the J-2 and component intelligence staff officers keep information above the tear line and disseminate the intelligence below). Having intelligence production agencies use such tear lines facilitates intelligence sharing.

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

(c) Intelligence support is critical to the commander's force protection mission. Every effort must be made to share data that could impact the commander's force protection mission.

(6) **Conduct Complementary Operations.** Intelligence efforts of each nation should be complementary. Each nation possesses strengths and limitations, along with unique and valuable capabilities within its individual intelligence system. Host-nation security services' capabilities, for example, may contribute significantly to force protection. Furthermore, planning with friendly nations to fill shortfalls, especially linguist requirements, may help overcome such limitations. All intelligence resources and capabilities should be made available for application to the whole of the intelligence problem. Establishing a multinational collection management element is essential for planning and coordinating multinational collection operations.

b. See Figure II-3 for examples of common organizations with which DoD intelligence forces may form relationships. 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 a shared understanding. 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 the JFC, staff, J-2, subordinate units, mission, and multinational partners understand the permissions and restrictions on information sharing.

c. 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 share intelligence accordingly.

d. The CCMD FDO plays a key role in any intelligence-sharing plan with multinational, interagency, or nongovernmental entities. The FDO can guide the JFC and staff in the proper procedures for the release of classified or sensitive information IAW NDP. The FDO provides staff review and advises the JFC on approval of sanitized or downgraded military intelligence products. CCMDs can establish releasable cell teams,

Common Entities and Agencies Encountered In Multinational Operations

- Allies: Great Britain, Canada, Australia, New Zealand
- Interagency: CIA, FBI, DOS, DHS
- International: UN, NATO, OSCE, ASEAN
- Nongovernmental: Red Cross, World Food Programme, Save the Children

Legend

ASEAN	Association of Southeast Asian Nations	NATO	North Atlantic Treaty Organization
CIA	Central Intelligence Agency	OSCE	Organization for Security and Co-operation in Europe
DHS	Department of Homeland Security	UN	United Nations
DOS	Department of State		
FBI	Federal Bureau of Investigation		

Figure II-3. Common Entities and Agencies Encountered in Multinational Operations

which produce and disseminate releasable versions of ongoing JIOC production. This process should closely match the topics and timeliness of normal ongoing production, by anticipating the demand signal from foreign partner sharing. 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 and request exceptions to disclosure policy as appropriate. Ideally, a cross-domain (network) solution would be established with parameters, which are vetted and approved by the FDO to ensure safeguarded and efficient dissemination to multinational partners.

For more information on foreign disclosure programs, policies, and guidance, see NDP-1, National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations; *DoDD 5230.11,* Disclosure of Classified Military Information to Foreign Governments and International Organizations; *and CJCSI 5221.01,* Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations.

12. Multinational Intelligence Collaboration

a. Typically, in a multinational operation, allied military intelligence counterparts may locate or co-locate around the JTF HQ in the form of national intelligence cells and may contribute to the multinational intelligence fusion cell that develops the combined intelligence picture. The JTF/J-2 should establish good working relationships with multinational partners to encourage a shared view of the OE and their contributions to the combined intelligence picture. 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. 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 within 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 United States, 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 SIPRNET 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. 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 United States. 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 United States Indo-Pacific Command (USINDOPACOM) 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. Within the United States Africa Command's AOR, the BICES-X [Battlefield Information Collection and Exploitation System Extended] network connecting PNs is referred to as the African Data Sharing 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 are 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 Headquarters 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 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, and 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 CJTF 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 CJTF 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 combined intelligence picture and 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 CJTF and staff. In many cases, the US JISE or JIOC responds to requests for information from the multinational intelligence center (see Figure II-4).

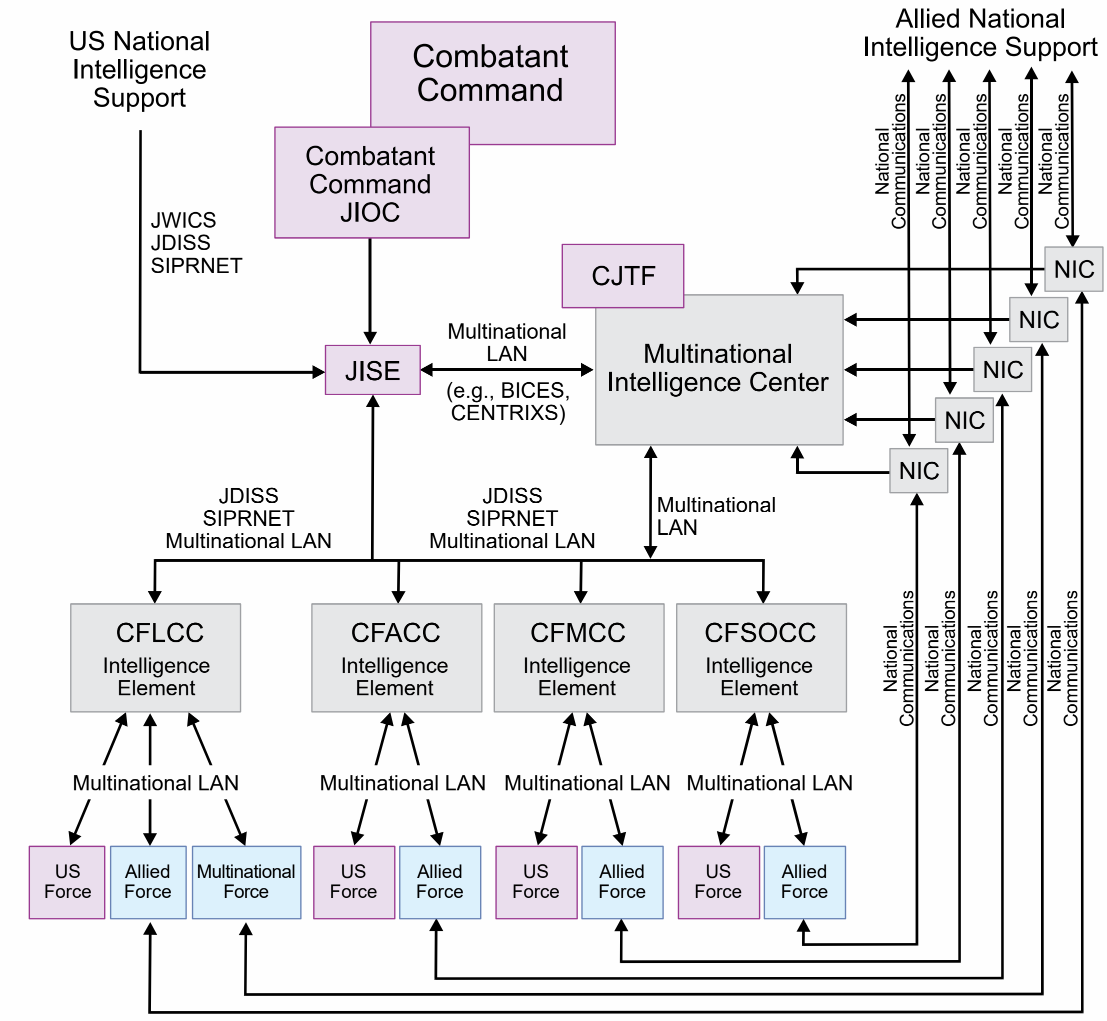
NATO uses fully developed and coordinated doctrine, contained in Allied joint publications and standardization agreements. When the Armed Forces of the United States participate in multinational operations, US commanders should follow multinational doctrine and procedures that have been ratified by the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

g. Operational requirements may necessitate working with and sharing intelligence with new local or host-nation partners, which may not have robust information sharing or government capabilities to host, process, or safeguard information. Planning for working with unexpected or lower capacity partners should take into account the limits of communications infrastructure, as well as requirements to share and safeguard intelligence. JFCs may need to support or build partner capacity with such partners, potentially while conducting operations, to enable effective intelligence sharing.

(1) The DoDIN enables data collected by any means to be communicated directly to a user or to a processing site or platform by the most efficient path, then passed on or through to the user, as appropriate. A critical aspect of the information network is its ability to make all intelligence accessible by way of standardized file servers to standards-compliant workstations.

(2) The DoD Intelligence Information System enterprise is the global set of resources (people, facilities, hardware, software, and processes) that provide IT and information management services to the DoD military IC through a tightly integrated, interconnected, and geographically distributed regional service center architecture. The

Notional Multinational Intelligence Architecture



Legend

BICES	Battlefield Information Collection and Exploitation System
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFACC	combined force air component command
CFLCC	combined force land component command
CFMCC	combined force maritime component command
CFSOCC	combined forces special operations component command
CJTF	combined joint task force
JDISS	joint deployable intelligence support system
JIOC	joint intelligence operations center
JISE	joint intelligence support element
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
NIC	national intelligence cell
SIPRNET	SECRET Internet Protocol Router Network
US	United States

Figure II-4. Notional Multinational Intelligence Architecture

enterprise capabilities are centrally managed and decentrally executed under the authority and direction of the DIA Chief Information Officer.

(a) **SCI Support.** The JWICS is an SCI element of the Defense Information System Network. JWICS incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and VTC. Additionally, the JDISS provides a transportable workstation and communications suite that electronically extends a joint intelligence center to a JTF or other tactical user. Both systems currently form the common baseline for all SCI support systems in the intelligence architecture.

1. **JWICS** satisfies the requirement for secure, high-speed, multimedia transmission services for SCI. JWICS incorporates advanced networking technologies that permit greater throughput and capacity, making possible the use of applications that take advantage of multimedia technologies including VTC. Video-capable JWICS nodes can create, receive, transmit, and store video images, as well as voice, text, graphics, and data. Information can be either broadcast or shared interactively among JWICS subscribers on a point-to-point or multipoint basis. The JWICS circuit can be managed by way of allocation of bandwidth, allowing simultaneous use of the link for multiple applications.

2. **JDISS** provides the standard workstation server software configuration. The basic backbone for the dissemination of intelligence to and from deployed JDISS nodes is the JWICS network. Where JWICS is not required or not available, JDISS has a versatile communications capability that can interface with existing communications systems, such as tri-Service tactical communications systems. The system architecture optimizes flexibility to focus intelligence efforts efficiently and ensures that support is maximized for a joint force conducting military operations.

(b) **Non-SCI Support.** The SIPRNET, NIPRNET, and Global Command and Control System (GCCS) provide common, non-SCI support systems for joint forces and interagency partners.

(c) **Multinational Support.** Multinational intelligence sharing should be facilitated by establishing a shared LAN using systems such as BICES, CENTRIXS, or other emerging multinational mission networks. As the current DoD multinational information-sharing portion of the DoDIN, CENTRIXS defines the standards for establishing and maintaining multinational connectivity at the tactical and operational level, with reachback capability to the strategic level. Missions requiring information sharing with NGO partners can leverage the All Partners Access Network, which facilitates information sharing between military and nonmilitary organizations. The establishment of a collaborative environment for mission partners facilitates information sharing within a multinational force. Operations require US forces and mission partners to understand the tactics, techniques, and procedures (TTP) for establishing and operating a collaborative network that is enabled by the technical capabilities that each PN brings to the operation. Within a collaborative environment with PNs, the US commander needs to balance "need-to-know" with the responsibility to share and understand the associated risk.

h. Standardized procedures for disseminating and exchanging intelligence constitute the third component of an intelligence-sharing architecture. These procedures are critical to joint and multinational operations and interagency coordination.

EXAMPLES OF MULTINATIONAL INTELLIGENCE SHARING LEVELS

Procedures established to support United States (US) and United Nations (UN) forces in Somalia as members of the United Nations Operations in Somalia (UNOSOM II) effort used two levels of intelligence: Level 1 data could be shown to but not retained by coalition forces or the UN, while Level 2 data was cleared for release to the coalition and the UN. Level 1 intelligence remained within US-only channels, while Level 2 data flowed to the UNOSOM II information center in Mogadishu either from the UN Headquarters or via the US joint intelligence support element.

In some situations, there may be more than two levels of intelligence required. For example, an operation involving a mixture of North Atlantic Treaty Organization (NATO) and non-NATO forces could have "United States Only," "Releasable to NATO," and "Releasable to Non-NATO" levels. The multinational force commander (MNFC) plays a major role in advising the national intelligence community on the intelligence requirements for each of the allies and coalition partners. The MNFC recommends what intelligence should be provided to each member.

Various Sources

(1) The procedures and methodology for intelligence and information sharing should be conceived and exercised as part of multinational and interagency planning before operations begin. Special attention should be paid to intelligence classification and levels of access of multinational personnel. To this end, the J-2 should consider adding extra FDO billets to facilitate information sharing. The effectiveness of the procedures and methodology should be monitored and, when necessary, adapted during operations to meet changing circumstances.

(2) Data intended for inclusion in DoD databases should be labeled and marked IAW IC data formatting standards to enable discoverability and fusion with other all-source data.

13. Synchronization of International Efforts

JFCs recognize the complex, interconnected, and largely unpredictable nature of the OE and the need to better understand the associated military challenges. 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 or insight and understanding that these organizations possess. Establishing sharing arrangements with partners fosters a common understanding of the associated military challenges and the conditions necessary to achieve success. This approach provides a common framework to achieve unity of effort with our partners. 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.

14. Interorganizational Intelligence Collaboration

a. The role of DoD intelligence elements in an operation involving interagency partners is dictated by the nature of the support relationship. DoD intelligence organizations should expect to operate alongside interagency partners as needed to conduct authorized intelligence functions in support of operations conducted in the homeland IAW Executive Order 12333, *United States Intelligence Activities;* DoDD 5240.01, *DoD Intelligence Activities;* and DoDM 5240.1, *Procedures Governing the Conduct of DoD Intelligence Activities.*

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 continuously and includes IC liaison officers (LNOs). One of the primary functions of the NOC is to provide SA of potential incidents and threats to the United States. The NOC maintains continuous contact with other federal agency operations centers, including the NJOIC, and issues situation reports on emerging crises.

c. In terrorism or security-related incidents, the FBI Strategic Information and Operations Center (SIOC) acts as the FBI's worldwide emergency operations center (EOC) by maintaining SA of criminal or terrorist threats, critical incidents, and crises, providing command, control, and communications connectivity. The SIOC is also the FBI's COP for managing operational responses, establishing the HQ command post, developing connectivity to joint operations centers (JOCs), and sharing information and intelligence with other EOCs at all levels of government, to include the DHS NOC. The SIOC ensures effective coordination and liaison with partner agencies and coordination and information sharing with other leaders, as appropriate and IAW classification and legal requirements, to manage the threat.

d. During homeland defense (HD), military forces may be used to counter threats and aggression against the United States. DoD will be designated as the LFA, supported by other USG departments and agencies, in defending against traditional threats or aggression. When ordered to conduct HD operations, United States Northern Command (USNORTHCOM) or USINDOPACOM normally designates 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 joint interagency coordination groups (JIACGs). In addition, the JTF may request the presence of liaison elements representing other USG departments and agencies.

e. DSCA is support provided by US federal military forces, DoD civilians, DoD contractor 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 are always used in a support role. DHS or the Federal Emergency Management Agency (FEMA) designates a LFA to coordinate the USG response. The nature of the emergency drives the selection of the LFA. The LFA establishes a joint field office (JFO) in proximity to the emergency area. The JFO may be thought of as an 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 co-locate the JOC within the JFO. The JOC acts as the lead for all investigative and intelligence issues. National intelligence agencies work with the JOC to provide and receive SA. Additional information on the structure and concepts of operation for the JOC and JFO can be found in the DHS's National Response Framework.

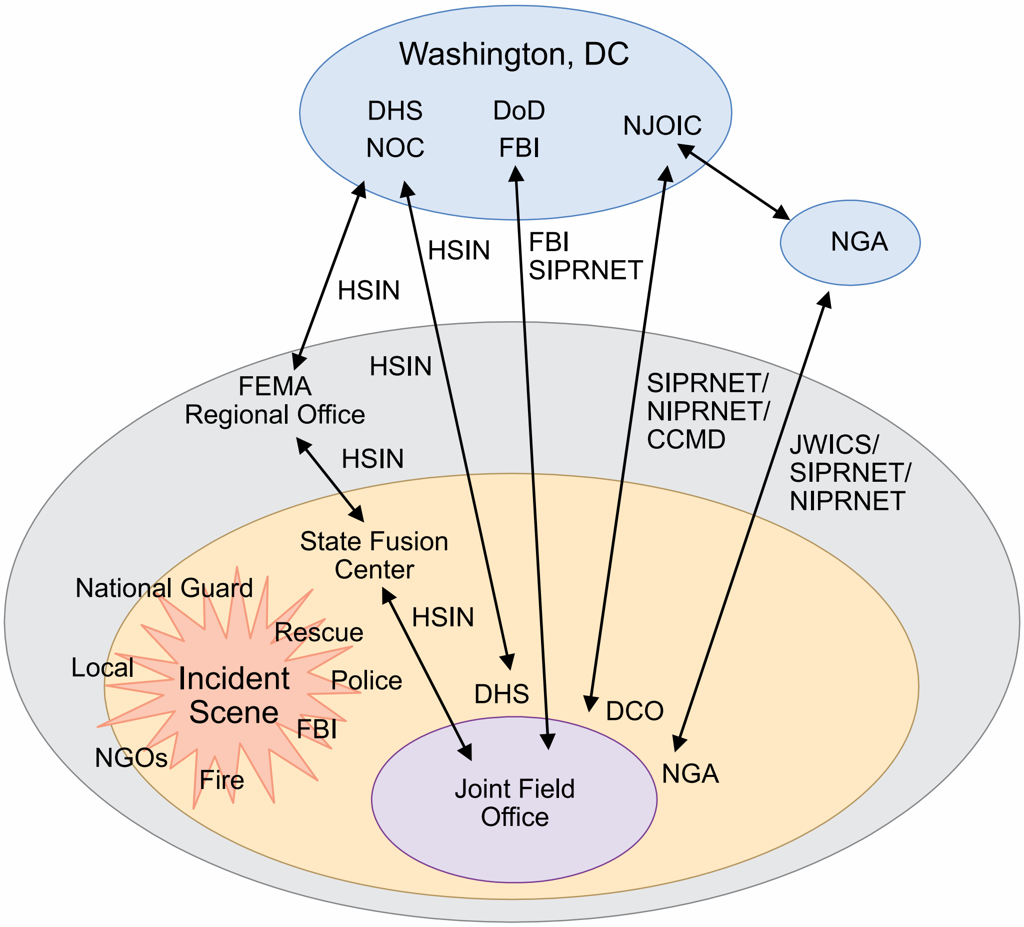
f. USNORTHCOM or USINDOPACOM designates a defense coordinating officer (DCO) upon receipt of a request for assistance from the LFA. The USNORTHCOM DCOs are typically United States Army North, O-6-level staff officers who are in support of one of the nine FEMA regions and have interagency experience. USINDOPACOM DCOs (based in Hawaii and Guam) work closely with United States 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.

g. Intelligence sharing between interagency participants frequently occurs on an ad hoc basis (see Figure II-5). If designated, the JTF J-2 needs to dedicate sufficient resources to provide liaison to interagency IC elements to encourage a robust exchange of information. The lack of an LFA J-2 staff function in most USG crisis response means there is little pre-planning for intelligence operations. DHS uses its Homeland Security Information Network (HSIN) as its primary C2 and SA tool. 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.

h. 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.

i. 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. DoD imagery collection within the United States should conform to US

Interagency Crisis Response Information Flow



Legend

CCMD	combatant command	JWICS	Joint Worldwide Intelligence Communications System
DCO	defense coordinating officer	NGA	National Geospatial-Intelligence Agency
DHS	Department of Homeland Security	NGO	nongovernmental organization
DoD	Department of Defense	NIPRNET	Non-classified Internet Protocol Router Network
FBI	Federal Bureau of Investigation	NJOIC	National Joint Operations Intelligence Center
FEMA	Federal Emergency Management Agency	NOC	National Operations Center
HSIN	Homeland Security Information Network	SIPRNET	SECRET Internet Protocol Router Network

Figure II-5. Interagency Crisis Response Information Flow

laws and DoD policies. During DSCA operations, military IAA elements should coordinate efforts with the DHS interagency remote sensing coordination cell.

j. In some cases, high-profile events, such as Presidential inaugurations and Olympic games hosted in the United States, are designated as national special security events (Title 6, USC, Section 601), allowing for detailed pre-planning of a government-wide security operation. Depending on the venue and purpose of the event, the United States 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 USINDOPACOM. The NJOIC may stand up a CAT with a corresponding ITF or working group in response.

k. 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 guidance to share information. These entities are designed to support collection, analysis, and dissemination of intelligence to meet standing information needs. Many operate watch centers that are manned on a continuous basis. 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.

l. A number of cleared federal representatives may be available to assist in communication with these centers, including representatives from the 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 (SBU) connectivity to these centers is provided through a variety of shared SA and collaboration tools, including HSIN.

Intentionally Blank

CHAPTER III
THE JOINT INTELLIGENCE PROCESS

1. Introduction

The joint intelligence process provides the basis for common intelligence terminology and procedures. It consists of six interrelated categories of intelligence operations characterized by broad activities conducted by intelligence staffs and organizations for the purpose of providing commanders and national-level decision makers with relevant and timely intelligence. The six categories of intelligence operations include planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback.

2. The Intelligence Process

a. The intelligence process describes how the various types of intelligence activities 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 activities and their interrelationships. Not all activities necessarily continue throughout the entire intelligence process and multiple activities can be carried out simultaneously.

b. **JIPOE.** JIPOE is the analytical process joint intelligence organizations use to produce intelligence assessments, estimates, and other intelligence products in support of the JFC's decision-making process. The JIPOE process provides a holistic understanding of the OE. JIPOE is the continuous process through which J-2 manages the analysis and development of products that help the commander and staff understand the complex and interconnected OE—the composite of the conditions, circumstances, and influences that affect the employment of capabilities, including the civilian environment, that bear on the decisions of the commander. A holistic understanding of the OE enables planners to account for civilian considerations, including population density, patterns of life, cultural norms, and the interconnected relationships between the civilian population, natural resources, infrastructure, and essential services. The J-2 manages the JIPOE process with input from intelligence planners and other staff directorates or elements (see Figure III-1).

c. To support planning activities, intelligence staffs initiate the JIPOE process when the higher HQ receives a planning directive or maintains a running JIPOE product for possible scenarios. JIPOE is conducted both prior to and during an operation, as well as during the planning for follow-on operations. The most current information available regarding the actor and the OE is continuously integrated into the JIPOE process. The outcomes derived from the JIPOE process support planning activities by identifying the objectives, COGs, critical capabilities, requirements, vulnerabilities, COAs, and related decisive points.

d. Incorporating collected information and data into the JIPOE process is a continuous effort. The intelligence staff element continuously evaluates the available intelligence and information databases to determine if the required information is available and sufficient to conduct the remainder of the JIPOE process. There will be gaps in available information

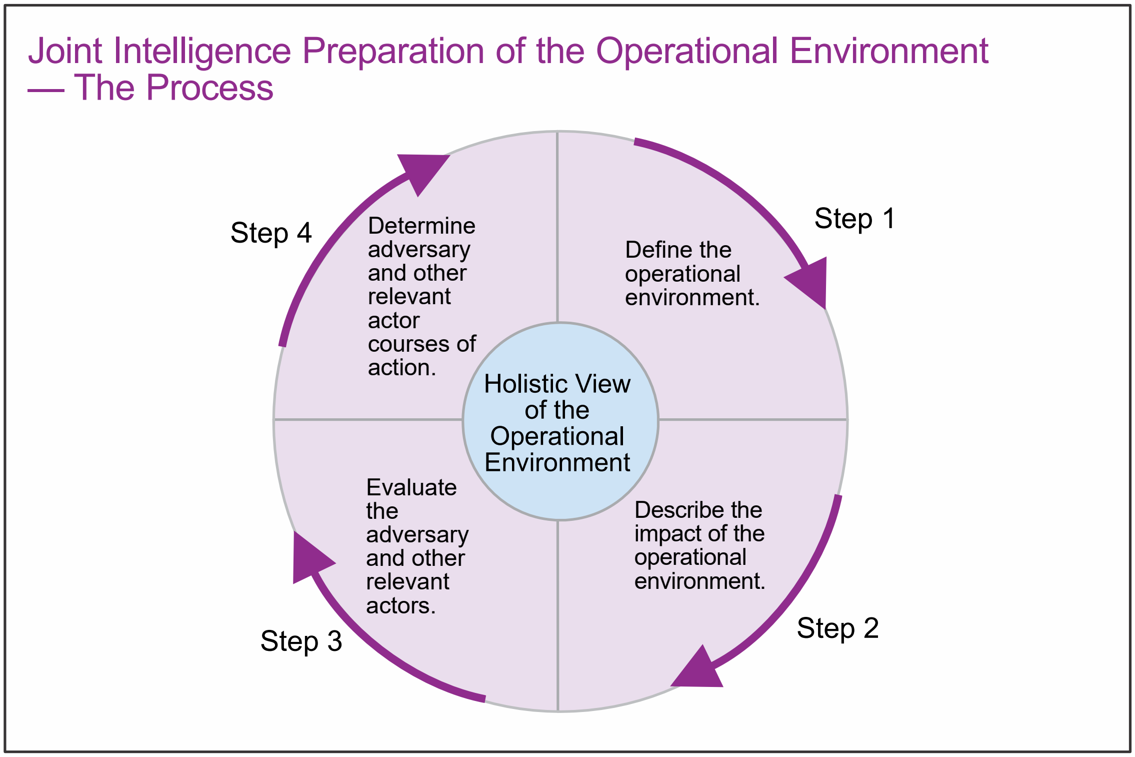

Joint Intelligence Preparation of the Operational Environment — The Process
Step 1
Define the operational environment.
Step 2
Describe the impact of the operational environment.
Step 3
Evaluate the adversary and other relevant actors.
Step 4
Determine adversary and other relevant actor courses of action.
Holistic View of the Operational Environment

Figure III-1. Joint Intelligence Preparation of the Operational Environment—The Process

and shortfalls in the ability of the intelligence staff to fill these gaps. These gaps and shortfalls must be identified early in the process to develop the appropriate IRs and CRs as required.

e. The outputs of JIPOE inform planning for joint operations and the joint targeting process. Additionally, JIPOE assists in the mitigation of and response to civilian harm, including identifying and nominating objects to the no-strike and restricted target lists.

The JIPOE process is described in detail in the Joint Guide for Joint Intelligence Preparation of the Operational Environment.

SECTION A. PLANNING AND DIRECTION

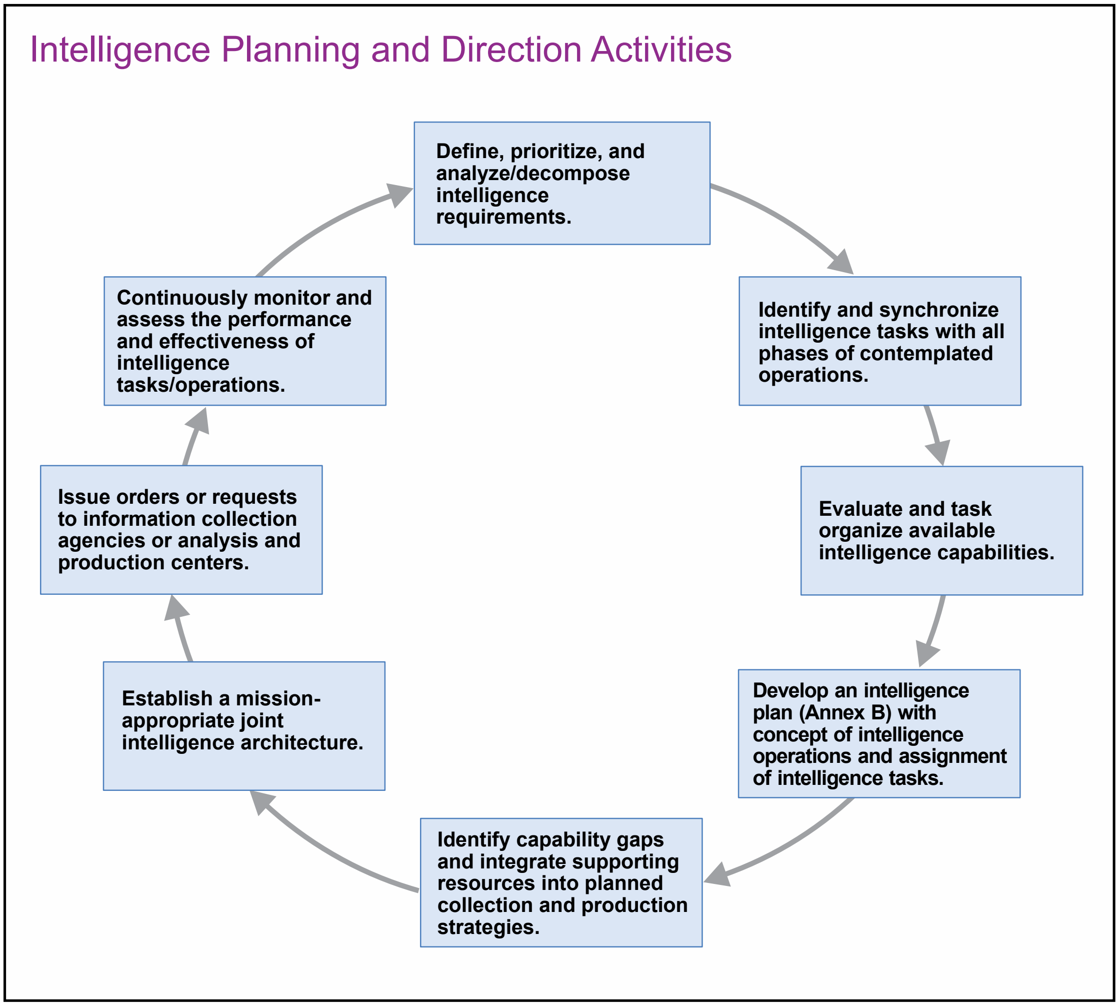
3. Overview

The planning and direction portion of joint intelligence operations occurs continuously as the intelligence component of a command's planning effort across the competition continuum. Joint and Service intelligence planners, through participation in joint planning and assessment processes, lead development of the PIRs, concept of intelligence operations, and detailed intelligence plans (i.e., annex B [Intelligence] to a plan or order), which includes integrated collection strategies and federated analysis and production plans and describes joint intelligence architectures appropriate for the mission. In collaboration with the intelligence staff, they coordinate joint intelligence operations on behalf of the joint force J-2 to satisfy the intelligence needs of the commander and staff. Planning and direction involves the activities shown in Figure III-2.

4. Intelligence Requirements and Information Requirements Planning

a. CCMD- and JTF-level intelligence planners lead IP teams to define, recommend the priority of, and analyze/decompose IRs. They participate in planning and decision-making processes to receive guidance and help focus the intelligence effort. Through participation in the JPP and battle rhythm events, intelligence planners help develop mission success criteria (i.e., desired effects, operational objectives, and end states) and associated metrics to determine what intelligence support may be required to facilitate CCDR and JFC decision making.

b. As an output of the 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-


Intelligence Planning and Direction Activities

Define, prioritize, and analyze/decompose intelligence requirements.

Identify and synchronize intelligence tasks with all phases of contemplated operations.

Evaluate and task organize available intelligence capabilities.

Develop an intelligence plan (Annex B) with concept of intelligence operations and assignment of intelligence tasks.

Identify capability gaps and integrate supporting resources into planned collection and production strategies.

Establish a mission-appropriate joint intelligence architecture.

Issue orders or requests to information collection agencies or analysis and production centers.

Continuously monitor and assess the performance and effectiveness of intelligence tasks/operations.

Figure III-2. Intelligence Planning and Direction Activities

5 is the overall staff proponent to develop FFIRs. During execution, the J-3 is the overall staff proponent to monitor FFIRs. The J-2 leads the development of IRs and the development of information requirements, and PIRs. IRs that are deemed most important to understand the enemy or other aspects of the OE and upon which a commander's decision may be based are identified by the commander as PIRs. Commander involvement is essential in the development of CCIRs, especially identifying and articulating those that focus on neutral and friendly relevant actors. The prior education and professional and life experience of the analysts, staff personnel, and commanders involved in this process will constructively or adversely affect the sufficiency of the range of relevant actors and associated CCIRs considered necessary to understanding the OE.

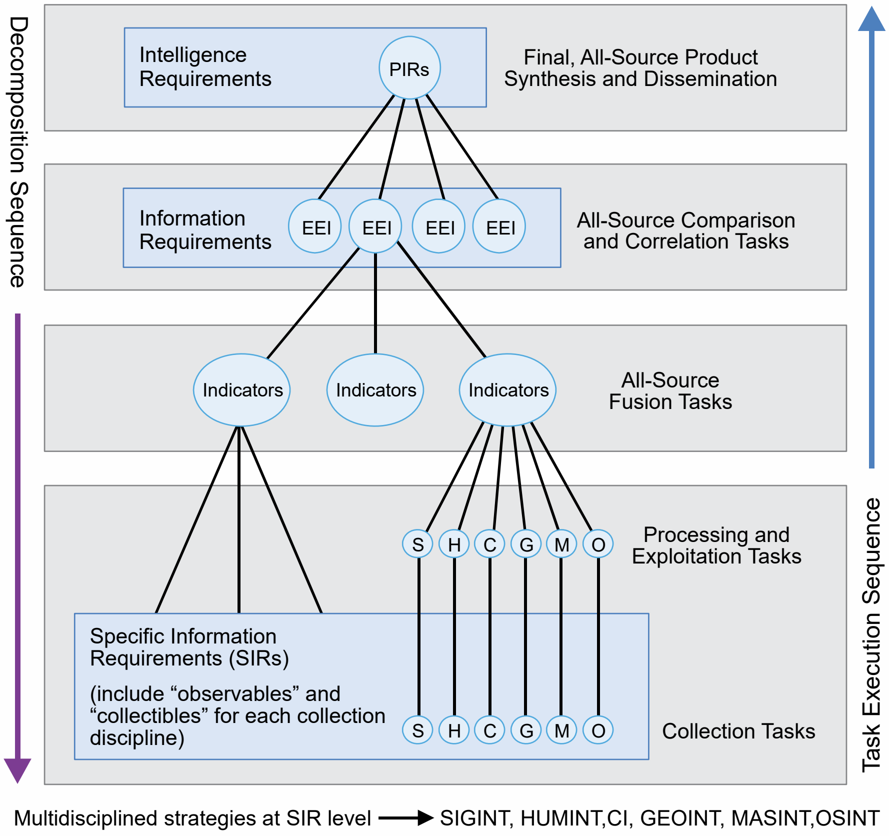
c. Information requirements that are deemed critical or that would answer PIRs are known as EEIs. Satisfying EEIs may require the identification of a series of indicators. Indicators can be identified by focusing collection capabilities against specific information requirements (SIRs). Depending on the nature of collection targets, these indicators may be considered observables or collectables. The former refers to physical characteristics and relates to HUMINT, GEOINT, and some forms of MASINT, while the latter refers to emanations from a target and relate to SIGINT and other forms of MASINT. Properly crafted SIRs should include observables or collectables and anticipated locations to facilitate selection of the appropriate collection capability. The analysis or decomposition of IRs is illustrated in Figure III-3.

d. 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. The time horizons of the decisions the commanders make at the theater level, component level, and tactical level vary and therefore the information required to support the decisions differ. 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.

e. An RFI response disseminates existing products, integrates, or tailors on-hand information, or provides collected data for original production to satisfy customer requirements. It differs from a PIR in that it is not necessarily developed to support a commander's decision regarding the employment of forces. 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 CR is prepared and entered into the appropriate CRM application. The bifurcation of RFIs into either PRs or CRs is illustrated in Figure III-4.

(1) RFIs should be satisfied at the lowest level possible. Requirements that cannot be satisfied are submitted as RFIs to the next higher echelon. Each echelon validates, prioritizes, and, if possible, satisfies the RFI or CR before forwarding it to the

Intelligence Problem Decomposition and Task Execution


Decomposition Sequence
Intelligence Requirements
PIRs
Final, All-Source Product Synthesis and Dissemination
Information Requirements
EEI
EEI
EEI
EEI
All-Source Comparison and Correlation Tasks
Indicators
Indicators
Indicators
All-Source Fusion Tasks
S
H
C
G
M
O
Processing and Exploitation Tasks
Specific Information Requirements (SIRs)
(include "observables" and "collectibles" for each collection discipline)
S
H
C
G
M
O
Collection Tasks
Task Execution Sequence

Multidisciplined strategies at SIR level → SIGINT, HUMINT,CI, GEOINT, MASINT,OSINT

Legend

CI	counterintelligence	OSINT	open-source intelligence
EEI	essential element of information	PIR	priority intelligence requirement
GEOINT	geospatial intelligence	SIGINT	signals intelligence
HUMINT	human intelligence		
MASINT	measurement and signature intelligence		

Ⓢ SIGINT	Ⓖ GEOINT
Ⓗ HUMINT	Ⓜ MASINT
Ⓒ CI	Ⓞ OSINT / other

Figure III-3. Intelligence Problem Decomposition and Task Execution

next level. In certain cases, staffing simultaneously through the multiple echelon submissions is necessary when the request is time sensitive. 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 allocate 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.

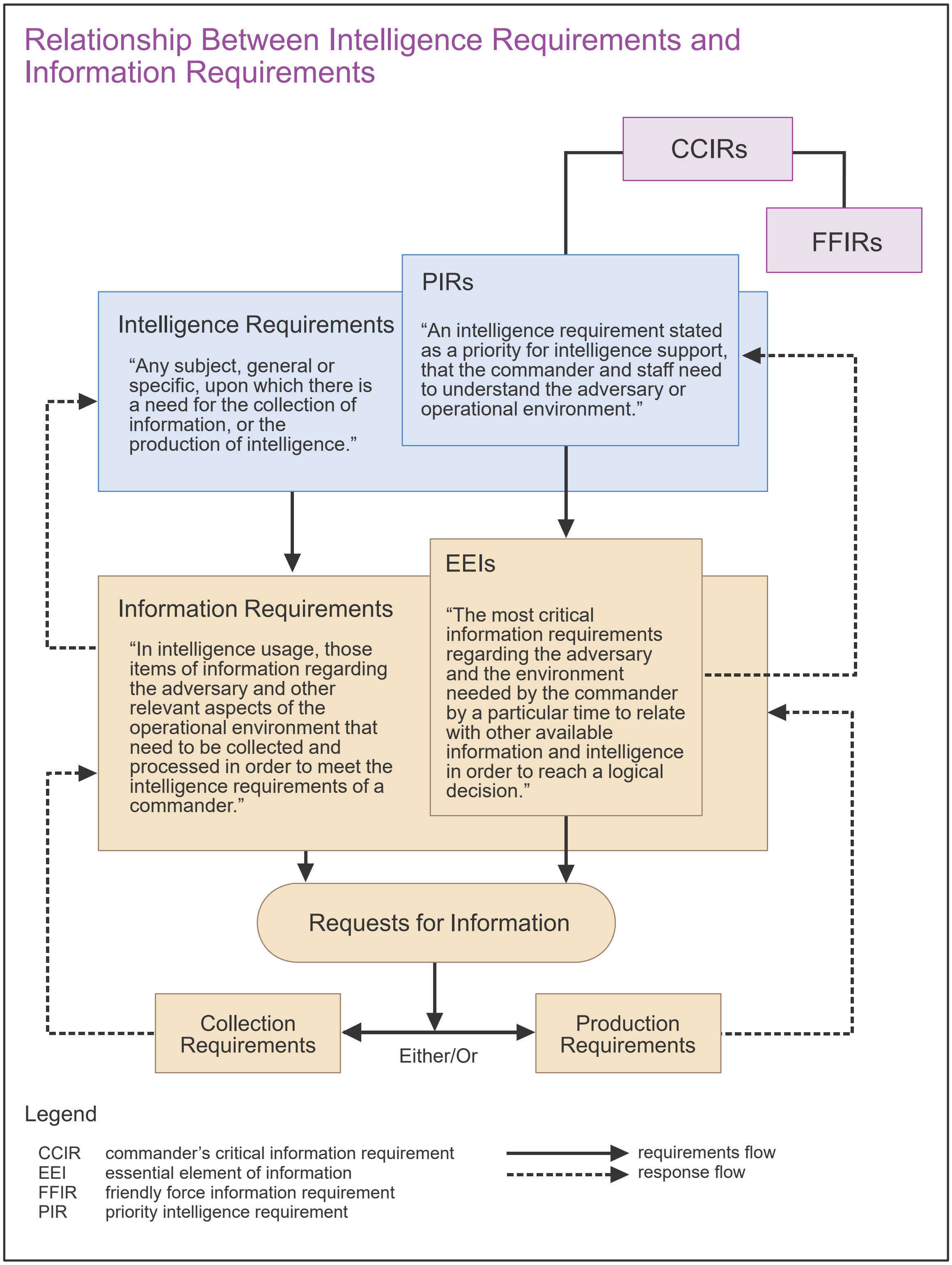

Relationship Between Intelligence Requirements and Information Requirements
CCIRs
FFIRs
PIRs
"An intelligence requirement stated as a priority for intelligence support, that the commander and staff need to understand the adversary or operational environment."
Intelligence Requirements
"Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence."
EEIs
"The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to reach a logical decision."
Information Requirements
"In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander."
Requests for Information
Collection Requirements
Either/Or
Production Requirements
Legend
CCIR commander's critical information requirement
EEI essential element of information
FFIR friendly force information requirement
PIR priority intelligence requirement
requirements flow
response flow

Figure III-4. Relationship Between Intelligence Requirements and Information Requirements

5. Intelligence Planning

a. As the intelligence component of the JPP, IP provides a methodology to coordinate, integrate, and synchronize all available intelligence capabilities to meet the commander's IRs for joint planning, execution, and assessment. It ensures the intelligence system is focused on providing the commander with the intelligence required to make timely, informed decisions that lead to desired effects and achieve operational objectives. An intelligence plan ensures the integration and optimal employment of national-to-tactical collection capabilities and associated PED systems, federated analysis and production centers, and appropriate architectures to support joint operations.

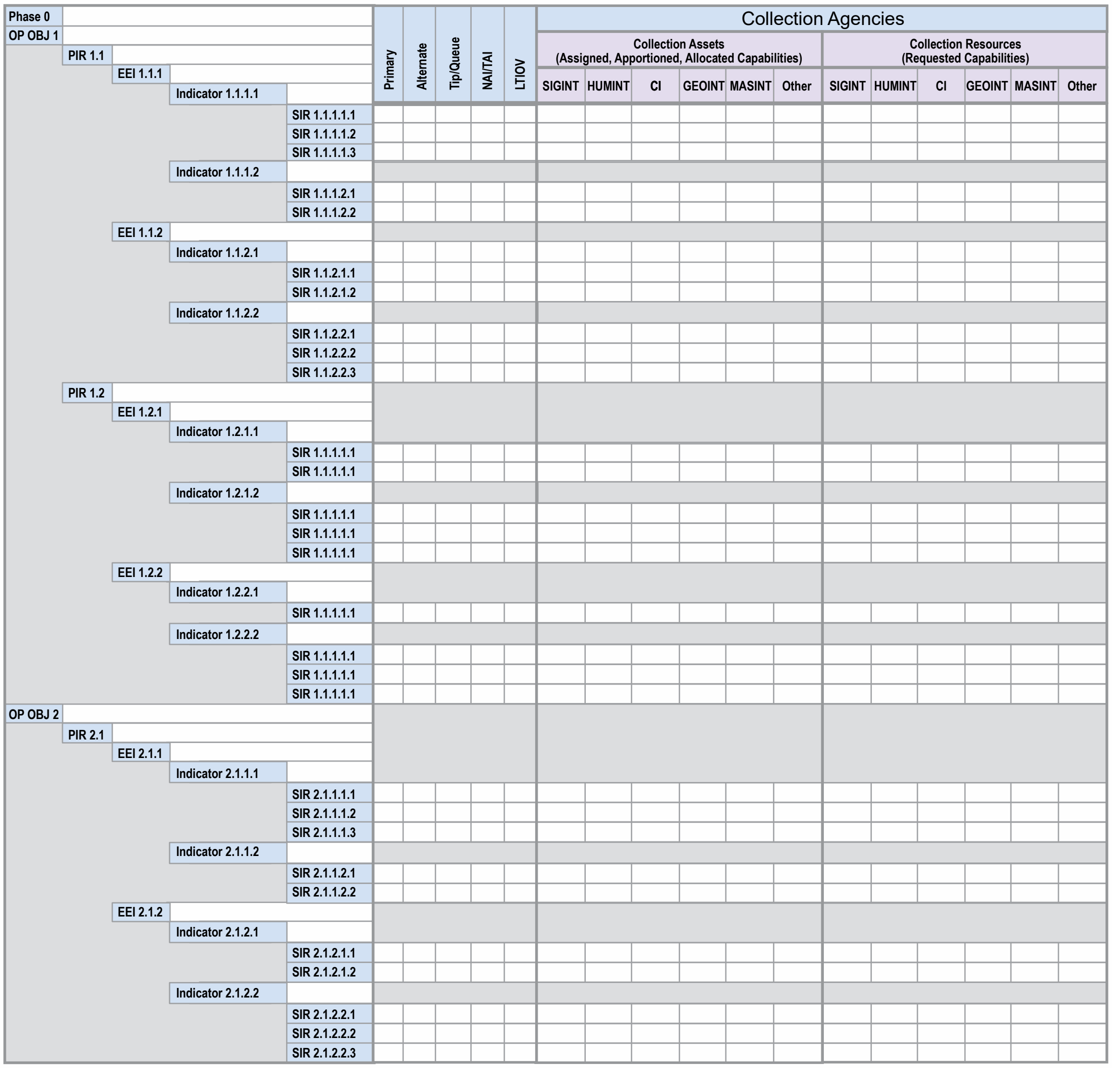
b. The CCMD J-2 leads the development of annex B (Intelligence) to a plan or order that provides detailed information on the enemy or adversary situation, establishes priorities, assigns intelligence tasks, identifies required intelligence products, requests support from higher echelons, describes the concept of intelligence operations, and specifies intelligence procedures. The format for annex B (Intelligence) may be supplemented with a series of functional appendices through which J-2s communicate more specific instructions. Integrated collection planning matrices and federated analysis and production matrices with discrete collection and production tasks are often included in appendix 1 (Priority Intelligence Requirements) to annex B (Intelligence). The detailed format and guidance for the development of an annex B (Intelligence) are contained in CJCSM 3130.03, *Planning and Execution Formats and Guidance.*

(1) The **CRMx** is an integrated, national-tactical, multidiscipline collection planning matrix that addresses anticipated CRs expressed as SIRs, with imbedded observables or collectables. The CRMx correlates the identified requirements with the collection capabilities that are best suited to satisfy collection tasks. This correlation results in a multidiscipline strategy for each anticipated CR. If appropriate, tipping and cueing indicators should be identified. The intent of the CRMx is to optimize the allocation and employment of all available collection assets and resources across all phases of contemplated operations. CRMx development occurs during the collection planning portion of the IP process. As members of the IP team, collection managers support intelligence planners in the development of the integrated collection plan captured in the CRMx. Figure III-5 provides an example of a CRMx or integrated collection planning matrix.

(2) The **PRMx** is a compilation of prioritized, all-source analysis and production tasks and subtasks. When completed, the PRMx reflects a crisis federated production plan that is intended to optimize the employment of all available Defense Intelligence and Security Enterprise analytic resources. The PRMx is intended to be a living document and maintained accordingly.

(3) 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. An **intelligence estimate of the situation** is an appraisal, consisting of the available intelligence relating to a

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.

Collection Asset: A collection system, platform, or capability that is supporting, as assigned, or attached to a particular commander.

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

Figure III-5. Sample Integrated Collection Planning Matrix

specific situation to determine the enemy's COAs and their probability and is contained in appendix 11 (Intelligence Estimate) to annex B (Intelligence).

c. The Joint Staff J-2, in close coordination with the supported CCMD J-2, coordinates, integrates, and synchronizes the activities of the Defense Intelligence and Security Enterprise to develop and staff a NISP for approval by the supported CCDR. NISPs are scalable intelligence support plans (ISPs) to integrated contingency plans and select standalone plans that detail how the Defense Intelligence and Security Enterprise will employ capabilities to satisfy a CCDR's IRs. CSAs and supporting intelligence centers will produce organizational support plans that detail concepts for agency and functional support, identify knowledge gaps and shortfalls, and outline support agency mitigation strategies. The NISP also identifies tasks requiring non-DoD intelligence entities support. A NISP consists of the NISP base plan, capability assessments, and ISPs.

(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) 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.

(3) An **ISP** 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 ISP also assesses agency/organizational capabilities and identifies significant knowledge gaps and capability shortfalls in supporting the CCMD mission and identifies mitigation strategies where appropriate.

d. **Collection Planning**

(1) Collection planning is a component of the IP process that identifies schedules and informs the management of collection assets and/or resources. The collection manager performing collection operations management (COM) reviews mission requirements, considered along 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 (TASKORDs) issued to a commander with tactical control of the assets in question.

(2) Collection system effectiveness is assessed by analyzing the capability and availability of intelligence collection assets and resources to collect against specific targets and to mitigate potential biases in collection, such as through multidisciplinary approaches, which can reduce the potential for additional biases throughout the intelligence process. Collection system efficiency is assessed 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 TASKORD produced by a theater air operations center. The collection asset allocation plan includes PIRs, their associated EEIs and related indicators, CRs 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 is part of an annex B (Intelligence) to a plan or order and forms the basis for further collection actions.

(4) After establishing a collection plan, the collection manager converts 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.

e. **Resource Availability and Capability.** During the planning process, intelligence planners and collection managers collaborate to review anticipated collection tasks or ad hoc CRs to determine the capabilities of available collection assets and resources that might contribute to satisfying SIRs. To that end, they assess platform and sensor suitability and capability factors against key element sets of the target. The result informs the selection of the most appropriate capability to satisfy the SIRs (see Figure III-6). This is reflected in the CRMs or similar integrated collection planning matrix by designating the collection agency responsible for a given SIR.

(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.

For a more detailed description of collection asset selection considerations, refer to Army Techniques Publication (ATP) 3-55.3/Marine Corps Reference Publication (MCRP) 2-10A/Navy Tactics, Techniques, and Procedures (NTTP) 2-01.3/Air Force Tactics, Techniques, and Procedures (AFTTP) 3-2.88, Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization.

(2) **Collection Capabilities Factors.** Intelligence 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

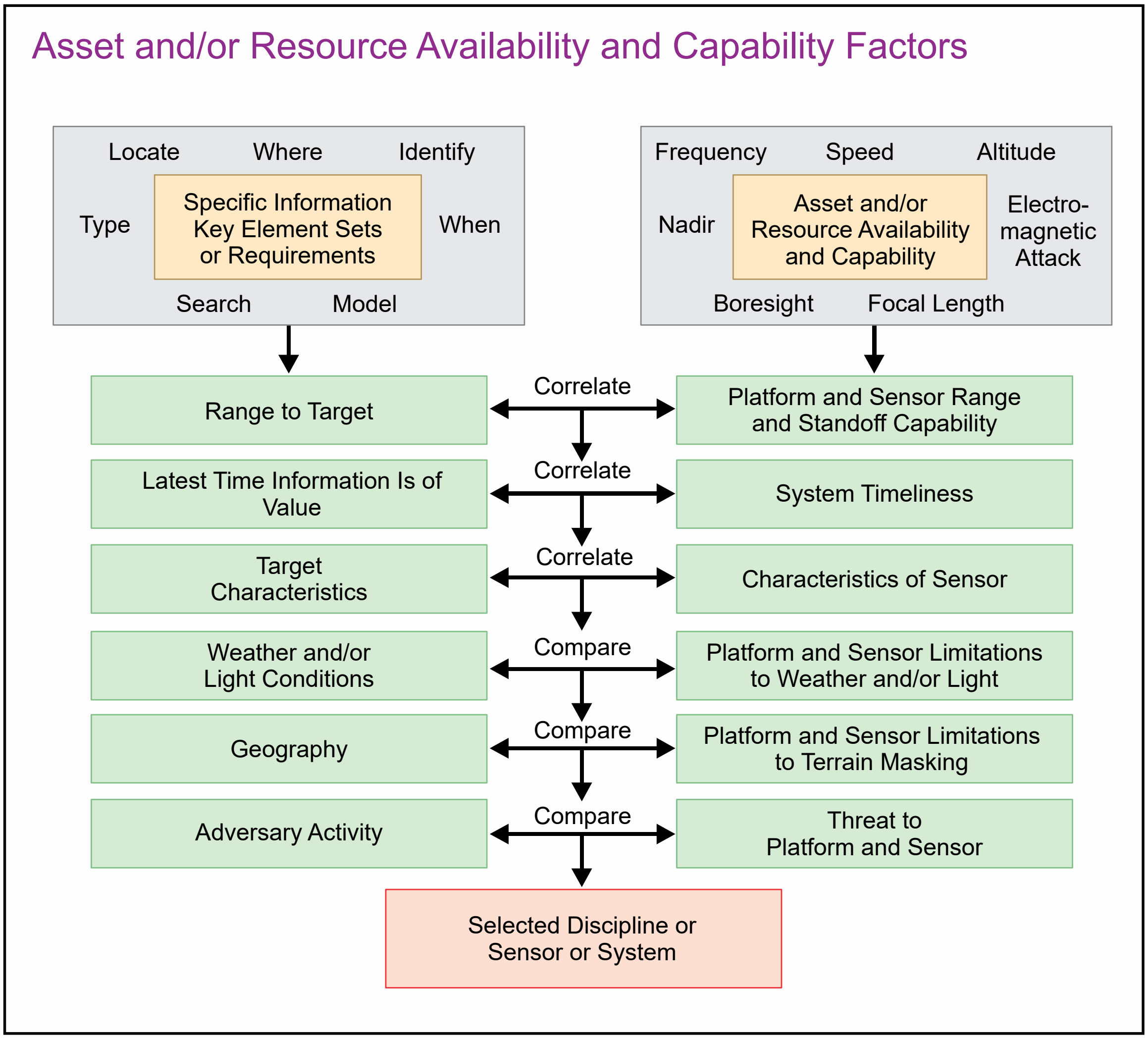

Asset and/or Resource Availability and Capability Factors
Locate
Where
Identify
Type
Specific Information Key Element Sets or Requirements
When
Search
Model
Frequency
Speed
Altitude
Nadir
Asset and/or Resource Availability and Capability
Electro-magnetic Attack
Boresight
Focal Length
Range to Target
Correlate
Platform and Sensor Range and Standoff Capability
Latest Time Information Is of Value
Correlate
System Timeliness
Target Characteristics
Correlate
Characteristics of Sensor
Weather and/or Light Conditions
Compare
Platform and Sensor Limitations to Weather and/or Light
Geography
Compare
Platform and Sensor Limitations to Terrain Masking
Adversary Activity
Compare
Threat to Platform and Sensor
Selected Discipline or Sensor or System

Figure III-6. Asset and/or Resource Availability and Capability Factors

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

(a) A system within a particular discipline may or may not be able to satisfy the CR for a particular target. For example, SIGINT collection systems operate in discrete frequency ranges; therefore, if the enemy or adversary system operates outside those ranges, that particular sensor is not viable as a potential collector.

(b) 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.

(c) 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 OB.

(d) Electromagnetic battle management capability is the joint electromagnetic spectrum operations (JEMSO) material solution used by JEMSOCs that provide user-defined operational pictures, relevant data, and supporting C2 capabilities.

(3) **Correlation.** Target collection and target signatures 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 requested accuracy/fidelity and time required.

(4) **OE Factors.** After correlation, the candidate sensors are compared with OE factors to support final sensor selection. OE factors include, but are not limited to, the threat, terrain, contamination, solar position, electromagnetic interference, and weather that might influence the technically capable 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, sensor platforms that penetrate enemy territory or airspace are the most vulnerable. As the distance between sensor and target increases, stand-off sensors become less vulnerable. Threat assessment is an evaluation of risk (military risk and political sensitivity) versus intelligence gain. When so designated by the commander, sensitive reconnaissance operations can be employed within predetermined high-threat areas. Such operations require additional protective measures, some of which involve increased and/or specialized tasking of intelligence assets looking for enemy reactions that may require a threat warning alert.

(b) Weather and atmospheric conditions are also considerations, particularly with EO and infrared sensors. Weather conditions in and around the collection area may prevent the collection platform and/or sensor from successfully satisfying the CR.

(c) Terrain is also a consideration. It may mask a target, thereby driving strict collection parameters limiting flexibility in platform or sensor choices.

(d) The dynamic nature of the civilian environment may require alternate collection methods such as persistent sensors or a multidiscipline collection strategy.

(e) CBRN hazards can present unique conditions within the OE. 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) 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.

For more information on IP products and processes, see CJCSM 3110.02, Intelligence Planning Objectives, Guidance, and Tasks.

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 CCDR intelligence forces. For allocation of intelligence forces, the Director, DIA, through the Joint Staff J-23, [Deputy Directorate for Intelligence Operations], supports DoD and CCMDs 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 CCMD-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 should be prepared and submitted. The flow of RFIs from JIOCs to national intelligence agencies differs only slightly between cooperation, competition, and conflict. 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 the 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 ODNI Deputy Director for Intelligence Integration to provide support. If determined that the information 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 ODNI Deputy Director for Intelligence Integration to recommend an appropriate strategy to collect, process, analyze, produce, and disseminate the required information. This strategy should be included in annex B (Intelligence) to the plan or order and in a NISP, as appropriate.

(1) **Cooperation and Competition Request Procedures.** DIA ensures the expeditious flow of intelligence from the national level through the JIOCs to deployed forces in cooperation and competition (see Figure III-7). 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) **Responding to Crisis and Armed Conflict Request Procedures.** The NJOIC is the focal point for responding to all crisis and armed conflict intelligence federation requirements (see Figure III-8). 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

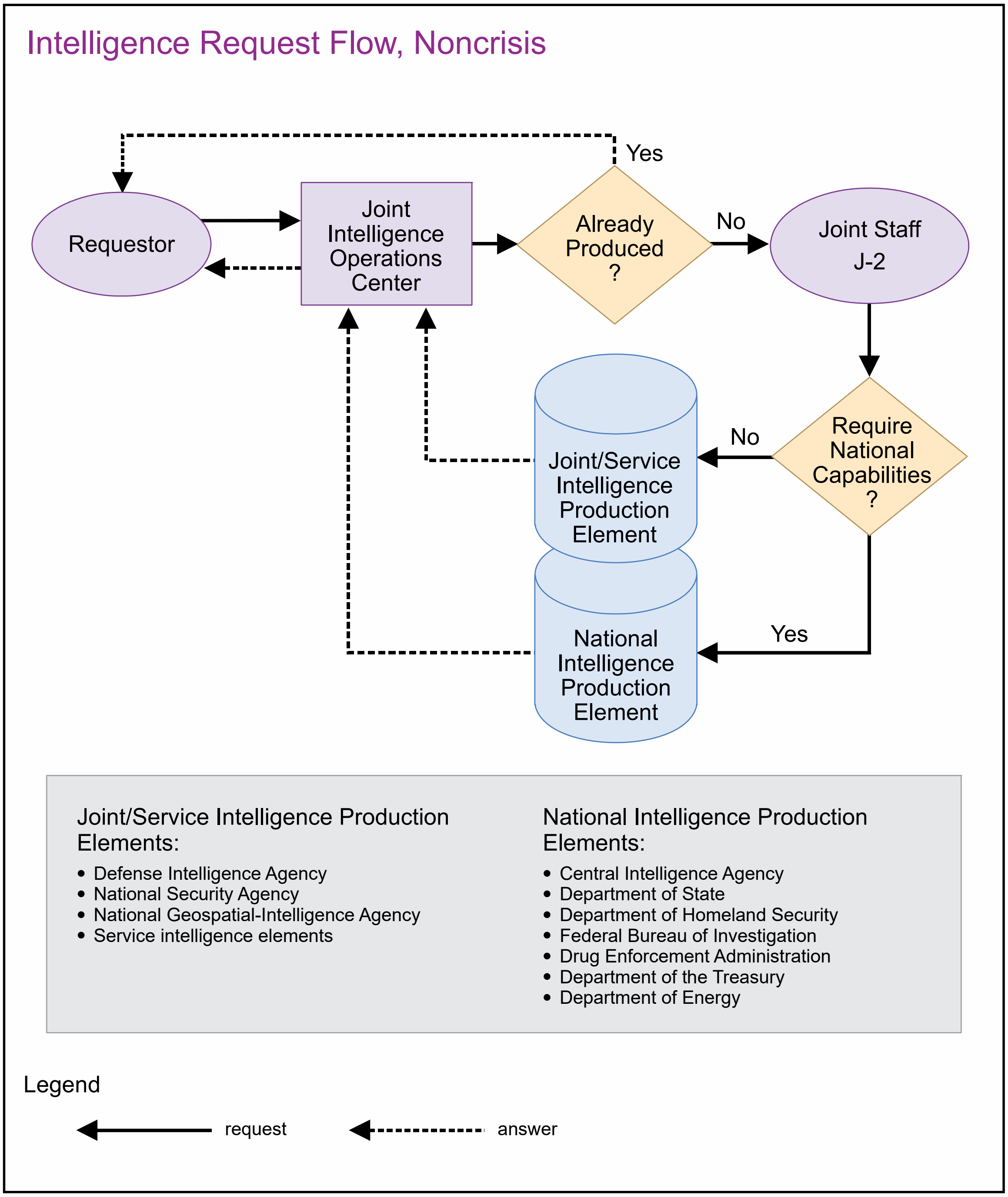
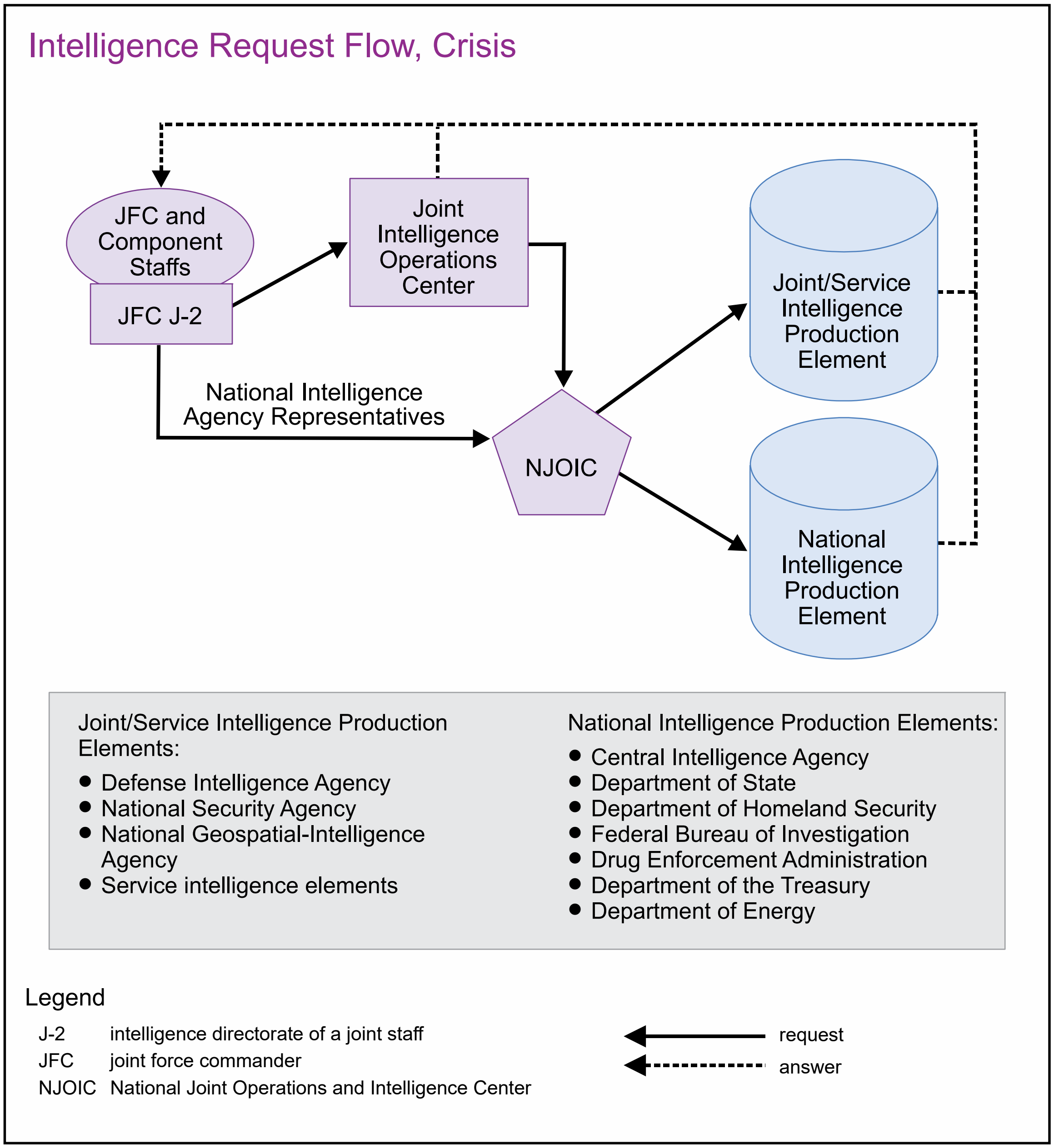

Intelligence Request Flow, Noncrisis
Yes
Requestor
Joint Intelligence Operations Center
Already Produced ?
No
Joint Staff J-2
Joint/Service Intelligence Production Element
No
Require National Capabilities ?
National Intelligence Production Element
Yes
Joint/Service Intelligence Production Elements:
• Defense Intelligence Agency
• National Security Agency
• National Geospatial-Intelligence Agency
• Service intelligence elements
National Intelligence Production Elements:
• Central Intelligence Agency
• Department of State
• Department of Homeland Security
• Federal Bureau of Investigation
• Drug Enforcement Administration
• Department of the Treasury
• Department of Energy
Legend
request
answer

Figure III-7. Intelligence Request Flow, Noncrisis

coordination is required for time-sensitive CRs or RFIs require national support. For tracking purposes, the CCMD JIOC should monitor the status of all RFIs originating from theater.

b. **National Intelligence Augmentation Support.** CCMDs coordinate with the Joint Staff J-2 on 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.


Intelligence Request Flow, Crisis
JFC and Component Staffs
JFC J-2
Joint Intelligence Operations Center
National Intelligence Agency Representatives
NJOIC
Joint/Service Intelligence Production Element
National Intelligence Production Element

Joint/Service Intelligence Production Elements:

- Defense Intelligence Agency
- National Security Agency
- National Geospatial-Intelligence Agency
- Service intelligence elements

National Intelligence Production Elements:

- Central Intelligence Agency
- Department of State
- Department of Homeland Security
- Federal Bureau of Investigation
- Drug Enforcement Administration
- Department of the Treasury
- Department of Energy

Legend

J-2	intelligence directorate of a joint staff
JFC	joint force commander
NJOIC	National Joint Operations and Intelligence Center

Figure III-8. Intelligence Request Flow, Crisis

c. **The 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, state, and non-state actors to formulate a global standing priority matrix. National CRs 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 the 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.

8. Collection Management

a. **Principles of Collection Management.** If, during the conduct of operations, it is determined that an RFI must be converted into a CR, a nomination for collection is submitted and collection management begins. Collection management is the process of converting intelligence-related information requirements into CRs, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. Anchored on the appropriate CMA, collection management is composed of two functions, CRM and COM, and requires collection orchestration.

(1) CRM is the authoritative development and control of collection, processing, exploitation, and information reporting requirements. This process normally results with the collection manager either tasking requirements to units over which the commander has authority or generating requests to CMAs at higher, lower, or lateral echelons to accomplish the collection mission. During CRM, all active CRs are prioritized and appropriately registered. Prioritization should be based on the commander's intent, objectives, approved PIRs, and the current situation to ensure limited assets or resources are directed against the most critical requirements. A coordinated, coherent, collection target-specific strategy is developed to satisfy validated and prioritized CRs. The collection strategy is a scheme for collecting information from all available sources to satisfy SIRs. The scheme is applied as discipline-specific CRs are sent to internal intelligence organizations for tasking or are submitted for validation and sent out as tasking requests to external organizations or agencies. Activities then transition from CRM to COM.

(2) COM is the authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and information reporting resources. This includes the selection and tasking of specific assets and sensors. The collection operations manager synchronizes the timing of collection with the operational scheme of maneuver and with other intelligence operations such as processing and exploitation, analysis and production, and dissemination. The collection operations

manager then selects assets best suited to collect the information needed to satisfy the SIR. The collection operations manager prepares a collection plan or revises the one previously published in annex B (Intelligence) to efficiently and effectively meet CRs and then tasks collection assets with sufficient direction to accomplish the mission. The collection operations manager develops and coordinates sensor employment guidance that helps to refine collection plans and strategies and enables the optimum employment of collection capabilities to CRs (see Figure III-9 and Figure III-10).

(3) Collection orchestration is the integration, synchronization, and optimization of the intelligence process and operations, to include: national and theater collection integration; all-domain, multidiscipline collection strategy development; and end-to-end synchronization of CRM, COM, and overhead reconnaissance and DoD ISR mission management systems.

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 requests. Early consideration of collection factors enhances the ability to respond to new CRs in a timely manner, ensures thorough planning, and increases flexibility in the choice of disciplines and systems. Early

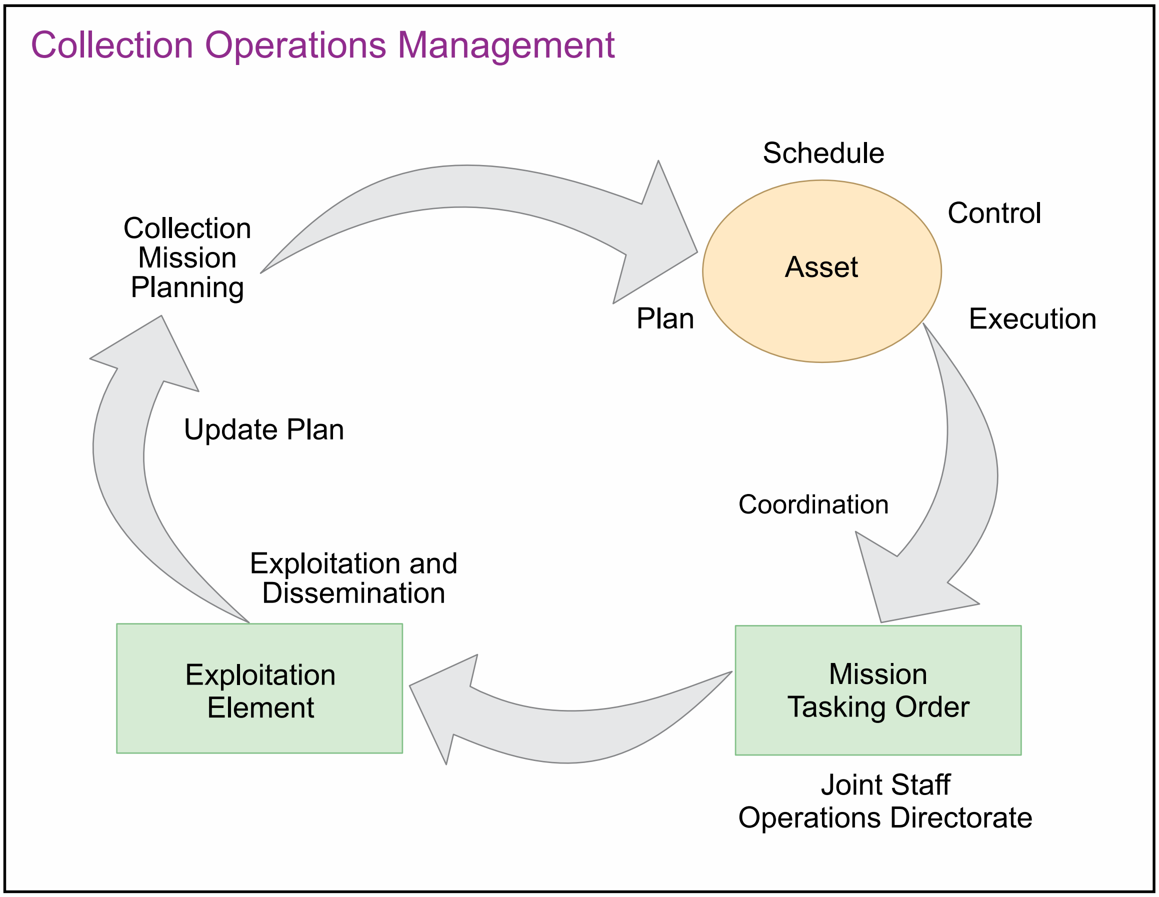

Collection Operations Management
Schedule
Control
Asset
Execution
Plan
Collection Mission Planning
Update Plan
Coordination
Exploitation and Dissemination
Exploitation Element
Mission Tasking Order
Joint Staff Operations Directorate

Figure III-9. Collection Operations Management

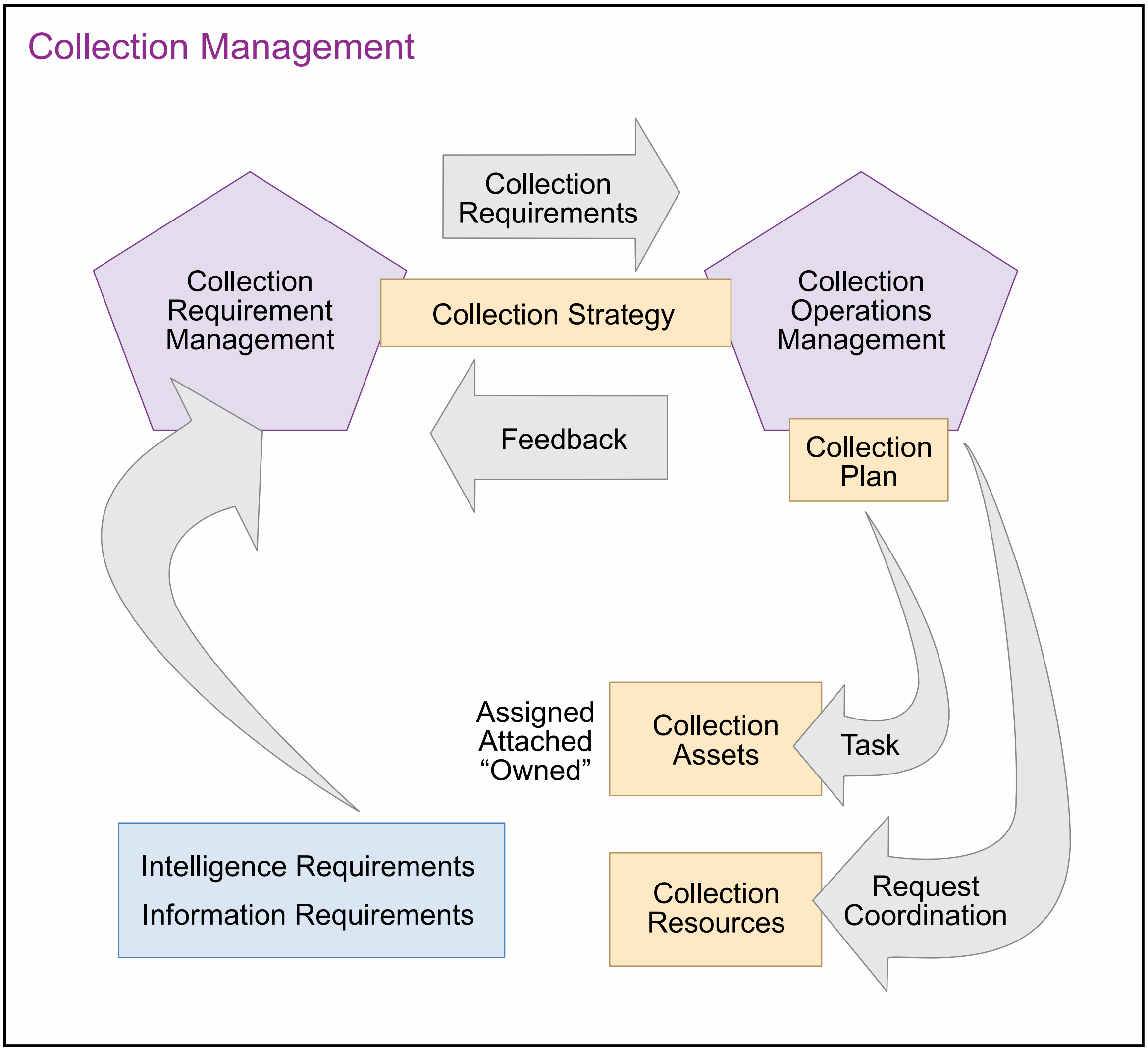


Figure III-10. Collection Management

requirement identification also enables the collection manager time to accomplish needed research, run analysis tools if required, and establish and/or refine a POC list.

(a) **Requirements Origination.** The subordinate joint force units develop CRs 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.

(b) **Requirements Validation.** The CCMD J-2 validates or modifies standing CRs submitted by subordinate joint force or component commands. The CCMD J-2 tracks the status 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 CRs and the coordination of collection operations. All CRs 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.

(2) **Prioritization of Requirements.** Prioritization assigns a distinct ranking to each CR. 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 CRs. 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. CRs 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 CR to an appropriate NIPF issue to establish a numerical tasking priority value. Depending on the intelligence issue, urgency, and criticality, priority exceptions may be applied 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. A multidisciplinary approach to collection can help reduce the prevalence or impact of common cognitive biases throughout the intelligence process. 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. 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

multidisciplinary CRs based on CCDR mission needs and PIRs. Collection managers define multidiscipline CRs in support of 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 CRs to appropriate, available theater collection assets; CRs that are not able to be satisfied by theater assets are forwarded for collection by Service or national-level collection resources.

(4) **During Execution Task Available Collection Assets First.** Use of available collection assets enables a timely and tailored response to CRs 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. CRM is the authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of requirements to units over which the commander has authority or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission and COM, the authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources.

(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. If performed by separate individuals/staffs, constant interaction should be maintained between the two.

(2) **CRM, COM, and collection orchestration are performed at all levels of the IC.** Each level interacts with the levels above and below as well as 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 CRs for themselves and their supported units, validates and prioritizes them, and then determines if they can be satisfied using organic assets. CRs 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 CRs 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 CRs; 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 for a given CCMD. 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) **Theater Collection Management.** The theater J-2 should be kept apprised of all intelligence CRs being levied on assets and resources within the CCDR's AOR, including other IC organizations 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. This authority may be delegated to a subordinate JFC.

SECTION B. COLLECTION

9. Overview of Theater-Level and Below Collection

a. Collection operations acquire raw data and information about relevant aspects of the OE and provide that information to intelligence processing and exploitation elements.

b. 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 is requested and coordinated through the chain of command of the unit that directs and controls them. It is important to note that resources and assets are not necessarily designated as "collection assets." Electromagnetic warfare, information activities, civil affairs, cyberspace forces, SOF, and scouts all collect information during the course of their activities or operations and should be considered in collection management.

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

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

(1) There are two primary methods for collection tasking:

(a) FRAGORD. These are well documented in Service doctrine and most widely used by commanders at all levels to direct the employment of forces, including the execution of reconnaissance and surveillance (R&S) missions. As an example, an intelligence section may request a low-level voice intercept team or HUMINT patrol to collect specific information. These teams are tasked in a FRAGORD format.

(b) Mission-Type Order (MTO). ISR MTOs identify a supported unit's overall ISR requirements. An R&S MTO provides the purpose and intent behind the mission rather than specifying collection tasks against predetermined targets. It provides flexibility to intelligence and operations staffs to refocus efforts when unforeseen circumstances emerge. An MTO narrative provides boundaries within which collection plans can adjust to satisfy the supported command's emerging requirements. An MTO is an order to a unit to perform a mission without specifying how it is to be accomplished.

For an example of the ISR collection process at the joint operational level, see the AOC Collection Management Handbook for ISR Operations.

For more information on collection FRAGORDs and MTOs, refer to ATP 3-55.3/MCRP 2-10A/NTTP 2-01.3/AFTTP 3-2.88, Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization.

(2) Collection support request forms or messages are methods of requesting collection support for time-sensitive situations from pre-determined sensors and/or weapons or 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 often 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, DIA manuals and the Defense Human Intelligence Enterprise Manual (DHE-M) 3301.001, *(U) 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-11. 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.

For more information on collection management employment concepts, refer to ATP 3-55.3/MCRP 2-10A/NTTP 2-01.3/AFTTP 3-2.88, Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization.

e. The CCMD J-2 staff/JIOC and J-3/joint reconnaissance center (JRC) need to dynamically manage theater collection assets. They also need to ensure collection support is synchronized with the CCDR's intent, national requirements, 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, including operations, weather, sustainment, and communications. They need to be closely integrated into the mission

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-11. Guidelines for Requesting National Resource Collection

planning effort. Intelligence sensor planners and managers of processing and exploitation elements should fully understand the requirements and mission profile.

f. **Execution.** During mission execution, collection managers performing a combination of COM authorities are often tasked to monitor and, in certain circumstances, exercise sensor tasking authority (STA). STA, as a delegated authority for COM, executes authority for all sensors tasked to the supported unit for information collection when requested by the supported tactical ground, naval, or air commander and in coordination with the supported ground, naval, or air intelligence chief. The individual with STA is responsible for managing sensor tasking and executing the collection plan, within the designated operating area, to satisfy specific IRs identified during planning. This may include the authority to retask the collection assets as CRs change. The STA enables communication between the allocated PED teams and collection assets.

For more information on STA, refer to ATP 3-55.3/MCRP 2-10A/NTTP 2-01.3/AFTTP 3-2.88, Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization.

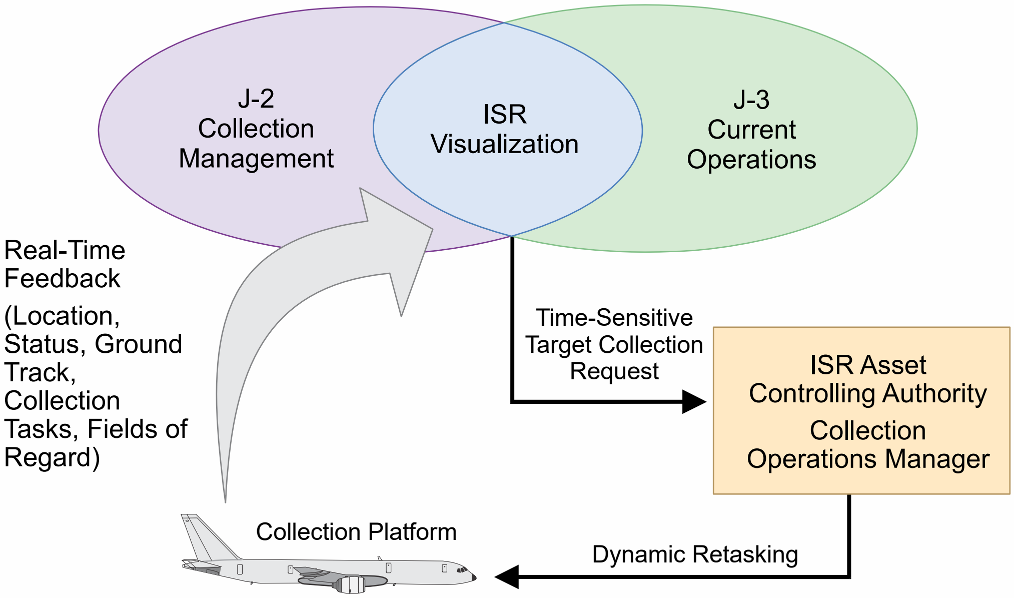
(1) **Resource Integration.** Resource integration is a process whereby a new CR is integrated with current or planned missions to increase the efficiency of the overall collection effort. By tasking a mission already in progress, it may be possible to reduce timelines, make collection more responsive 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 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 that were not performed to be retasked at the earliest available opportunity. When integration of a new CR 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 that facilitates coordination and synchronization of collection activities supporting the joint force and component commands. It provides the J-2/J-3 a valuable tool for managing available platforms to rapidly respond to changing CRs. ISR visualization enables collection managers performing COM to monitor and control collection missions and dynamically update the collection plan during mission execution. 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. Successful ISR visualization is contingent on timely reporting of collection asset status, vigilant maintenance of the COP and its supporting data set, and successful integration with collection asset activities (see Figure III-12).

(a) **Time-Sensitive Decision Making.** Based on the current military situation and the overall collection picture, the commander, through the J-2 and J-3, may identify fleeting opportunities for collection or strike operations against 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 collection tasking and support to friendly force SA and combat identification efforts. ISR visualization also helps clarify ambiguous operational situations by optimizing the

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-12. Intelligence, Surveillance, and Reconnaissance Visualization

reconnaissance or surveillance of possible new targets or emergent, high-probability threats to friendly forces developed through intelligence tip-offs. At the request of and in coordination with the J-3 current operations staff, the J-2 collection management staff forwards a request for dynamic retasking to the controlling authority of the most appropriate collection asset. The collection manager performing COM accomplishes the actual retasking of the appropriate collection asset.

(b) **ISR Visualization Architecture.** At the joint force level, personnel maintaining the current status and disposition of all available collection platforms should be integrated with the joint force J-3 current operations element, either through physical co-location or by virtual connectivity. Likewise, the joint force's ISR visualization capabilities should be interoperable with corresponding COM systems used by the component commands. A common set of ISR visualization tools 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/collection orchestration 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 CRs. CRs can be unsatisfied after a collection mission for a variety of reasons (e.g., asset unavailability, maintenance, sensor failure, weather, or 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 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 CRs and provides feedback to the requesters and collectors.** Monitoring outstanding requirements ensures 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 requester should also let the collection manager know if the information collected is of value so the collection manager can inform the collector. 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, and where possible, pushed to the appropriate IC databases for wider discoverability. 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.

10. Collection Assets and Resources

a. It is crucial for intelligence planners and collection managers to understand the various ways information might be collected; that is, the types of collection operations and how they relate to the types of collection platforms and disciplines. This knowledge ensures the right type of collection tasks (i.e., surveillance, interrogation, reconnaissance) are assigned to the right platforms and sensors during the development of plans and orders.

b. Collection assets and resources can be categorized by three types: technical collection (not to be confused with technical intelligence [TECHINT]), human-based collection, and a combination of technical and human-based collection.

(1) **Technical Collection Platforms.** Technical collection platforms conduct collection by use of various collection sensors. Technical collection platforms are typically associated with the GEOINT, MASINT, or SIGINT disciplines.

(2) **Human-Based 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.

SECTION C. PROCESSING AND EXPLOITATION

11. Overview

During processing and exploitation, collected raw data is sorted, correlated, and converted into intelligible forms that are suitable for immediate use or subsequent analysis and production of intelligence. Processing converts raw data into forms suitable for exploitation. Exploitation refers to the interpretation of the data. Exploitation, commonly referred to as single-source analysis, remains distinct from all-source analysis in that the resulting information has not yet been subjected to evaluation or corroboration from other sources. Nevertheless, relevant time-sensitive information resulting from processing and exploitation (especially joint 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 COP to provide the most current view of the OE. See the relationship between processing, exploitation, and analysis in Figure III-13.

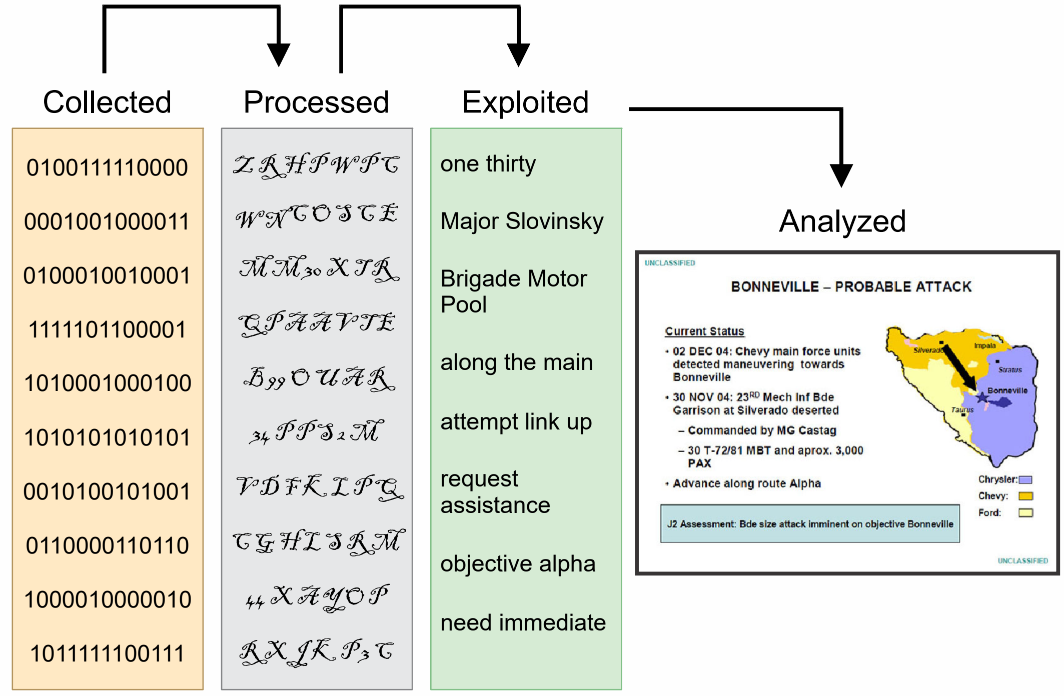
For more information on exploitation, see Appendix E, "Joint Exploitation Support to Intelligence."

For more information on the various intelligence disciplines, see Appendix B, "Intelligence Disciplines."

12. Geospatial Intelligence

GEOINT is an intelligence discipline that has evolved from the integration of imagery, IMINT, and GI 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 leverage geography by integrating more sophisticated visualization, analysis, and dissemination capabilities to depict a fused view of the OE. This capability provides many advantages for the warfighter, national

Notional Intelligence Data Processing Example



Collected

0100111110000
0001001000011
0100010010001
1111101100001
1010001000100
1010101010101
0010100101001
0110000110110
1000010000010
1011111100111

Processed

ZRHPWPC
WNCOSCE
MM30XTR
QPAAVTE
B99OUAR
34PPS2M
VDFKLPQ
CGHLSRM
44XAYOP
RXJKP3C

Exploited

one thirty
Major Slovinsky
Brigade Motor Pool
along the main
attempt link up
request assistance
objective alpha
need immediate

Analyzed

UNCLASSIFIED

BONNEVILLE – PROBABLE ATTACK

Current Status

- 02 DEC 04: Chevy main force units detected maneuvering towards Bonneville
- 30 NOV 04: 23RD Mech Inf Bde Garrison at Silverado deserted
  - Commanded by MG Castag
  - 30 T-72/81 MBT and aprox. 3,000 PAX
- Advance along route Alpha

J2 Assessment: Bde size attack imminent on objective Bonneville

Chrysler: 🟪
Chevy: 🟨
Ford: 🟨

UNCLASSIFIED

Legend

Bde	brigade
Inf	infantry
J-2	intelligence directorate of a joint staff
MBT	main battle tank
Mech	mechanized
MG	major general
PAX	personnel

Figure III-13. Notional Intelligence Data Processing Example

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.

13. Human Intelligence

HUMINT is an intelligence discipline derived from information collected and provided by human sources. 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.

Additional information on the J-2X organization and responsibilities can be found in classified Appendix C, "(U) Classified Appendix on Joint Intelligence (Counterintelligence and Human Intelligence/Department of Defense Cover)."

14. Signals Intelligence

SIGINT support to joint operations includes communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). COMINT processing is accomplished by NSA/CSS elements either assigned to or in support of the joint force mission. Depending on the level required for subsequent analysis and reporting, processing may be performed by assigned units in the operational area, at the regional 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 for approval by the designated SIGINT operational tasking authority.

15. Measurement and Signature Intelligence

MASINT provides technically derived intelligence to detect, locate, and describe the specific characteristics of targets. As an integral part of the all-source collection effort, MASINT can provide unique and complementary information to satisfy 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. In other cases, some sensors may be deployed specifically to support MASINT analysis. MASINT is employed as a global system with capabilities to exploit opportunities worldwide. Service scientific and technical intelligence (S&TI) centers play a critical role in processing, exploiting, and analyzing MASINT data. Additionally, the Services generate MASINT products in support of their respective components assigned to joint forces. The resulting MASINT products contribute to, but are not limited to, warning intelligence, JIPOE, force protection, and foreign materiel exploitation. MASINT also includes forensic analysis of collected and historical technical data to support identity analysis, activity attribution, and signature development. In addition, MASINT provides intelligence on WMD capabilities and weapons system capabilities based on analysis of collected telemetry data.

16. Open-Source Intelligence

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. Publicly available information is information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting a place or attending an event that is open to the public.

See DoDM 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities, *for more information on publicly available information.*

17. Technical Intelligence

TECHINT is derived from the exploitation of foreign materiel, CEM, and scientific information. TECHINT begins with the acquisition or recovery 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. 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. CCMDs or subordinate joint forces should notify the NJOIC through command channels when they require JCMEC support to ensure appropriate Service component resources are requested to meet the support requirement.

18. Counterintelligence

CI encompasses the following five functions: collection, analysis and production, investigations, operations, and functional services. CI is conducted to identify, deceive, exploit, disrupt, or protect against espionage, sabotage, assassinations, or other intelligence activities conducted by organizations or persons on behalf of foreign powers or international terrorist organizations. CI is both offensive and defensive and should be factored in whenever US intelligence or national security capabilities are deployed or when they are threatened.

For detailed information on CI, see classified Appendix C, "(U) Classified Appendix on Joint Intelligence (Counterintelligence and Human Intelligence/Department of Defense Cover)."

SECTION D. ANALYSIS AND PRODUCTION

19. Overview

Intelligence is produced through the integration, evaluation, analysis, and interpretation of information from a single source or from multiple sources (see Figure III-14). Intelligence results from analysis and production, which is accomplished in response to expressed and anticipated user requirements. Joint intelligence assessments and estimates, produced through the continuous JIPOE process, support the JFC's decision-making process by identifying COGs and their critical capabilities, requirements, and vulnerabilities; evaluating current military capabilities of enemy, adversary, friendly, and neutral forces; and providing estimates of enemy COAs in relative order of probability of adoption.

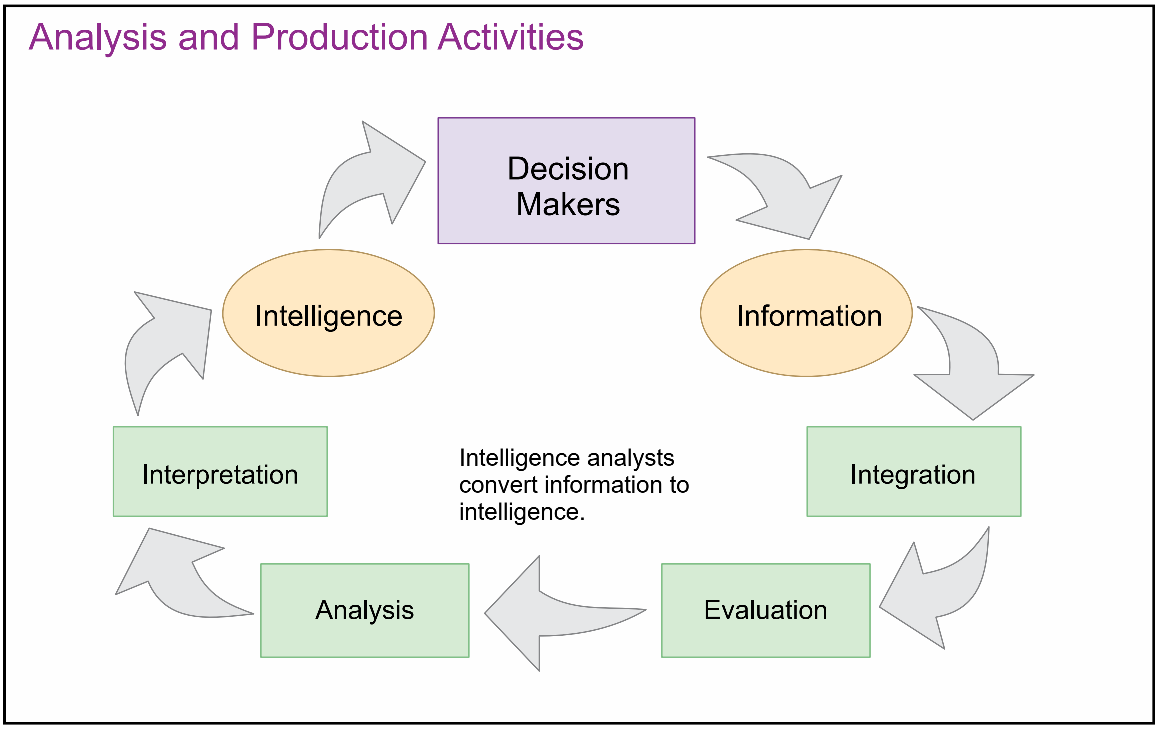

Analysis and Production Activities
Decision Makers
Information
Integration
Evaluation
Analysis
Interpretation
Intelligence
Intelligence analysts convert information to intelligence.

Figure III-14. Analysis and Production Activities

20. Conversion of Information into Intelligence

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.

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

b. **Evaluation.** Each new item of information is evaluated by the appropriate analysis and production element with respect to the reliability of the source and the credibility of the information.

c. **Interpretation.** Interpretation is an objective mental process of comparison and deduction based on common sense, life experience, and military knowledge covering enemy and friendly forces, as well as existing information and intelligence. This mental process involves the identification of new activity, or lack thereof, and a postulation regarding the significance of that activity.

21. Collaboration

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

b. 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 cooperation and competition, informal collaboration among intelligence analysts should be encouraged, within guidelines established by the JFC or joint force J-2.

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

22. 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 NSA Pulse contains current and historical finished SIGINT products. Similarly, the Biometrics Identity Intelligence Resource, soon to be the Identity Intelligence Analytic Resource, contains I2 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. To overcome this limitation, virtual knowledge bases serve as integrated repositories of multiple databases, as well as reference documents and open-source material.

b. Virtual knowledge bases are 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.

23. All-Source Product Categories

Intelligence products are generally placed in one of eight all-source production categories: warning intelligence, current intelligence, general military intelligence (GMI), target intelligence, S&TI, CI, estimative intelligence, and I2 (see Figure III-15). The

Categories of Intelligence Products

- Warning intelligence
- Current intelligence
- General military intelligence
- Target intelligence
- Scientific and technical intelligence
- Counterintelligence
- Estimative intelligence
- Identity intelligence

Figure III-15. Categories of Intelligence Products

categories are distinguished from each other primarily by the purpose for which the intelligence is produced. The categories can and do overlap, and some of the same intelligence and information can be found and used by analysts in each of the categories.

a. **Warning Intelligence.** Warning intelligence activities are intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. Warning provides a distinct communication to a decision maker about threats against US security, interests, or citizens. Warning carries a sense of urgency, implying the decision maker should take action to deter or mitigate the threat's impact. Warning analysis focuses on the opportunities to counter and alter only those threats that have detrimental effects for the United States. This includes US military or political decision cycles, infrastructure, COA, or loss of governance. Defense intelligence recognizes two types of warning: emerging and enduring. If relevant to national security, both emerging warning issues and enduring warning problems may warrant DoD leadership attention. Emerging warning issues may be ambiguous and may be formalized as an enduring warning problem based on a risk evaluation to national security and planning guidance. The latter is usually linked to contingency plans, which are potential threats to US interests.

b. **Current Intelligence**

(1) Current intelligence provides updated support for ongoing operations. It involves the integration of time-sensitive, all-source intelligence and information into concise, objective reporting on the current situation in a particular area. The term current is relative to the time sensitivities of the decision maker and the context of the type of operation supported. For example, in some contexts, previously gathered intelligence may be considered current, whereas other circumstances may require intelligence in NRT.

(2) As a temporal category, current intelligence relates to a number of other categories. For instance, the location of a threat weapon system is both current intelligence

and target intelligence. In addition, once the location is databased, this current intelligence may be considered foundational GMI for use in subsequent intelligence assessments and estimates.

c. **GMI.** GMI focuses on the military capabilities of foreign countries and organizations, to include non-state actors, and other topics that could affect US or multinational operations. This broad foundational category of intelligence is databased for use in other product categories. To that end, foundational GMI regarding the organization, operations, facilities, and capabilities of selected foreign military forces, and other relevant characteristics of the OE, is applied through the JIPOE process to produce assessments and estimates tailored to the JFC's mission.

d. **Target Intelligence.** Target intelligence portrays and locates the components of a target or target complex, networks, and support infrastructure and indicates its vulnerability and relative importance to the adversary. Target intelligence includes the characterization of a target and its placement in a larger system or network. Characterization includes analyses of physical and virtual attributes (including the biographic, biologic, behavioral, and reputational attributes of human targets, to support weaponeering) and signatures (to support target detection and positive identification). Target intelligence also includes BDA composed of physical damage/change assessment, functional damage/change assessment, and a functional assessment of the higher-level target system resulting from the application of lethal or nonlethal force. It is critical that intelligence analyses supporting targeting remain consistent throughout the joint force. Target intelligence must holistically analyze the target so it can support all target engagement options. Throughout the targeting process, intelligence personnel should consider available information to support proper target nomination, target development, and assessment. Throughout the targeting process, intelligence personnel should be aware of and seek to mitigate biases. Target intelligence includes nominations for the no-strike list and restricted target list.

See Appendix F, "Target Intelligence;" JP 3-60, Joint Targeting; *and CJCSI 3370.01,* Target Development Standards, *for further information.*

e. **S&TI.** S&TI is a foundational intelligence category that examines foreign developments in basic and applied sciences and technologies with 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 traditional intelligence sources, as well as foreign materiel exploitation, foreign materiel acquisition, and CEM programs, the information is analyzed to preclude scientific and technological surprises and advantages by an enemy that could be detrimental to friendly personnel and operations.

f. **CI.** CI is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. CI includes conducting strategic CI analysis to identify and produce all-source finished intelligence on the foreign intelligence entities threat to DoD. CI develops and implements strategies and action plans to counter the CI threat, tasks CI collection capabilities, and leverages HUMINT, SIGINT, GEOINT, MASINT, and OSINT to fill CI collection gaps. 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 lines of communications (LOCs) and main supply routes. Multidisciplined CI analysis includes detailed input to JIPOE.

g. **Estimative Intelligence.** Estimative intelligence identifies, describes, and forecasts adversary capabilities and the implications for military operations.

(1) The estimative intelligence product category refers to the original product line of the intelligence cycle; the intelligence estimate or rather, the intelligence portion of the commander's running estimate of the situation. Estimative intelligence may provide a decision temporal advantage to commanders at all levels of warfare by delivering forecasts of alternative force situations with implications for the development of the national and military strategy, and joint planning and execution of military operations. The product of estimative intelligence considers relevant actors' capabilities, effects the OE may have on them, and their current disposition and historical patterns of behavior to address unresolved variables. This allows the analyst to deduce potential COAs (as many as time allows) that may be available to relevant foreign actors in relative order of probability. To support friendly COA selection, the predictive methodology provides commanders and planners estimates of a foreign actor's potential response to friendly options under consideration. Estimative intelligence is produced at every echelon and commanders at all levels should expect living intelligence estimates to be maintained to continuously provide near-, mid-, and long-term forecasts to support the various planning horizons of the command.

(2) As a temporal product category, estimative intelligence cuts across a number of topical product categories. For instance, current threat OB held in intelligence databases is considered GMI. However, a projection of how a threat OB may evolve over time is estimative GMI. Similarly, the NRT location of a threat weapon system on a joint target list is current intelligence, but when the location of said weapon system is forecasted to change over time, the resulting analysis is a cross between estimative and target intelligence. See Figure III-16 for an example of the relationship between topical and temporal product categories.

h. **I2.** I2 results from the fusion of identity attributes (e.g., biographic, biologic, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes collected across multiple disciplines. I2 utilizes enabling intelligence activities like BEI, FEI, and DOMEX to discover the existence of unknown potential threat actors by connecting individuals to other persons, places, events, or materials, analyzing pattern of life, and characterizing their level of potential threats to US interests. I2 enables identity discovery, identity resolution, identity protection, and force protection by identifying, characterizing, locating, and tracking persons, entities, groups, networks, or populations of interest. I2 is used to disrupt

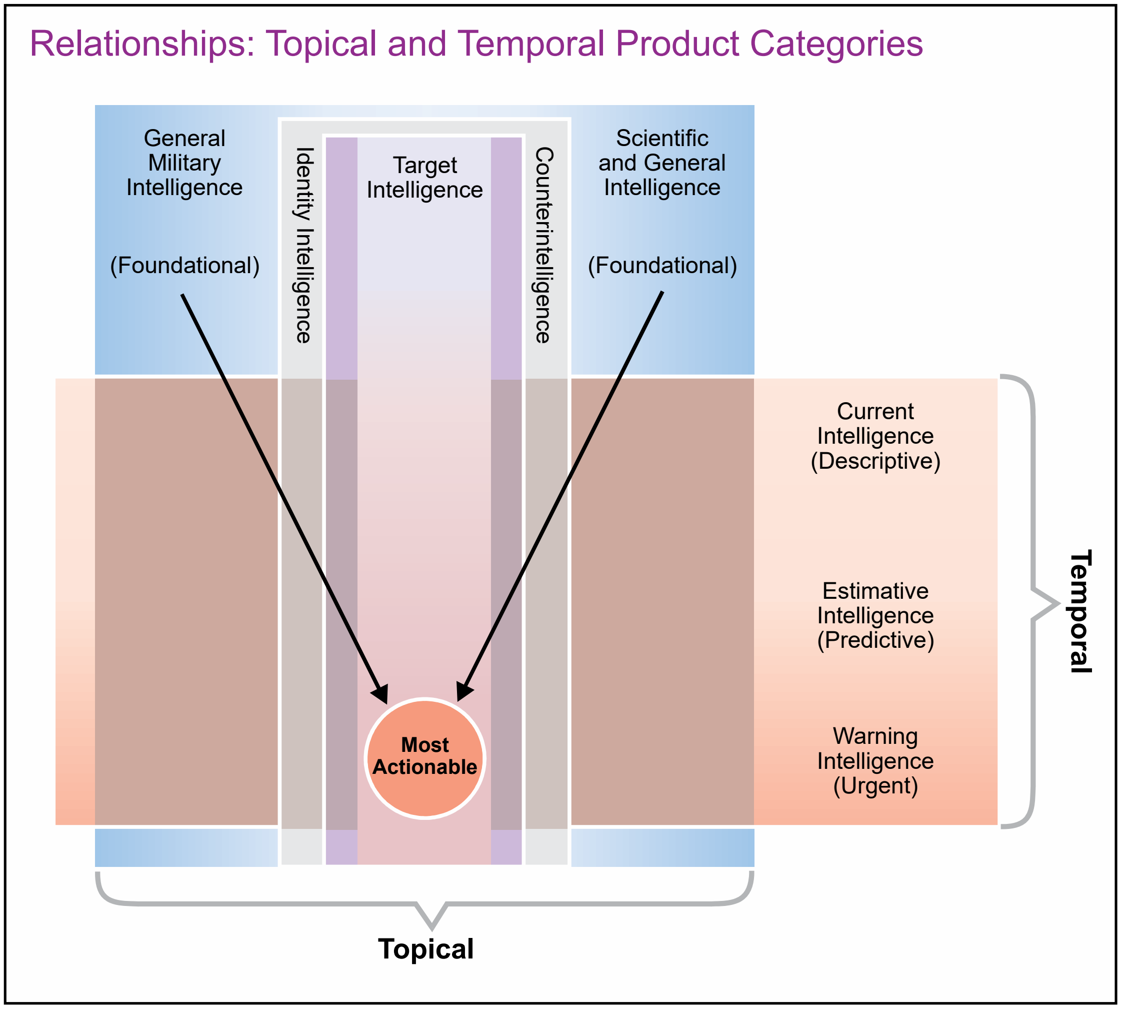

Relationships: Topical and Temporal Product Categories
General Military Intelligence
(Foundational)
Identity Intelligence
Target Intelligence
Counterintelligence
Scientific and General Intelligence
(Foundational)
Current Intelligence (Descriptive)
Estimative Intelligence (Predictive)
Warning Intelligence (Urgent)
Temporal
Most Actionable
Topical

Figure III-16. Relationships: Topical and Temporal Product Categories

competitors, support joint operations, counter threats, deny anonymity to our adversaries, and protect our assets, facilities, and forces while ensuring full spectrum superiority.

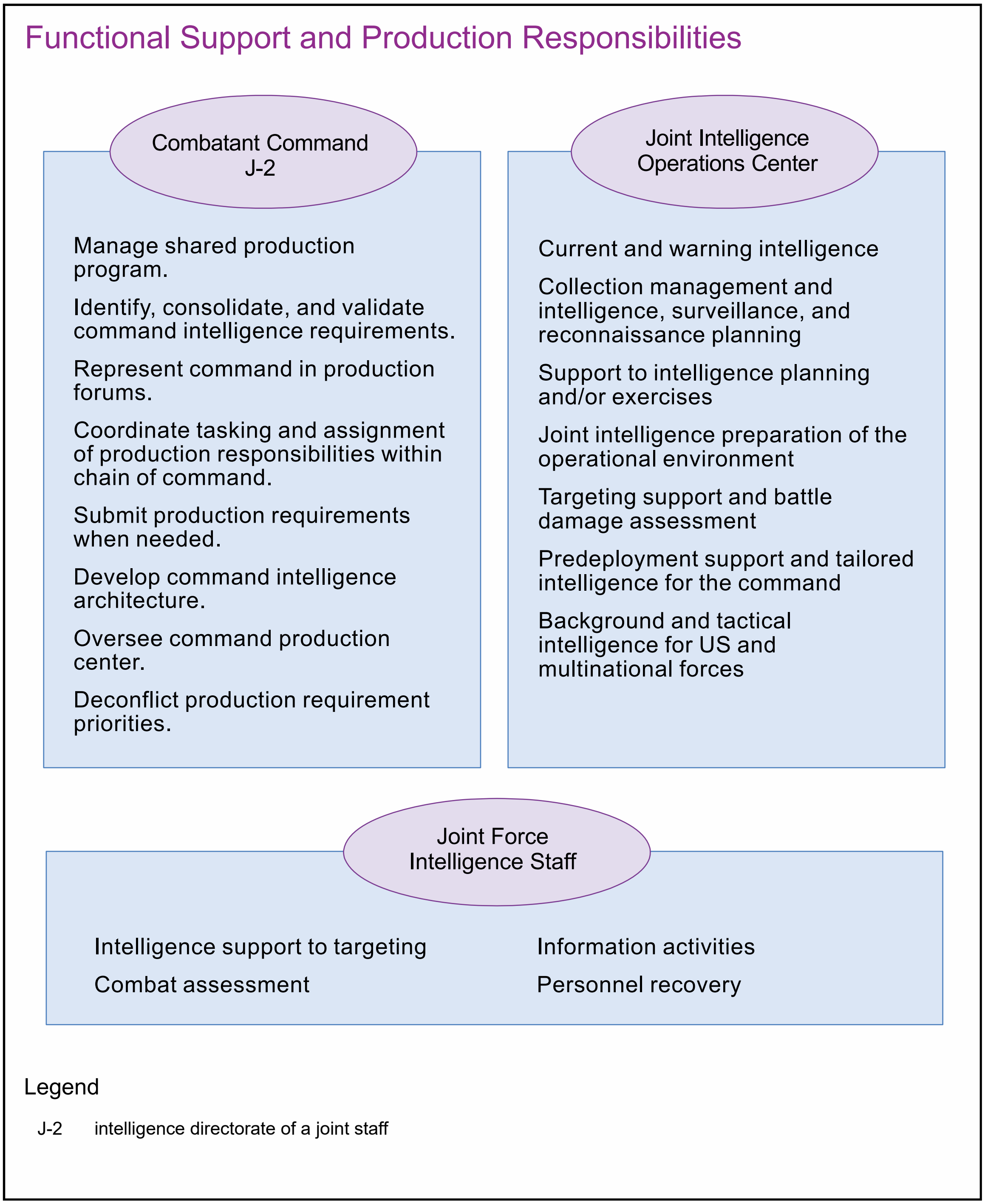
For a discussion on I2, see Appendix D, "Intelligence Applications."

24. 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-17) 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 (Intelligence) for CCPs and level 3, 3T, and 4 contingency



Functional Support and Production Responsibilities

Combatant Command J-2

- Manage shared production program.
- Identify, consolidate, and validate command intelligence requirements.
- Represent command in production forums.
- Coordinate tasking and assignment of production responsibilities within chain of command.
- Submit production requirements when needed.
- Develop command intelligence architecture.
- Oversee command production center.
- Deconflict production requirement priorities.

Joint Intelligence Operations Center

- Current and warning intelligence
- Collection management and intelligence, surveillance, and reconnaissance planning
- Support to intelligence planning and/or exercises
- Joint intelligence preparation of the operational environment
- Targeting support and battle damage assessment
- Predeployment support and tailored intelligence for the command
- Background and tactical intelligence for US and multinational forces

Joint Force Intelligence Staff

- Intelligence support to targeting
- Combat assessment
- Information activities
- Personnel recovery

Legend

J-2	intelligence directorate of a joint staff

Figure III-17. Functional Support and Production Responsibilities

plans and to develop the PRMx and analysis and production capability assessments in annex A (Task Organization) 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 CCDR's AOR.

(2) ISR planning in collaboration with CCMD J-3 COM and joint METOC personnel.

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

(4) In close coordination with CCMD and joint METOC personnel, JIOC intelligence planners support target intelligence PRs, such as supporting development of target materials (TM), TSA, ETFs, target lists, CA, and maintaining no-strike lists in MIDB/MARS as required.

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

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

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

c. Detailed intelligence information is critical for conducting joint targeting. Responsibility for joint targeting resides with the JFC. The joint force J-2 is responsible for the production and maintenance of target intelligence products. Target intelligence utilizes TSA to provide the foundation for target coordination mensuration, development, weaponeering, strike lists management, and CDE.

For a detailed description of joint intelligence procedures for joint targeting, see JP 3-60, Joint Targeting.

d. **CA is the determination of the overall effectiveness of force employment during military operations.** CA is composed of three related elements that may result in a reattack recommendation (RR): BDA, munitions effectiveness assessment (MEA), and collateral damage assessment (CDA). 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 joint 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, *and CJCSI 3162.02,* Methodology for Combat Assessment.

e. **Information and Intelligence Integration.** Information and intelligence integration is a vital military capability that supports operations in the IE. Information and intelligence integration greatly facilitates understanding the interrelationship between the physical, informational, and human aspects 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 information integration planning and execution efforts, and properly assess effects in the IE, intelligence planners and collection managers are intimately involved in the planning process. DIA/NSA/CIA/NGA, Service intelligence and information 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 information activities.

25. Production Responsibilities

a. Production centers at all levels are assigned clearly delineated areas of analytical responsibility. 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 unique from that possessed by the designated primary production center for the same topics and geographical areas. A center designated as collaborative is 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 AOIs.

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 enables JFCs to acquire relevant intelligence, based on their mission and the 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."

26. Request Production Management

a. 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 RFIs.

b. After the supporting intelligence office surveys local resources to ensure the requirement does not duplicate existing or scheduled production, it completes and forwards the RFI to the supporting intelligence center at the next level in the Service, CCMD, or DIA chain. At the joint force command or Service component, the next level supporting intelligence center is resident at the CCMD JIOC. The Defense Intelligence Agency Directorate for Analysis (DI), each Service, and each CCMD has a supporting intelligence center to process and validate the RFIs submitted by their organizations' supporting intelligence offices. The CCMD supporting intelligence center normally accepts RFIs via e-mail or other informal means. However, the supporting intelligence center 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 CR or request for personnel or operational support).

c. Upon validation, the supporting intelligence center 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. It 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 DI.

d. Once requirements are assigned to a primary production center, the center coordinates the efforts of all collaborating production centers for the designated product. All centers schedule the production of each PR consistent with other assigned projects and 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.

e. After coordination with collaborating centers, the primary production office provides a written interim response to the customer, stating the format and type of document it should produce and citing a final response date. Copies of the response are sent simultaneously to the assigning supporting intelligence centers, the collaborating production centers, and the defense intelligence production functional manager.

27. 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-18).

SECTION E. DISSEMINATION AND INTEGRATION

28. Overview

a. Military commanders depend on timely intelligence and METOC information; they require the ability to identify opportunities in time to exploit them. Awareness of the OE, as well as rapidly achieving and maintaining an operational advantage through the use of information, is critical to decision making and, ultimately, success of the joint force.

b. Intelligence support to C2 is the primary vehicle for integrating intelligence and operations. Intelligence support to C2 encompasses intelligence systems, networks, functions, activities, personnel, processes, TTP, data, and products that support C2 via a common intelligence picture (CIP). Together, the COP and its CIP deliver the SA necessary to enable information advantage, promote unity of effort, and enable decisive combat advantage.

c. The term CIP needs to be clarified to understand its relationship to the COP and shared SA. Use of the term COP implies the existence of an integrated CIP. Use of the term CIP refers to the intelligence component of the COP that is developed and managed by intelligence personnel and delivers a data-intensive information picture from which intelligence can be derived, informing the COP in support of C2. It is more than an enemy’s location on a map. The CIP is a visual depiction of relevant, instructive, and contextual intelligence information regarding enemy and neutral force disposition, intentions, and supporting infrastructures. It is important to note that enemy intentions are not proven facts but analytic judgements based on the interpretation of numerous indicators

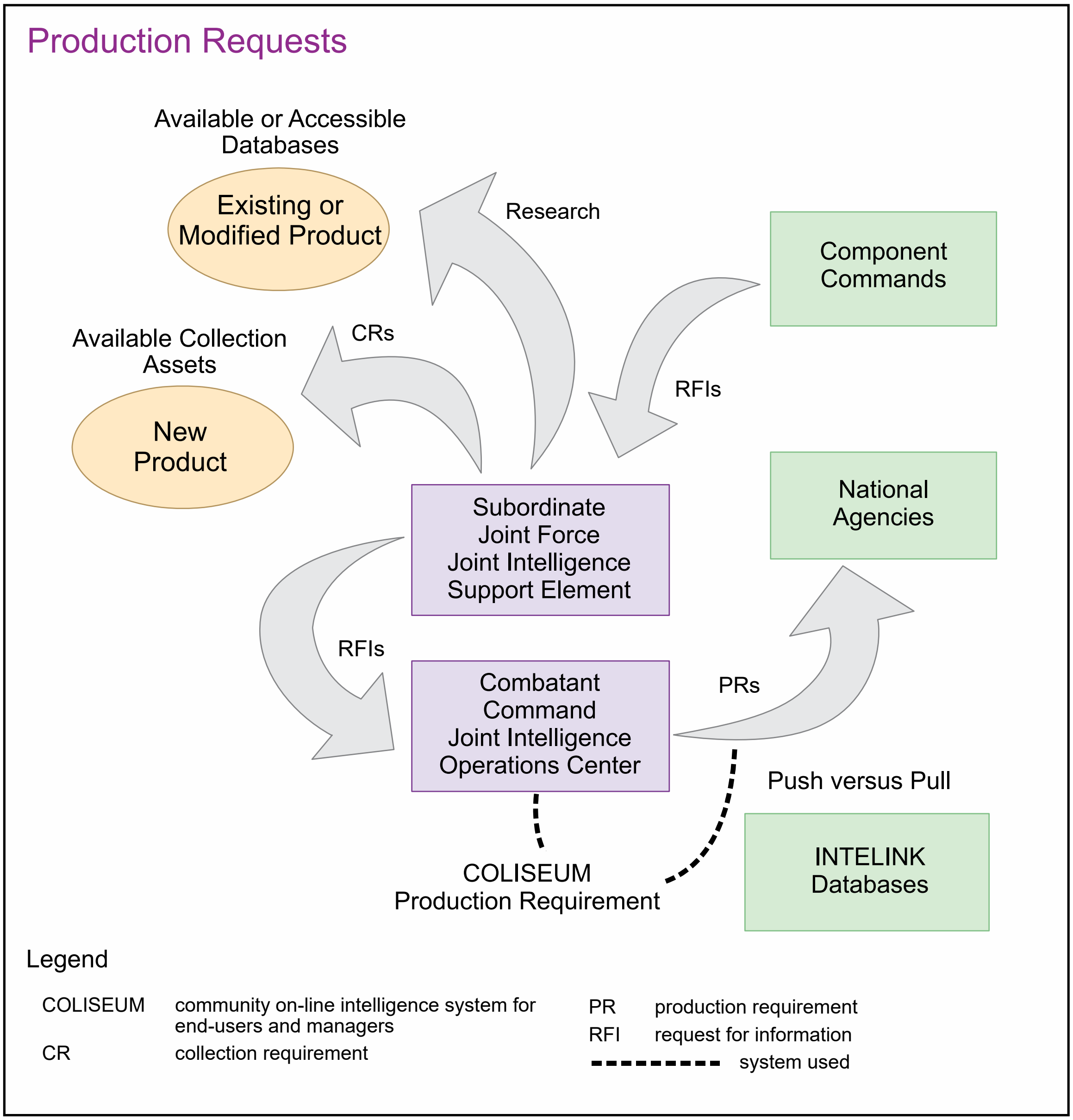

Production Requests
Available or Accessible Databases
Existing or Modified Product
Research
Component Commands
Available Collection Assets
CRs
RFIs
New Product
National Agencies
Subordinate Joint Force Joint Intelligence Support Element
RFIs
PRs
Combatant Command Joint Intelligence Operations Center
Push versus Pull
INTELINK Databases
COLISEUM Production Requirement
Legend
COLISEUM community on-line intelligence system for end-users and managers
CR collection requirement
PR production requirement
RFI request for information
system used

Figure III-18. Production Requests

and, in most cases, not timely when compared to other CIP/COP reporting. The CIP is derived from all intelligence sources at any level of classification. It facilitates collaborative planning and assists all echelons to achieve shared SA of the OE and decision advantage.

d. Intelligence should be disseminated in such a manner that it is readily accessible by the user. The timely dissemination of critical information and finished intelligence and METOC information to appropriate consumers is vital to achieve SA and enable effective decision making. Commanders need a comprehensive understanding of the OE to confidently predict, visualize, and understand the future OE with the accuracy necessary to act decisively, with optimum effectiveness, and faster than the threat.

(1) Dissemination is facilitated by a variety of means, which are determined by the needs of the user, the timeliness and relevance required, and the intended use of the intelligence. The diversity of dissemination paths enables a globally integrated intelligence architecture that is interoperable across joint and multinational forces, DoD agencies, and interagency partners.

(2) The architecture encompasses agile, all-domain communication systems that operate dynamic, networked-sensing processing at the nearest point of collection and multi-cast, direct downlink to operational users. This facilitates the timely communication of collected data, processed information, and fused intelligence among dispersed producers and consumers. The dissemination architecture accommodates transmission of relevant data to the consumer.

(3) Tactically relevant data provides time-sensitive information to the tactical edge for planning engagements and special missions. The data, at a minimum, should comply with joint interoperability standards and consist of positive identification, latitude/longitude position, speed, heading, target location error, and periodic updates as applicable.

(4) Additionally, intelligence organizations push information and/or intelligence to the consumer by leveraging direct downlinks and edge node processing with the most expeditious means available and accommodate the consumer's pull on demand allowing automated access to theater and national databases. This construct delivers timely intelligence and sensor-derived information about the OE, makes maximum use of automation, and minimizes the flow of RFI messages and intelligence reports.

e. Time and accuracy considerations dictate that information is "pushed," to the maximum extent possible, in a way that is automatically rendered or visualized in the GCCS COP. The integration of the CIP into the COP is facilitated by the Global Command and Control System-Integrated Imagery and Intelligence (GCCS-I3) mission application. GCCS-I3 enhances the COP by providing a standard set of integrated, linked tools and services that give ready access to imagery, intelligence, and METOC information, which is seamlessly plotted on the COP.

f. The J-2, at each echelon, manages the dissemination of intelligence to the user. Intelligence should be provided in time and succinctly (minimal byte size, readily understood and directly usable by the recipient) without overloading either the dissemination systems, presentation systems, or the users at every level. It is also important to provide for maximum possible release of appropriate classified reporting, analysis, and joint targeting data to multinational forces. When a joint force J-2 is supported by national agencies, 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.

g. Dissemination consists of both "push" and "pull" control principles. 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 repositories by intelligence organizations at all levels. Both push and pull also need to take into account network constraints on how the intelligence is displayed. An increasing number of intelligence pull products are available on Intelink 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 Enterprise, Service intelligence centers, the Services, 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 forces 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.

h. 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 deployed to austere locations and LOCs are extended.

i. 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 planning.

29. Dissemination Methods

a. **Digital Dissemination**

(1) Digital dissemination has become the predominant method of communicating finished intelligence products to the consumer. Most 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. This transition has resulted in reducing costs, simplifying rework when required, facilitating aggregation and searchability, and simplifying security considerations. 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 JWICS, SIPRNET, JDISS, NIPRNET, GCCS, Intelink and/or Intelink-S, and IBS are being integrated within the DoDIN to deliver intelligence and METOC information whenever and wherever required.

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

(3) Each J-2 site routinely has access to several daily current intelligence documents, including a variety of DoD and national agency products. Other documents, (current and finished intelligence), as well as intelligence information reports (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) Much of the material on Intelink is available to anyone with access to a JWICS or SIPRNET terminal. With many documents already located on Intelink/Intelink-S, it may only be necessary for a site to tell the requester where the document exists. Requests for other existing electronic documents should be made directly via Intelink or, if not directly accessible, the request should be directed to the appropriate DPM to satisfy the request. The electronic document should in turn be placed on the dissemination server for requester pull or electronic push.

(5) The Services and CCMDs are integrating digital production management and 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.

(6) DoD and Service distributed common ground/surface system (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.

(7) To provide digital intelligence products in bandwidth-limited situations, processes exist that enable physical delivery of digital media. These options include delivery of hard-drives from the producing agency or Defense Logistics Agency, up to delivery of servers that can replicate digital products on local networks. CCMD and joint

force personnel should determine potential impacts of reduced bandwidth on intelligence dissemination and identify requirements for mitigation.

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, logistics directorate of a joint staff (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.

30. Integration of Intelligence and Operations

a. Information advantage requires the timely integration of intelligence and METOC information 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 continuous integration of intelligence, METOC information, and operations allows commanders and all operational planners access to the most current information available, thereby optimizing intelligence and METOC support to C2 and planning. The combined COP and CIP is the nexus of intelligence and operations integration. 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, and METOC 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 merging of inputs from a wide variety of tactical, operational, and strategic/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 and direction. The COP depicts friendly, enemy, 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 maps and aeronautical charts). It includes a variety of NRT friendly, enemy, and adversary air, ground, and maritime tracks (single entities reported on a CIP, such as an aircraft, ship, theater ballistic missile, or emitter location); threat/warning data; and intelligence broadcasts. Information received from the IBS feeds from orbiting satellites and other passive sensors is automatically plotted on COP graphic displays.

c. To create a comprehensive presentation of the OE and depiction of the enemy situation, the CIP is developed and managed at the Top Secret//SCI level to the maximum extent feasible. Within the CIP, intelligence from all sources/classifications can be accessed, managed, and displayed and then shared across networks, as appropriate. This guidance is not contrary to the requirement for CIP data to be classified at the lowest level permitted by policy and regulation.

(1) Figure III-19 illustrates the disposition of friendly, enemy, neutral, and unknown tracks and/or objects and shows the relationships between COP displays across multiple security domains. It shows the Top Secret//SCI COP to be the most informative depiction of the OE because of the rich intelligence it can display.

(2) The figure also shows threat and neutral tracks that are generated at all levels of classification and shared both up and down domains dependent upon the source/classification of the individual track. To facilitate information sharing both internally and externally (including allies/mission partners), CIP data is classified at the lowest level permitted by policy and regulation. In some cases, tracks may be sanitized (higher classification/compartmented intelligence stripped) for sharing at lower classification levels on lower domains, as appropriate.

(3) Intelligence objects derived from object-based production (OBP) are the result of correlating, fusing, and arranging intelligence from all sources around an object rather than storing them in the traditional data source silos (e.g., SIGINT, MASINT, HUMINT, local databases). In most instances, an OBP object has associated geospatial and METOC data and can be displayed in the same manner as a CIP track.

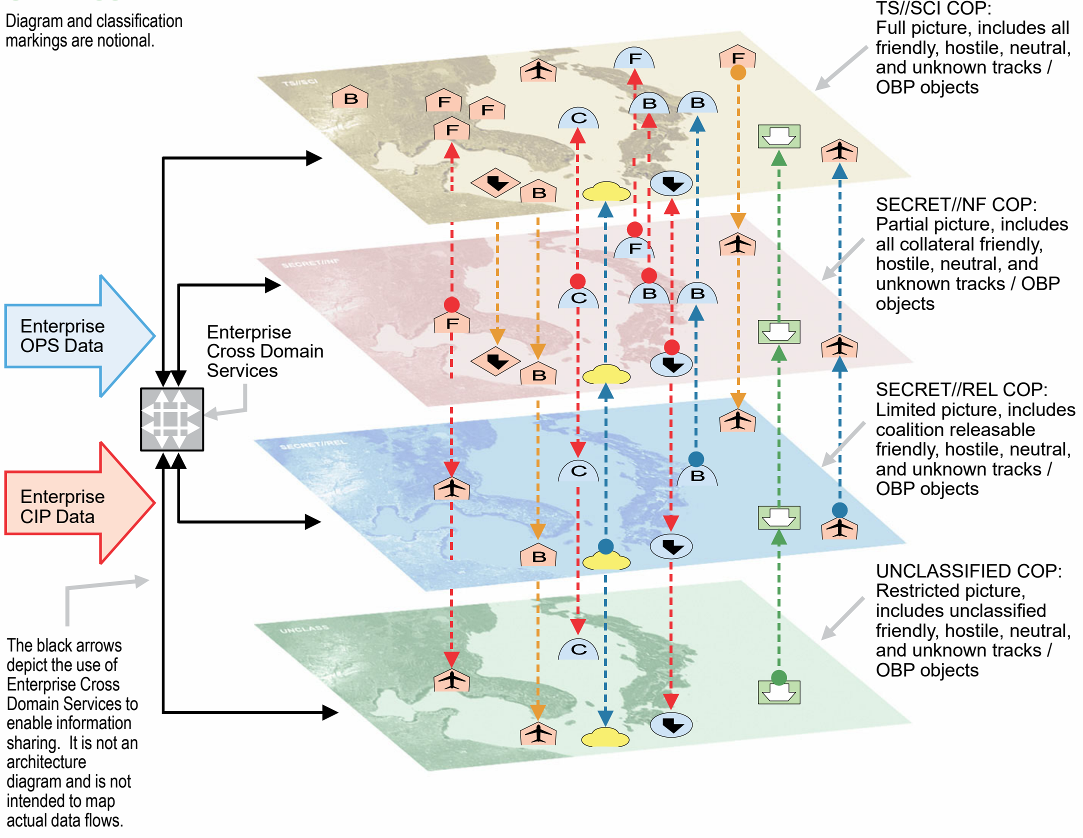
d. A CIP is required by decision makers at all echelons. CIP development, management, and sharing follows a hierarchical flow from the tactical-level common tactical picture (CTP) to the strategic-level global COP and CIP. The global picture is then shared back down echelon to enable global SA across the joint force. See CIP reporting structure at Figure III-20.

e. As the intelligence component of a CTP and the foundational element of intelligence and operations integration, the tactical-level CIP is an integral component necessary for understanding the OE at the tactical level and above. To achieve this SA, JTFs and the components maintain a tactical CIP within their respective operational area and designate enemy and neutral track production and reporting responsibilities to subordinate elements that are designated as CIP inject sites (see paragraph 30.f.[1] and Figure III-21 for additional details). Components are the principal CIP producers for their assigned mission and operational areas.

Common Operational Picture Display Across Multiple Security Domains Example

UNCLASSIFIED

Diagram and classification markings are notional.



TS//SCI COP: Full picture, includes all friendly, hostile, neutral, and unknown tracks / OBP objects

SECRET//NF COP: Partial picture, includes all collateral friendly, hostile, neutral, and unknown tracks / OBP objects

SECRET//REL COP: Limited picture, includes coalition releasable friendly, hostile, neutral, and unknown tracks / OBP objects

UNCLASSIFIED COP: Restricted picture, includes unclassified friendly, hostile, neutral, and unknown tracks / OBP objects

The black arrows depict the use of Enterprise Cross Domain Services to enable information sharing. It is not an architecture diagram and is not intended to map actual data flows.

NOTE:
Tracks are generated at all levels of classification and shared both up and down domain dependent upon the source/ classification of the individual track. In some cases, tracks may be sanitized (higher classification information stripped) for sharing at lower classification levels.

Legend

CIP	common intelligence picture
COP	common operational picture
NF	no foreign
OBP	object-based production
OPS	operations
REL	releasable
SCI	sensitive compartmented information
TS	top secret

Friend:
- B air – bomber
- F air – fighter
- C air – cargo
- sea surface – carrier

Hostile:
- B air – bomber
- F air – fighter
- ✈ air – fixed-winged air – cargo
- sea surface – carrier

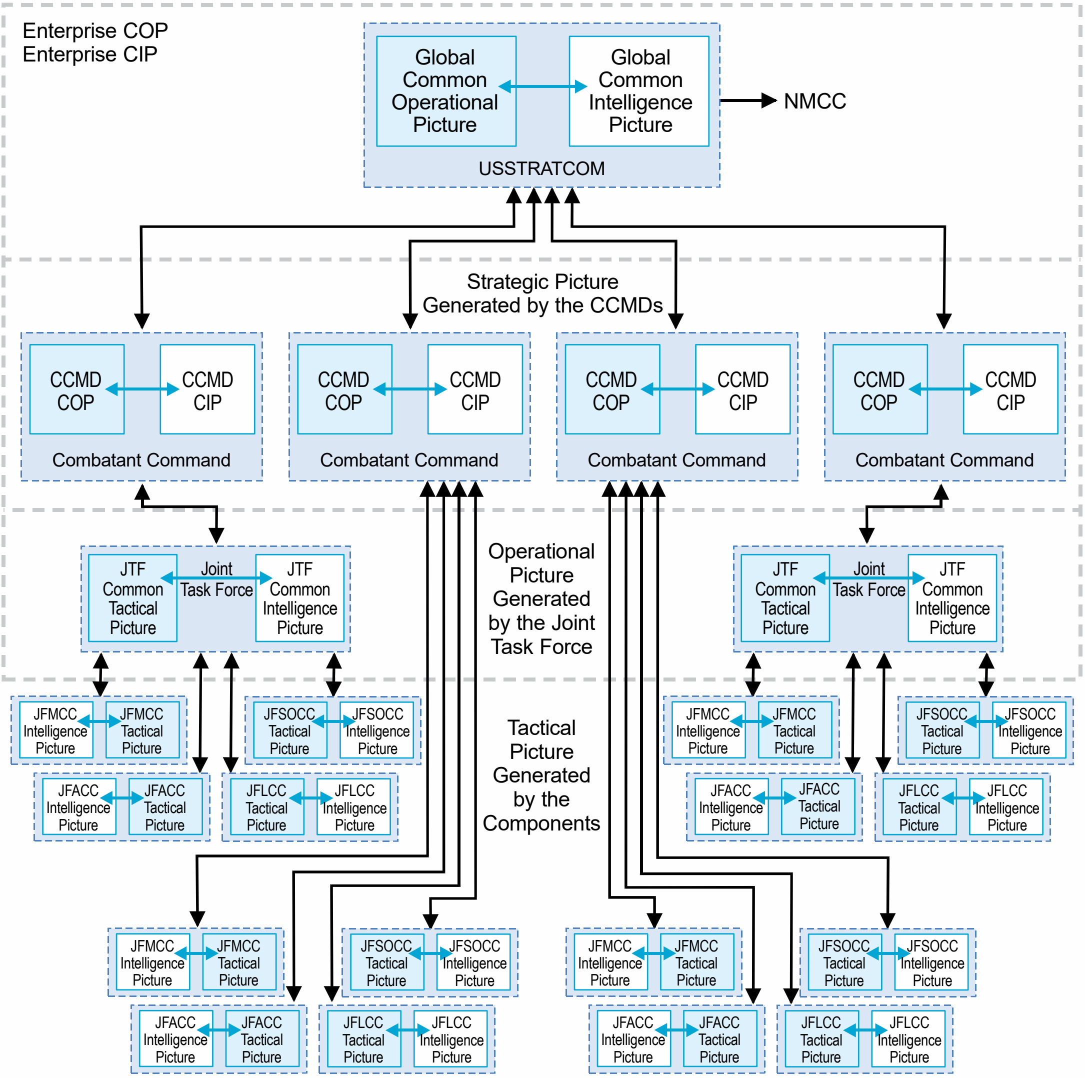
Neutral:
- sea surface – merchant ship

Unknown:
- air

Track Domain of Origin:
- ●- - - -▶ TS//SCI COP
- ●- - - -▶ Secret//NF COP
- ●- - - -▶ Secret//REL COP
- ●- - - -▶ Unclassified COP

Figure III-19. Common Operational Picture Display Across Multiple Security Domains Example

Notional Common Intelligence Picture Reporting Structure


Enterprise COP
Enterprise CIP
Global Common Operational Picture
Global Common Intelligence Picture
USSTRATCOM
NMCC
Strategic Picture Generated by the CCMDs
CCMD COP
CCMD CIP
Combatant Command
CCMD COP
CCMD CIP
Combatant Command
CCMD COP
CCMD CIP
Combatant Command
CCMD COP
CCMD CIP
Combatant Command
Operational Picture Generated by the Joint Task Force
JTF Common Tactical Picture
Joint Task Force
JTF Common Intelligence Picture
JTF Common Tactical Picture
Joint Task Force
JTF Common Intelligence Picture
Tactical Picture Generated by the Components
JFMCC Intelligence Picture
JFMCC Tactical Picture
JFSOCC Tactical Picture
JFSOCC Intelligence Picture
JFACC Intelligence Picture
JFACC Tactical Picture
JFLCC Tactical Picture
JFLCC Intelligence Picture

NOTE:
The diagram's depiction of the tactical picture generated by the components is representative in nature and may vary based on policies, processes and procedures set by the commands. Also, it only depicts functional component commands at the tactical level; depending on a CCMD's organizational structure, Service component commands could serve the same function.

Legend

CCMD	combatant command	JFSOCC	joint force special operations component commander
CIP	common intelligence picture	JTF	joint task force
COP	common operational picture	NMCC	National Military Command Center
JFACC	joint force air component commander	USSTRATCOM	United States Strategic Command
JFLCC	joint force land component commander		
JFMCC	joint force maritime component commander		

Figure III-20. Notional Common Intelligence Picture Reporting Structure

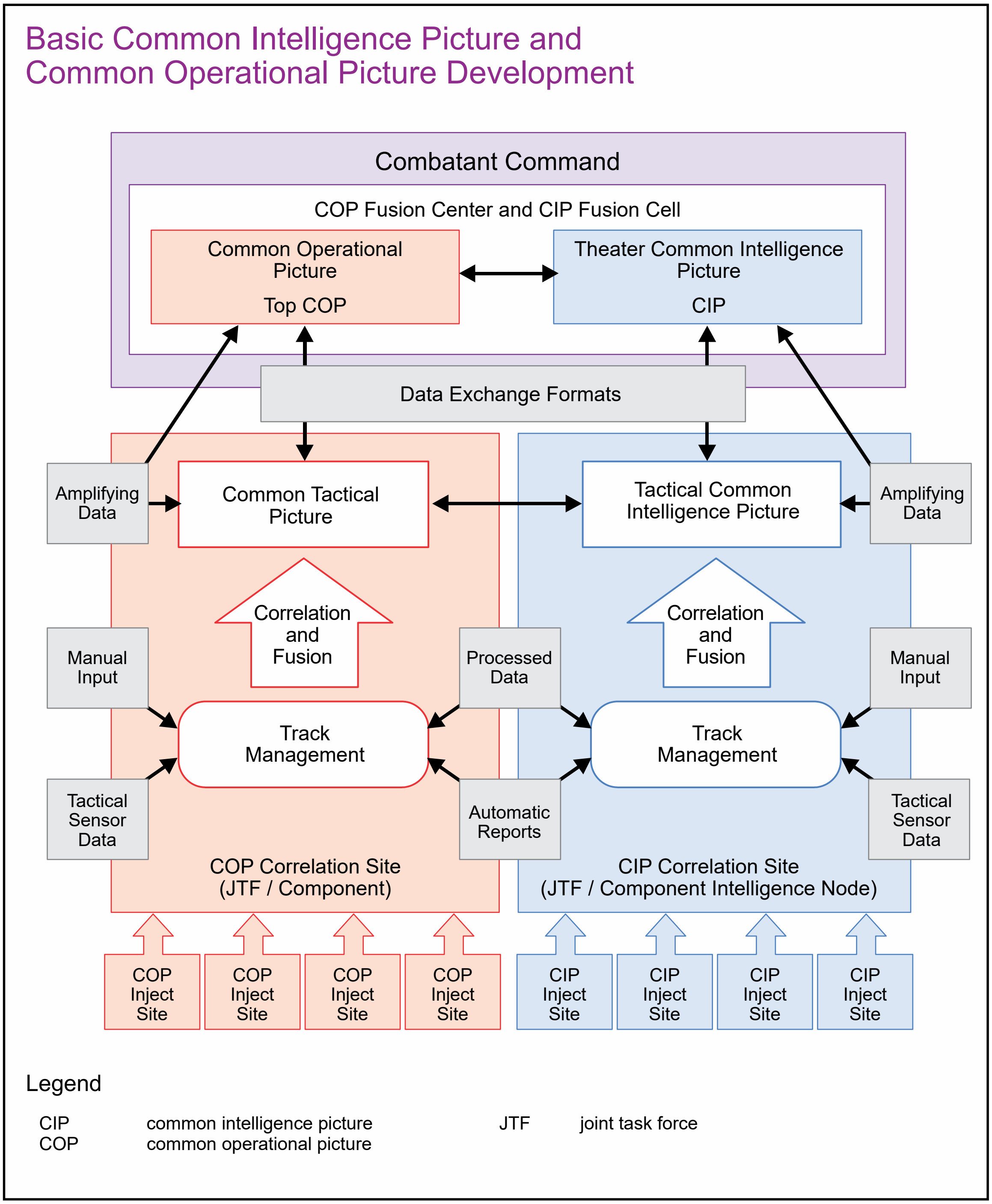


Figure III-21. Basic Common Intelligence Picture and Common Operational Picture Development

(1) Dependent on the CCMD's organizational structure, JTFs and/or the components provide tactical-level CIPs to the CCDR using the GCCS architecture. This responsibility applies to the JTFs, as well as components of subordinate unified commands. These requirements may be altered or modified by the CCDR and/or JTF if conditions warrant. However, the use of Global Command and Control System-Joint (GCCS-J)/GCCS-I3 is critical to shared SA across the joint force.

(2) Active participation and collaboration with and between JTFs/components and allies at the tactical level is critical to providing a comprehensive and accurate theater CIP.

f. CIP is the primary output of the NRT analysis of time-sensitive reporting that is necessary to support enemy and neutral track production. This effort is core to achieving information superiority and provides SA that supports theater plans, operations, and decision making.

(1) A tactical-level CIP consists of a collection of intelligence data injects into GCCS on enemy and neutral air, space, land, and maritime tracks and units, of all threat types, both in and out of garrison. A CIP inject site can designate operationally significant items, such as an aggregation of enemy military personnel, weapon systems, vehicles, and support elements as a single CIP track. Manual inputs may be necessary. The organizational size of reported forces varies by CCMD, operation, situation, and plan.

(2) JTFs/components should leverage the analytical, fusion, and tracking tools available to them, (e.g., DCGS, force disposition tracker) to support development and maintenance of the CIP. Use of tools that are interoperable with GCCS-I3 increases timeliness and efficiency while reducing workload and errors associated with manually transferring data between systems.

g. At the operational level, the CIP consists of a collection of CIPs from the tactical level (**intelligence** component of CTPs), as well as graphical overlays and other intelligence data, such as tracks outside subordinate operational areas contributed by national technical means or other systems and ISR collection routes and schedule information.

(1) CCDRs have the responsibility to direct procedures for components and deployed forces within their respective operational areas to maintain an accurate theater CIP. The processes and procedures are very similar to those employed at the tactical level. The CCDR coordinates/tasks organizations via theater CONOPS or TASKORD messages.

(2) The key nodes within a CCDR's AOR that function to consolidate, deconflict, and forward appropriate data required to create the theater CIP parallel those of the COP or CTP. The key nodes are called common intelligence picture fusion cells (CIPFCs) at the operational level and at the tactical level, common intelligence picture correlation sites (CIPCSs) and CIP inject sites.

h. While the functions and processes to develop and maintain the CIP are similar to those of the COP, there are significant differences in both the information that is being managed and the tradecraft necessary to conduct and leverage the NRT analysis of time-sensitive reporting necessary to develop and maintain a relevant, timely, and accurate depiction of enemy and neutral force disposition. This requires the CIP management key nodes be led and operated by intelligence personnel and the work accomplished in intelligence workspaces.

(1) CIP inject sites are the foundational sources for tactical intelligence entering the CIP. CIP inject sites are designated by commander's guidance and generally include component-level and subordinate-element ISR units. CIP inject sites are task-organized based on standing and/or situation-dependent mission events and guidance from higher-level authority, which is generally included in TASKORD messages.

(2) Elements within a CCMD AOR that consolidate, manage, and track unit data are designated CIPCSs and typically include JTF HQ, component HQs, and intelligence nodes (e.g., joint force land component commander analysis and control element or joint force air component commander analysis, correlation, and fusion branch). The majority of CIP data is shared among CIPCSs within a given theater through GCCS-J/GCCS-I3 communication interfaces. CIPCSs forward their local CIP to the theater CIPFC for creation of the CCMD's theater CIP. Intelligence developed by the JIOC is added to the CIP by the CIPFC (the CCDR may designate the JIOC to serve as the CIPFC).

SECTION F. EVALUATION AND FEEDBACK

31. Overview

Evaluation and feedback occur continuously during each step of the intelligence process and assess the intelligence process as a whole. Intelligence personnel should assess the execution of the intelligence tasks they perform and gauge their impacts. Evaluation and feedback require a collaborative dialogue between intelligence planners, collection managers, collectors, single and all-source analysts, and intelligence systems architects to identify deficiencies within the intelligence process. They also require consultation with intelligence consumers to determine if IRs are being satisfied. Immediate applications of evaluation and feedback may include, but are not limited to, the rephrasing of an IR for clarity, the dynamic retasking of a sensor, the rerouting of data to an alternate exploitation node, or the revision of an information report or a finished intelligence product. The goal of evaluation and feedback is to identify issues as early as possible to minimize information gaps and to mitigate capability shortfalls, as well as ensuring intelligence operations meet established analysis tradecraft and objectivity standards (see Appendix A, "Analytic Standards").

32. 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 Chapter I, "The Nature and Role of Intelligence."

33. 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 ideas to improve the intelligence process from intelligence personnel and consumers.

34. Assessment

a. Information gathered during evaluation and feedback may inform broader assessments of the intelligence joint function. Assessments provide leaders with the information to make decisions about reprioritization of IRs, shifts in collection emphasis, changes to analytic levels of effort, reallocation of available intelligence assets, training of intelligence personnel, and the development of new intelligence capabilities.

b. To perform assessments of intelligence activities and operations, intelligence planners develop and document intelligence measures of performance (MOPs) and intelligence measures of effectiveness (MOEs) in annex B (Intelligence). These measures are informed by a variety of indicators related to the conduct of intelligence tasks or their impact. Task-related metrics are informed by quantitative indicators. They determine whether a particular platform or sensor is performing according to technical specifications, the number of sorties conducted, the number of images taken, or the number of interrogations conducted or all-source products generated. On the other hand, effectiveness of intelligence activities and operations is determined by gauging the impact of intelligence tasks performed within the intelligence process. Effectiveness-related metrics are informed by indicators that tend to be qualitative. Factors considered in determining the effectiveness of intelligence activities and operations include the reliability of a source, whether a particular information reported is considered actionable, or if a particular product is cited in finished intelligence as contributing to an increase in analytic confidence. Establishing intelligence MOEs requires addressing the question of intelligence or information value. The value of information or intelligence is tied to the decision that it supports and the amount of uncertainty it clarifies or resolves. Ultimately, the effectiveness of intelligence activities and operations is assessed by devising metrics and indicators associated with the attributes of intelligence excellence discussed in Chapter I, "The Nature and Role of Intelligence," paragraph 3, "Principles of Joint Intelligence." The ability of the intelligence staff to assess the totality of intelligence operations relies on product satisfaction as determined by the user. For this reason, feedback from the user should be consistent and formal, with some element of systematic analysis to add rigor to the process.

c. Formal assessment methods and procedures for the intelligence staff provide decision makers with actionable information backed by analytical rigor. Assessors collect, evaluate, and understand the significance of data regarding both the conduct of intelligence tasks (MOPs) and the effectiveness of intelligence (MOEs) in satisfying the requirements of the commander and staff. Data resulting from assessments supports the identification and resolution of procedural issues and contributes to resolving gaps and shortfalls.

Intentionally Blank

CHAPTER IV
INTELLIGENCE PLANNING AND ASSESSMENT

SECTION A. INTELLIGENCE PLANNING

1. Overview

a. The planning of joint operations is accomplished through the JPP. The IP process is conducted by the organizations within the DoD component of the IC. IP is the structured integration and management support to the Joint Strategic Planning System (JSPS) and JPP and is executed through an established methodology to coordinate and integrate available Defense Intelligence and Security Enterprise capabilities in support of CJCS direction and the problem set's coordinating authority or lead CCDR's plans or orders. IP involves planning and directing DoD intelligence operations and collaboration with interagency partners and IC, allied, and PN intelligence organizations to achieve integrated intelligence support during execution of contingency and campaign plans to align with objectives of an operation. The Joint Staff J-2, CCMD J-2, and subordinate unified command J-2s direct IP activities and approve IP products synchronized to CJCS global integration requirements and CCDR decision cycles. As appropriate, the Joint Staff J-2 and CCMD J-2s coordinate non-DoD IC support with the ODNI and collaborate with cooperating non-DoD intelligence organizations. IP activities and products are underpinned by the JPP, the joint planning and execution community plan review, and the assessment processes. These processes require a continuous, collaborative, and shared understanding of the OE among participating DoD, IC, allied, and PN intelligence organizations. This shared understanding enables the iterative refinement of campaign and contingency plans, supporting intelligence plans, and associated intelligence products. Intelligence products that support the JSPS include the Joint Strategic Assessment and the Joint Strategic Intelligence Estimate.

For more information on the intelligence products, see CJCSI 3110.02, Intelligence Supplement to the Joint Strategic Campaign Plan.

b. **IP Products that support the JPP include DTA or xCIE.** The DTA is a defense strategic intelligence assessment to support CCMD problem framing and mission analysis for contingency planning. The DTA provides analysis of adversary intent, capability, and enemy COAs with scenarios for each problem integrated contingency plan directed in CJCSI 3110.01, *(U) 2018 Joint Strategic Capabilities Plan (JSCP)* [short title: JSCP]. The xCIE is a national strategic estimative intelligence product intended to inform development of GCPs by emphasizing how key actors and underlying factors may be affected by the conditions in the strategic environment throughout the 2–5-year lifespan of the CCPs, functional campaign plans, and regional campaign plans. The "x" in xCIE is a variable that represents the type of campaign plan the estimate supports. These DIA-produced strategic intelligence assessments enable development of the CCMD intelligence staff estimate to conduct mission analysis and develop COAs.

For additional information on IP, refer to CJCSM 3314.01, Intelligence Planning. *For more information on DTA and xCIE, see CJCSI 3110.02,* Intelligence Supplement to the Joint Strategic Campaign Plan.

SECTION B. JOINT PLANNING

2. Joint Planning

Joint planning consists of four functions (strategic guidance, concept development, plan development, and plan assessment), the JPP, and an operational design methodology as depicted in Figure IV-1.

a. Operational design and the JPP are complementary tools of the overall planning process. Operational design provides an iterative process that enables the commander's vision and mastery of operational art to help planners answer ends-ways-means-risk questions and appropriately structure campaigns and operations in a dynamic OE. The commander, supported by the staff, gains an understanding of the OE, defines the problem, and develops an operational approach for the campaign or operation through the application of operational design during the initiation step of the JPP. Commanders communicate their operational approach to their staff, subordinates, supporting commands, agencies, multinational partners, and NGOs as required in their initial planning guidance

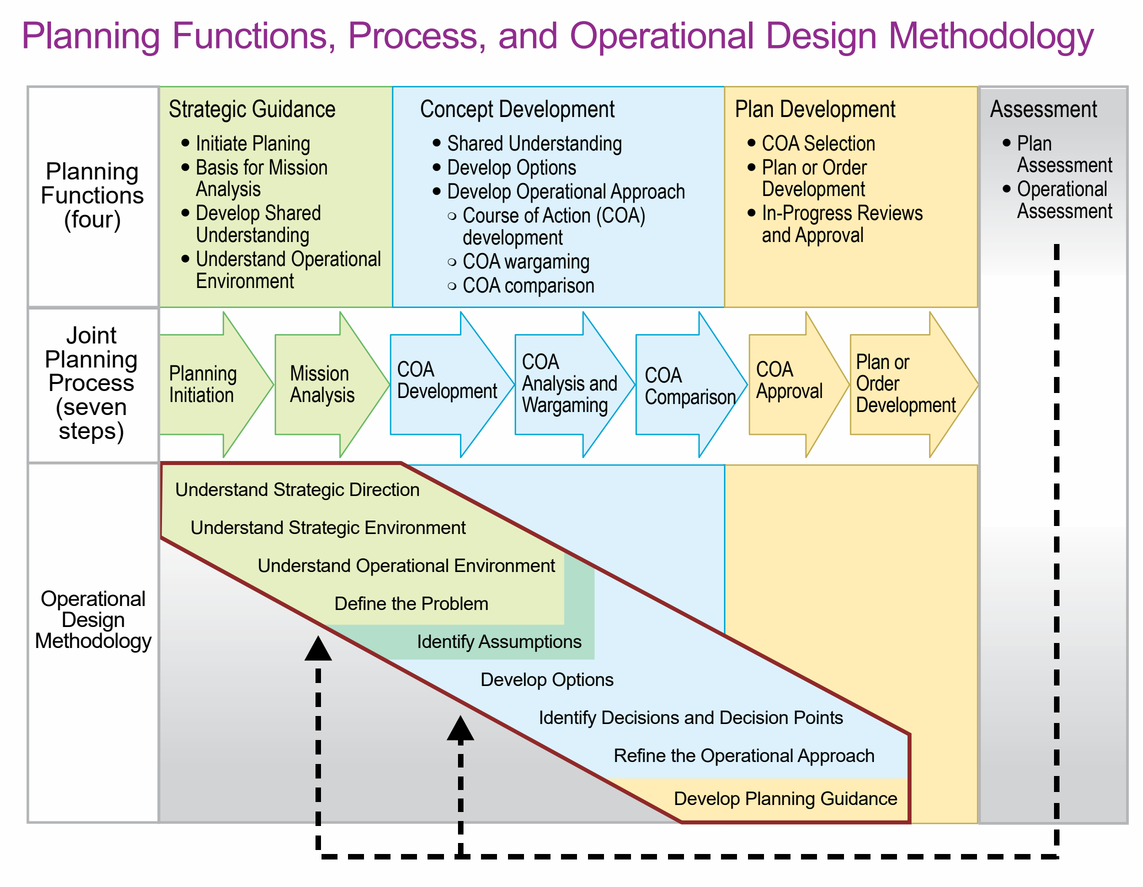

Planning Functions, Process, and Operational Design Methodology
Planning Functions (four)
Strategic Guidance
• Initiate Planing
• Basis for Mission Analysis
• Develop Shared Understanding
• Understand Operational Environment
Concept Development
• Shared Understanding
• Develop Options
• Develop Operational Approach
○ Course of Action (COA) development
○ COA wargaming
○ COA comparison
Plan Development
• COA Selection
• Plan or Order Development
• In-Progress Reviews and Approval
Assessment
• Plan Assessment
• Operational Assessment
Joint Planning Process (seven steps)
Planning Initiation
Mission Analysis
COA Development
COA Analysis and Wargaming
COA Comparison
COA Approval
Plan or Order Development
Operational Design Methodology
Understand Strategic Direction
Understand Strategic Environment
Understand Operational Environment
Define the Problem
Identify Assumptions
Develop Options
Identify Decisions and Decision Points
Refine the Operational Approach
Develop Planning Guidance

Figure IV-1. Planning Functions, Process, and Operational Design Methodology

so their approach can be translated into executable plans. As the JPP is applied, commanders may receive updated guidance, learn more about the OE and the problem, and refine their operational approach. Commanders provide their updated approach to the staff to guide detailed planning. This iterative process facilitates the continuing development and refinement of possible COAs into a selected COA with an associated initial CONOPS and eventually into a resource-informed executable plan or order.

b. During the JPP, CCMD J-2s lead development of annex B (Intelligence). Annex B is the intelligence annex to a plan or order that provides detailed information on the threat 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. The joint force J-2 products normally include, but are not limited to, the following: a description of the operational area, an evaluation of the threat, identification of threat COGs, prioritized threat COAs, event templates, named AOIs and target AOIs, a decision support template, wargame support, and an ISM.

For additional information on the JPP, refer to JP 5-0, Joint Planning.

SECTION C. THE INTELLIGENCE PLANNING PROCESS

3. Intelligence Planning Activities

a. Joint and national intelligence activities help identify and monitor threats to national security that inform the development of policy and the DoD's overall planning efforts. Through joint planning, intelligence priorities are further refined to focus the employment of limited DoD intelligence resources. Thus, IP activities are generally organized along two distinct lines: providing intelligence to joint planning and planning intelligence operations.

b. **Providing Intelligence to Joint Planning.** IP activities supporting the JSPS include the production of intelligence assessments and estimates of enemy intentions, capabilities, and COAs. Specific intelligence outputs of the JSPS are the DIA-produced DTA, or xCIE, and the development of tailored products from the CCMD's JIPOE process that culminate in the production and maintenance of the intelligence estimate. These finished intelligence products are disseminated to inform joint planning and the development of the commander's estimate through which CCDRs provide SecDef with military options to meet strategic objectives. Activities in support of the JSPS are continuous and typically conducted in parallel with and in support of the CCMD's planning and assessment.

c. **Planning Intelligence Operations through the JPP.** IP activities in the JPP include identifying information gaps, prioritizing IRs, developing federated production and integrated collection plans, and assessing intelligence capabilities for the purpose of identifying shortfalls and mitigation strategies. Specific intelligence outputs of the JPP are the CCMD J-2 staff estimate, which identifies available CCMD intelligence capabilities and anticipated shortfalls, CSA and Service intelligence center estimates, annex B

(Intelligence) to a campaign or a contingency plan, and, when appropriate, an NISP or the joint intelligence posture assessment. Additional outputs may include intelligence resource demand signals that may be articulated through the CCDR's integrated priorities list or request for forces (RFF). Intelligence activities in the JPP are also continuous and are typically conducted internal to the command JIOC as facilitated by an intelligence planning team (IPT) or through the IP steering group in coordination with the Joint Staff J-2 to facilitate the integration of national-level intelligence support.

4. Intelligence Planning Activities During Strategic Guidance

a. IP Activities Providing Intelligence to Joint Planning

(1) DIA will validate, update, or produce a DTA or an xCIE.

(2) At the CCMD level and below, intelligence planners orchestrate the command's continuous JIPOE effort for analysts to provide a baseline assessment of the OE, enemy capabilities, objectives and associated COGs, critical capabilities, critical requirements, critical vulnerabilities, and COAs and related decisive points. The analytical cell of the CCMD JIOC evaluates relevant databases and intelligence holdings to identify gaps relevant to the planning effort under consideration. This includes the status of targeting information. The J-2 may form a JIPOE coordination cell to draw relevant information from other staff elements, IC representatives, and PNs as appropriate, as well as request tailored products from the defense IC. The JIPOE process culminates with the production of an intelligence estimate, which is incorporated into the plan as appendix 11 (Intelligence Estimate) to annex B (Intelligence).

(3) As core members of the JPG, intelligence planners contribute to the overall plan development and nominate operations objectives, desired effects, and other mission success criteria. In nominating mission success criteria, intelligence planners also advocate for the adoption of measurable and achievable objectives while considering how intelligence capabilities might be employed to assess them.

b. IP Activities While Planning Intelligence Operations

(1) Intelligence planners assemble an IPT or similar community of interest with all-source analysts and collection strategists as its core members (see Figure IV-2). Intelligence systems architects; single source analysts; and representatives from CSAs, Service components, allies, and partners (if appropriate and authorized), and the JRC may also collaborate with the IPT.

(2) The IPT develops an IP timeline that is synchronized with the command's planning timeline. This ensures tailored JIPOE products, the initial intelligence estimate, and the initial J-2 staff estimate are developed to meet the JPG's requirements.

(3) To generate the J-2 staff estimate, the IPT, in coordination with representatives from Service components and subordinate joint force commands, identifies and analyzes all intelligence capabilities of assigned forces available to support the execution of the plan. For contingency plans, this may include apportioned forces. For

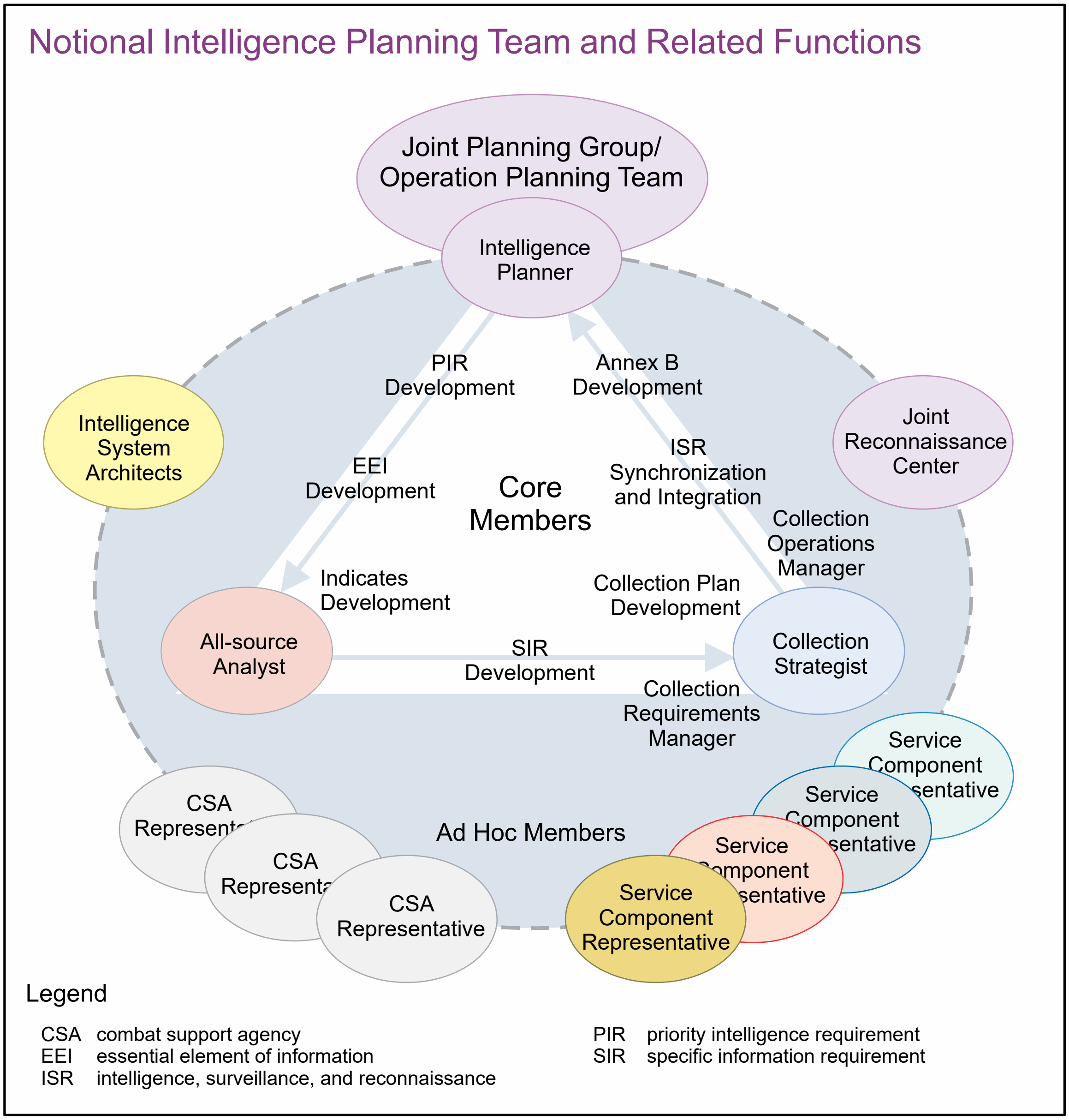


Figure IV-2. Notional Intelligence Planning Team and Related Functions

ongoing operations and campaign plans, this may include allocated forces. Conducting this analysis for ongoing operations, campaigns, and planning may inform requests for additional forces.

(4) The IPT evaluates current theater collection and production postures to identify available assets that may need to be redirected to support the planning effort or the execution of the plan under consideration. In collaboration with the CCMD's collection managers, J-2X, the JRC, and representatives from the Joint Staff J-32 [Deputy Directorate for Intelligence, Surveillance, and Reconnaissance Operations], the IPT conducts a preliminary assessment of available collection assets and capabilities. In collaboration with the CCMD production manager, and representatives from the JIOC's analytical cell, the IPT performs an initial assessment of available analytic capabilities.

(5) Based on the list of all available intelligence capabilities, the IPT drafts and submits the initial J-2 staff estimate to the JPG to support the command's overall force structure analysis. In addition to listing all available intelligence capabilities, the initial J-2's staff estimate identifies all factors that may affect the employment of these capabilities. Factors such as logistical supportability, basing rights, communications and intelligence systems architecture, linguist availability, and legal restrictions should be considered. Certain employment limitations can be mitigated during COA development in coordination with the JPG. Other limitations, however, may require mitigation through friendly actions outside the immediate control of the command. In these instances, intelligence planners, in collaboration with the JPG, may nominate appropriate planning assumptions. To validate these planning assumptions prior to COA approval, they may nominate initial FFIRs. If left unanswered prior to plan development, initial FFIRs may be included as part of the final CCIRs to be monitored during plan assessment to inform refine, adapt, terminate, execute (RATE) decisions.

(6) Considering all of the identified intelligence gaps relevant to the planning effort and recognizing the uncertainties in analytical conclusions, intelligence planners, in collaboration with the JPG, may nominate additional planning assumptions and initial PIRs for validation during the current planning cycle. Upon approval by the J-2 and the CCDR, initial PIRs are then passed to the IPT or appropriate mission managers for action. If left unanswered prior to plan development, initial PIRs may be included as part of the final CCIRs to be monitored during plan assessment to inform RATE decisions.

5. Intelligence Planning Activities During Concept Development

a. **IP Activities Providing Intelligence to Joint Planning**

(1) Intelligence planners evaluate JIPOE products to be disseminated to the JPG. The intelligence planner or the analyst presents these products to the JPG IAW the established planning timeline.

(2) Intelligence planners coordinate personnel to participate in COA analysis and wargaming. The J-2 may employ multiple representatives to support the JPG during the wargame. These may include:

(a) Intelligence planner to develop and analyze the overall intelligence support strategy.

(b) Red cell personnel to play the role of uncooperative enemy/adversary and red team personnel to challenge planning assumptions and provide alternative viewpoints.

(c) Intelligence analyst to nominate indicators of progress or regression used in the command's assessment process.

(d) Collection strategists to initiate the development of a supporting collection plan.

(3) Intelligence planners determine intelligence governing factors and highlight the advantages and disadvantages of each COA.

b. **IP Activities While Planning Intelligence Operations**

(1) During COA development, intelligence planners consider how theater intelligence assets and external intelligence resources could be employed to support the execution of the plan.

(2) Based on potential enemy/adversary reactions evaluated during COA analysis and wargaming, the intelligence planner and the collection strategist determine how the various collection disciplines could be employed to monitor relevant indicators.

(3) The intelligence planner revises the J-2 staff estimate capturing additional factors, unique to each of the proposed friendly COAs, which may limit the employment of intelligence capabilities. Once identified, the intelligence planner ensures these factors are considered during COA comparison.

(4) The intelligence planner consolidates final PIR nominations from across the staff and drafts PIRs as required to support CCDR decisions. During COA approval, the intelligence planner recommends PIRs through the J-2 for CCDR approval. PIR nominations not approved by the CCDR are processed at a lower priority and satisfied when intelligence resources become available.

(5) Following COA approval, the intelligence planner, in collaboration with the IPT, develops EEIs and associated indicators required to satisfy the PIR. To maximize support to the commander’s operational objectives, the IPT integrates and reconciles these requirements with MOEs and their associated indicators.

(6) Coordinate with CCMD GI&S personnel to identify GI&S support necessary for selected COA.

(7) Based on IRs (to include PIRs), information requirements (to include EEIs), their associated indicators, and anticipated SIRs, the IPT then generates a matrix of anticipated PRs to guide the development of federated production plans and a matrix of anticipated CRs to guide the development of integrated collection plans.

(8) The J-2 staff estimate process culminates with the collection and production capability assessments performed against anticipated requirements entered on the collection and PRs matrices.

(9) The Joint Staff J-2, in coordination with the CCMD J-2, determines when a NISP is required for each integrated contingency plan and will task development based on all of the CCMD J-2 staff estimates included in the integrated set of plans, and IAW CJCSI 3110.02, *(U) Intelligence Supplement to the Joint Strategic Campaign Plan.* The Joint Staff J-2 publishes a NISP plan order detailing the plan of actions and milestones and scope of the NISP. Development of the NISP is based on the integrated CCMD PIRs, EEIs, concept of intelligence operations, PRMx, CRMx, and the CCMD’s J-2’s staff estimate of

available capabilities to satisfy its requirements. Collaboration between the CCMDs, Joint Staff J-2, CSAs, and Service intelligence centers is encouraged and can occur at any time during the planning process.

6. Intelligence Planning Activities During Plan Development

a. **IP Activities Providing Intelligence to Joint Planning**

(1) The JIOC's analytical cell completes the intelligence estimate. Selected portions of the intelligence estimate are used to complete the enemy situation paragraphs throughout the plan.

Refer to CJCSM 3130.03, Planning and Execution Formats and Guidance, *for a complete intelligence estimate format.*

(2) The CCMD J-2 may also provide analytical support and input to other portions of the plan, to include annex H (Meteorological and Oceanographic Operations) and other annexes as required.

b. **IP Activities While Planning Intelligence Operations**

(1) Intelligence planners develop the base annex B (Intelligence), which outlines the intelligence mission; concept of intelligence operations; PIRs; and guidance for how collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback will be performed during execution. Annex B (Intelligence) also specifies tasks to subordinate intelligence organizations and requirements for external support.

(2) Intelligence planners evaluate whether targeting is necessary to accomplish the operation. If so, the IPT facilitates TSA, target development, and target list management.

(3) Intelligence planners collaborate with discipline-specific managers and other subject matter experts to develop required functional appendices to annex B (Intelligence) (i.e., J-2X for appendix 3, [Counterintelligence]).

(4) To ensure the collection plan is fully integrated and synchronized with the contemplated operation, intelligence planners and collection strategists contribute to other portions of the plan such as appendix 8 (Reconnaissance) to annex C (Operations), annex S (Special Technical Operations), and other annexes as required.

(5) If the contingency plan will be supported by a NISP, the Joint Staff J-2 and CCMD J-2 collaborate to lead the NISP development, production, completion, staffing, and approval process.

For additional information on NISP development, IP support to campaign plans, and contingency planning, refer to CJCSM 3314.01, Intelligence Planning.

7. Intelligence Communications Architecture Planning

a. 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 US and PN 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 J-4 and other logistic elements for the timely delivery and installation of intelligence and communications systems.

b. **Communications Planning Methodology.** Key constructs 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 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 the threat's cyberspace exploitation and 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 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 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.

c. **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 and METOC information 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, METOC information and 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.

d. **System Planning.** 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 the higher HQ for resolution.

e. **Planning Considerations**

(1) Joint intelligence dissemination relies on a federated architecture across many agencies and systems. The federated architecture enables JFCs access to relevant intelligence and METOC information when needed, based on their mission and the priority 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. 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) During interagency coordination, information and intelligence sharing are facilitated by each CCMD's JIOC, DNI representative, DIA forward element, and JIACG.

(a) The CCMD JIOC is the theater focal point to plan, synchronize, coordinate, and integrate the full range of intelligence operations in the CCDRs' AOR. The JIOC works with the DNI representative to the CCMD and liaison personnel from DoD and non-DoD national intelligence organizations to ensure all relevant intelligence and information is fully shared in the timeliest manner possible.

(b) The JIACG facilitates the application of the instruments of national power in a coherent manner and provides a means to integrate interagency perspectives into military planning and execution. The JIACG, consisting of various representatives from USG departments and agencies, serves as a multifunctional advisory element that can facilitate information sharing, operational-level planning and coordination, and political-military synthesis across interagency partners for the CCDR and staff. A typical JIACG may connect to the various US embassies and their country teams, as well as to national-level planners. Its primary role is to bridge the gap between civilian agency and military campaign planning efforts for regional military engagement and potential regional crises. Specific objectives of the JIACG are to:

1. Improve operational interagency planning and execution.

2. Exercise secure collaboration processes and procedures with participating agencies.

3. Promote continuous relationships among interagency planners.

Further information on the JIACG is contained in JP 3-08, Interorganizational Cooperation.

f. **Systems Network.** A network of integrated work stations, file servers, and communications links comprises the second component of an integrated intelligence architecture. The components of the systems network must work together and comply with the evolving defense information infrastructure, COP, data strategies, and DoD Information Technology Standards Registry to create the interoperable collaborative IE required to support joint and multinational operations and interagency coordination. The network includes direct connectivity by appropriate communications or communications relay link (landline, radio, satellite, and others as appropriate) and broadcast capability to support time-sensitive needs.

SECTION D. PLAN ASSESSMENT AND EXECUTION

8. Intelligence Support to Plan Assessment and Decision Making

a. Continual and timely assessments are essential to measure progress of the joint force toward achieving objectives (see Figure IV-3). Commanders continuously assess the OE and the progress of their operations and campaigns and then compare them to their initial vision and intent. Commanders and their staffs determine relevant assessment actions and measures during planning. They consider assessment measures as early as mission analysis and include assessment measures and related guidance in commander and staff estimates. They use assessment considerations to help guide operational design to

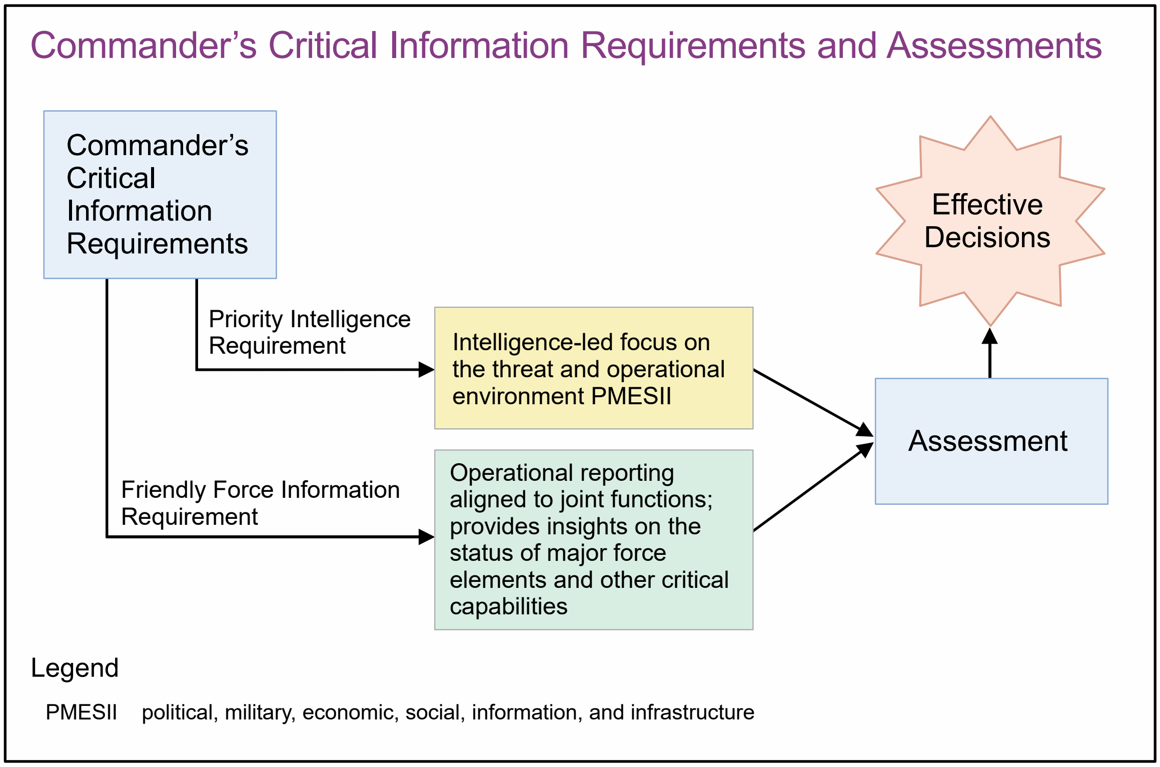

Commander's Critical Information Requirements and Assessments
Commander's Critical Information Requirements
Priority Intelligence Requirement
Intelligence-led focus on the threat and operational environment PMESII
Friendly Force Information Requirement
Operational reporting aligned to joint functions; provides insights on the status of major force elements and other critical capabilities
Assessment
Effective Decisions
Legend
PMESII political, military, economic, social, information, and infrastructure

Figure IV-3. Commander's Critical Information Requirements and Assessments

improve the sequence and type of actions along lines of operation. During execution, they continually monitor progress toward accomplishing tasks, creating effects, and achieving objectives. Assessment requirements, and the collection and analytic resources required to perform them, are built into plans and monitored. Plans for intelligence collection and analytic support to execution and continuous plan assessment are based on the supported CCMD's anticipated requirements reflected in appendix 1 (Priority Intelligence Requirements) to annex B (Intelligence) of the order. During execution, preplanned collection and PRs may change in response to dynamic changes to the CCDR's PIRs.

b. Assessment actions and measures help commanders adjust operations and align future operations strategic- and operational-level assessment efforts concentrate on broad tasks, effects, objectives, and progress toward the end state, while tactical-level assessment focuses on specific task accomplishment. Even in operations that do not include combat, assessment of progress is just as important and can be more complex than traditional CA. Normally, the joint force J-2 assists the J-3 or J-5 in coordinating assessment activities.

c. The joint force J-2, through the CCMD JIOC, assesses threat capabilities, vulnerabilities, and intentions and monitors the OE. The J-2 helps the commander and staff decide what aspects of the OE to measure and how to measure them to determine progress toward accomplishing a task, creating an effect, or achieving an objective. Intelligence personnel use the JIPOE process to provide JFCs and their staffs with a detailed understanding of the threat and other relevant aspects of the OE. Monitoring changes in the civilian environment is essential to maintaining a thorough understanding of the OE. Civilian harm assessments are a critical information source for planners.

d. Intelligence personnel in the CCMD JIOC provide objective assessments to planners that gauge the overall impact of military operations against threat forces, as well as provide an assessment of likely threat reactions and counteractions. The CCDR and subordinate JFCs should establish an assessment management system that leverages and synergizes the expertise of operations and intelligence staffs.

e. The assessment process is continuous and linked to the CCIR process by the commander's need for timely information and recommendations to make decisions throughout the operation or campaign as shown in Figure IV-3. Intelligence support to plan assessment applies during shaping execution. By supporting assessments of the impacts of shaping activities, the J-2 supports decisions to refine or adapt campaign plans or to refine, adapt, or terminate contingency plans. During execution, the J-2 continues to provide support to assessments to inform FRAGORD development reflecting decisions to refine, adapt, or terminate ongoing military operations. Intelligence assessments of the current situation provide the means for intelligence analysts to draw conclusions of a potential future situation and estimate the next series of enemy COAs. In so doing, analysts revise and maintain a running intelligence estimate to facilitate continuous planning across multiple timeframes during the conduct of operations.

9. Intelligence and the Assessment Process

a. The assessment process uses MOPs to evaluate task performance at all levels of warfare and MOEs to determine progress of operations toward achieving objectives. MOPs are used to measure task accomplishment and answer the questions "was the action taken, were the tasks completed to standard?" to produce the desired effect. MOEs are used by the strategic-, operational-, and tactical-level intelligence staffs to assess changes in the threat's behavior, capabilities, or the OE. MOEs help answer questions like: "are we doing the right things, are our actions producing the desired effects, or are alternative actions required?" Well-devised measures can help the commanders and staffs understand the causal relationship between specific tasks and desired effects.

b. Both MOPs and MOEs can be quantitative or qualitative in nature, but meaningful quantitative measures are preferred because they are less susceptible to subjective interpretation. Through these measures, the J-2 and the J-3 assist the commander in determining if military operations are creating desired or undesired effects, when objectives have been achieved, and when unforeseen opportunities can be exploited or require a change in planned operations to respond to unforeseen threat actions.

c. MOE assessment is implicit in steps 1, 2, and 3 of the JIPOE process. By continuously performing JIPOE, intelligence analysts have the ability to compare the baseline intelligence estimate used to inform the plan with the current situation and facilitate continuous planning during execution. MOE assessment is informed through the detection of observable or collectable indicators that provide evidence that certain conditions exist. Several indicators may make up an MOE, just like several MOEs may assist in measuring progress toward achievement of an objective. Indicators may be either favorable or unfavorable. While favorable indicators reflect progress towards the achievement of an objective, unfavorable indicators reflect regression and could provide warning of a potential crisis and the need to execute a branch plan (see Figure IV-4).

d. Indicators are developed through the JIPOE process and detected through intelligence disciplines and friendly unit reports (e.g., mission reports or situation reports). Friendly unit reports are used in most aspects of CA, since they typically offer specific, quantitative data or a direct observation of an event to determine accomplishment of tactical tasks.

For more information on the relationships between the CCIR process and the assessment process and continuous planning during execution, refer to JP 5-0, Joint Planning.

10. Intelligence Support to Strategic and Operational-Level Assessment

a. Strategic- and operational-level assessment efforts concentrate on broad tasks, effects, and progress toward objectives (Figure IV-5). Continuous assessment helps the JFC and joint force component commanders determine if the joint force is "doing the right

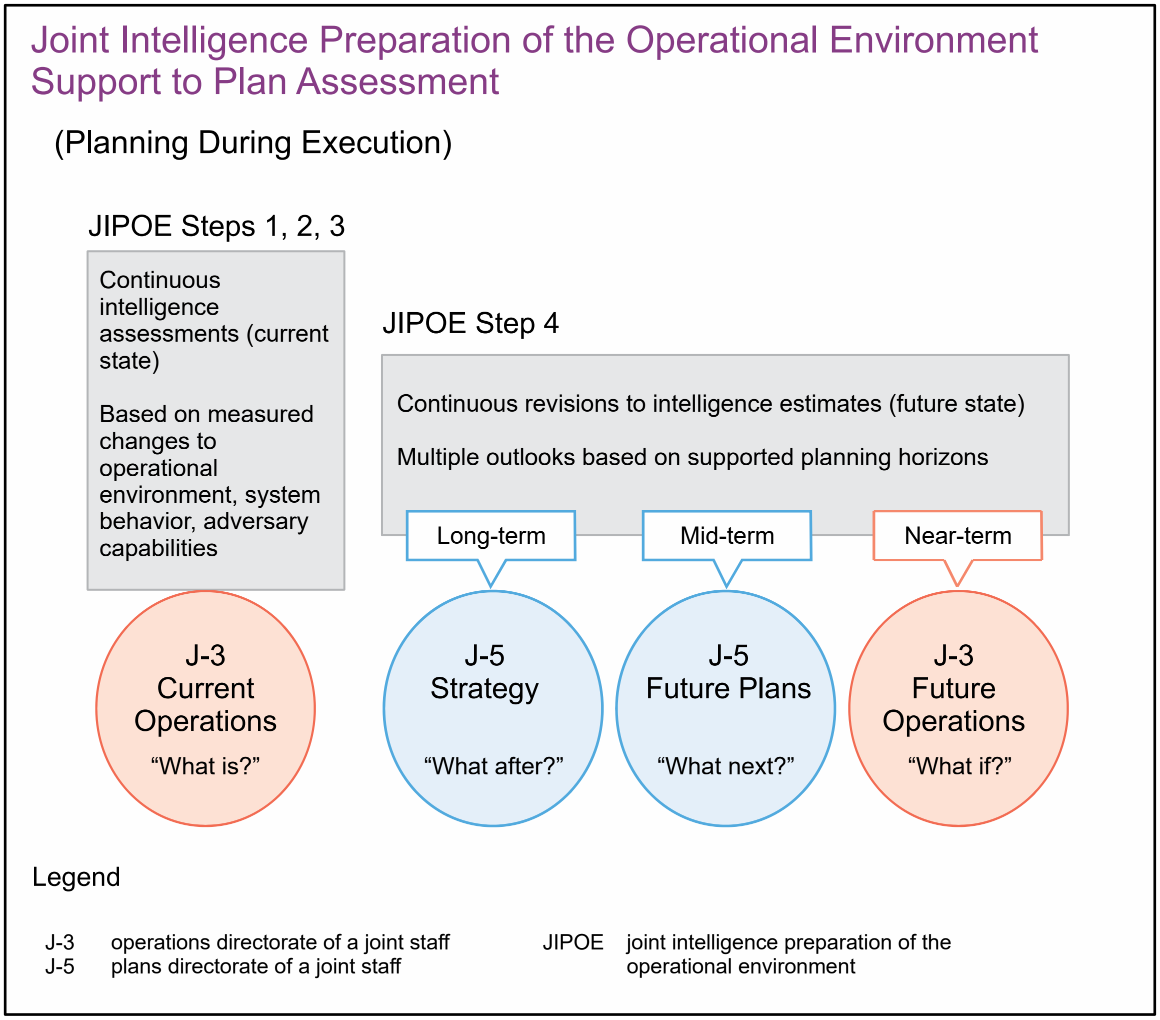

Joint Intelligence Preparation of the Operational Environment Support to Plan Assessment
(Planning During Execution)
JIPOE Steps 1, 2, 3
Continuous intelligence assessments (current state)
Based on measured changes to operational environment, system behavior, adversary capabilities
JIPOE Step 4
Continuous revisions to intelligence estimates (future state)
Multiple outlooks based on supported planning horizons
Long-term
Mid-term
Near-term
J-3 Current Operations "What is?"
J-5 Strategy "What after?"
J-5 Future Plans "What next?"
J-3 Future Operations "What if?"
Legend
J-3 operations directorate of a joint staff
J-5 plans directorate of a joint staff
JIPOE joint intelligence preparation of the operational environment

Figure IV-4. Joint Intelligence Preparation of the Operational Environment Support to Plan Assessment

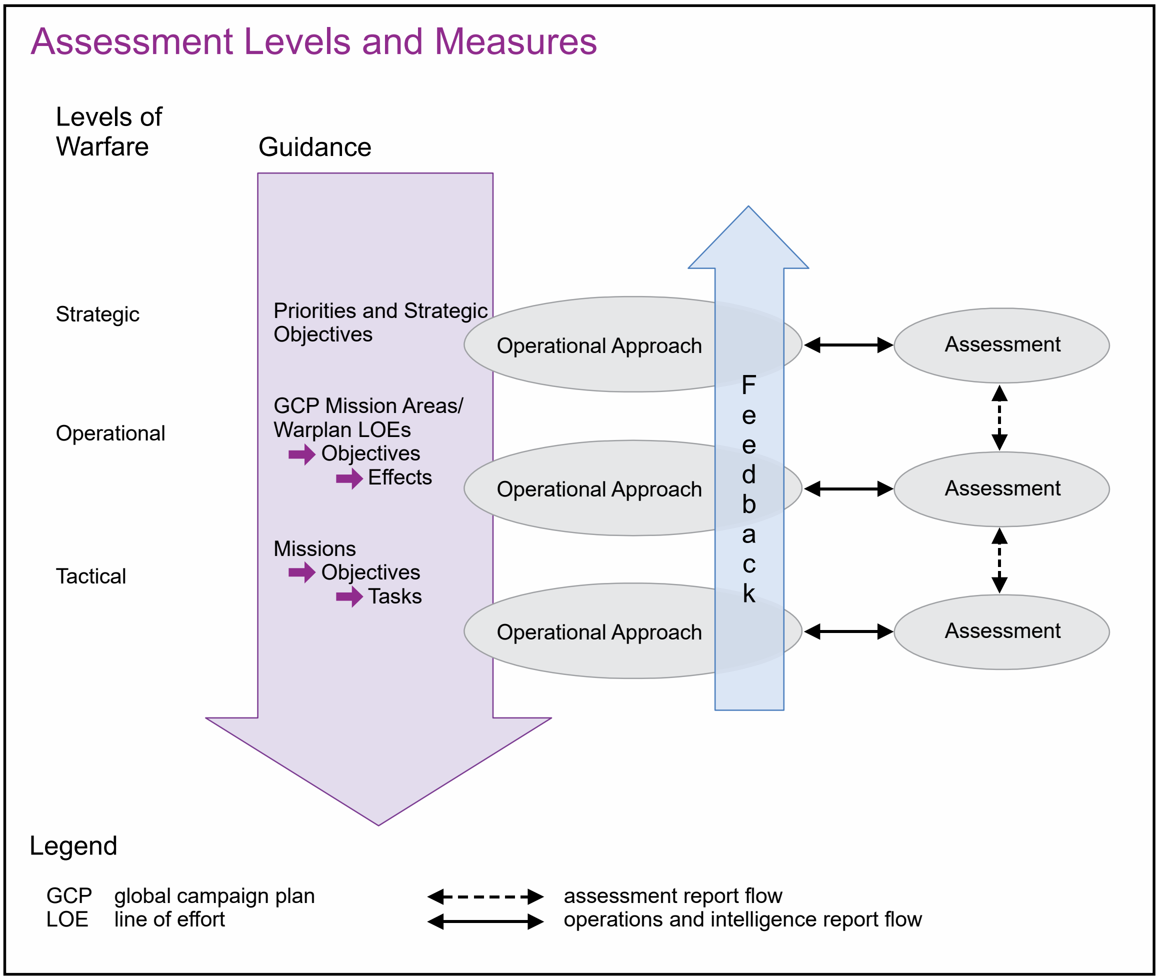


Figure IV-5. Assessment Levels and Measures

things" to achieve objectives, not just "doing things right," and if executing the correct actions are creating the required effects against the adversary or enemy. The use of a red team to critically examine the MOE from the perspective of the threat helps the JFC in measuring the correct information. The JFC can use MOEs to determine progress toward success in those operations for which tactical-level CA ways, means, and measures do not apply.

b. A systems-oriented JIPOE effort is crucial to the identification of enemy/threat objectives and associated COGs, critical capabilities, critical requirements, critical vulnerabilities, COAs, and related decisive points. Human social structures are often complex adaptive systems from which human and automated networks emerge. These may—but will often not—have highly central or critical nodes that may behave like COGs. A COG can be viewed as a source of power that provides moral or physical strength, freedom of action, or will to act. COG analysis requires knowledge of a threat's physical and psychological strengths and weaknesses and how the threat organizes, behaves, fights, and makes decisions. Human factors analysis of the threat's leadership characterizes the assessment with strengths, weaknesses, and how decisions are made. Analysts should evaluate biometric, biographic, forensic, and DOMEX data in concert with the JIPOE. The

JIPOE analyst also requires a detailed understanding of how each aspect of the OE links to the others and how various permutations of such links and nodes may combine to provide the critical capabilities that the COGs require to be effective.

For additional information on COGs, see JP 5-0, Joint Planning.

c. JIPOE analysts should assess the importance of the critical requirements and associated critical vulnerabilities from a systems perspective. This supporting analysis of all operationally relevant nodes and all primary and alternative links to those nodes can directly support our efforts to deny the enemy or selected neutrals the ability to achieve their objectives. This understanding, combined with an analysis of the constraints imposed by the OE, a sequencing of threat objectives, and an evaluation of the threat's preferred method or means of conducting a specific type of operation or activity (e.g., attack, defense, proliferation, WMD production, financing terrorist cells) helps to achieve those objectives. The resulting product may take the form of a situation template or model that identifies all the nodes and links associated with individual COAs or options available to the adversary within a specific category of activity. The situation templates may be combined, modeled, and compared to identify key nodes and primary and alternate links among nodes. The consolidated template (event template) provides the means for determining specific events in time and space that, if detected, would indicate changes in threat behavior, systems, or the OE. These events, or indicators of change, may be assigned qualitative or quantitative thresholds and may be used as the basis for MOEs. Figure IV-6 is an example of a systems-oriented JIPOE event template demonstrating nodal and link analysis to identify potential indicators of change.

The JIPOE process and its relationship to assessment is described in greater detail in the Joint Guide for Joint Intelligence Preparation of the Operational Environment.

11. Tactical-Level Assessment

While tactical-level information informs higher-level assessments related to MOEs, tactical-level assessment itself typically uses MOPs to evaluate task accomplishment. The results of tactical tasks are often physical in nature but can also reflect the impact on specific functions and systems. Tactical-level assessment may include assessing progress by geographic phase lines; neutralization of enemy forces; control of key terrain, people, or resources; and security or reconstruction tasks. CA, consisting of a BDA, MEA, and CDA, is an example of a tactical-level assessment and is a term that can encompass many tactical-level assessment actions. CA typically focuses on determining the results of weapons engagement (with both lethal and nonlethal capabilities) and is an important component of joint fires and the joint targeting process. This includes assessing intermediate force capabilities including nonlethal weapons, operations in the IE, electromagnetic warfare, and CO. Integration and effective employment of intermediate force capacities enable the joint force to respond with options to compete with adversaries across the competition continuum, including below the threshold of armed conflict. It helps the CCDR, the subordinate JFC, and component commanders understand how the joint operation is progressing and assists in shaping future operations. For further information on CA, see JP 3-60, *Joint Targeting.*

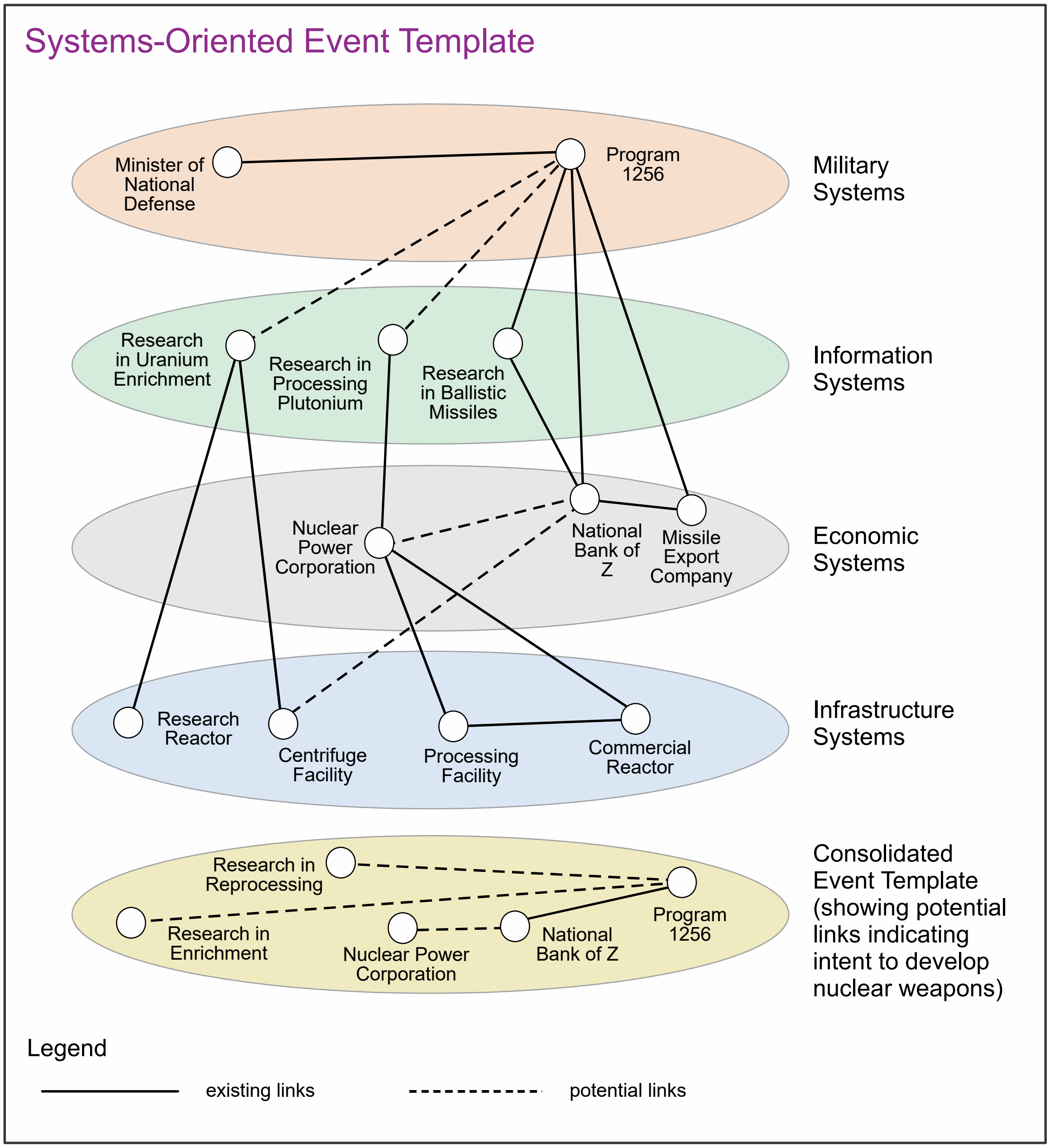


Figure IV-6. Systems-Oriented Event Template

SECTION E. INTELLIGENCE SUPPORT TO JOINT OPERATONS ACROSS THE COMPETITION CONTINUUM

12. General

Intelligence support is crucial to all aspects of military operations across the competition continuum because it identifies changes in the strategic and operational environment that may reveal opportunities or signal an emerging crisis. In competition, intelligence can identify if the outcome is unfolding as expected and aid in identifying and exposing the adversaries' deception, disinformation, and subversion. In armed conflict, immediate, precise, and focused intelligence support to force employment is a particularly important prerequisite for military success, regardless of how the battles evolve. This requires intelligence staffs to be familiar with specific schemes of maneuver, phasing, and timing of single operations and the arrangement of operations within a campaign or contingency plan. For example, CI support to force protection and OPSEC is important during mobilization and deployment; intelligence assessments generated through JIPOE regarding the current status of foreign transportation infrastructure (e.g., airfields, seaports) are vital to success; medical intelligence enables decision makers to devise protection measures to mitigate combat-related battle injuries and disease and nonbattle injuries during deployment, employment, and redeployment; and intelligence analyses of threats to air, land, and maritime LOCs are critical to sustainment operations. During execution, intelligence supports operational requirements and anticipates future requirements. Execution of joint operations requires optimizing the use of limited intelligence assets and maximizing the efficiency of intelligence production resources and is the ultimate test of the efficacy of intelligence support planning.

13. Global Campaign Plans

a. The JSCP and the *2018-2020 Contingency Planning Guidance (CPG)* provide guidance for the CCDRs' strategies and campaigns. Based on strategic direction, CCDRs implement the JSCP's directed campaigns and conduct preparations for armed conflict, if required. A prerequisite to preparing a long-term campaign is the development of a strategic estimate containing factors and trends that influence the CCDRs' AORs. This estimate informs the relationship between ends, ways, means, and risks involved in the conduct of JSCP-directed GCPs. Intelligence activities support the CCDRs' strategic estimates. JFCs continually pursue an evolving array of operational-level objectives to achieve multiple strategic objectives within the global campaigns. Besides their own GCP or CCP, CCDRs also have a role in supporting other CCMDs. Intelligence support to JFCs includes continuous assessment and revision of GCP execution.

b. **Intelligence Support to GCPs**

(1) Every day, JFCs are executing global campaigns that organize actions around and against US adversaries. In many cases, these actions enhance bonds between future multinational partners, increase regional understanding, ensure timely access, strengthen future multinational operations, and prevent crises. Campaigns seek to achieve national strategic objectives, to include deterring adversaries. The GCP's activities include long-term persistent actions within the mission areas to assure friends, build partner capacity and capability, and promote and protect US interests. They help commanders identify, deter, counter, and/or mitigate competitor and adversary actions that challenge stability. In many cases, campaign activities are conducted with other international participants with DoD in a supporting and enabling role. Where US and PN interests converge, cooperation is possible. Some partners are quite capable already; others may benefit from US assistance. When a nation shares our interests and has the capacity to absorb US training, security can be increased. Military engagement and security cooperation activities are executed continuously to enhance international legitimacy and gain multinational cooperation. These activities should improve perceptions and influence adversaries' and

allies' behavior; develop allied and friendly military capabilities for self-defense and multinational operations; improve information exchange and intelligence sharing; provide US forces with access, influence, advantage, and leverage in cooperation, competition, and armed conflict; and positively affect conditions to deter or mitigate the impact of a crisis.

(2) Intelligence liaison and the establishment of intelligence-sharing arrangements with multinational partners are critical aspects of global campaign execution. Whenever possible, and in coordination with the responsible ODNI representative, JFCs should coordinate with PNs by ensuring the participation of US personnel in mutual intelligence training, temporary exchanges of intelligence personnel, federated intelligence arrangements, and the integration and exercise of ISR support architectures. National intelligence cells should be formed as early as possible, and a multinational intelligence center established to coordinate their activities. Information management approaches relating to intelligence collection processing, production, and dissemination that upholds "write for release" principles and policy, as well as foreign disclosure procedures should be established and exercised to the maximum extent feasible throughout and PNs participation in the JIPOE effort encouraged.

(3) Theater intelligence collection capabilities should be optimized by integrating the various intelligence capabilities of the CCMD and its PNs. Many potential multinational partners have capabilities that may prove invaluable to successful intelligence operations.

(4) Information and intelligence-integration activities are critical aspects of GCP execution and rely heavily on accurate intelligence. Analysis and assessment of the adversary's leadership capabilities and decision-making process should be performed continuously to identify effective messages and actions. Units tasked with identifying host-nation audiences should assess messaging potential during all phases of operations within the campaign, especially influence efforts. Additionally, units should identify potential audiences as early as possible in subsequent phases to facilitate information coordinating efforts. Early identification of potential audiences allows greater responsiveness of information integration.

(5) Intelligence support, especially human aspects analysis, including SCA, is essential to maximize the effectiveness of civil-military operations (CMO). An analysis and assessment of the human aspects in countries of interest that identifies physical, informational, and human aspects of civil society, including their key areas, structures, influences and relevant actors, should be performed as early as possible to determine what operations, activities, and investments may be effective. Likewise, intelligence support focuses CMO and provides the lead time necessary for timely CMO planning, resource allocation, and mission execution. Incorporating a systemic analysis throughout campaigning serves as an early warning indicator of instability and helps identify vulnerabilities to military COAs and friendly force employment.

(6) Information and finished intelligence pertinent to understanding the human aspects of the OE, such as social structures, relevant actors, and cultures, will originate in and be visualizable with GEOINT. These elements will be reflected in the cross-functional

data layers. Development of additional data layers may be necessary to reflect a deeper understanding of populations and relevant actors. Allies and partners often possess sociocultural and psychological information, intelligence, and analytic expertise otherwise unavailable to the United States. Sharing of databases and data layers across the joint force, interagency partners, allies, and PNs will therefore be required.

(7) Deterring adversaries is one of the primary objectives of day-to-day campaigning. To successfully deter an adversary, the JFC requires a clear understanding of adversary motivations; adversary and US strategic objectives; desired and undesired effects; actions likely to create those effects; adversary and US COGs and decisive points; and required joint, multinational, and nonmilitary capabilities matched to available forces. The joint force J-2 assists the JFC in visualizing and integrating relevant deterrence considerations into plans. It is, therefore, imperative that the JIPOE (conducted as part of the ongoing campaign) provide the JFC with an understanding of the OE required for deterrence and be updated as it changes.

(8) Information and intelligence integration is also critical in supporting the GCPs' deter mission area. The adversary structure and leadership decision-making process should be continuously monitored and assessed to determine effective influence activities and the impact the ongoing campaign has on them. The receptivity of foreign target audiences to specific messages and actions should also be continuously assessed to support overall influence efforts.

(9) Throughout execution of the GCP, the ongoing JIPOE focuses on monitoring the current situation while simultaneously assessing adversary capabilities to affect future operations. JIPOE analysts support decision making, for refinement of ongoing activities, as well as early warning, by looking for specific indications of imminent adversary activity that may require an immediate response or an acceleration of friendly decision making. JIPOE also concentrates on confirming adversary COGs and supports the continuous refinement of estimates of adversary capabilities, dispositions, intentions, and probable COAs within the context of the current situation. At the same time, however, JIPOE analysts should look ahead and prepare threat assessments to support future operations, to include possible crisis and contingency should deterrence fail. In crisis or contingency operations, COA development is dependent on detailed TSAs to identify the functional components in the OE that may be affected to support the commander's objectives.

(10) Selected intelligence operations may support a wide array of flexible deterrent options—preplanned actions carefully tailored to bring a contested interest issue to resolution without armed conflict. For example, the deployment of additional intelligence resources in the operational area not only increases intelligence collection capabilities and provides early warning but may also demonstrate US resolve without precipitating an armed response from the adversary. Likewise, intelligence-sharing arrangements and exchanges with PNs may reinforce US commitment to the host nation.

(11) Intelligence also supports actions designed to isolate an adversary by identifying their potential allies and sanctuaries. Intelligence may also identify and assess the vulnerability of the adversary's sources of support to interdiction or disruption, to

include intelligence support from other sources. Neutralizing the adversary's intelligence collection capabilities is particularly important to reinforce their isolation and facilitate their susceptibility to deception operations, while at the same time protecting friendly forces from detection.

(12) Intelligence support to CMO during a campaign and operation can amplify operations to isolate the adversary. An analysis and assessment of the civil dimension of potential allies or supporters of the adversary may determine what civil engagement actions may serve as effective points of influence. Additionally, analysis of the civil dimension of friendly countries, especially in countries where US forces will require access for subsequent operations, will suggest appropriate CMO activities that may reduce enemy freedom of action while enhancing that of the US operational commander.

14. Crisis and Contingency Response

a. Many instances of responding to crises occur within the construct of a GCP. Some situations may require additional authorities, operations, and activities in one or more of the mission areas. If an evolving situation exceeds the scope of the global campaign, the joint force senior leadership will begin to organize around the problem through a more comprehensive analysis. Intelligence informs senior joint leadership, to include the likely supported and supporting commanders, enabling them to diagnose all the situational factors, range of possible outcomes, likely long-term consequences, and begin to form a globally integrated approach of all the joint force capabilities. The IC updates intelligence estimates based on changes resulting from operation and campaign activities.

b. When responding to a crisis or a contingency, the JFC needs to exploit friendly asymmetric advantages and capabilities to shock, demoralize, and disrupt the enemy. The JFC seeks decisive advantage through the use of all available elements of combat power to seize and maintain the initiative, deny the enemy the opportunity to achieve its objectives, and generate in the enemy a mindset of inevitable failure. Additionally, the JFC coordinates with the appropriate interagency representatives through a joint interagency task force, JIACG, or individually, to facilitate coherent use of all instruments of national power in achieving strategic objectives. JFCs and their J-2s should be on continuous guard against any enemy capability, which may impede friendly force deployment from bases, to ports of embarkation, to lodgment areas.

c. The JFC's target intelligence element is more active in combat operations compared to campaigning. Gathering target nominations, vetting targets, capabilities analysis, and target list management results in a completed joint integrated prioritized target list. When initiating combat operations, targeteers monitor ongoing operations and recommend changes to the plan, conduct assessment, and provide input for further strategy and planning efforts. JFCs seek to seize the initiative in all situations through decisive use of joint force capabilities. In combat, this involves both defensive and offensive operations at the earliest possible time, forcing the enemy to culminate offensively and setting the conditions for decisive operations. Rapid application of joint combat power may be required to delay, impede, or halt the enemy's initial aggression and to deny the enemy its initial objectives. Operations to gain access to theater infrastructure and expand friendly freedom of action continue, while the JFC seeks to degrade enemy capabilities with the intent of resolving the crisis at the earliest opportunity.

d. Information and intelligence integration and OPSEC are particularly important when responding to crises or transitioning to armed conflict. CI supports force protection during deployment from home bases to lodgment areas. I2 supports the identification of key adversary personnel, persons of interest, and their support and facilitation networks. HUMINT, SIGINT, OSINT, and intelligence collected in cyberspace may detect indications of enemy demoralization and provide insight into the military information support operations success or failure and potential for exploitation of psychological vulnerabilities. Both the CCMD red team and red cells add value to friendly deception planning efforts. The red team analyzes the proposed plan from the threat's perspective, and red cells provide insight into the possible times and locations of the enemy's intelligence collection plan. This insight assists deception planners in determining the best times and locations to plant deceptive information designed to mislead the enemy.

JIPOE support to deception planning is discussed in greater detail in the Joint Guide for Joint Intelligence Preparation of the Operational Environment.

e. Real-time surveillance and dynamic collection management are important throughout the execution of joint operations but are particularly critical to seize initiative and defeat the enemy in armed conflict. Enemy capabilities should be tracked with a level of persistence and accuracy sufficient to support retargeting and precision engagement. Active, key enemy HUMINT identities should also be discovered, resolved, and tracked as an additional layer for CI and force protection. An integrated collection strategy that fully optimizes the use of all available US, PN, and host-nation collection capabilities assets is essential to focused surveillance. Furthermore, the CCMD JIOC facilitates collection management through ISR visualization—the continuous real-time monitoring of the status, location, and reporting of intelligence platforms and sensors. ISR visualization provides real-time cross cueing and provides a basis for re-tasking and time-sensitive decision making.

f. As situations evolve, JFCs conduct sustained combat operations by simultaneously employing conventional forces, SOF, and information activities throughout the breadth and depth of the operational area. CMO is executed to preclude civilian interference in achievement of operational objectives or to remove civilians from operational areas. Operations may be linear (i.e., global strike is directed toward the enemy in concert with adjacent units) or nonlinear (i.e., forces orient on objectives without geographic reference to adjacent forces).

g. Intelligence must be equally prepared to support linear and nonlinear operations. Nonlinear operations are particularly challenging due to their emphasis on simultaneous operations along multiple lines of operations. The complexity of nonlinear operations places a premium on a continuous flow of accurate and timely intelligence to help protect individual forces. This flow of intelligence supports precise targeting, mobility, and freedom of action and is enabled by focused surveillance, dynamic ISR management, and a CIP.

h. Intelligence also anticipates and addresses the information requirements for subsequent operations, both branches and sequels. For example, intelligence should be prepared to assist the JFC in determining how to fill the power vacuum after the conclusion of combat operations. To set the groundwork for stability, security, transition, and reconstruction operations, the JFC requires detailed intelligence regarding the status of key infrastructure, enemy government organizations and personnel, and anticipated humanitarian needs.

15. Intelligence During Stabilization and Transitions

a. Campaign requirements for support to stabilization can occur anywhere along the competition continuum and be unassociated with armed conflict. However, the particular demands of the transition from armed conflict to the new competition are complex and can require continued significant military involvement, to include some combat operations for years. As commanders make progress, military forces may increase their focus on supporting the efforts of host-nation authorities, but achieving and maintaining the strategic objectives is the priority.

b. When conducting stabilization, intelligence collection and analysis should focus on actual or potential threats to the joint force (e.g., former enemy activities, insurgent groups, criminal elements, terrorist cells). Particular attention should be paid to identifying and assessing the leaders of groups posing potential threats to civil authority and reconstruction efforts. Intelligence should also identify critical infrastructure and analyze its vulnerability to disruption by elements hostile to stabilization efforts. Critical infrastructure vulnerability analysis may require coordination and assistance from other organizations.

c. CI support to force protection is critical throughout the transition. Host-nation authorities, other organizations, international organizations, and NGOs working closely with US forces may pass information (knowingly or unknowingly) to hostile elements that enables them to interfere with stabilization activities. Likewise, members of the local populace may have access to US bases to provide essential services and friendly forces may recruit former regime officials to participate in stabilization efforts. CI elements provide “secondary interviews” after initial screening and verification of foreign personnel and investigate instances of compromised sensitive information.

d. Assessment assists transition efforts by assessing the relative effectiveness of information activities and other operations supporting civil authorities and reconstruction efforts. Additionally, DIA’s human aspects assessments of foreign leadership’s susceptibility to influence can assist commanders in determining the best COAs to secure the gains achieved during armed conflict and establish enduring stability.

e. These actions and activities are typically characterized by a shift in focus from sustained combat operations to a broad array of efforts, to include stabilization. Success requires continuity of effort over a long period. These operations help reestablish a safe and secure environment and provide essential government services, emergency infrastructure reconstruction, and humanitarian relief. The intent is to help restore local political, economic, and infrastructure stability. Civilian officials may lead operations during part or all of stabilization efforts, but the JFC typically provides significant supporting capabilities and activities. The joint force may be required to perform limited local governance (e.g., military government) and integrate the efforts of other supporting interagency and multinational partners until legitimate local entities are functioning. The JFC continuously assesses the impact of operations on the ability to transfer authority for remaining requirements to a legitimate civil entity.

f. Similar to stabilization, joint force support to legitimate civil governance can occur anywhere along the competition continuum. The commander provides support by agreement with the appropriate civil authority. In most examples, this is a recurring event within the continental United States and the military support is part of a DSCA effort under direction of the civil authority; where this is the case, intelligence support has a different character. The purpose is to help the civil authority improve or regain its ability to govern and administer the services and other needs of their military or population at large. Typically, the military is not the lead in these operations. CCMD involvement with other nations and other USG departments and agencies beyond the termination of the combat operation, such as lower-level stabilization activities and foreign humanitarian assistance, may be required to achieve national objectives.

g. In some situations, intelligence support may remain in place after transition of the initial joint operation to a continuing military operation that supports the civil authority and/or to continue to monitor the situation. As in support to campaigns, intelligence resources may serve as a valuable tool for demonstrating US resolve and commitment to the host nation. To facilitate this critical role in establishing friendly relations with the new civil authority, intelligence-sharing agreements should be promulgated as soon as practicable.

h. Before the operation transitions, all intelligence lessons learned are recorded in the Joint Lessons Learned Information System. Likewise, the joint force J-2 should ensure all JIPOE products, intelligence assessments, collection plans, and J-2X source registries are appropriately archived. This material may prove valuable to operation planning in the event US forces are directed to redeploy to the area.

APPENDIX A
ANALYTIC STANDARDS

1. General

Intelligence analysts should distinguish between what is known with confidence based on the facts of the situation and the OE and what are untested assumptions. Intelligence can be facts that have been observed, or it can be a conclusion based on facts of such certainty that it is considered to be knowledge. Intelligence can also be conclusions and estimates deduced from incomplete sets of facts or induced from potentially related facts. The commander's determination of appropriate objectives and operations may rest on knowing whether intelligence is "fact" or "assumption" and knowing the particular logic used to develop an intelligence estimate, as well as knowing the confidence level the J-2 places on the provided intelligence and related analytic conclusions.

2. Analytic Standards

The IC analytic standards described in Intelligence Community Directive (ICD) 203, *Analytic Standards,* guide analysis and analytic production. IC analytic products should be consistent with the following five analytic standards, including the nine analytic tradecraft standards, IAW ICD 203.

a. **Objective:** Analysts should perform their responsibilities with objectivity and with an awareness of their own assumptions, biases, and reasoning. Analysts should not be influenced by existing analytic positions or judgments and need to consider alternative perspectives and contrary information. Analysis should not be unduly constrained by previous judgments when new developments indicate a modification is necessary.

b. **Independent of political consideration:** Analytic assessments must not be distorted by, nor shaped for, advocacy of a particular audience, agenda, or policy viewpoint.

c. **Timely:** Analysis must be disseminated in time for it to be actionable by customers. Analytic elements have the responsibility to be continually aware of events of intelligence interest, of customer activities and schedules, and of IRs and priorities, to provide useful analysis at the right time.

d. **Based on all available sources of intelligence information:** Analysis should be informed by all relevant information available. Analytic elements should identify and address critical information gaps and work with collection activities and data providers to develop access and collection strategies.

e. **Implements and exhibits analytic tradecraft standards, specifically:**

(1) Properly describes quality and credibility of underlying sources, data, and methodologies: Analytic products should identify underlying sources and methodologies upon which judgments are based, and use source descriptors IAW ICD 206, *Sourcing Requirements for Disseminated Analytic Products,* to describe factors affecting source

quality and credibility. Such factors can include accuracy and completeness, possible denial and deception, age and continued currency of information, and technical elements of collection, as well as source access, validation, motivation, possible bias, or expertise. Source summary statements, described in ICD 206, are strongly encouraged and should be used to provide a holistic assessment of the strengths or weaknesses in the source base and explain which sources are most important to key analytic judgments.

(2) Properly expresses and explains uncertainties associated with major analytic judgments: Analytic products should indicate and explain the basis for the uncertainties associated with major analytic judgments, specifically the likelihood of occurrence of an event or development, and the analyst's confidence in the basis for this judgment. Degrees of likelihood encompass a range from remote to nearly certain. Analysts' confidence in an assessment or judgment may be based on the logic and evidentiary base that underpin it, including the quantity and quality of source material, and their understanding of the topic. Analytic products should note causes of uncertainty (e.g., type, currency, and amount of information, knowledge gaps, and the nature of the issue) and explain how uncertainties affect analysis (e.g., to what degree and how a judgment depends on assumptions). As appropriate, products should identify indicators that would alter the levels of uncertainty for major analytic judgments. Consistency in the terms used and the supporting information and logic advanced is critical to success in expressing uncertainty, regardless of whether likelihood or confidence expressions are used (see Figure A-1).

(a) For expressions of likelihood or probability, an analytic product uses one of the following sets of terms in Figure A-2.

(b) Analysts are strongly encouraged not to mix terms from different rows. If a mix of terms is used, the analyst should include a disclaimer clearly noting that the terms indicate the same assessment of probability.

(c) To avoid confusion, products that express an analyst's confidence in an assessment or judgment using a confidence level (e.g., high confidence) should not combine a confidence level and a degree of likelihood, which refers to an event or development, in the same sentence.

(3) Properly distinguishes between underlying intelligence information and analysts' assumptions and judgments: Analytic products should clearly distinguish statements that convey underlying intelligence information used in analysis from statements that convey assumptions or judgments. Assumptions are suppositions used to frame or support an argument; assumptions affect analytic interpretation of underlying intelligence information. Judgments are conclusions based on underlying intelligence information, analysis, and assumptions. Products should state assumptions explicitly when they serve as the linchpin of an argument or when they bridge key information gaps. Products should explain the implications for judgments if assumptions prove to be incorrect. Products should also, as appropriate, identify indicators that, if detected, would alter judgments.

Expressing Confidence in Analytic Judgment

Confidence in a judgment is based on three factors: number of key assumptions required, the credibility and diversity of sourcing in the knowledge base, and the strength of argumentation. Each factor should be assessed independently and then in concert with the other factors to determine the confidence level. Multiple judgments in a product may contain varying levels of confidence. Confidence levels are stated as Low, Moderate, and High.

Phrases such as "we judge" or "we assess" are used to call attention to a product's key assessment. Supporting assessments may use likelihood terms or expressions to distinguish them from assumptions or reporting. Below are guidelines for likeliness terms and the confidence levels with which they correspond.

Low

- Uncorroborated information from good or marginal sources
- Many assumptions
- Mostly weak logical inferences, minimal methods application
- Glaring intelligence gaps exist

Terms/Expressions

- Possible
- Could, may, might
- Cannot judge, unclear

Moderate

- Partially corroborated information from good sources
- Several assumptions
- Mix of strong and weak inferences and methods
- Minimum intelligence gaps exist

Terms/Expressions

- Likely, unlikely
- Probable, improbable
- Anticipate, appear

High

- Well-corroborated information from proven sources
- Minimal assumptions
- Strong logical inferences and methods
- No or minor intelligence gaps exist

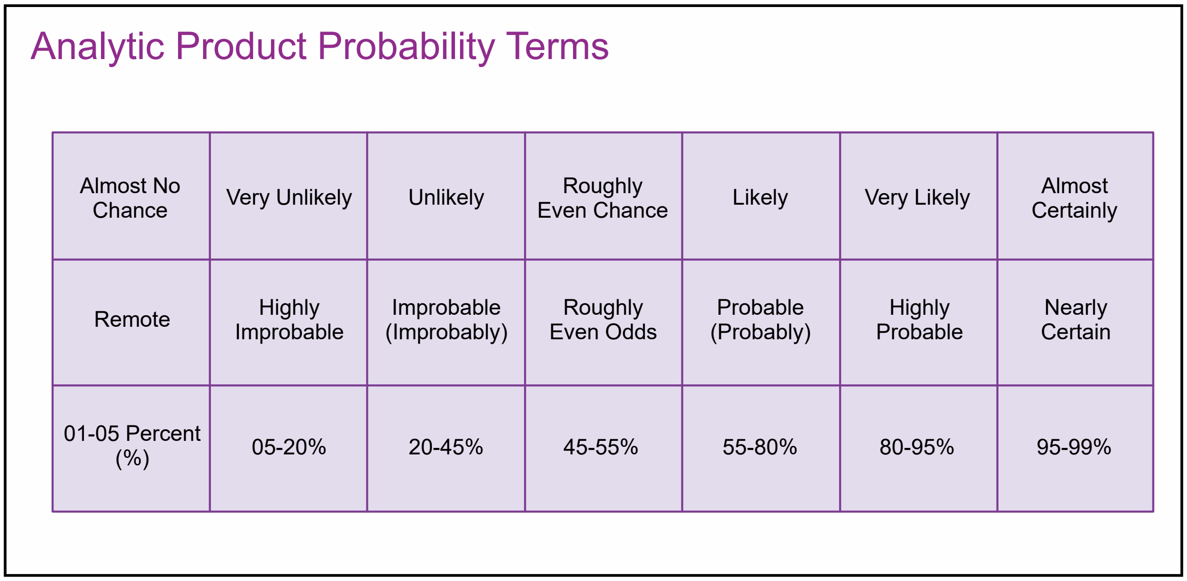
Terms/Expressions

- Will, will not
- Almost certainly, remote
- Highly likely, highly unlikely
- Expect, assert, affirm

Figure A-1. Expressing Confidence in Analytic Judgment

(4) Incorporates analysis of alternatives: Analysis of alternatives is the systematic evaluation of differing hypotheses to explain events or phenomena, identify biases, explore near-term outcomes, and imagine possible futures to mitigate surprise and risk. Analytic products should identify and assess plausible alternative hypotheses. This is particularly important when major judgments contend with significant uncertainties, or complexity (e.g., forecasting future trends), or when low probability events could produce high-impact results. In discussing alternatives, products should address factors such as associated assumptions, likelihood, or implications related to US interests. Products also should identify indicators that, if detected, would affect the likelihood of identified alternatives.

(5) Demonstrates customer relevance and addresses implications: Analytic products should provide information and insight on issues relevant to the customers of US intelligence and address the implications of the information and analysis they provide.



Analytic Product Probability Terms

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certainly
Remote	Highly Improbable	Improbable (Improbably)	Roughly Even Odds	Probable (Probably)	Highly Probable	Nearly Certain
01-05 Percent (%)	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Figure A-2. Analytic Product Probability Terms

Products should add value by addressing prospects, context, threats, or factors affecting opportunities for action.

(6) Uses clear and logical argumentation: Analytic products should present a clear main analytic message up front. Products containing multiple judgments should have a main analytic message that is drawn collectively from those judgments. All analytic judgments should be effectively supported by relevant intelligence information and coherent reasoning. Language and syntax should convey meaning unambiguously. Products should be internally consistent and acknowledge significant supporting and contrary information affecting judgments.

(7) Explains change to or consistency of analytic judgments: Analytic products should state how their major judgments on a topic are consistent with or represent a change from those in previously published analysis or represent initial coverage of a topic. Products need not be lengthy or detailed in explaining change or consistency. They should avoid using boilerplate language, however, and should make clear how new information or different reasoning led to the judgments expressed in them. Recurrent products such as daily crisis reports should note any changes in judgments; absent changes, recurrent products need not confirm consistency with previous editions. Significant differences in analytic judgment, such as between two IC analytic elements, should be fully considered and brought to the attention of customers.

(8) Makes accurate judgments and assessments: Analytic products should apply expertise and logic to make the most accurate judgments and assessments possible, based on the information available and known information gaps. In doing so, analytic products should present all judgments that would be useful to customers and should not avoid difficult judgments to minimize the risk of being wrong. Inherent to the concept of accuracy is that the analytic message a customer receives should be the one the analyst intended to send. Therefore, analytic products should express judgments as clearly and precisely as possible, reducing ambiguity by addressing the likelihood, timing, and nature

of the outcome or development. Clarity of meaning permits assessment for accuracy when all necessary information is available.

(9) Incorporates effective visual information where appropriate: Analytic products should incorporate visual information to clarify an analytic message and to complement or enhance the presentation of data and analysis. In particular, visual presentations should be used when information or concepts (e.g., spatial or temporal relationships) can be conveyed better in graphic form (e.g., tables, flow charts, images) than in written text. Visual information may range from plain presentation of intelligence information to interactive displays for complex information and analytic concepts. All of the content in an analytic product may be presented visually. Visual information should always be clear and pertinent to the product's subject. Analytic content in visual information should also adhere to other analytic tradecraft standards.

Intentionally Blank

APPENDIX B
INTELLIGENCE DISCIPLINES

Intelligence disciplines are well-defined areas that involve specific categories, collections, and analysis with emphasis on technical or human resources capabilities (see Figure B-1).

SECTION A. GEOSPATIAL INTELLIGENCE

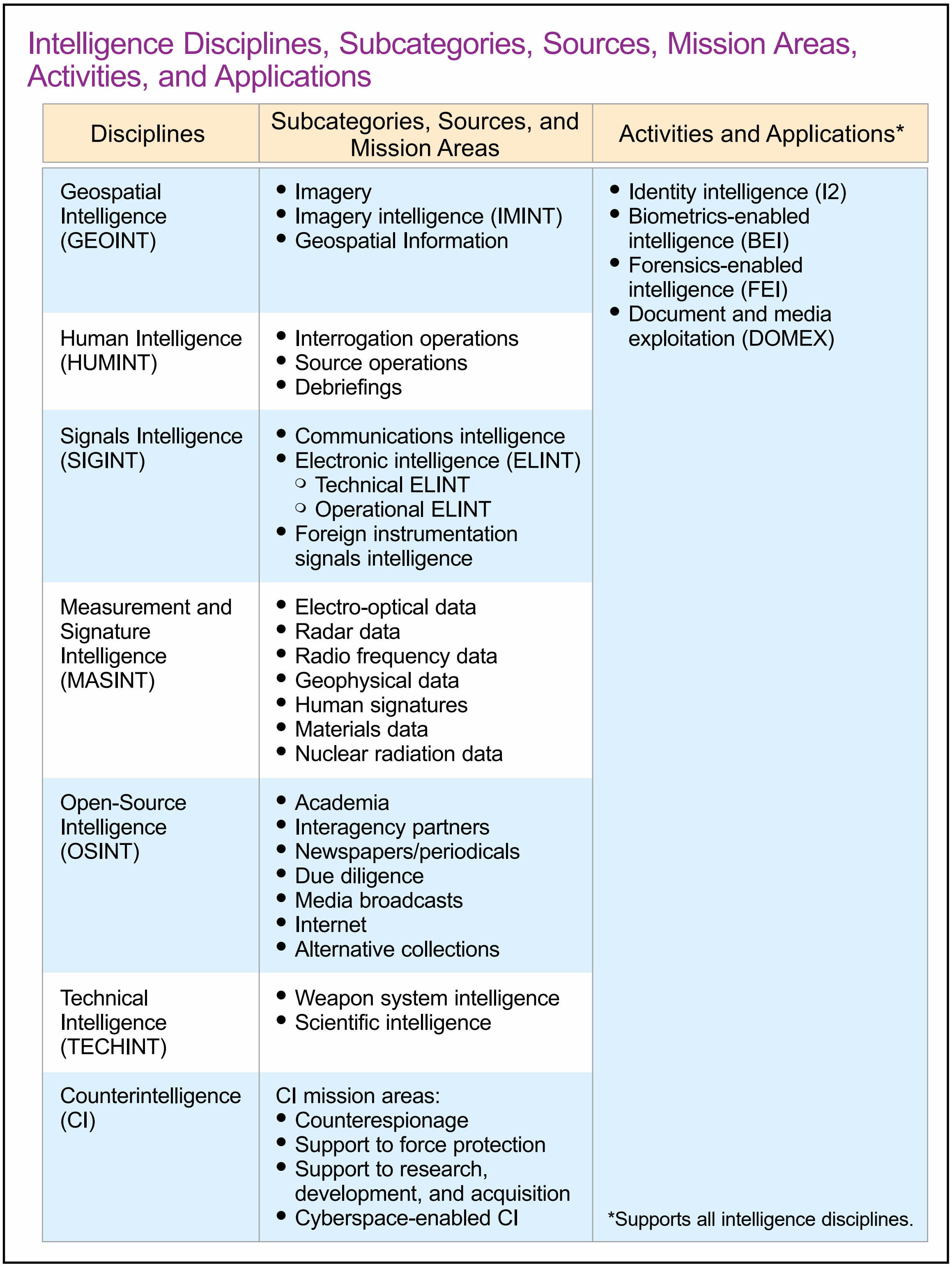
1. Overview of Geospatial Intelligence

a. GEOINT consists of imagery, IMINT, and GI. Any one or combination of these three GEOINT elements may be considered GEOINT. The full utility of GEOINT comes from the integration and use of imagery, IMINT, and GI, enabling customers to gain a more comprehensive perspective, an in-depth understanding, and a cross-functional awareness of the OE. GEOINT collection encompasses all aspects of EO, infrared, and synthetic aperture radar (SAR) imagery; overhead persistent infrared capabilities; and GI&S. GEOINT includes the exploitation and analysis of EO, infrared, and radar imagery, as well as the exploitation and analysis of geospatial, spectral, laser, infrared, radiometric, SAR phase history, polarimetric, spatial, and temporal data.

b. GEOINT encompasses a range of products from simple IMINT reports to complex sets of layered foundation and intelligence/mission-specific data. GEOINT products are often developed through a process, in which both the producer and the user of GEOINT update a database or product with current information. Full-motion video is another GEOINT collection capability that has proven key to activity-based intelligence collection by providing near-continuous or sustained collection on designated targets.

(1) **Imagery** is "a likeness or presentation of any natural or man-made feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems, and likeness or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations)" (Title 10, USC, Section 467). It is used extensively to update GEOINT foundation data and serves as GEOINT's primary source of information when exploited through IMINT. The vast majority of modern imagery products are created, processed, and disseminated in an electronic still or motion format.

(2) **IMINT** is "the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials" (Title 10, USC, Section 467). It includes exploitation of imagery data derived from EO, radar, infrared, multispectral, and laser sensors. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media. A wide variety of platforms and sensors support IMINT operations. IMINT is a product that is the result of processing and exploiting raw imagery (information) and creating an analyzed product (intelligence). An image alone is only information in the form of pixels, digits, or



Intelligence Disciplines, Subcategories, Sources, Mission Areas, Activities, and Applications

Disciplines	Subcategories, Sources, and Mission Areas	Activities and Applications*
Geospatial Intelligence (GEOINT)	• Imagery • Imagery intelligence (IMINT) • Geospatial Information	• Identity intelligence (I2) • Biometrics-enabled intelligence (BEI) • Forensics-enabled intelligence (FEI) • Document and media exploitation (DOMEX)
Human Intelligence (HUMINT)	• Interrogation operations • Source operations • Debriefings	
Signals Intelligence (SIGINT)	• Communications intelligence • Electronic intelligence (ELINT) ○ Technical ELINT ○ Operational ELINT • Foreign instrumentation signals intelligence	
Measurement and Signature Intelligence (MASINT)	• Electro-optical data • Radar data • Radio frequency data • Geophysical data • Human signatures • Materials data • Nuclear radiation data	
Open-Source Intelligence (OSINT)	• Academia • Interagency partners • Newspapers/periodicals • Due diligence • Media broadcasts • Internet • Alternative collections	
Technical Intelligence (TECHINT)	• Weapon system intelligence • Scientific intelligence	
Counterintelligence (CI)	CI mission areas: • Counterespionage • Support to force protection • Support to research, development, and acquisition • Cyberspace-enabled CI	*Supports all intelligence disciplines.

Figure B-1. Intelligence Disciplines, Subcategories, Sources, Mission Areas, Activities, and Applications

other forms of graphic representation and the data behind that portrayal. Imagery source categories include commercial remote sensing, EO, ground photo, hyperspectral imagery (HSI), infrared, lidar, multispectral imagery (MSI), panchromatic, polarmetric, and SAR.

(a) **EO sensors** provide digital imagery data in the infrared, visible, and/or ultraviolet regions of the electromagnetic spectrum (EMS). Panchromatic EO sensors detect a broad segment of the visible spectrum, while other EO sensors focus on infrared energy or detect multiple narrow bands across the EO spectrum. EO sensors generally provide a high level of detail or resolution as compared to radar or other sensors. EO sensors may not transmit successfully through bad weather. Panchromatic sensors provide the highest level of resolution but cannot image at night. EO offers many advantages over non-digital (i.e., film-based) systems, including improved timeliness, greater dissemination options, imagery enhancement, and additional exploitation methods.

1. **Infrared imaging sensors** provide a pictorial representation of the contrasts in thermal infrared emissions between objects and their surroundings and are effective during periods of limited visibility such as at night or in inclement weather. A unique capability available with infrared sensing is the ability to detect ongoing activity (based on heat levels), as well as past activity through residual thermal effects.

2. **Spectral imagery sensors** operate in discrete spectral bands, typically in the infrared and visible regions of the EMS. Spectral imagery is useful for characterizing the environment or detecting and locating objects with known material signatures. A multispectral image is made from a set of images taken at different intervals of continuous wavelengths, called “bands” within the EMS. Each pixel of imagery consists of three to ten bands. When these bands are processed and when viewed together, they produce a color image. It is similar to using a color filter when taking a black and white picture. Only the rays of the color of the filter are allowed to reach the film. Traditionally, multispectral sensors contain a red, green, and blue band but can contain tens of bands that image regions of the EMS to which the human eye is not sensitive. The advantage of taking multispectral images is the ability to discern different materials through their spectral signature. This information can be transferred into intelligence and aid in the analysis of targets. Some MSI sensors provide low-resolution, large-area coverage that may reveal details not apparent in higher resolution panchromatic imagery. Map-like products can be created from MSI data for improved area familiarization and orientation. HSI is derived from subdividing the EMS into very narrow bandwidths, which may be combined with, or subtracted from each other in various ways to form images useful in terrain analysis or target analysis. Unlike MSI, which only provides three to ten bands per pixel, HSI differs in that it can provide hundreds of bands per pixel. For example, HSI can analyze electromagnetic propagation characteristics, detect industrial chemical emissions, identify atmospheric properties, improve detection of blowing sand and dust, and evaluate snow depths.

(b) **Radar imaging sensors** provide all-weather imaging capabilities and the primary night capability. Radar imagery is formed from reflected energy in the radio frequency (RF) portion of the EMS. Some radar sensors provide moving target indicator capability to detect and locate moving targets such as armor and other vehicles.

(c) **Lidar sensors** are similar to radar, transmitting laser pulses to a target and recording the time required for the pulses to return to the sensor receiver. Lidar can be used to measure shoreline and beach volume changes, conduct flood risk analysis, identify waterflow issues, and augment transportation mapping applications. Lidar supports large-scale production of high-resolution digital elevation products displaying accurate, highly detailed, three-dimensional models of structures and terrain invaluable for operational planning and mission rehearsal.

(3) **GI "**identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including statistical data; information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data, and related products" (Title 10, USC, Section 467). This information is used for military planning, training, and operations including navigation, mission planning and rehearsal, modeling and simulation, and joint targeting.

2. Geospatial Intelligence and Joint Operations

a. GEOINT provides a common foundation for supporting joint operations to better enable mission accomplishment. GEOINT supports joint operations through the multidirectional flow and integration of geospatially referenced data from relevant GEOINT and other sources of intelligence and information to achieve a shared awareness of the OE, NRT tracking, and collaboration between forces. GEOINT provides a context of space and time regarding the OE, contributing to knowledge about capabilities, trends, and patterns for operational awareness and decision making. Geospatial data transport to the tactical edge is imperative to supporting fires.

b. Foundation GEOINT, in the form of topographic features, elevation data, controlled imagery, geodetic sciences, geographic names and boundaries, aeronautical and maritime information, and human geography, provides the basic framework for visualizing the joint COP. It is information produced by multiple sources and is streamed and stored using validated Department of Defense Information Technology Standards Registry interoperable data standards. GEOINT online on-demand services include tools that enable users to access and manipulate data and provide instruction, training, laboratory support, weapon systems analysis, and guidance for the use of geospatial data.

c. GEOINT activities support joint operations through the delivery of finished analytical products. The GEOINT operations process consists of interrelated and specific GEOINT activities and procedures to conduct GEOINT in support of joint operations. These activities are continuous and may be performed independently; in conjunction with one another; or integrated as a component of other intelligence disciplines or operational procedures that require information fusion, visualization, analysis, and sharing.

d. JFCs should consider establishing a GEOINT cell to manage GEOINT activities under the joint force's command structure. The JFC can request the establishment of this cell, which typically includes both NGA civilian and military personnel, with representation from Service GEOINT organizations. NGA frequently deploys a forward element with reachback connectivity to NGA analysts and data repositories in response to a crisis. Execution of the GEOINT support mission is conducted by personnel in theater and supported with continental US-based elements in a reachback capacity. Requests to establish this cell are initiated by contacting the NGA Operation Center and the NGA Director of Operations, Office of Expeditionary Operations via the CCMD NST. Early coordination with NGA and other GEOINT producers is essential as production and dissemination timelines may be significantly longer than other GEOINT products. The GEOINT cell interacts directly with customers and the National System for Geospatial Intelligence to obtain and provide the highest quality GEOINT support in response to validated mission requirements.

e. GEOINT supports joint operations through the multidirectional flow and integration of geospatially referenced data from relevant GEOINT and other sources of intelligence and information to achieve a shared awareness of the OE, NRT tracking, and collaboration between forces. There are five general categories of GEOINT support to joint operations:

(1) **GMI and Warning Intelligence.** As one component of GMI and warning intelligence, GEOINT supports monitoring scientific and technological developments and capabilities of foreign military forces for long-term planning purposes and for detecting and reporting foreign developments that could involve a threat to US and PNs' military, diplomatic, or economic interests or to US citizens abroad. Additionally, GEOINT supports SA by providing warning of possible increased threats or a significant increase in the tactical positioning of enemy assets.

(2) **Safety of Navigation.** Using bathymetric, hydrographic, maritime safety, gravimetric, aeronautical, atmospheric, and topographic information for sea, air, and land navigation. The Global Positioning System is the primary source of positioning, navigation, and timing information.

(3) **OE Awareness.** Visualizing the OE via change detection; tracking movements of interest; and monitoring land installations, support facilities, airfield site selection suitability, and port activity. GEOINT is a key component supporting JIPOE and provides the geospatial foundation to visualize all sources of intelligence and operational data within a COP.

(4) **Mission Planning, Rehearsal, and C2.** Employing GEOINT content to plan, rehearse, and execute missions; evaluate mission progress; adjust schedules; and assign and apportion forces, as appropriate. GEOINT can be used to create realistic, interactive scenarios that accurately depict the operational area in three dimensions and across time. The simulated air, land, or maritime environment prepares personnel for factors they may encounter in the planning and execution of missions.

(5) **Geospatial Support to Joint Targeting.** Targeting support products use advanced GEOINT analytical techniques and technologies, geodetically controlled source material, and precise point mensuration techniques and data. NGA provides intelligence, mission-specific data sets, and foundational data to support the targeting effort. NGA provides geospatial accuracy assurance through its accreditation, certification,

geopositioning tools validation, MIDB/National Production Workshop quality review, and testing and evaluation programs. NGA also performs numerous photogrammetric processes to generate targeting foundation products in response to CCMD and Service requirements.

3. Joint Intelligence Operations Center

The JIOC is the focal point for the command's IP, collection management, operations, exploitation, analysis, production, assessment, and dissemination effort. It is organized to satisfy the commander's IRs.

4. Joint Geospatial Intelligence Cell

The GEOINT cell integrates people, processes, and tools using multiple information sources and collaborative analysis to build a shared knowledge of the environment, the enemy, adversary, and friendly forces. The recommended composition of the GEOINT cell contains both core and extended cell representatives. Optimally, the core GEOINT cell would consist of a GEOINT officer; an imagery collection and production manager; a geospatial collection and production manager; a visualization, systems, and data expert; a GEOINT plans and requirements expert; an NST; and an NST LNO. An extended GEOINT cell consists of the core personnel augmented with additional members from across the organization and its mission partners to coordinate information fusion, visualization, analysis, and sharing.

5. National Geospatial-Intelligence Agency Intelligence Collaboration and Assistance Team

The NGA Intelligence Collaboration and Assistance Team, located within the NGA Intelligence Operation Center, provides continuous global SA and GEOINT assistance to joint operations, including support for declared events (e.g., personnel recovery).

6. Joint Intelligence Preparation of the Operational Environment

Subordinate commands should utilize compatible GEOINT products, data, and standards to facilitate JIPOE processes and products developed by the joint force J-2 to adequately support the mission. Advanced coordination of GEOINT support is essential among the joint force, national agencies, CCMDs, and multinational and host-nation forces to form a common point of reference and framework for JIPOE. The JFC may choose to establish a JIPOE coordination cell to integrate and synchronize the JIPOE effort with supporting organizations, related capabilities, and staff elements. The GEOINT officer is typically a member of the JIPOE coordination cell and provides advice and assistance regarding geospatial issues, including registering data to a common reference system. The METOC officer is typically a member of the JIPOE coordination cell and provides advice and assistance regarding METOC issues, including current and predictive METOC assessments. A multinational JIPOE effort requires interoperable GEOINT data, applications, and data exchange capabilities (Figure B-2).

Geospatial Intelligence in Joint Operations

NRT Feeds

- Message (AMHS, Freetext and USMTF)
- RSS
- Weather

Intelligence Layers

- Threats
- AOB/GOB/NOB
- Collections
- Assessments
- Targeting
- Cyberspace order of battle
- Space order of battle

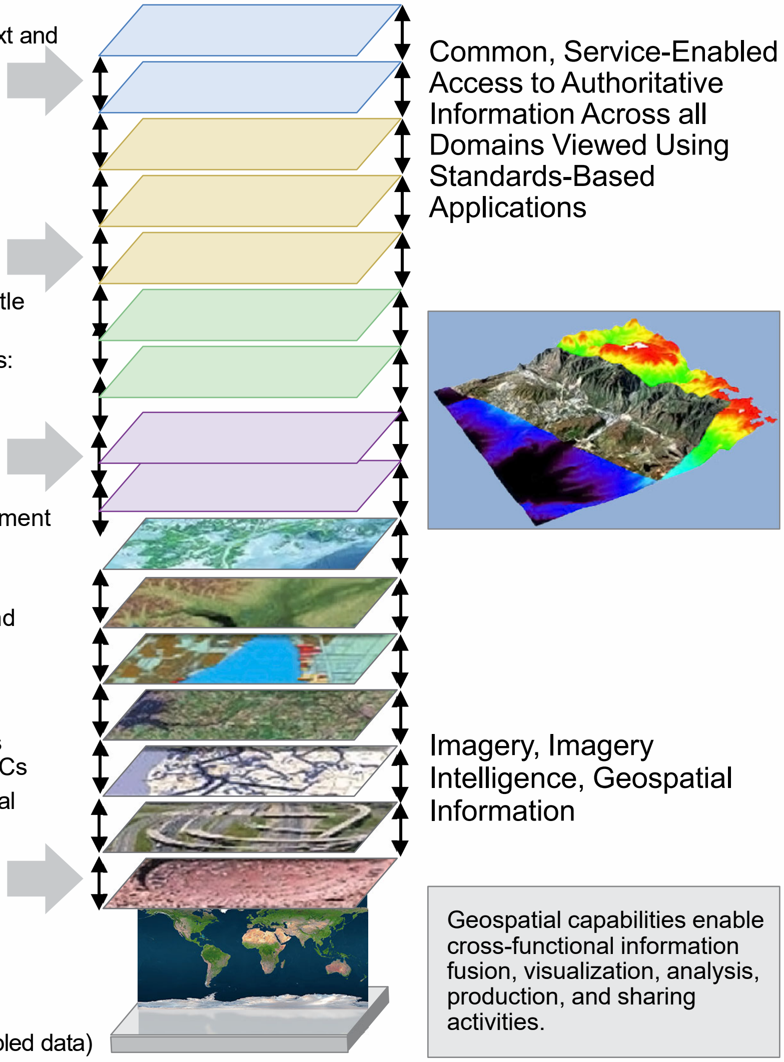
Cross-Functional Data Layers:

- UN, host nation, NGO
- Regional cooperation relationships
- Climate, ecosystem applications
- Water and land management
- Civilian environment
- Demographic, human geography
- Population, refugees, and migration
- Logistics plans and operations
- Medical
- Operation/concept plans
- Checkpoints, MSRs, LOCs

Shared Foundation Geospatial Database

- Map data
- Imagery data
- Elevation data
- Infrastructure
- Cyberspace data

(Notional Layers –
Can be any geospatially enabled data)



Common, Service-Enabled Access to Authoritative Information Across all Domains Viewed Using Standards-Based Applications

Imagery, Imagery Intelligence, Geospatial Information

Geospatial capabilities enable cross-functional information fusion, visualization, analysis, production, and sharing activities.

GEOINT provides a common framework for managing information in support of situational awareness, JIPOE, COP, targeting, and decision making.

Legend

AMHS	automated message handling system
AOB	air order of battle
COP	common operational picture
GEOINT	geospatial intelligence
GOB	ground order of battle
JIPOE	joint intelligence preparation of the operational environment
LOC	line of communications
MSR	main supply route
NGO	nongovernmental organization
NOB	naval order of battle
NRT	near real time
RSS	really simple syndication
UN	United Nations
USMTF	United States message text format

Figure B-2. Geospatial Intelligence in Joint Operations

7. Geospatial Intelligence Activities

a. **Introduction.** GEOINT activities are the tasks, actions, and events to collect, manage, analyze, generate, visualize, and provide imagery, IMINT, and GI necessary to support the NIPF, joint operations, international arrangements, safety of navigation, and joint targeting. GEOINT activities build upon the intelligence process, tasking, PED capabilities, and joint warfighter interoperable models.

b. **Direction, Planning, and Requirements Management**

(1) **Direction.** The GEOINT cell may develop and publish the CCMD's GEOINT CONOPS identifying the required resources, delineating the management of the CCMD GEOINT cell and specifying coordination and collaboration processes with the NST, unified geospatial-intelligence operations, and subordinate command GEOINT cells. The CCMD's GEOINT CONOPS should establish responsibilities, requirements, and procedures for the storage and maintenance of GEOINT products.

(2) **GEOINT Planning and Direction.** The GEOINT cell leads the planning and direction of GEOINT information and intelligence processes for fusion, safety of navigation, visualization, analysis, and sharing by developing appendix 7 (Geospatial Intelligence) to annex B (Intelligence) to plans and orders.

(3) **GEOINT Requirements Management.** To support appendix 7 (Geospatial Intelligence) to annex B (Intelligence) of the plan or order, the GEOINT cell coordinates across all functions of the command and subordinate commands to accomplish specified mission requirements to enable fusion, safety of navigation, visualization, analysis, and sharing.

For GI&S requirements policy and process, see CJCSI 3901.01, Requirements for Geospatial Information and Services.

c. **Discover and Obtain GEOINT.** The GEOINT cell coordinates the procedures and manages the tasks to search for, find, access, and gather GEOINT information and foundational data from existing holdings, databases, and libraries. The user can discover, exploit, and manipulate data from available libraries or databases to create tailored products or data sets for specific mission purposes or military applications. Available libraries or databases provide the foundation for a DoD-wide distributed network of content that includes, but is not limited to, topography, airspace, hydrology, and other GI, as well as EO imagery, geographic names, and boundary data.

d. **Tasking and Collection**

(1) Tasking involves submitting CRs necessary for acquiring data or information to meet mission objectives to the CMA. The process involves converting intelligence or mission requirements into CRs, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and re-tasking as required.

(2) Collection is acquiring GEOINT data or information necessary to satisfy tasked requirements. Primary collection systems used by NGA and the DoD community include satellite, airborne, surface-based, and open-source platforms and their associated sensors. The GEOINT cell coordinates the collection, acquisition, or procurement of GEOINT sources and the associated tasking and management of collection resources. The GEOINT cell determines if a coverage gap or shortfall exists and whether new collection is required.

(a) Geospatial Intelligence Information Management Services (GIMS) is the system used to manage and task national and commercial GEOINT CRs.

(b) Within GIMS, the Collection Operations Utility for Global Airborne Requirements is the system used to manage and task airborne asset GEOINT CRs.

(c) New airborne CRs are approved by the CMA, which constitutes the authority to establish, prioritize, and validate theater CRs; establish sensor tasking guidance; and develop theater collection plans.

(d) The GEOINT cell coordinates with the METOC cell to acquire climatology and real-time meteorology, oceanography, and space weather information to support GEOINT collection and dissemination.

JP 3-59, Meteorological and Oceanographic Operations, *contains detailed information on joint METOC operations.*

e. **Processing and Exploitation.** The GEOINT cell coordinates the assessment, correlation, and conversion of collected foundation GEOINT data into a useable form or formats suitable for analysis, production, and application by end users. The processing may include automated, semi-automated, and manual procedures to integrate data. Exploitation involves the evaluation and manipulation of processed GEOINT data to extract information related to a list of EEIs. Exploitation results in the extraction of information and data that is specifically selected for use or integration in subsequent tasks in the GEOINT operations process.

f. **Analysis, Production, and Visualization.** The GEOINT cell coordinates the use, interpretation, and integration of information into standard or tailored GEOINT products and data, visual presentations of SA, and trend analysis in response to expressed or anticipated information requirements. During this step of the process, information and intelligence is analyzed, produced, and visualized to satisfy the CCIRs (priority IRs and FFIRs) through the evaluation of EEIs.

g. **Dissemination, Collaboration, and Storage.** Dissemination is the timely conveyance of GEOINT content or products in an appropriate form and by any suitable means, whether in hard copy or electronic form, and ensuring they are discoverable and retrievable by the user on the appropriate network. Increasingly, the GEOINT community is moving toward a common approach to capture, store, standardize, and make GEOINT observations available. Using structured observation management (SOM), imagery observations may be captured and stored as structured data, allowing analysts to quickly discover information and intelligence, allowing them to focus on qualitative and quantitative analysis. SOM and all-source structured observations of OBP create and organize information making it easier for analysts to use data from multiple sources, discover new knowledge about objects and networks, and enable models that drive automated tipping and cueing.

h. **Evaluation and Feedback.** The joint force provides feedback to the developers of national-level GEOINT through their resident GEOINT cells (or similar organization). This feedback is provided through features embedded in the various tools and systems and is an extension of the previously mentioned collaboration process.

SECTION B. HUMAN INTELLIGENCE

8. Overview of Human Intelligence

There are 16 defense HUMINT executors. Collectively, they are known as the Defense HUMINT Enterprise. The Defense HUMINT Enterprise provides HUMINT support to military operations. The Defense HUMINT Enterprise and its members also partner with multinational HUMINT elements during multinational operations.

9. Intelligence Interrogation

Intelligence interrogation is a systematic process of using interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence CRs. Trained interrogators with current certification operating under DoD authority are permitted to conduct intelligence interrogations.

For more information on interrogation, see Field Manual 2-22.3, Human Intelligence Collection Operations*. For guidance on debriefing and questioning, see DoDD 3115.09,* DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning.

10. Source Operations

a. Designated and trained personnel in a unit with the "source operations" mission may develop information through the direct and indirect questioning of overt or clandestine sources. These personnel operate under the authority and direction of a designated defense HUMINT executor.

For more information, see DoDD S-5200.37, (U) Management and Execution of Defense Human Intelligence (HUMINT), *and DoDM 5240.01,* Procedures Governing the Conduct of DoD Intelligence Activities.

b. Overt and clandestine sources may include common HUMINT sources (e.g., foreign nationals overseas, foreign nationals in the United States, US and foreign military attaches, emigres, refugees, defectors, displaced persons, members of foreign governmental organizations, academicians, businesspersons, scientists, and US citizens). HUMINT sources fall into three types:

(1) One-time Source. One-time source is an individual the collector only expects to encounter once or use for a limited series of debriefings. One-time sources are usually overt in nature.

(2) Continuing Source. A continuing source is an individual the collector expects to meet more than once. Continuing sources may be overt or clandestine based on the sensitivity of the source and intended long-term use.

(3) Asset. A recruited source who has agreed to meet and cooperate with HUMINT collectors for the purpose of providing information or services in return for a USG commitment. An asset is clandestine in nature.

For more information, see DHE-M 3301.001, (U) Defense Human Intelligence (HUMINT) Enterprise Manual, Volume I: Collection Requirements, Reporting, and Evaluation Procedures, *and DHE-M 3301.002,* (U) Defense Human Intelligence (HUMINT) Enterprise Manual, Volume II: Collection Operations.

c. Debriefing is the process of questioning cooperative human sources to satisfy IRs, consistent with applicable law. The source usually is not in custody and usually is willing to cooperate. Debriefing may be conducted at all echelons and in all OEs. Through debriefing, face-to-face meetings, conversations, and elicitation, information may be obtained from a variety of human sources, such as:

(1) **Friendly forces personnel,** who typically include high-risk mission personnel, such as combat patrols, aircraft pilots and crew, long-range surveillance teams, and SOF, but can include any personnel with information that can be used for intelligence analysis concerning the enemy or other relevant aspects of the OE. Combat intelligence, if reported immediately during an operational mission, can be used to redirect tactical assets to attack enemy forces on a time-sensitive basis.

(2) **Refugees/displaced persons,** particularly if they are from enemy controlled areas of operational interest or if their former placement or employment gave them access to information of intelligence value.

(3) **Recovered persons,** including returned prisoners of war, defectors, freed hostages, and personnel reported as missing in action.

(4) **Volunteers,** who freely offer information of value to US forces on their own initiative.

There are important legal restrictions on interrogation and source operations. United States law and Department of Defense policy require that these operations be carried out only by trained and certified personnel in a unit with this mission. Violators may be punished under the Uniform Code of Military Justice. See Department of Defense Directive 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning,* for more detailed discussion on interrogation.

HUMINT is addressed in detail in Appendix C, "(U) Classified Appendix on Joint Intelligence (Counterintelligence and Human Intelligence/Department of Defense Cover)."

SECTION C. SIGNALS INTELLIGENCE

11. Overview of Signals Intelligence

SIGINT is intelligence produced by exploiting foreign communications systems and noncommunications emitters. SIGINT provides unique intelligence information, complements intelligence derived from other sources and is often used for cueing other sensors to potential targets of interest. For example, SIGINT that identifies activity of interest may be used to cue GEOINT to confirm that activity. Conversely, changes detected by GEOINT can cue SIGINT collection against new targets. The discipline is subdivided into three subcategories: COMINT, ELINT, and FISINT.

a. **COMINT** is intelligence and technical information derived from collecting and processing intercepted foreign communications passed by radio, wire, or other electromagnetic means. COMINT may also include imagery, when pictures or diagrams are encoded by a computer network/RF method for storage and/or transmission. The imagery can be static or streaming.

b. **ELINT** is intelligence derived from the interception and analysis of noncommunications emitters (e.g., radar). ELINT consists of two subcategories: operational ELINT and technical ELINT. Operational ELINT is concerned with operationally relevant information such as the location, movement, employment, tactics, and activity of foreign noncommunications emitters and their associated weapon systems while technical ELINT is concerned with the technical aspects of foreign noncommunications emitters such as signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels.

c. **FISINT** involves the technical analysis of data intercepted from foreign equipment and control systems such as telemetry, electronic interrogators, tracking/fusing/arming/firing command systems, and video data links.

SECTION D. MEASUREMENT AND SIGNATURE INTELLIGENCE

12. Overview of Measurement and Signature Intelligence

a. MASINT is information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify them. MASINT exploits a variety of phenomena from a variety of sensors and platforms to support signature development and analysis; to perform technical analysis; and to detect, characterize, locate, and identify targets and events. MASINT is derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event and it includes the use of quantitative signatures to interpret the data. The measurement aspect of MASINT refers to actual measurements of parameters of an event or object such as the demonstrated flight profile and range of a cruise missile. Signatures are typically the products of multiple measurements collected over time and under varying circumstances. These signatures are used to develop target classification profiles and discrimination and reporting algorithms for operational surveillance and weapon systems. The technical data sources related to MASINT include:

(1) **EO data,** derived from reflected or emitted energy across the optical portion (ultraviolet, visible, near infrared, and infrared) of the EMS to provide detailed information on a target including radiant intensities; dynamic motion; spectral, temporal, and spatial characteristics; and the material composition.

(2) **Geophysical data,** derived from the Earth and atmospheric transmitted signals, including emitted or reflected sounds, pressure waves, vibrations, electromagnetic, or ionosphere disturbances in the Earth's atmosphere, water, crust, or depths. Geophysical systems focus on acoustic (air acoustic, hydroacoustic, and infrasonic), seismic, gravity, magnetic, and electric field collections.

(3) **Material data,** intelligence information obtained from nuclear, chemical, biological, radiological, and conventional explosive weapons, and other materials' signatures that may have military, civil, or intelligence applications. Material intelligence is important for analyzing military and civil production, economic, public health concerns, and environmental problems.

(4) **Human signatures,** measurable characteristics derived from the physical and biological attributes of a human when leveraged for intelligence purposes.

(5) **Nuclear radiation data,** which focuses on detection, identification, and characterization of nuclear sources and events. Spaced-based nuclear radiation MASINT monitors X-rays, gamma rays, and neutrons to detect, identify, locate, and characterize.

(6) **Radar data,** the exploitation of information from collected electromagnetic waves (typically between 10 megahertz and 60 gigahertz) that have reflected off an object. Radars can be either line-of-sight or over-the-horizon. Radar data exploitation provides information on radar cross section, signatures, trajectory, identification, jet engine modulation, rotor revolution rate, precise spatial measurements of components, size, shape, motion, and absorption characteristics of targets.

(7) **RF data,** S&TI derived by measurement of the unintentional signatures of man-made RF signals. RF MASINT excludes intelligence gained from intentionally radiated or coded information in the RF signal or incidental features directly associated with intentional radiated or coded information and the narrow band radar signals in both monostatic and bistatic configurations. RF MASINT include passive bistatic collections.

b. **MASINT Support to Joint Operations**

(1) MASINT collects and produces the precise threat characteristics and performance information essential to joint operations mission accomplishment. MASINT supports the planning, development, and application of weapons systems, countermeasures, targeting, and battle damage assessments. CCMDs depend upon

MASINT to provide indications, warning, tactics, techniques, and procedures information deep into denied territory.

(a) **Strategic.** MASINT enhances the global intelligence picture. In some cases, different sensors are required than those used at the tactical level, but the requirement for integration still exist. Many of the questions posed by policy makers will require the integration of multiple results to properly answer. MASINT integration can be performed with a CCMD J-2 MASINT desk.

(b) **Operational.** The tasking of MASINT capabilities and sensors still requires integrating various inputs. The MASINT desk analyst in the CCMD J-2 is tasked to provide inputs to the planning process and assist in managing the OE. Specific requests for information can be provided or more general tasking can be assigned on a continuous basis. These RFIs are handled in the same manner as with other intelligence collection disciplines.

(c) **Tactical.** The key for use of MASINT is to ensure the information collected is passed back to the MASINT desk in the CCMD J-2. The information should be passed as quickly as possible to ensure it can be disseminated appropriately. For many sensors, this can be an automated process. The MASINT desk analyst correlates the information with other intelligence and produces both specific event reports and intelligence summaries IAW appropriate reporting instructions. They should also have the capability to submit urgent notices to the commander through inputs to the COP's CIP or other command display. If the sensor is not configured to provide real-time alerts to the tactical forces, the MASINT analyst should have the capability to provide the alerts directly.

(2) **Tasking Methods.** The sensor systems for collecting MASINT are generally maintained as a national asset with tasking managed by the on-line National Measurement and Signature Intelligence Requirements System (NMRS). Other sensors may be tasked to the CCMD for management. Other sensors and systems may be functionally assigned to lower echelons (such as the land component commander or maritime component commander). However, it is important to establish the MASINT desk as part of the CCMD J-2, since the sources of information could come from a wide variety of sensors, assigned to various commands and echelons of command. Elements in the air component, land component, maritime component, and SOF plus those assigned to the joint command level can all be integrated by the MASINT desk resulting in a single, integrated input for the commander. Tasking for the MASINT sensors is generally maintained at the national level but can be allocated to lower levels when appropriate. Within the CCMD J-2, the CMA is responsible for overseeing all MASINT sensor tasking, including both the inputs to NMRS for sensors managed by the national level, and normal tasking channels within the theater for assets allocated to theater or lower echelons of command.

(3) **Collection Methods.** Ground-based sensors are emplaced by either persons or airborne delivery. They collect information based on the detected phenomenology and the signature parameters selected for the specific situation or commander's requirements.

The sensors relay the detections and associated information by terrestrial radio, satellite link, or hard wire, depending on the situation.

(4) **Processing Methods.** The information and data collected by a given sensor is processed IAW its system design. Many sensor systems are designed with specific signatures with an automated processing function, while others require a higher degree of information and data collection processing to make the detected phenomenology meaningful. In each case, the sensor data is converted to a meaningful form for analysis by a single source analyst at the MASINT desk, which can then be incorporated with the results of other MASINT sensors or results derived from other intelligence collection disciplines.

(5) **MASINT Exploitation.** Once the data is processed, it is presented to a MASINT exploiter to make decisions on the significance of the detections and disseminate alerts and produce MASINT results based on the observed phenomenology. The exploiter must make judgements on the significance on the information in relationship to the commander's requirements.

c. **MASINT Standards.** The proper use of MASINT requires the development and coordination of technical standards to support interoperability between systems of different Services or when in a multinational force.

SECTION E. OPEN-SOURCE INTELLIGENCE

13. Overview of Open-Source Intelligence

OSINT is intelligence that is produced from publicly available information that is collected, exploited, and disseminated. OSINT can help cue intelligence collection/analysis, fill gaps, and/or supplement the accuracy and fidelity in classified information databases. OSINT is susceptible to manipulation and deception and, thus, requires tradecraft and review during processing.

a. OSINT, as an intelligence discipline, supports warnings, SA, and tips and cues other intelligence disciplines with context for understanding classified information. OSINT is a critical enabler for the integration, evaluation, and interpretation of information from all key disciplines such as all-source intelligence, SIGINT, MASINT, GEOINT, and CI. It can also reduce large target sets, quickly filling information gaps, enabling the more efficient use of other assets. OSINT can be employed in a number of ways, including gauging population sentiment, discerning trends in foreign media, identifying norms and irregularities, supporting sociocultural research and humanitarian assistance efforts, tracking scientific and technological developments, and enhancing foreign partnerships. OSINT products should conform to standing guidance related to analytic standards and sharing. To facilitate OSINT sharing and review, the DIA's Open-Source Collection Acquisition Requirements Management System (OSCAR-MS) is used to register CRs for IC action.

b. Similar to other intelligence disciplines, OSINT is susceptible to deception attempts. Incorrect information may be deliberately planted in public sources. OSINT is also subject to source bias and inaccuracy. All-source intelligence should combine, compare, and analyze classified and open-source material and attempt to cross-verify information obtained from different sources. In addition, OSINT requires tradecraft in the areas of research expertise and OPSEC for Internet-based activities.

c. **Gray Literature.** Gray literature refers to documents that are limited in distribution and not found in normal systems of publication. It can include, but is not limited to, semi-published works, flyers, brochures, graffiti, patents, academic papers, and newspapers with limited or local distribution. Regardless of media, gray literature can include data or primary source information, academic reports and institutional data, informal personal or draft papers, unofficial or government exchanges.

d. **Intelink SBU.** Intelink SBU network, formerly known as open-source information system, is a government-wide private network connecting members of the IC, DoD, DHS, law enforcement, and other information producers and consumers. Intelink SBU is a community protected medium for the sharing of sensitive unclassified and commercially obtained information.

e. **Open-Source Acquisition and Collection.** Open-source information may be acquired through a variety of means, including the purchase of publicly available data (however, in cases of purchase, an analysis may be required to ensure the data being purchased in fact meets the DoD definition of "publicly available"). As with other sources of information, open-source information is collected when it is received by the DoD intelligence component, IAW the standard contained in DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities.*

f. **Open-Source Management.** The OSINT functional manager for the IC is the CIA Director. The DoD lead for OSINT is the Director, DIA. The National Open Source Committee, overseen by the DNI, is comprised of members from across the IC that conduct OSINT. The Defense Open Source Council governs defense OSINT. The Defense Open Source Council, which is overseen by USD(I&S), serves as a forum for the coordination and facilitation of DoD OSINT activities and programs.

g. **OSCAR-MS.** An IC, web-enabled, application for performing OSINT CRM. This is the IC collection management "program of record" for OSINT CRs carried out by Director, National Open Source Enterprise. Unlike other CRM systems, OSCAR-MS does not task requirements but instead requests that IC members volunteer to fill advertised EEIs.

SECTION F. TECHNICAL INTELLIGENCE

14. Overview of Technical Intelligence

TECHINT is derived from the exploitation of foreign materiel and scientific information. TECHINT begins with the acquisition or recovery of a foreign piece of equipment or foreign scientific/technological information. The item or information is then exploited by specialized analysis teams. These teams assess the capabilities and vulnerabilities of CEM and provide detailed assessments of foreign technological threat capabilities, limitations, and vulnerabilities.

a. TECHINT products are used by US weapons developers, countermeasure designers, tacticians, and operational forces to prevent technological surprise, neutralize an enemy's and adversary's technological advantages, enhance force protection, and support the development and employment of effective countermeasures to newly identified enemy and adversary equipment. At the strategic level, the exploitation and interpretation of foreign weapon systems, materiel, and technologies is referred to as S&TI.

b. The DIA provides enhanced S&TI to CCDRs and their subordinates through the technical operational intelligence program, which uses a closed-loop system that integrates all Service and DIA science and technology centers in a common effort. This program provides timely collection, analysis, and dissemination of theater-specific S&TI to CCDRs and their subordinates for planning, training, and executing joint operations.

c. The JCMEC is the primary forward-deployed DoD contingency TECHINT capability. When deployed, a JCMEC is subordinate to the CCMD and may be managed by staff from the DIA Foreign Material Program Office who are under OPCON of the CCDR. Activities of a JCMEC include recovery of CEM and encompasses CCMD and national requirements. Subsequent exploitation of this material provides critical information on enemy and adversary strengths and weaknesses that may influence operational planning and force protection. The identification, recovery, in-theater analysis, and evacuation of this material is done by the JCMEC or other CCMD-designated theater exploitation capability.

Intentionally Blank

APPENDIX C
CLASSIFIED APPENDIX ON JOINT INTELLIGENCE (COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE/DEPARTMENT OF DEFENSE COVER)

This classified appendix includes two annexes and is provided under separate cover. Annex A expands information related to CI and HUMINT. Annex B provides information and standards related to the defense cover program.

Intentionally Blank

APPENDIX D
INTELLIGENCE APPLICATIONS

1. Identity Intelligence

a. **I2**

(1) I2 is the intelligence resulting from the processing and characterization of identity attributes concerning individuals, groups, networks, or populations of interest. I2 fuses identity attributes (e.g., social, cultural, psychological, biographical, biological, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes collected across multiple activities, sources, and methods, to identify, assess, and characterize threats and networks, their capabilities and capacity, COGs, objectives, intent, and potential COAs (see Figure D-1).

(2) I2 utilizes enabling intelligence analysis activities, such as BEI, FEI, and DOMEX, to discover the existence of unknown potential threats; associate individuals to other persons, places, events, or materials; analyze patterns of life; and characterize their

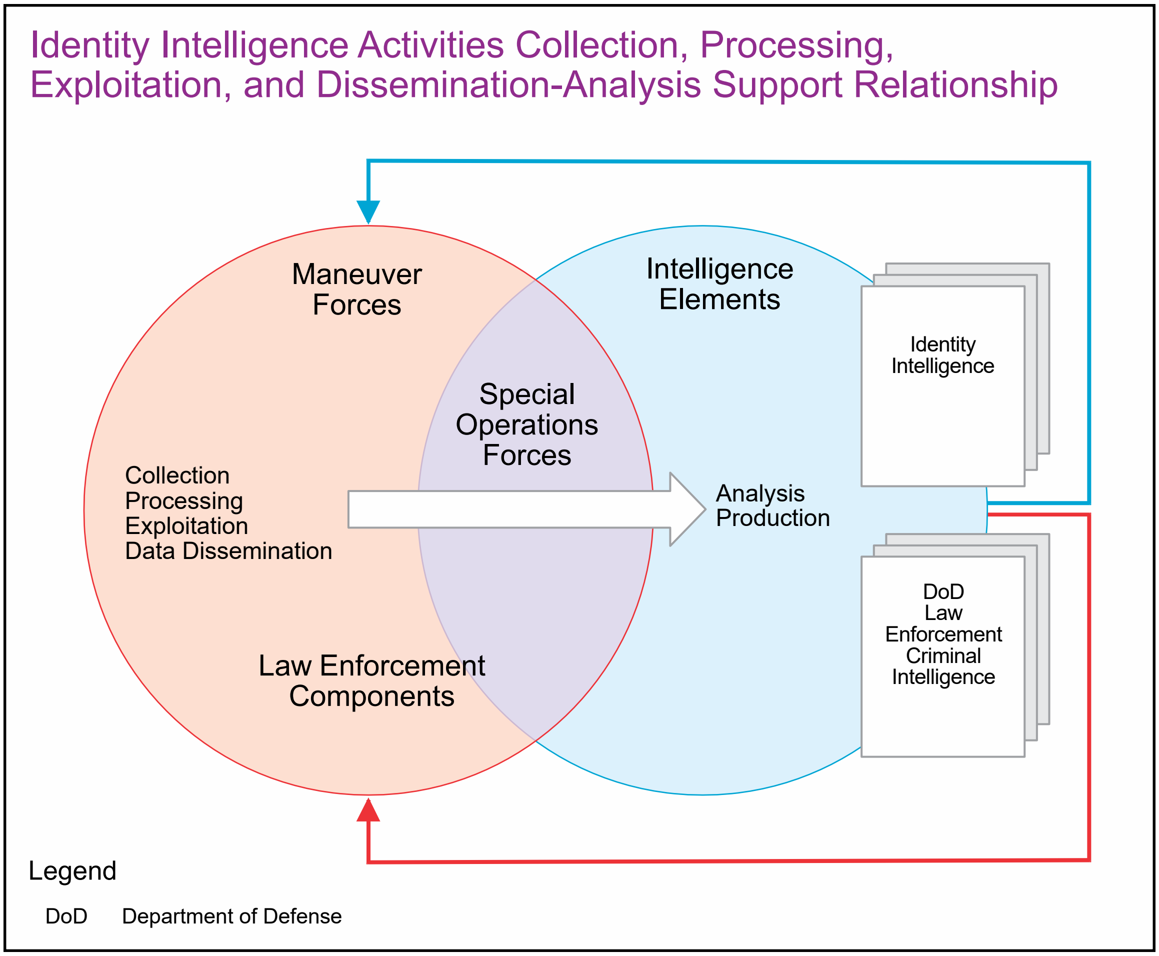

Identity Intelligence Activities Collection, Processing, Exploitation, and Dissemination-Analysis Support Relationship
Maneuver Forces
Intelligence Elements
Identity Intelligence
Special Operations Forces
Collection
Processing
Exploitation
Data Dissemination
Analysis Production
DoD Law Enforcement Criminal Intelligence
Law Enforcement Components
Legend
DoD Department of Defense

Figure D-1. Identity Intelligence Activities Collection, Processing, Exploitation, and Dissemination-Analysis Support Relationship

level of potential threats to US interests. These assessments can be used to characterize the OE; identify threat strategies and COAs; and provide insight into the physical, cultural, and social environments that influence human behavior. JFCs can exploit biometric, forensic, and document and media data collections and integrate that data with other all-source intelligence to locate and track unattributed identities across multiple or disparate encounters, cases, and events and map out human networks.

(3) Commanders should clearly define the focus areas of I2 analysis at each echelon to maximize economy of effort. Roles and responsibilities for I2 production should be assigned from Service intelligence centers and JIOCs/joint analysis centers, CCMD staff, and Service staffs, as appropriate, across task force and brigade intelligence cells and down to individual unit support elements. Clear guidance and direction helps ensure a sustainable distribution of effort between strategic-theater production (e.g., JIPOE, criminal indictments), operational assessments (e.g., named AOIs), and tactical support (e.g., watch listing, warrant support packages).

(4) I2 has evolved beyond the CT and COIN environment into an "all-threats" enduring requirement. In today's era of transregional, all-domain, and multifunctional threats, I2 provides DoD with an unprecedented insight into potential and existing threats and their plans, intentions, and networks; it supports the force on the battlefield. I2 identifies and monitors foreign threat-based persons, groups, and networks of military interest and their supporting relationships that are critical to the success of weapons, plans, strategy, and operations and their development, proliferation, and deployment. I2 provides foundational intelligence enabling the development of a COP of the OE human layer, determining friendly, neutral, and adversary. This includes the ability to maintain SA of connections and changes of key persons of interest, their proxies, associates, and allies. During competition, I2 enables triggers to determine OBs. I2 also identifies individuals, and populations either vulnerable to malign influence, or receptive to building PN capacity, and can be used to support the processing of detainees. Conducting I2 activities and operations prior to armed conflict is imperative to success by establishing foundational knowledge, including driving collections, as well as conducting engagements leveraging foreign-partner and US interagency relationships. This includes forensic, intelligence, and biometric partnerships, practiced in exercises, and executed in cooperative operations thereby building PN capacity and enriching foundational intelligence.

b. **The Role and Placement of I2 in Military Operations**

(1) The OE is the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander, encompassing physical areas and factors of all domains. The human aspects are present throughout the OE. As ISR for the human aspects, I2 assists the commander in better understanding and identifying the problem and human aspect of the OE; anticipating outcomes; understanding the results of various friendly, adversary, and neutral actions; and understanding how these actions may affect the desired objectives. JFCs should clearly define the focus areas of I2 analysis at each echelon to maximize economy of effort. Roles and responsibilities for I2 production should be coordinated and assigned via operation order from Service intelligence centers and joint intelligence centers/joint analysis centers,

CCMD staff, and Service staffs, as appropriate, across JTF and brigade intelligence cells, and down to individual unit support elements. Clear guidance and direction will help ensure a sustainable distribution of effort between strategic-theater production (e.g., JIPOE, criminal indictments), operational assessments, and tactical support (e.g., watch listing, warrant support packages).

(2) I2 supports many joint functions across the competition continuum, including protection, fires, and movement and maneuver. The broad nature of I2 requires several key factors to underpin the operational art and operational design of planning. The ways in which I2 is conducted is often just as important as access to the adequate means to conduct them. JFCs can choose multiple operational approaches to employ I2 throughout each phase of an operation to achieve military objectives. Each approach has advantages and drawbacks but all may be restricted in their implementation if adequate pre-mission planning does not occur. While the capabilities, functions, and processes inherent to the I2 construct are utilized by multiple USG departments and agencies to support any number of individual applications and uses, within DoD, I2 is employed to facilitate one of the following seven primary purposes:

(a) **Discovery of Unknown Threats.** Through the analysis and characterization of encountered persons of interest and their associated groups and networks, I2 seeks to uncover the presence, capabilities, and intent of individual threats, their associates, and networks operating within the OE. I2 informs the commander by providing a greater understanding of the threat, neutral, and friendly networks; their capabilities and capacities; their facilitation networks; and support structures, key personnel, and other relevant actors, as well as greater SA. I2 provides robust, scalable, and sharable mechanisms to map and monitor the human aspects of the OE. SCA and network analysis may identify underlying social structures (e.g., network nodes and COGs) and identify relevant actors' issues, goals, and means of influence and exploit identified opportunities and vulnerabilities. Similarly, I2 activities provide a rational set of means to assess operational effectiveness by monitoring the resilience of threat networks after an attack or maneuver.

(b) **Assessment of Risk.** I2 enables the JFC to more fully understand and evaluate the potential risks presented by individual actors operating within the OE and/or seeking access to military personnel, equipment, or facilities. Through I2 production processes, the JFC can rigorously and routinely assess and characterize the level of threat or trust presented by persons of operational interest and their networks to inform follow-on actions, mission planning, screening and vetting, and force protection postures.

(c) **Targeting.** Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. Joint targeting provides planners with access to detailed information on the targets, supported by the nominating component's analytical reasoning that links the targets with the desired effects. I2 may facilitate targeting for JFCs to generate operational effects and achieve military objectives. I2-generated data and subsequently developed knowledge about individuals and their associates, as well as their assessed capabilities, capacities, and ideological underpinnings, provide an ample resource to inform the analysis and prioritization of military targets and assign and organize appropriate resources with which to execute targeting. I2 may provide a capability to identify and track specific individuals across time and space with a high degree of confidence; it facilitates an ISR capability that goes beyond point-in-time encounter-based observation to inform a depth of understanding regarding the adversary's habits, behavioral and temporal recurrence, COGs, network components, and areas of exposure or weakness.

(d) **Attribution.** I2 can be used to attribute relevant events, materials, locations, associations, or activities to specific individuals. In competition, the joint forces' ability to quickly, accurately, and defensibly attribute actions, events, or materiel to both state and non-state actors alike has a direct and measurable impact on our ability to prevail in strategic competition.

(e) **Support to National and Homeland Security.** I2 supporting capabilities and programs inject vital data and information that, when effectively analyzed and organized into knowledge, facilitate the actionable recognition of threat actors and networks (i.e., the discovery of unknowns) and enable corresponding action. Accordingly, I2 facilitates development of one of the most valuable knowledge bases of information on persons of interest available to the national security community; supporting both IC and homeland security missions and activities; and enabling a broad range of partners—from domestic law enforcement and immigration officials to the military, intelligence, and broader security elements of our close foreign partners.

(f) **Support to National Law Enforcement.** A key aspect of any defense in-depth or offensive counter-network strategy includes the use of multiple instruments of national power in concert with PNs to achieve both military and national security objectives. Within modern warfare, key nodes of any adversarial network may well be outside the reach of lethal operations. To effectively neutralize these elements, a JFC looks to our partners to support a coordinated strategy that focuses on, among other things, the use of law enforcement tools, authorities, and reach. The I2 construct consciously seeks to enable these military-to-law enforcement partnerships through collaborative alignment and conformance of collection, processing, exploitation, and information sharing methods and management.

(g) **Assessment of Operational Effectiveness.** I2 assists the continuous evaluation of military operations by objectively assessing their impact on the threat and other relevant actors and networks with respect to the JFC's intent and objectives. I2 assists JFCs in determining whether operations are creating desired or undesired effects, when objectives have been achieved, and whether unforeseen opportunities can be exploited or require a change in planned operations to respond to threat actions.

(3) The main challenge for planners is to adeptly plan for timely deployment and fielding of I2 capabilities by correctly anticipating the capacity requirements for long-lead time and/or low-density collection, exploitation, and analysis elements within the event-driven phasing of operations. Each force provider maintains some level of exploitation capability capacity to support CCDR force requirements. The United States Army maintains the DoD's authoritative biometrics storage and matching repository, a biometrics

collection capability, and a biometrics production program, as well as deployable forensics collection and exploitation capabilities. The United States Marine Corps deploys a full biometrics and forensics collection and exploitation suite within a Marine expeditionary force (MEF) and also maintains a web-based data transport and collection management architecture supported by a small but effective analytic cell. The United States Navy maintains both a biometric collection capability to support maritime boarding activities and an expeditionary forensics exploitation program focused on explosive ordnance disposal support. Additionally, United States Special Operations Command (USSOCOM) maintains a SOF-unique collection, processing, and exploitation architecture supported by a continuously manned analytic cell and integrated into multiple interagency partners, including federal law enforcement and the national IC. These capabilities are all technically interoperable and capable of supporting a variety of mission applications and activities.

2. Identity Activities Overview

a. The use of identity to make decisions is commonplace across the joint force. Accordingly, the functions, tasks, and actions that comprise the I2 activities can be conducted both jointly and independently by maneuver, intelligence, and/or law enforcement components across their individual missions and authorities. Given the unique attributes and authorities of each functional community and their varying degrees of relevance and bearing for any given mission set and specific phase of operation, I2 does not in any way establish a hierarchy of users, functions, outcomes, force providers, or mission priorities but instead simply illustrates how the JFC can make optimal use of both identity information and analysis to support military operations and activities, while simultaneously enabling more strategic efforts to achieve broader national security objectives.

b. At its foundation, I2 activities are executed to support decision making at the tactical, operational, and strategic levels. Such decision support is most routinely provided through the production of I2 and/or law enforcement products. DoD law enforcement criminal intelligence is the result of the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations. DoD law enforcement criminal intelligence utilizes information gathered from law enforcement sources, in a manner consistent with applicable law, to provide tactical and strategic criminal intelligence on the existence, identities, and capabilities of criminal suspects and organizations. DoD law enforcement criminal intelligence analysis is conducted under circumstances that provide a reasonable suspicion that specific individuals or organizations may be planning or engaging in criminal activity having a connection to DoD.

c. Production of I2 and DoD law enforcement criminal intelligence is directly supported by the following primary collection, processing, exploitation, and dissemination activities:

(1) **Biometrics.** Biometrics is the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. This includes the

use of collection, processing, storage, matching, and sharing of biometric data and associated biographic and contextual information from enemy combatants, adversaries, unknown local populations, and persons of interest to support military operations and activities.

(2) **Traditional Forensics.** Traditional forensics is the application of multidisciplinary scientific processes to establish facts. This includes the collection, processing, preservation, storage, exploitation, and sharing of CEMs obtained through the course of military operations and activities organized to achieve a specific objective in a foreign country.

(3) **Digital/Multimedia Forensics.** Digital/multimedia forensics is the application of computer science and investigative procedures in the examination of digital and/or multimedia material. This includes the extraction, collection, and sharing of data and metadata contained within digital devices obtained through the course of military operations and activities organized to achieve a specific objective in a foreign country.

(4) **DOMEX.** See paragraph 5, "Document and Media Exploitation."

d. These capabilities, and the functions and tasks they support, can be executed individually by either intelligence and law enforcement units operating under their individual mission authorities or by conventional and special operations forces executing operations or campaigns.

e. The I2 activities construct leverages a nonlinear and recurrent cycle for leveraging collection, processing, exploitation, and data dissemination, which leads to all-source analysis and production capabilities to support decision making. It requires unity of action between operational collection, processing, and exploitation and all-source analysis and production to create actionable information. The tasks within the I2 activities operational cycle are conducted continuously as part of tactical operations executed across the OE. This cycle is depicted in Figure D-2.

f. To employ I2 activities, joint force components and organizations conduct five interrelated tasks for the purpose of providing commanders with relevant and timely assessments and estimates to inform decisions and actions. These tasks integrate the roles of the planner, operator, analyst, and commander into a single recursive cycle to ensure robust support to military operations regardless of type of operation or level of warfare. The five tasks are:

(1) **Plan and Direct I2 Activities.** Planning and direction functions include, but are not limited to: the identification and prioritization of identity-related information CRs; the development of a CONOPS and architectures required to support the commander's mission; tasking subordinate maneuver, intelligence, and/or DoD law enforcement elements for the collection of identity information or the production of I2; submitting requests for additional collection, exploitation, or analytic capabilities to higher HQs; and submitting requests for collection, exploitation, or all-source production support to external supporting entities (e.g., multinational partner, host nation, interagency elements).

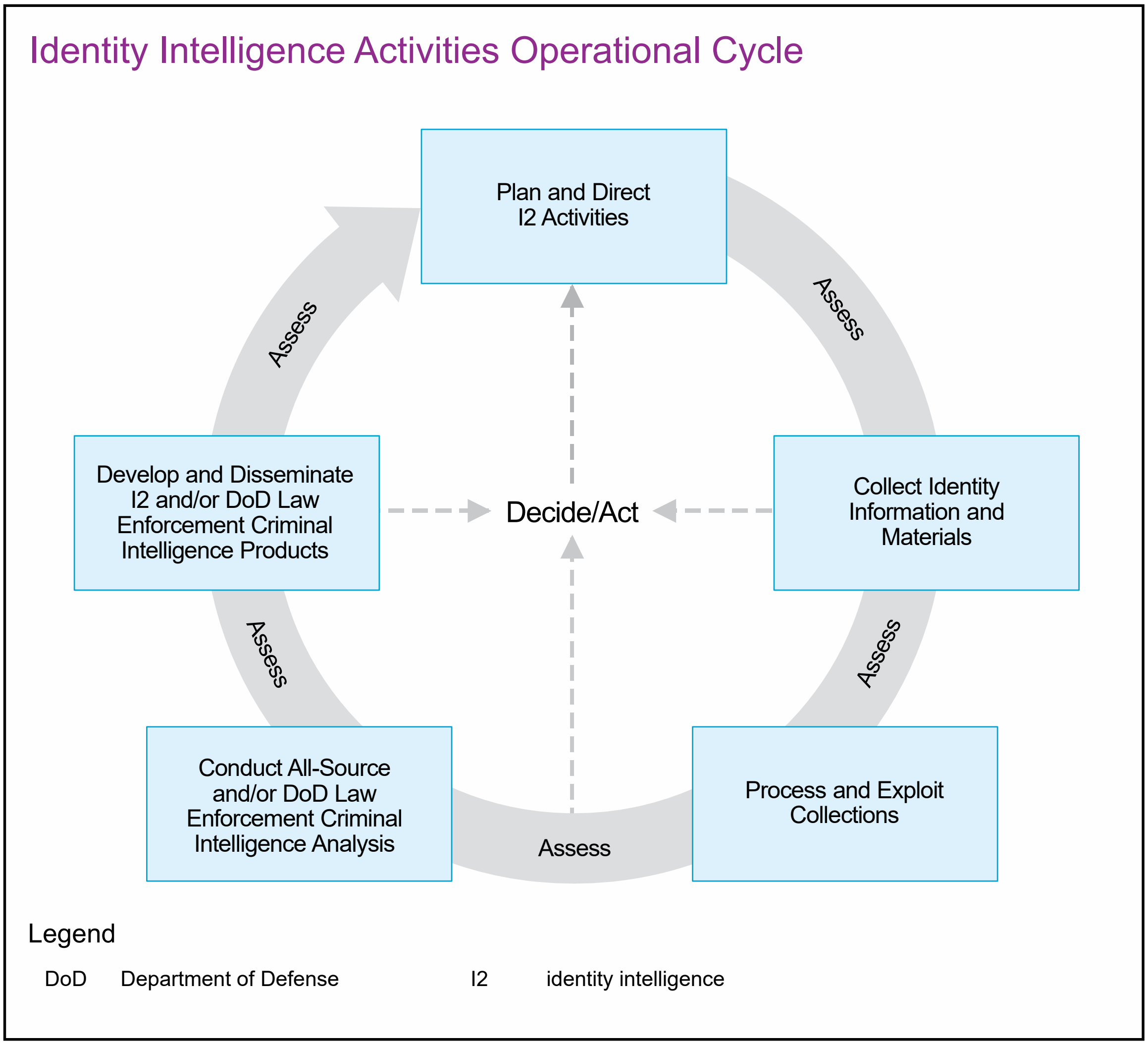

Identity Intelligence Activities Operational Cycle
Plan and Direct I2 Activities
Assess
Collect Identity Information and Materials
Assess
Process and Exploit Collections
Assess
Conduct All-Source and/or DoD Law Enforcement Criminal Intelligence Analysis
Assess
Develop and Disseminate I2 and/or DoD Law Enforcement Criminal Intelligence Products
Assess
Decide/Act
Legend
DoD Department of Defense
I2 identity intelligence

Figure D-2. Identity Intelligence Activities Operational Cycle

Planning and direction occurs continuously as part of the command's adaptive planning effort. Support to planning allows for the prioritization of identity capabilities across all ongoing operations and simultaneous planning efforts and products, such as JIPOE. Conversely, support to planning informs the development and prioritization of capacity and enhances readiness to respond to potential crises. Through these efforts, planners determine the personnel, equipment, and information sharing and intelligence architecture essential for I2 support to joint operations.

(2) **Collect Identity Information and Materials.** Collection includes those activities related to the acquisition of identity attributes (i.e., biologic, biographic, behavioral, and reputational data), forensic materials, and documents and electronic media of operational or intelligence interest. Collection is conducted by military forces and DoD law enforcement agencies. While some identity information (i.e., attributes contained on an identity credential) can be used immediately at the point of collection, most collected data and materials are sent to authoritative data repositories or local, regional, or reachback facilities or laboratories (including interagency partners) for appropriate processing, exploitation, and long-term storage.

(3) **Process and Exploit Collections.** During processing and exploitation, raw collected identity data and physical materials can be examined and analyzed by automated systems and/or trained personnel to determine their information value, correlate data to previously collected data, and report findings to command and I2 analysts. Processing and exploitation include data normalization, biometric matching, forensic analysis, technical (i.e., electronic and mechanical) analysis, and document and media translation and content analysis, as well as reporting the results of these actions to I2 analysis and production elements. Processing and exploitation may be federated or performed by the same element that collected the data.

(4) **Conduct All-Source and/or DoD Law Enforcement Criminal Intelligence Analysis.** Identity attributes (i.e., biologic, biographic, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes gathered from all intelligence disciplines or law enforcement sources are integrated to produce I2 or DoD law enforcement criminal intelligence, as appropriate. I2 utilizes enabling intelligence analysis activities, like BEI, FEI, and DOMEX, to discover the existence of unknown potential threat actors; associate individual actors to other persons, places, events, or materials; analyze patterns of life; and characterize their level of potential threats to US interests.

(5) **Develop and Disseminate I2 and/or DoD Law Enforcement Criminal Intelligence Products.** I2 and DoD law enforcement criminal intelligence products can be presented in many forms. They may be oral presentations, hard copy publications, or electronic media. The means are determined by the needs of the user and the implications and criticality of the intelligence. Rather than being the end of a process, I2 and/or DoD law enforcement criminal intelligence production is a continuous dialogue between the user and the producer. I2 production for joint operations is accomplished by JIOCs, Service intelligence centers, and CCMD-assigned intelligence brigades typically form the backbone of any operational I2 production support. DoD law enforcement criminal intelligence products are created by DoD law enforcement agencies as prescribed by the JFC.

(6) **Conduct Operational Assessments.** In addition to the five interrelated tasks, commanders and their staffs conduct assessments of I2 activities to determine whether they are generating the desired products to support military operations. Identity activities require a greater application of operational art due to the complexity of the human aspects of the OE. Likewise, I2 activities' assessments demand staffs conduct analysis more intuitively and consider both anecdotal and circumstantial information. Assessments over time that show trends are much more valuable for I2 activity planning and operational support than a single snapshot over a short timeframe. Tactical unit reporting such as patrol debriefs and unit after action reports may provide the most valuable information on assessing the impact of I2 activities, particularly when correlated across an OE.

g. Typical I2 assessments and products include:

(1) **Biometric-Enabled Watchlist (BEWL).** The DoD capability that enables screening for persons of interest based primarily on their biometrics (mostly fingerprints

enrollments and latents but may include iris and facial matching, as well). The persons of interest are identified by intelligence analysis usually for the purpose of screening, vetting, persistent targeting, or population management by DoD ground forces. It is centrally managed by the United States Army National Ground Intelligence Center (NGIC) where the intelligence information (available to the IC in Identity Intelligence Analytic Resource) on DoD persons of interest is maintained in collaboration with the associated biometrics storing and matching system (Department of Defense Automated Biometric Identification System [ABIS]) managed by the Defense Forensics Science Center (DFSC). The NGIC responds to all significant BEWL matches with a timely encounter notification, while DFSC responds with an automated match report.

(a) The term BEWL also refers to the set of associated biometrics from the DoD BEWL. The term BEWL may also refer to the entirety of the associated contextual and intelligence information in the DoD BEWL usually shared with other USG departments and agencies or foreign partners in the form of an XML [Extensible Markup Language] document often in conjunction with the set of associated biometrics.

(b) A customized BEWL is an extract or subset of biometrics of the DoD BEWL provided to a requesting customer for a specified use (e.g., a set of biometrics small enough to fit on a given handheld device) with identities determined through intelligence analysis to be relevant to a particular operation or operational area.

(c) The BEWL refers to four closely related and interdependent intelligence products:

1. **Encounter Notification.** A quick-turn intelligence product resulting from a biometrics match to a BEWL person of interest sent by the NGIC to all relevant customers via general service message, IIR, e-mail, or secure telephone. An encounter notification comes in an initial form and, when relevant, in a follow-up version resulting from further intelligence analysis of any newly available information.

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

3. **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.

4. **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.

(d) **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.

(2) **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.

(3) **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. Information planners and US military or diplomatic delegations are the primary audience for this product.

(a) **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 information planners.

(b) **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 information planners in mind.

(c) **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 information planners.

(4) **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 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.

(5) **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.

(6) **Person of Interest Packets.** Person of interest packets provide I2 analytic support to the initial and recurrent vetting of foreign personnel working with forward-

deployed military and/or USG personnel. Person of interest packets provide tailored summaries of significant derogatory information on individual persons of interest, combining biometric, DOMEX, and screening information in an easily briefed format.

h. I2 is supported by three primary functional components:

(1) **Maneuver Components.** Deployed maneuver units provide multiple Service collection, processing, and exploitation capabilities to support military operations. The results of these activities often provide the basis for all-source intelligence analysis supporting the production of I2 to meet the commander's information requirements. These products, in turn, inform, enable, and enhance continuous operational activities planned and executed by maneuver units to achieve the commander's military objectives.

(2) **Intelligence Elements.** Intelligence elements can conduct collection, processing, and exploitation activities under their own individual authorities in support of the JFC without the capabilities of maneuver or law enforcement units. Their primary contributions to the JFC requirements, however, are analysis and production capabilities, reachback support, specialized exploitation capabilities, and foreign disclosure. Collected identity attributes provide limited value to operational commanders and tactical units without a corresponding assessment and characterization of the identity to provide relevance and context, making I2 production the central aspect of I2 activities.

(3) **Law Enforcement Components.** Similarly, DoD law enforcement components can conduct collection, processing, and exploitation activities under their own individual authorities in support of the JFC without the capabilities of maneuver or intelligence units. These components may also produce law enforcement criminal intelligence to support military criminal investigations and support military prosecution activities.

i. Identity information and data collection and exploitation activities should be included in every OPORD to the extent appropriate for the operation. I2 activity considerations should be discussed in any applicable place in a plan or order but should be considered for the following annexes and appendices: annex B (Intelligence), annex C (Operations), annex E (Personnel), annex G (Civil-Military Operations), and appendix 14 (Force Protection) to annex C (Operations).

j. I2 is an organizing construct established to demonstrate a repeatable framework to guide the planning, application, and management of related capabilities by a JFC to support missions or operations that leverage or require identity information and analytic judgment to enable decision making. For this reason, DoD components may or may not refer to their existing supporting programs as I2 or I2 activities, while still providing capabilities that execute the function, tasks, and processes that comprise the I2 activities construct. Regardless of a component's chosen terminology, the I2 activities construct and its characteristic considerations described below provide a common and repeatable framework for operational planning, execution, and assessment. In each program instance, there are more similarities in function and design than there are differences. The differences typically lie in the individual authorities for collection and use.

(1) Defense intelligence components like the Army Deputy Chief of Staff for Intelligence or the Marine Corps Intelligence Activity refer to their programs as I2.

(2) The DIA describes its biometric and forensic capabilities and its document and media collection and exploitation capabilities as MASINT and DOMEX, respectively.

(3) USSOCOM describes its program of record as sensitive site exploitation and its use as I2 operations within formal USSOCOM policy directives.

(4) The United States Marine Corps describes its program and strategy as identity operations, while the United States Navy and United States Army Provost Marshall General call their programs I2 activities.

(5) Similarly, program initiatives at the CCMDs oscillate between I2 activities and I2, depending on which CCMD staff component has primary management responsibility (e.g., J-3 or J-2).

3. Biometrics

a. Biometrics is the measurement and analysis of unique physical or behavioral characteristics (e.g., fingerprint, voice patterns), especially as a means of verifying personal identity. Biometrics are a key enabler of I2. Regardless of disguises, aliases, or falsified documents, an individual's biometrics positively identify them to a high degree of confidence across time and space. The more biometrics that can be assembled for an identity, the greater degree of detection and accuracy results for identity resolution. Biometrics enhances targeting, security vetting, and force protection by helping to positively identify insurgents, terrorists, criminals, and others who would do harm to force, friendly forces, and facilities. Intelligence-related biometric collections can support or enhance CI, intelligence analysis, interrogation and detention tasks, HVT confirmation, source vetting, and attribution, among other activities.

b. DoD biometric capabilities consist primarily of stationary, man-portable, and untethered collection mechanisms; local and authoritative digital storage systems; and modality-specific, as well as fusion-matching algorithms. These capabilities are available through each Service and USSOCOM, with the exception of the DoD ABIS.

(1) The Secretary of the Army is the DoD executive agent for DoD biometrics IAW DoDD 8521.01E, *DoD Biometrics.* Within this role, the Secretary of the Army leads the requirements, architecture, and standards development efforts for joint, common, and interagency biometric capabilities. The Secretary of the Army has designated the Army Provost Marshal General as the responsible official for executing the assignments of the executive agent.

(a) **DoD ABIS.** The Army's Defense Forensics and Biometrics Agency (DFBA) operates and maintains the authoritative DoD repository for multi-modal biometrics collected on foreign nationals throughout the course of military operations and shared by PNs and interagency partners, known as the DoD ABIS. The DoD ABIS contains fingerprints, iris scans, facial images, and palm prints collected through direct enrollments, site exploitation activities, direct allied and multinational submissions, and information shared by interagency and foreign partners. This data is normalized and stored in an unclassified repository for comparison against future biometric collections. Through the ABIS, DFBA executes the common storage, processing, and matching activities of the DoD biometrics enterprise. DFBA also manages the systematic sharing of DoD collected biometric data with and from PNs and provides the conduit for matching against interagency authoritative data sets, including dissemination of the DoD BEWL.

(b) **Biometrics Automated Toolset-Army,** the primary multi-modal biometrics collection device, is a man-portable biometrics collection capability that collects fingerprints, facial images, and iris scans, as well as biographic and contextual information relevant to the collection event. It operates primarily on the SIPRNET and maintains its own server and communications architecture. All collected files are transmitted to the DoD ABIS for storage and matching.

(2) Commander, USSOCOM, provides for all USSOCOM biometric collection capabilities required within a theater of operations. Handheld multi-modal biometrics collection devices are fielded with every SOF unit and supported by a Special Operations Forces Exploitation (SOFEX) portal. USSOCOM provides individual training for all levels of exploitation requirements, including chain-of-custody to support strategic exploitation and follow-on efforts. The SOFEX architecture provides a single web-based portal to submit, manage, and respond to all SOF enrollments in NRT. The SOFEX architecture leverages biometric data and matching capabilities across the USG to support SOF mission planning and execution. All USSOCOM-collected files are transmitted to the DoD ABIS for storage and matching. USSOCOM also maintains robust partnerships (often with system-to-system connections) with multiple IC elements and national centers, as well as interagency partners, such as DHS and the FBI.

(3) The Office of the Chief of Naval Operations manages the Navy's Identity Dominance System (IDS) to support the processing of multi-modal biometric information collected from encountered individuals during maritime interception operations. The IDS provides a real-time mechanism to check unknown individuals against the DoD BEWL and support the identification, targeting, and force protection activities of visit, board, search, and seizure teams. All IDS-collected files are transmitted to the DoD ABIS for storage and matching. Separately, the Naval Criminal Investigative Service (NCIS) maintains multi-modal biometric collection kits to enable NCIS special agents and Navy Sailors to establish identity, affiliations, and authorizations of known individuals; deny anonymity to adversaries; and protect personnel, facilities, and assets.

(4) The Commandant of the Marine Corps employs a variant of the IDS (Identity Dominance System-Marine Corps [IDS-MC]) collection capability augmented by a variant of the SOF architecture, known as the Department of the Navy Identification and Screening Information System (DONISIS). IDS-MC is a multi-modal identity system that provides a Marine air-ground task force (MAGTF) the ability to collect and submit for matching and storage biometric and related biographic and contextual data in support of operations.

(5) The Director, DIA, provides biometric capabilities to meet both joint force and national IC IRs.

c. **FBI's Next Generation Identification (NGI).** NGI is a national law enforcement biometric and criminal history system maintained by the FBI's Criminal Justice Information Services Division. NGI provides automated fingerprint, iris, palm, and face search capabilities; latent matching capabilities; electronic image storage; and electronic exchange of biometrics files to more than 18,000 law enforcement agencies and other authorized interagency partners. NGI is the largest criminal fingerprint database in the world, housing the fingerprints and criminal histories of more than 90 million subjects. The DoD ABIS is the primary conduit for submitting and receiving biometric files to and from the NGI.

d. **DHS Automated Biometric Identification System (IDENT).** IDENT is the central DHS-wide system, managed by the Office of Biometric Identity Management, for the storage and processing of biometric and associated biographical information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses. IDENT stores and processes biometric data—digital fingerprints and facial images—and links biometrics with biographical information to establish and verify identities presented at the point of encounter. IDENT maintains more than 230 million biometric files of individuals seeking entry to the United States, which DoD leverages to enhance employment of I2 activities.

e. The IC maintains multiple classified biometric storage and matching capabilities, some of which are accessible via JWICS.

f. **National Central Bureaus (NCBs).** Each member nation hosts an International Criminal Police Organization-International Police (ICPO-INTERPOL) NCB. The US NCB is the single USG interface with ICPO-INTERPOL and its 192 participating countries. The NCB can be leveraged to submit both point-to-point (often referred to as diffusion requests) and ICPO-INTERPOL-wide requests for biometric matching against national law enforcement biometric repositories.

4. Forensics

a. Forensics is the application of multidisciplinary scientific processes to establish facts that can be used by a JFC to support military operations. Forensic disciplines include deoxyribonucleic acid (DNA), serology, firearms and tool marks, latent prints, questioned documents, forensic chemistry, and trace materials. Forensic capabilities can be used to support intelligence functions, operational activities, force protection, host-nation legal support, and other related efforts. Forensic capabilities aid operations by adding depth and scope to the comprehensive operational picture. Exploited materials allow the linking of specific persons to places, materials, or events. The resulting information can provide usable intelligence to target, attribute, apprehend, and detain or prosecute enemy combatants, terrorists, and criminals.

(1) The Secretary of the Army is the DoD executive agent for traditional forensics, IAW DoDD 5205.15E, *DoD Forensic Enterprise (DFE)*. Within this role, the Secretary of the Army leads the requirements, architecture, and standards development efforts for nontraditional forensic capabilities. The Secretary of the Army has designated the Army Provost Marshal General as the responsible official for executing the assignments of the executive agent.

(a) **The DFSC** provides full-service forensic support (criminal, expeditionary, and reachback) to the JFC and provides specialized forensic research capabilities to the CCMDs. It contains two primary elements.

1. The **United States Army Criminal Investigation Laboratory** provides traditional forensic capabilities to support worldwide criminal investigation across all Services.

2. The **Forensic Exploitation Directorate** provides expeditionary and reachback battlefield forensic capabilities to support JFC requirements, to include forensic-related I2 activities.

(b) The **Intelligence and Information Warfare Directorate (I2WD)** of the Army's Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center provides advanced technical exploitation capabilities of certain materials collected. C5ISR provides forensic and reachback support in the exploitation of foreign materiel and other CEM to support science and technology and countermeasure development activities.

(2) Commander, USSOCOM, provides for all USSOCOM forensic collection and exploitation capabilities. Forensic collection kits are fielded with every SOF unit and supported by a SOF-unique expeditionary exploitation analysis cells and regional exploitation centers, as well as the SOFEX architecture. This architecture leverages additional reachback forensic capabilities resident in DFSC, I2WD, FBI, DIA, and other elements of the IC to meet mission requirements (e.g., timeliness, national intelligence, special targeting) and support follow-on SOF missions.

(3) The Office of the Chief of Naval Operations manages the Navy's Expeditionary Exploitation Unit One (EXU-1) program to provide advanced expeditionary exploitation capabilities to collect, process, exploit, and analyze improvised and conventional weapons, ordnance, and their components on both land and sea. The EXU-1 program directly supports weapons TECHINT activities and counter-IED LOEs, as well as other explosive ordnance disposal and countermeasure development efforts.

(4) The Commandant of the Marine Corps employs a Marine Corps variant of the USSOCOM expeditionary forensics collection and exploitation capabilities supported by the DONISIS architecture. Each MEF deploys with one or more expeditionary forensics exploitation capabilities assigned under the MEF command element. The expeditionary forensics exploitation capabilities provide task-organized, functionally specialized capabilities that can be tailored to support the operational requirements of the MAGTF commander.

(5) The Director, DIA, provides forensic capabilities to meet both joint force and national IC IRs.

(6) **FBI Terrorist Explosive Device Analytical Center (TEDAC).** TEDAC is a specialized reachback exploitation element of the FBI Crime Lab focused primarily on the forensic and technical exploitation of IEDs and unmanned aerial systems used in an improvised manner. TEDAC coordinates the efforts of the entire government, from law enforcement to intelligence to military, to gather and share intelligence about these devices. TEDAC performs IED exploitation using both established and innovative forensic techniques in a high-capacity, multi-agency environment with scientists, engineers, and technicians. TEDAC is the final strategic-level exploitation facility and final disposition repository for all IED material, once all DoD investigation and exploitation requirements are complete.

b. DoD maintains multiple repositories and case management systems for forensically derived information collected on the battlefield.

(1) **National Deoxyribonucleic Acid Index System (NDIS) and Joint Deoxyribonucleic Acid Index System (JDIS).** Both NDIS and JDIS store and manage digitized DNA profiles. NDIS is limited to DNA profiles collected during the course of law enforcement activities. DNA profiles loaded into NDIS are automatically checked against other DNA index systems connected to the national architecture to support investigations. NDIS data is only collected and used for law enforcement purposes and can only be accessed by law enforcement professionals. JDIS was created as the DoD's intelligence-focused counterpart to the NDIS. JDIS serves as the comprehensive DoD repository for human DNA collected through military operations for intelligence purposes. All JDIS files are presumed non-US persons information and may be of intelligence value.

(2) **Weapons Technical Intelligence Exploitation Analysis Tool** serves as the DFSC's laboratory process management system with an exploitation material tracking capability. The case management system provides forensic and FEI analysts access to all DFSC exploitation reports and products.

(3) **SOFEX Portal and DONISIS** are web-based tools that serve as the submission point and case management system for forensically derived data and reporting. These systems facilitate the federation of submitted CEMs across DoD and interagency partners for strategic exploitation and analysis. Responses are either loaded into the portal or a web-accessible link is provided to access exploitation results within another authoritative holding. SOFEX is supported around the clock by a team of analysts at USSOCOM to coordinate, synchronize, and integrate SOF collections across DoD and the USG.

c. For the purposes of this discussion, forensic exploitation activities are divided into four distinct tiers. Each tier is defined specifically by its depth of exploitation activities and not by its proximity to the collection, the experience of the exploiter, or the precision or rigor of the exploitation mechanism(s). They describe function and mission outcome, not organizational primacy or ownership (e.g., under this tiering structure, it could be possible to conduct tiers 3 or 4 exploitation activities at the point of collection, if the appropriate technologies were available).

(1) **Tier 1.** Tier 1 forensic exploitation is a tactical-level activity that consists of actions to collect, preserve, document, and manage material collected from a site, as well as any initial assessment and/or presumptive testing of collected materials to support tactical decisions. Tier 1 exploitation activities can be accomplished by any trained member of the joint force and typically do not require specialized skills or expertise.

(2) **Tier 2.** Tier 2 forensic exploitation is an operational-level activity that provides the JFC with detailed technical, forensic, and scientific analysis of CEM using scientific methods and techniques to support intelligence, operations, and/or law enforcement activities within a theater of operations. Tier 2 exploitation may also include PED and/or all-source analysis activities to inform current and follow-on operational activities. Tier 2 forensics exploitation activities are typically executed by expeditionary assets, including Army forensic exploitation laboratories, USSOCOM exploitation analysis cells, Marine Corps expeditionary forensics exploitation capabilities, Navy EXU-1 elements, and DIA joint document exploitation centers (JDECs). However, tier 2 forensic activities can also be conducted by reachback capabilities if operational constraints permit or require.

(3) **Tier 3.** Tier 3 forensic exploitation is a strategic-level activity that provides the JFC with specialized technical, forensic, and/or scientific analysis using advanced techniques, scientific capabilities, and equipment (including equipment too large or fragile to be readily forward deployed). Tier 3 capabilities are designed to deliver full-spectrum exploitation and intelligence to inform operational and/or strategic assessments and decisions. Tier 3 exploitation typically occurs in the continental US-based reachback facilities but can be forward deployed to regional exploitation elements with enough advance planning.

(4) **Tier 4.** Tier 4 forensic exploitation is reserved for specialized strategic missions and targets that serve specific, and sometimes classified and/or highly sensitive, national IRs. These collection and exploitation activities are often managed outside of the regular exploitation mission workflow of the JFC. Examples of tier 4 missions include the foreign materiel program and various counter-CBRN activities.

5. Document and Media Exploitation

a. DOMEX activities can increase the value of information gained, provide timely and relevant information to commanders, support the intelligence and operational decision-making processes throughout the competition continuum, and assist judicial proceedings through application of preservation and chain-of-custody procedures. Collected or captured documents and media, when processed and exploited, may provide valuable information such as enemy and adversary plans, intentions, locations, capabilities, and status. The category of "collected documents and media" includes all media capable of storing fixed information, to include computer storage material. DOMEX may be conducted by any intelligence personnel with appropriate technical exploitation and language support.

b. **General**

(1) 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 ICD 302, *Document and Media Exploitation.*

(2) DOMEX is the processing, translation, analysis, and dissemination of information and intelligence derived from 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, that 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.

(3) 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 as intelligence and information generated for future targeting and biometric and forensic processes supporting the legitimate prosecution of individuals associated to the exploited materials. Human signature exploitation, from captured or acquired documents and media, also enables the development of I2 analytical products to support urgent information needs and operational planning.

c. **Function**

(1) The NMEC coordinates FBI, CIA, DIA, and NSA efforts to exploit, analyze, and disseminate information gleaned from paper documents, electronic media, videotapes, audiotapes, and electronic equipment seized by the military and IC in operational theaters around the globe. These exploitation and analysis activities can provide valuable insights into the capability, capacity, and intent of threat actors operating within the OE. NMEC products can be used by I2 and DoD law enforcement criminal intelligence analysts to inform detailed assessments and estimates to meet the commander's information and IRs. As the national IC center for DOMEX, the NMEC advances the IC's collective capabilities on behalf of the DNI and the Defense Intelligence and Security 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.

(2) 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.

(3) 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 capabilities conduct exploitation activities according to their ability. They collaborate 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. Battlefield exploitation may require the application of several DOMEX capabilities, including document exploitation, media exploitation, and cellular phone exploitation. Specific DOMEX organizations and entities include:

(a) **DOMEX Senior Staff Organization.** This organization functions as part of the theater commander's J-2 staff to coordinate and synchronize theater DOMEX operations.

(b) **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 is under the OPCON of the CCDR and under the staff supervision of the CCMD J-2. A JDEC collects and exploits collected DOMEX materials (e.g., documents, cell phones, and electronic media such as computer files, video) in theater to obtain intelligence. 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. Material exploitation can obtain information on a great range of topics, such as information on enemy intentions and planning (including deception), locations, dispositions, tactics, communications, logistics, and morale, as well as a wealth of information for subsequent long-term exploitation. Exploited materials can support the identification of threat actors and the mapping of their networks and inform capability, capacity, and impact assessments of those networks. The resulting I2 products support follow-on strategic and operational planning as applicable. 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.

(c) **Exploitation Analysis Center (EAC).** A SOF EAC may be deployed to provide dedicated DOMEX support to a CCDR during contingency operations planning and execution. SOF EACs are a SOF-unique, CCMD-level capability to support the information requirements of the theater SOF commander while planning and executing campaigns and major operations. In most cases, an EAC is under the OPCON of the CCDR and under the staff supervision of the CCMD J-2 or subordinate J-2 as appropriate. The EAC links multiple tactical exploitation capabilities within a theater of operation to out-of-theater strategic exploitation capabilities. This enables intelligence professionals to meet both in-theater and strategic out-of-theater information requirements more quickly than existing joint force efforts. Theater SOF commanders can scale and deploy an EAC to support tactical operations or augment the EAC with strategic exploitation capability based on mission analysis, access to reachback, and available communications resources. When properly augmented, an EAC may serve as the only in-theater exploitation capacity for the joint force. EACs are networked to provide a global view of exploitation operations conducted by SOF worldwide and have direct access to other DoD and USG exploitation capacities. Intelligence planners should seek to optimize the effective integration of SOF and conventional forces' exploitation capabilities by emphasizing synchronization of activities and unity of effort. The EAC 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 EAC 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. NMEC, the Services, component commands, CI organizations, or other intelligence and law enforcement organizations can provide key personnel augmentation and mission equipment for the EAC.

(d) **Service-Component-Level DOMEX Capabilities.** 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 or EAC for exploitation and inclusion in databases accessible to the IC.

d. **Location.** The JDEC, EAC, or other DOMEX capabilities may be adjacent to the joint strategic exploitation center, the joint interrogation and debriefing center (JIDC), or the JCMEC to provide mutual support and concurrent exploitation of captured enemy personnel and equipment.

e. **Processing**

(1) 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 enemy prisoner of war (EPW)/detainee property that remains with the detainee. When possible, the JDEC and Service DOMEX capabilities provide direct support to the JIDC and other strategic and theater EPW holding areas in exploiting detainee property.

(2) 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, collected, captured, and acquired documents and media are considered controlled unclassified information unless sensitive sources, methods, or activities were used to acquire the information. 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.

(3) 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.

(4) 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.

(5) DOMEX capabilities 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.

f. **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.

g. **Digitizing and Imaging.** DOMEX capabilities digitize documents and media into a searchable theater exploitation database. This is done to create working copies and to enable 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. 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.

h. **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.

i. **Reporting and Dissemination.** DOMEX capabilities 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 enable PN access to releasable documents.

6. Identity Intelligence and Department of Defense Law Enforcement Criminal Intelligence

Identity attributes (e.g., biographical, biological, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes gathered from all intelligence disciplines or law enforcement sources are integrated to produce I2 or DoD law enforcement criminal intelligence, as appropriate.

a. Within the joint force, I2 principally supports the find, fix, exploit, and analyze phases of the F3EAD process. I2 supports the identification of key adversary personnel, persons of operational or intelligence interest, and their support and facilitation networks. I2 utilizes enabling intelligence activities, like biometrics, forensics, DOMEX, and other information to discern the existence of unknown potential threat actors by connecting individuals to other persons, places, events, or materials; analyzing patterns of life; and characterizing their level of potential threats to interests. This analysis leverages codified analytic methodologies and compliance with the ODNI analysis standards to produce timely and actionable estimates and assessments to inform the commander's decision cycle. The intelligence generated through all-source analysis of I2 activities can take several forms, ranging from graphic displays to traditional reports, disseminated from unclassified to top secret security protocols, in support of a wide variety of military operations and activities. I2 products can be developed and tailored to specific situations by any I2-trained, all-source analyst, limited only by their intelligence, imagination, and creativity. These products enable tasks, missions, and actions that span the competition continuum. Additionally, biometrics and corresponding I2 products support the persistent identification and targeting of adversaries between and across operations and campaigns, which enables a range of military and civilian functions.

b. DoD law enforcement components support the collection, processing, and exploitation of identity attributes that enable I2 activities. These components may also conduct law enforcement criminal intelligence analysis and production to support investigations, identify and track criminals, assess criminal informants, and support prosecution activities. DoD law enforcement elements utilize information gathered from law enforcement sources, in a manner consistent with applicable law, to provide tactical and strategic DoD law enforcement criminal intelligence on the existence, identities, and capabilities of criminal suspects and organizations. DoD law enforcement criminal intelligence analysis is conducted when there is a reasonable suspicion that specific individuals or organizations with a connection to DoD may be planning or engaging in criminal activity.

c. The USD(I&S) Identity Intelligence Division (I2D) is the defense intelligence focal point and advocate for all matters relating to I2, BEI, and FEI. The I2D provides subject matter expertise to CCDRs and staff on planning, executing, and assessing I2 activities; I2 analysis and production; and partner engagement activities. The USD(I&S) I2D develops and synchronizes identity collection planning in support of CCMD operational objectives, supports CCMD military engagement and media operations center development activities, and facilitates DIA's Office of Partner Engagement coordination and approval of I2-related sharing arrangements and agreements.

See DoDI O-3300.04, Defense Biometrics Enabled Intelligence (BEI) and Forensics Enabled Intelligence (FEI), *for additional information about the USD(I&S) I2D.*

d. Identity Intelligence Analytic Resource is an analytic tool set, data repository, and production support system that ingests biometrics and associated intelligence data on biometrically enrolled persons of interest. The Identity Intelligence Analytic Resource disambiguates identity data from multiple systems and networks and pushes correlated data to other intelligence systems to baseline and resolve encountered identities. The system automatically estimates and scores the threat probability for each identity maintained within the system and prioritizes production workflow based on those scores. The Identity Intelligence Analytic Resource is the primary mechanism used to develop and maintain the DoD BEWL.

7. Authorities

Pursuant to US and international law, DoD components have authority to collect, process, and exploit identity information, forensic materials, and captured materials. These activities, however, may be subject to limitations, restrictions, or conditions on collection and data use depending on the circumstances (time, place, manner, and purpose) of the activity. I2 activities may be conducted during times of peace or conflict, at home, abroad, or on the high seas. The collection may be obtained through a variety of means and methods, and the identity information may be used for a variety of purposes supporting operations. Additionally, in certain circumstances, a JFC may choose to apply or conform to host-nation law. JFCs and their staffs must be cognizant of these circumstances to assess their legal impacts (restrictions, limitations, or conditions), if any, on the operation and the I2 activities conducted to support it. In each instance, commanders should seek the counsel and recommendations of their operational law staff judge advocates to ensure the legal sufficiency of their actions.

a. **Law of War.** IAW DoD policy, DoD personnel comply with the law of war during all armed conflicts, however characterized, and in all other military operations. In all other military operations, DoD personnel continue to act consistent with the law of war's fundamental principles and rules, which include those in Common Article 3 of the 1949 Geneva Conventions and the principles of military necessity, humanity, distinction, proportionality, and honor. For more information, see DoDD 2311.01, *DoD Law of War Program.* I2 activities must fit within the scope and authority of the mandate that authorizes the operation (e.g., Presidential directive, congressional authorization to use military force, UN Security Council resolution, and/or general principles of self-defense [UN Charter Article 51]). The law of war regulates the resort to armed force; the conduct of hostilities and the protection of war victims in international and non-international conflict; belligerent occupation; and the relationships between belligerent, neutral, and non-belligerent states. It is derived from the treaties and customary international law binding on the United States. Other purposes of the law of war are to facilitate restoration of peace, assist military commanders in ensuring the disciplined and efficient use of military force and preserve the professionalism and humanity of combatants. The protections provided by the law of war generally will not inhibit, limit, or restrict the routine means of conducting I2 activities during periods or in places of conflict. For example, the taking of a facial photograph for identification purposes is not prohibited, but the use of the photo to degrade or humiliate a prisoner of war is prohibited under the protection against insults and public curiosity of Article 13 of the Third Geneva Convention.

b. **Law of the Sea.** Within the maritime domain, the conduct of I2 activities is principally challenged by the circumstances of the activity. During times of armed conflict or hostilities, employment of I2 activities will be guided by the law of war, UN Security Council resolutions, and congressional authorizations to use force. Outside of armed conflict for encroachments on the rule of law and sovereignty, different laws apply depending on the physical location (e.g., internal waters, territorial waters, archipelagic waters, contiguous zones, or the high seas) where the activity is being conducted. Rules pertaining to innocent passage, transit passage, and sovereign immunity may affect collection and use. Different rules also apply depending on the types of operations being conducted (e.g., approach, visits, searches). Under these rules, certain classes of individuals (e.g., foreign naval personnel) may be specifically protected. Specific case-by-case authorizations may be required prior to conducting I2 activities depending on the circumstances.

For more information, refer to NTTP 3-07.11M/Coast Guard Tactics, Techniques, and Procedures 3-93.3/Marine Corps Interim Publication 13-10Ii, Visit, Board, Search, and Seizure Operations.

c. **Geneva Conventions and UN Declarations**

(1) The four Geneva Conventions of 1949 apply as a matter of international law to all military operations that qualify as international armed conflicts and cases of partial or total occupation, as well as providing certain minimum standards for non-international armed conflicts. These treaties are intended to provide comprehensive humanitarian standards for the treatment of war victims and detainees, and the protection of civilians without adverse distinction. Commanders ensure the employment of I2 activities complies with the Geneva Convention treaties, most notably in the treatment of EPWs and the protection of civilians in a time of war.

(2) Certain I2 activities may be broadly interpreted within the UN's Universal Declaration of Human Rights as subjecting individuals to arbitrary interference with their privacy. However, it should be noted that legitimate interference is clearly permitted within international and intergovernmental law (e.g., European Union law) by a state interested in enforcement of the just requirements of morality, public order, and the general welfare. As such, JFCs are traditionally authorized to obtain and use identity information for legitimate purposes as a matter of public order or general welfare, which include national security, in both international and non-international armed conflict situations.

d. **Host-Nation Law.** Commanders should coordinate with their staff judge advocates and the country team to review host-nation law, as well as pertinent agreements between DoD and the host nation (e.g., defense cooperation agreements, status-of-forces agreements). The appropriate senior defense official/defense attaché should have SA of all I2 activities being conducted within the host nation.

Intentionally Blank

APPENDIX E
JOINT EXPLOITATION SUPPORT TO INTELLIGENCE

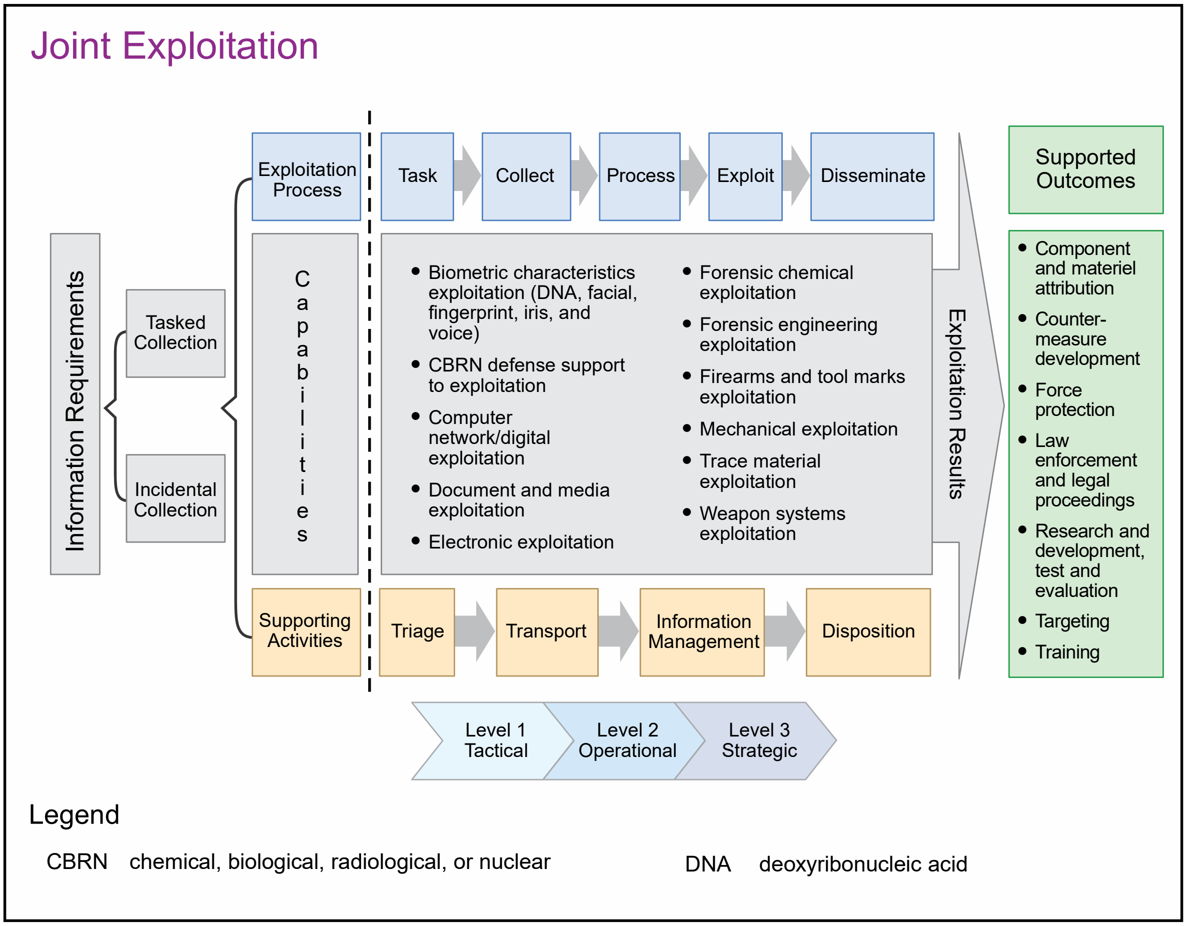
1. Introduction

a. Joint exploitation is the synchronization, coordination, and integration of operations and/or activities using S&T means to establish facts and develop actionable information and intelligence from material and materiel captured, collected, or handled by DoD. Joint exploitation requires a coordinated and synchronized approach among exploitation stakeholders that includes the CCMDs, Services, the Defense Intelligence and Security Enterprise, industry, academia, international partners, and the whole of government.

b. The IC supports the immediate intelligence needs of the deployed force, including the type of information that can be derived from analysis of CEM. CEM is all data, information, physical material, and materiel in the possession of DoD, regardless of its classification or how it was obtained, that can be exploited in support of DoD and national interests. Some examples of CEM include explosives, conventional and improvised weapons, documents, ballistic missiles, digital media, vehicles, storage devices, cellphones, SIM [subscriber identification module] cards, satellites, weapon systems, pocket litter, military aircraft, photographs, and unmanned systems. CEM does not include CBRN material but does include delivery systems and associated components. A deployable exploitation capability meets challenges posed by enemies seeking to hide their identities and avoid attribution and can provide immediate feedback on the tactical and operational relevance of threat equipment, materials, documents, and personnel encountered by the force. The deployable exploitation capability is expeditionary, modular, scalable, and includes collection, technical, and forensic exploitation and analytical capabilities linked to the national labs and the intelligence enterprise.

c. Processing of CEM in a theater is conducted under the authority and direction of CCDRs. Unique information, material, and other exploitation capabilities developed by the Services, USSOCOM, CSAs, interagency partners, and multinational partners can be utilized to answer CCIRs, answer operational commanders' requirements, or inform IC requirements. 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.

d. Joint exploitation results can not only answer CCIRs but can inform planning by supporting activities such as force protection; joint targeting; signature characterization; component and materiel sourcing; prosecution, research, development, testing, and engineering; and special activities (Figure E-1).


Joint Exploitation
Information Requirements
Tasked Collection
Incidental Collection
Exploitation Process
Capabilities
Supporting Activities
Task
Collect
Process
Exploit
Disseminate
Biometric characteristics exploitation (DNA, facial, fingerprint, iris, and voice)
CBRN defense support to exploitation
Computer network/digital exploitation
Document and media exploitation
Electronic exploitation
Forensic chemical exploitation
Forensic engineering exploitation
Firearms and tool marks exploitation
Mechanical exploitation
Trace material exploitation
Weapon systems exploitation
Triage
Transport
Information Management
Disposition
Exploitation Results
Supported Outcomes
Component and materiel attribution
Counter-measure development
Force protection
Law enforcement and legal proceedings
Research and development, test and evaluation
Targeting
Training
Level 1 Tactical
Level 2 Operational
Level 3 Strategic

Legend

CBRN chemical, biological, radiological, or nuclear

DNA deoxyribonucleic acid

Figure E-1. Joint Exploitation

(1) Support to force protection, including identifying threat TTP and weapons capabilities that defeat friendly countermeasures, including jamming devices and armor.

(2) Support to targeting, which occurs as a result of technical and forensic exploitation of recovered materials used to identify participants in the activity and provide organizational insights that are targetable.

(3) Identification of signature characteristics derived from threat weapon fabrication and employment methods that can aid in cuing collection assets.

(4) Support to component and material sourcing and tracking and supply chain interdiction uses exploitation techniques to determine origin, design, construction methods, components, and precursors of threat weapons to identify where the materials originated, the activities of the threat's logistical networks, and the local supply sources. Once identified, the supply chain can be targeted for collection of additional information or for subsequent operations.

(5) Support to prosecution is accomplished when the results of the exploitation can link individuals to illicit activities. When supporting law enforcement activities, recovered materials are handled with a chain of custody that tracks materials through the

progressive stages of exploitation. The materials can be used to support detainment and prosecution of captured personnel or to associate suspected perpetrators who are connected later with a hostile act.

(6) Support to research, development, testing, and engineering is accomplished when the results of the exploitation can enable further development or recreation of a capability encountered on the battlefield.

(7) Support to special activities may take several forms to support national objectives.

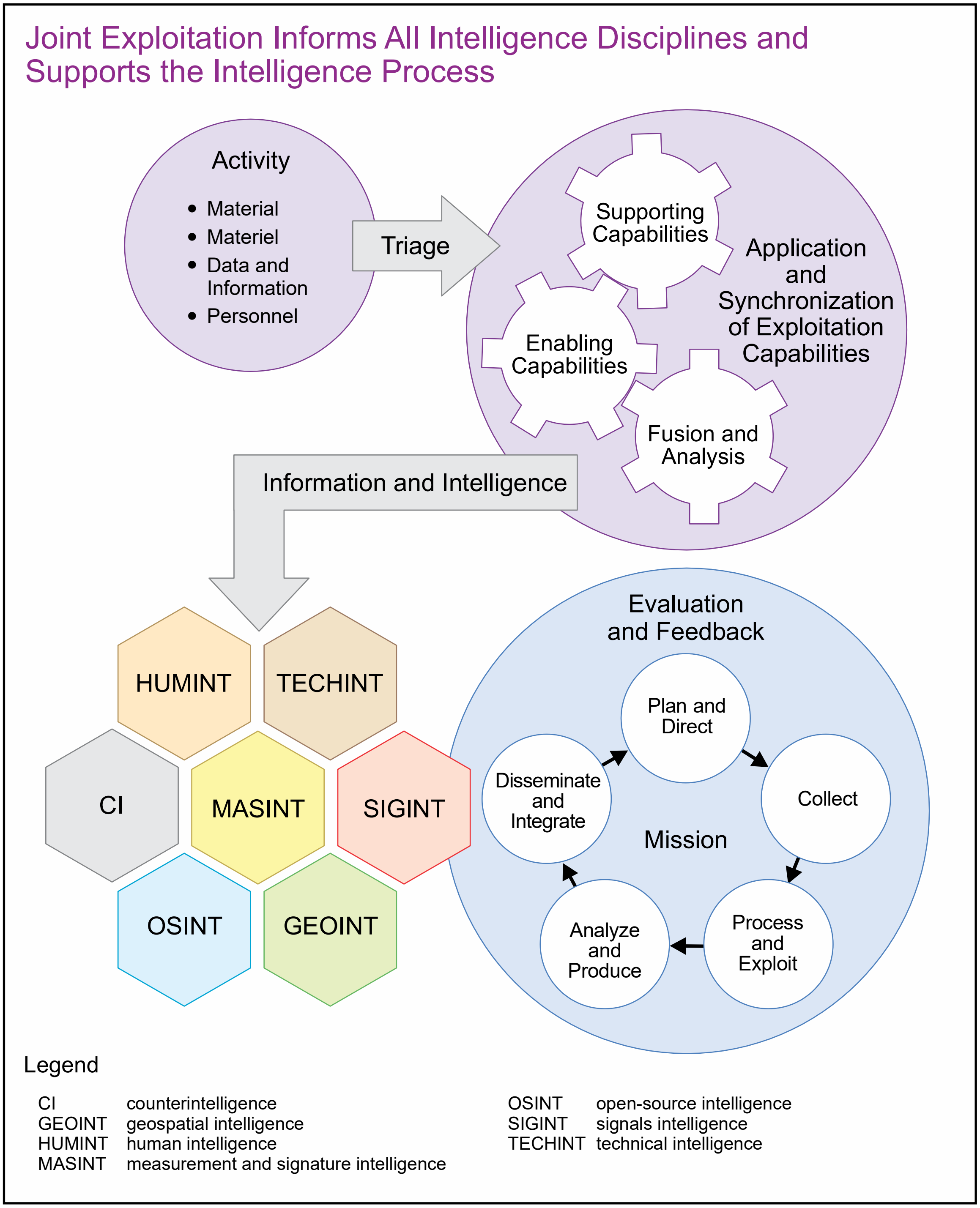
2. Joint Exploitation

a. Exploitation occurs across the competition continuum regardless of the level 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 [Figure E-2]).

b. Tactical exploitation delivers preliminary assessments and information about the devices and weapons employed and the people who employed them. Operational-level exploitation combines the outputs of tactical exploitation activities with more sophisticated exploitation results to inform all-source analysis. Operational-level exploitation can be conducted by deployed labs and provides detailed forensic and technical analysis of captured materials. When combined with all-source intelligence reporting, it supports detailed analysis of threat networks to inform subsequent joint targeting activities. In an irregular warfare environment, where the mission and time permit, commanders should routinely employ forensics-trained collection capabilities in their operations to take advantage of battlefield opportunities.

(1) Tactical exploitation begins at the point of collection. The point of collection includes turnover of material from host-nation government or civilian personnel; material and information discovered during a maritime interception operation; cache discovery; raid; small, unmanned aircraft system; or IED incident or post-blast site. These activities focus on gathering all relevant information and material and include limited field exploitation of that material, as well as tactical questioning of any detained personnel to meet the immediate needs of tactical units. It informs recommendations for immediate adjustment to friendly TTP and can provide information to support immediate targeting of individuals or activities associated with local threat networks.

(2) Operational-level exploitation employs technical and forensic examination techniques of collected data and material and is conducted by highly trained examiners in expeditionary or reachback exploitation facilities. Information derived from operational exploitation supports operational activities including, but not limited to, targeting, intelligence operations, force TTP enhancements, force protection initiatives, and regional activities to affect network supply sources/chains. Field/tactical collection assets conduct



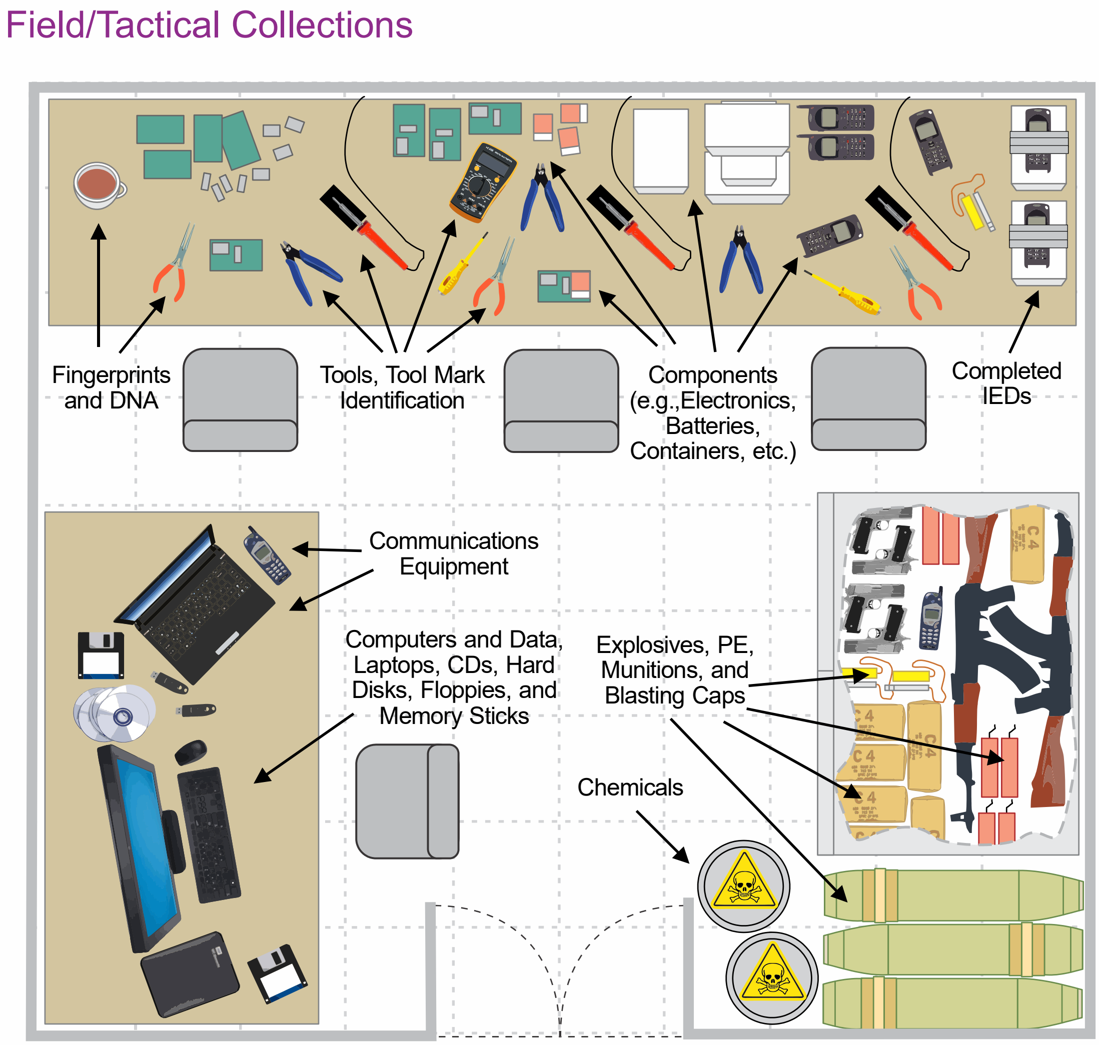
Joint Exploitation Informs All Intelligence Disciplines and Supports the Intelligence Process

Legend

CI	counterintelligence
GEOINT	geospatial intelligence
HUMINT	human intelligence
MASINT	measurement and signature intelligence
OSINT	open-source intelligence
SIGINT	signals intelligence
TECHINT	technical intelligence

Figure E-2. Joint Exploitation Informs All Intelligence Disciplines and Supports the Intelligence Process

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); and adequately document the site using photography, video, and sketching. (See Figure E-3.)


Field/Tactical Collections
Fingerprints and DNA
Tools, Tool Mark Identification
Components (e.g.,Electronics, Batteries, Containers, etc.)
Completed IEDs
Communications Equipment
Computers and Data, Laptops, CDs, Hard Disks, Floppies, and Memory Sticks
Explosives, PE, Munitions, and Blasting Caps
Chemicals
C 4

Legend

CD	compact disc	IED	improvised explosive device
DNA	deoxyribonucleic acid	PE	plastic explosive

Figure E-3. Field/Tactical Collections

c. Strategic exploitation informs theater- and national-level decision makers. A commander’s strategic exploitation assets may include forward-deployed or reachback JCMECs and exploitation labs capable of conducting formally accredited and/or highly sophisticated exploitation techniques. These assets can respond to theater strategic IRs and, when very specialized capabilities are leveraged, provide support to national requirements. Strategic theater- and national-level exploitation capabilities facilitate the synthesis of multidisciplinary scientific, forensic, financial, and commercial intelligence information that exceeds the capabilities and time constraints characteristic of expeditionary capabilities. Strategic exploitation is designed to support national strategy and policy development. Strategic requirements usually involve targeting of high-value or high-priority actors, force protection design improvement programs, and source interdiction programs designed to deny the enemy or adversary externally furnished resources. An example of this level of exploitation is electronic exploitation of conventional or improvised weapon material to determine how the electronic components of a device or component function, including switches for arming and firing and their relationship to other features of the weapon system, including the mechanical components.

d. Exploitation activities provide a progressively detailed multidisciplinary analysis of materials recovered from the OE. From the initial tactical evaluation at the point of collection to the operational forward deployed technical/forensic field laboratory and subsequent evaluation, the enterprise is designed to provide a timely, multidisciplinary analysis to support decision making at all echelons. Exploitation capabilities vary in scope and complexity, span the competition continuum, and can be applied during all joint operations. Support ranges from providing exploitation advice and assistance to a host nation during military engagement operations, to employing operational-level exploitation facilities during limited-contingency and large-scale operations, to supporting national-level requirements and activities.

3. Supporting the Intelligence Process

a. Within their operational areas, commanders are concerned with identifying competitors and systematically targeting enemies, addressing threats to force protection, denying enemies access to resources, and supporting the rule of law. Information derived from exploitation can provide specific information and actionable intelligence to address these concerns. Exploitation reporting provides specific information to help answer the CCIRs. Exploitation analysis is also used to inform the intelligence process by identifying specific individuals, locations, and activities that are of interest to the commander.

b. Exploitation products may inform follow-on intelligence collection and analysis activities. Exploitation products can facilitate a more refined analysis of the threat network's likely activities and can help identify threats and likely countermeasures in advance of any combat operations.

4. Planning Considerations

a. Exploitation supports all military operations and should be addressed early in and throughout 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 serves as a basis to determine the size and mix of capabilities required to support initial operations. 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 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 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 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.

(1) **J-2E.** During the planning process, the JFC should consider the need for exploitation support to help fulfill the requirements for information about the OE, identify potential threats to US forces, and understand the capabilities and capacity of the threat network. The J-2E is established as necessary to integrate and synchronize disparate theater-level military, intelligence, law enforcement, multinational, and host-nation collection and exploitation capabilities and processes. The J-2E (when organized) establishes policies and procedures for the coordination and synchronization of the exploitation of captured threat materials. The J-2E:

(a) Evaluates and establishes the commander's collection and exploitation requirements for deployed laboratory systems or material evacuation procedures based on the mission, its object and duration, threat faced, military geographic factors, and authorities granted to collect and process captured material.

(b) Ensures broad discoverability, accessibility, and usability of exploitation information at all levels to support force protection, targeting, material sourcing, signature characterization of enemy activities, and the provision of materials collected, transported, and accounted for with the fidelity necessary to support prosecution of captured insurgents or terrorists.

(c) Prepares collection plans for a subordinate exploitation task force responsible for finding and recovering battlefield materials.

(d) Provides direction to forces to ensure the initial site collection and exploitation activities are conducted to meet the commanders' requirements and address critical information and intelligence gaps.

(e) Ensures exploitation enablers are integrated and synchronized at all levels and their activities support collection on behalf of the commander's PIRs. Planning includes actions to:

1. Identify units and responsibilities.

2. Ensure exploitation requirements are included in the collection plan.

3. Define priorities and standard operating procedures for materiel recovery and exploitation.

4. Coordinate transportation for materiel.

5. Establish TECHINT points of contact at all levels to expedite dissemination.

6. Identify required augmentation skill sets and additional enablers.

(2) **Exploitation Task Force**

(a) As an alternative to using the JFC's staff to manage exploitation activities, the JFC can establish an exploitation task force, integrating tactical-level and operational-level organizations and streamlining communications under a single HQ whose total focus is on the exploitation effort. The task force construct is useful when a large number of exploitation assets have been deployed to support large-scale, long-duration operations. The organization and employment of the task force depends on the mission, the threat, and the available enabling forces. The task force is normally built around an appropriately augmented brigade-level HQ or its equivalent. In addition to controlling the subordinate organizations and battalions, the exploitation task force commander may exercise tactical control of the JFC's specialized collection and exploitation assets, as necessary. The combination of collection assets with specialized exploitation enablers allows the task force to conduct focused threat network analysis and targeting, provide direct support packages of exploitation enablers to higher HQs, and organize and conduct unit-level training programs.

(b) In establishing a task force to manage exploitation activities, the JFC normally aligns supporting resources to provide the task force commander with the means necessary to accomplish the mission. Under the task force construct, the exploitation task force provides task-organized teams of exploitation resources in direct support of the components. The components provide sustainment to the assigned exploitation team.

c. There may be significant sustainment requirements necessary to support joint exploitation activities. This may include the timely and safe storage and transportation of CEM and custody of personnel. Consideration is also given to transporting hazardous materials and to maintaining the chain of custody to maintain the integrity of CEM, 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.

5. Support to Site Exploitation

a. Site exploitation operations involve highly trained team members who have specific duties during the operation but should also be cross-trained so they can accomplish the mission if something happens to a team member. Regardless of whether conducting a deliberate or hasty site exploitation, prior planning is the key to success. Information collected is used for a variety of future missions but two important aspects of site exploitation are to properly record and preserve the evidence for future prosecutions.

b. Exploitation (forensic, technical, and mechanical) of physical materials is accomplished through a combination of forward-deployed and reachback resources to support the commander's operational requirements. The exact mix of exploitation resources depends on the threats identified by JIPOE, the JFC's mission, and the resources available from PNs. Commanders are concerned with identifying the members of and systematically targeting the threat network, addressing threats to force protection, denying threat actors access to resources, and supporting the rule of law. Information derived from exploitation can provide specific information and actionable intelligence to address these concerns. Exploitation capabilities employ a wide array of enabling capabilities and resources, from forward-deployed experts to small cells or teams providing scientific or technical support, interagency or partner laboratories, and centers of excellence providing real-time support via reachback. These exploitation capabilities can be employed individually to provide targeted support to distinct missions and/or functions or together in a modular format under a common C2 construct.

(1) Site exploitation teams are specifically detailed and trained to conduct systematic search and discovery operations and properly identify, document, and preserve items at the point of collection.

(2) Explosive ordnance disposal personnel have special training and equipment to render explosive ordnance safe, make intelligence reports on such ordnance, and supervise its safe removal. Explosive ordnance disposal personnel exploit an incident site, providing post-blast investigation expertise and site exploitation support, including a tactical characterization of the incident and a technical categorization of the device.

(3) Intelligence exploitation teams (IETs) are task-organized teams that exploit a site of intelligence value by collecting exploitation-related materials, performing tactical questioning, collecting forensic materials, preserving and documenting DOMEX, providing in-depth documentation of the site, evaluating the effects of threat weapons systems, and preparing material for evacuation.

(4) When WMD or hazardous chemical precursors may be present, CBRN response teams can be detailed to supervise the site exploitation. CBRN personnel are trained to properly recognize, preserve, neutralize, and collect hazardous chemical, explosive, or drug-related materials. The CBRN personnel have an integrated explosive ordnance disposal capability to mitigate CBRN threats. All site exploiters should be trained on WMD and precursor recognition should an exploitation uncover indicators of hazardous materials.

(5) United States Navy surface combatants and United States Marine Corps units employ visit, board, search, and seizure teams for detecting CBRN materials; collecting biometric and biographical information; conducting tactical questioning; and preserving and documenting captured enemy documents and media, including cellphones and contextual and electronic data for DOMEX. Marine Corps and Navy visit, board, search, and seizure teams can be augmented by IETs to facilitate HUMINT and tactical site exploitation activities. Where IEDs or explosive hazards are likely, explosive ordnance disposal and combined explosives exploitation cell (CEXC) platoons can be assigned to support the visit, board, search, and seizure missions.

(6) The United States Marine Corps and USSOCOM maintain deployable EACs to support tactical forensic exploitation requirements around the globe. Each EAC provides a tactical forensic capability with the necessary equipment and trained personnel to execute select tactical forensic exploitation activities in an expeditionary environment.

(7) The United States Army CCMD-level forensic exploitation laboratory is a full spectrum forensic laboratory accredited to International Organization for Standardization and FBI standards that provides a theater analytic capability in the forensic disciplines of DNA, latent print, firearms and toolmarks, and drug and explosive chemistry combined with intelligence analysis. This combined capability enhances all-source analysis and enables operational decision making. The United States Army also maintains and deploys forensic exploitation teams (FXTs) staffed by forensic scientists, who conduct confirmatory scientific testing when requested by a CCMD or JTF. FXTs provide an expeditionary forensic exploitation capability, including latent print examiners, DNA examiners, forensic chemists, firearms/tool mark examiners, electronic engineers, DOMEX personnel and support personnel from a modular pool, task-organized to meet mission requirements. An FXT can also be deployed modularly with other Service exploitation capabilities. FXTs support I2 and DoD law enforcement criminal intelligence analysis and production at all echelons with exploitation results that meet International Organization for Standardization accreditation standards, although their primary customers are tactical and operational commanders.

(8) CEXCs are a Naval Surface Warfare Center, Explosive Ordnance Disposal Technology Division deployable capability that is scalable in skills and size, allowing them to be tailored to meet the commander’s requirements, including incorporation of multinational and interagency partners. CEXC personnel are trained and equipped to conduct TECHINT operations involving recovered improvised weapons systems and provide NRT intelligence on their construction and employment. CEXC processes support I2 activities by identifying IED trends and bomb makers, providing insights into enemy tactics, and assisting in the development of defensive and offensive counter-IED and other improvised weapons defeat measures. CEXC supports I2 and DoD law enforcement criminal intelligence analysis and production at all echelons, although its primary customers are tactical and operational commanders.

(9) The FBI’s TEDAC is the final strategic-level exploitation facility and final disposition repository for all IED material, once all DoD investigation and exploitation requirements are complete. The TEDAC serves as the single interagency organization to receive, fully analyze, exploit, and provide a repository for all terrorist IEDs of interest to the United States. The TEDAC coordinates efforts of the entire government, including law enforcement, intelligence, and military, to gather and share intelligence about these devices. TEDAC provides direct support to broader USG efforts to prevent and mitigate IED attacks by performing advanced exploitation of IEDs through physical examination, resulting in S&T information and valuable intelligence. Through its integration of intelligence resources, the TEDAC also provides expeditious reporting of raw and finished intelligence to intelligence and law enforcement partners about device attributes and terrorist TTP to enhance knowledge and understanding of current and future threats.

APPENDIX F
TARGET INTELLIGENCE

1. Overview

Target intelligence is all-source intelligence that reveals vulnerabilities in enemy target systems and targets, describes a target's characterization and location, indicates a target's vulnerabilities and relative importance to the enemy, 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 through analysis and preparation of products in support of known or anticipated user requirements (e.g., 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

a. 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.

(1) **Inherent.** When assigned objectives within an operational area, 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.

(a) CCMDs that are assigned AORs in the *Unified Command Plan* and objectives in the GCP and JSCP produce target intelligence related to defeating the identified adversaries within their AOR.

(b) 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 fulfills target intelligence production responsibilities, either organically or through further reachback, while evaluating whether it is appropriate and feasible to enable the subordinate joint force to become self-sufficient.

(c) Joint forces with inherent target intelligence production responsibilities may task subordinate organizations with explicit target intelligence production responsibilities.

(2) **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., appendix 4 [Target Intelligence] to annex B [Intelligence]). 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.

b. 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.

c. 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 F-1).

3. Target Intelligence and the Joint Targeting Cycle

a. Target intelligence guidance, products, and TM for joint fires are located throughout the joint targeting cycle.

The Relationship Between Data, Information, and Intelligence Within Target Intelligence

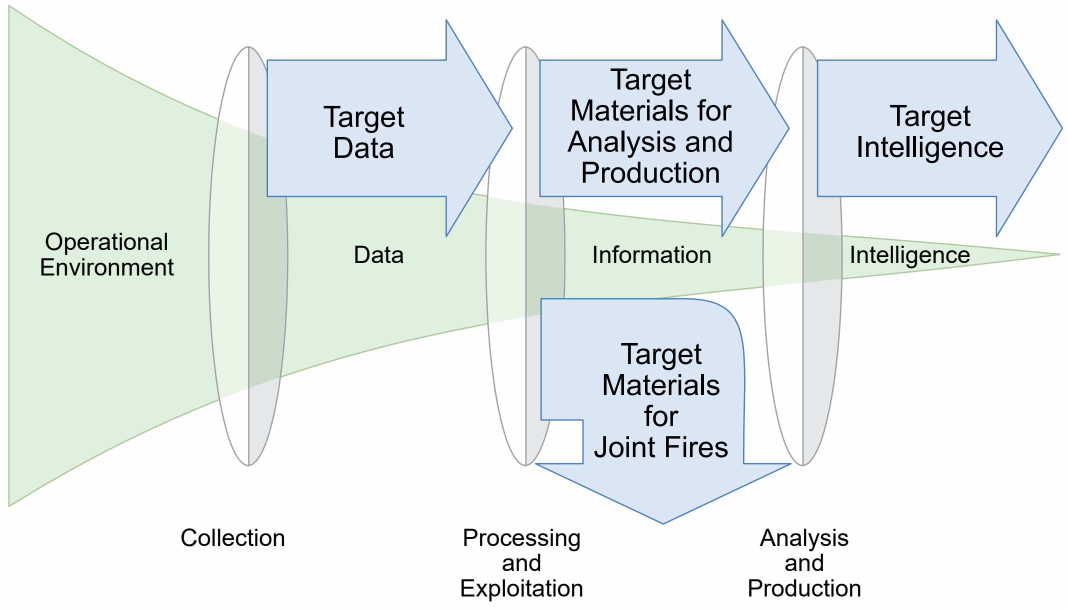


Figure F-1. The Relationship Between Data, Information, and Intelligence Within Target Intelligence

(1) Phase 1. Commander's Objectives, Targeting Guidance, and Intent: It articulates the commander's desired end state, objectives, guidance, and intent. The JFC develops and issues targeting guidance.

(2) Phase 2. Target Development and Prioritization: TSA, ETFs, some target lists.

(3) Phase 3. Capabilities Analysis: The desired effect of engaging the target at the target element level is defined, and the undesired effects (e.g., collateral damage) of that particular target engagement method are estimated.

(4) Phase 4. Commander's Decision and Force Assignment: It is primarily an operations function but requires considerable intelligence support to ensure intelligence CRs are validated and sufficient intelligence collection assets are made available and properly integrated into the plan.

(5) Phase 5. Mission Planning and Force Execution: Any TM depicting the location of a non-facility target.

(6) Phase 6. Combat Assessment: BDA, TM for joint fires, RR.

b. Joint 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, joint 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. TSA documents the hierarchical and functional relationships of the components and entities that give an enemy a particular capability to wage war. TSAs include (not all-inclusive) targeting strategies; critical factors analysis, to include a systemic and network analysis; HVTs; and high-payoff targets. The value of thorough and updated TSA production cannot be overstated; one of the most frequent targeting-related deficiencies reported is insufficiency of TSA production.

See JP 3-60, Joint Targeting, *for more information on TSA.*

c. **ETF.** An ETF is 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 can include input from operations, plans, advisors, 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. Identifiers for a target are an alphanumeric convention that can be assigned to entities for the purposes of unique identification. One example of an entity identifier is the widely recognized basic encyclopedia numbering system. Currently, many C2 systems can accommodate current standards for target numbering (basic encyclopedias, unit identifiers, and candidate target identifiers) as defined by DIA and the IC.

See JP 3-60, Joint Targeting, *for more information on ETFs.*

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, target development nomination list, joint target list, restricted target list) are joint 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 joint target intelligence products.

e. **CA.** The determination of the overall effectiveness of force employment during military operations. The CA phase is a continuous process that assesses the effectiveness of the activities that occurred during the first five phases of the joint targeting cycle. The CA process helps the commander and staff determine if the ends, ways, and means of joint targeting have resulted in progress toward accomplishing a task, creating an effect, or achieving an objective. CA occurs at the tactical, operational, and strategic levels of warfare. The assessment of target engagement results must be integrated to provide the overall joint CA.

See JP 3-60, Joint Targeting, *and CJCSI 3162.01,* Methodology for Combat Assessment, *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 targeting and/or fires personnel use the input to conduct the CDE methodology.

d. **Target imagery analysis for collateral effects 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 the level of collateral effects 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 targeting and/or 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 joint target requires another engagement to achieve the desired level of functional damage or other effect IAW the commander's intent. Joint fires personnel use the input in their reattack decision.

6. Target Intelligence and Intelligence Support to Joint Targeting

Target intelligence is a subset of intelligence support to joint targeting. While target intelligence is a discrete set of products and TM, intelligence professionals ensure those products are integrated into the joint targeting cycle. Therefore, intelligence support to targeting is target intelligence production plus the intelligence activities required to enable production of target intelligence and to integrate target intelligence into the joint targeting cycle.

Intentionally Blank

APPENDIX G
SECURITY OF CLASSIFIED MATERIAL

1. Overview

a. Security policy 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, as well as IRs that, in turn, have OPSEC implications. All intelligence operations depend 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 during multinational operation, the J-2 continues to maintain and enforce thorough effective security procedures.

b. The J-2 makes a major contribution to the success of operational missions through 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.

c. Although the responsibility of the originating agency, J-2 can assist by ensuring all guidance, especially plans and orders, include classification guidance as part of the plan or order.

For more information regarding personnel security, refer to DoDM 5200.02, DoD Procedures for the Personnel Security Program (PSP).

2. Sensitive Compartmented Information Facility

Before SCI can be handled, processed, or stored, a SCIF is 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 DoDM 5105.21, *Sensitive Compartmented Information (SCI) Administrative Security Manual.*

For information on establishing and accrediting a tactical SCIF, refer to DoDM 5105.21, Volume 2, Sensitive Compartmented Information Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security.

3. 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 United States. US national interests require that foreign governments provide US classified information with a degree of security protection comparable to what it would receive while under US control. There are a number of international and bilateral security agreements in effect to ensure this. When restrictive dissemination controls are applied to intelligence information, originators shall separate sources, methods, and activities content from the substantive classified intelligence information as appropriate using tear lines, write for release, or other sanitization methods. In these cases, when authorized by the Military Intelligence Disclosure Policy Committee as exceptions to policy, a balance is sought between US national interests and the security of the classified information.

For additional information on sanitizing and/or releasing intelligence, refer to NDP-1, National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations.

4. 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 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 with 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.

APPENDIX H
INTELLIGENCE DIRECTORATE OF A JOINT STAFF PLANNING 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. 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 to planning. In many cases, an OPLAN or CONPLAN may already exist and require modification, but often a crisis is unanticipated and contingency plans are developed in the days or months before military action. Intelligences includes the following:

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

See Joint Guide for 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,* Planning and Execution Formats and Guidance, *for more information on the commander's estimate.*

(3) Prepare annex B (Intelligence) and all necessary appendices to the commander's operations plan or concept plan, as required (refer to CJCSM 3130.03, *Planning and Execution Formats and Guidance*). Identify 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 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, down to EEIs and indicator level of detail. PIRs should be tied to the CCDR decision points and plan objectives. Once PIRs/EEIs/indicators are prepared in draft, J-2 personnel should develop detailed CRMx and PRMx.

c. Produce an ISR CONOPS in coordination with the joint force J-3. Disseminate general collection priorities and requirements for subordinate joint force support and

CONDUCT INTELLIGENCE PLANNING

- **Establish missions and/or tasks**
- **Identify support needed**
  - **Intelligence services and products**
  - **Personnel**
  - **Logistics**
  - **GI&S support**
  - **METOC support**
  - **MASINT support**
  - **DOMEX support**
- **Establish a forward JIOC or JISE**
- **Intelligence collection management**
  - **CI and HUMINT collection**
  - **GEOINT collection**
  - **SIGINT collection**
  - **MASINT collection**
- **Intelligence production management**
- **Communications system support (for subordinate joint force intelligence)**
- **Multinational interaction**
- **CI**
- **Security**

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. The ISR CONOPS should include the equities of all the joint functions that require intelligence support.

(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 an 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) Coordinate with USTRANSCOM to determine vulnerabilities impacting the movement of intelligence assets.

(7) Implement and enforce procedures for requesting sensitive 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 United States Government.* All intelligence and other USG departments and agencies affected by or involved with sensitive support should also be kept informed.

d. Establish effective external liaison relationships with required national and DoD intelligence elements, interagency partners, and multinational entities.

(1) Coordinate with USSPACECOM and USSF for space support.

(2) Coordinate with USCYBERCOM via the assigned CO-IPE and the JIOC directly, as appropriate, for augmentation support to CO and planning.

(3) Coordinate through with the Joint Staff and the Joint Information Operations Warfare Center for OIE expertise.

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

(5) Coordinate with USSTRATCOM and its Joint Electromagnetic Warfare Center for joint EMS operations reachback expertise.

(6) Coordinate through the CCMD JEMSOC for JEMSO support.

(7) Coordinate with USSPACECOM and the Joint Navigation Warfare Center for navigation warfare expertise.

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

e. 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. Plan for and coordinate with NJOIC, JS J-2, and/or DIA for formation of an ITF if the situation/crisis warrants, and to establish processes, procedures, and interface during periods of increased warning.

(2) If required, request Tactical Exploitation of National Capabilities Program (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 NCMI.

f. 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) Provide the JEMSOC with prioritized EMS-use requirements for intelligence operations and collection, to include joint restricted frequency list (JRFL) inputs and collections plans. Coordinate a JRFL with the command, joint frequency management office (if not incorporated in the JEMSOC), J-2, J-3, 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.

g. 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 other nations 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 CRs 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 GFM processes. Obtain waivers for release of appropriate levels of intelligence to multinational partners, if required.

h. Review facility security requirements. Prepare request(s) for accreditation of facilities, if required. Refer to Appendix G, "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 coordinates with the CCMD J-2 and begins 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, to include the interrelationship with the ITF (if established). 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 and coordinate other intelligence-related functions with appropriate staff elements and subordinate and supporting commands. Specific responsibilities include, but are not limited to, the following:

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

(2) Joint fires element (J-3).

(3) Counterproliferation (J-3).

(4) CI (J-2).

(5) Personnel recovery (J-3).

(6) CT (J-3).

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

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

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

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

(11) Transportation intelligence (USTRANSCOM/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, ETF production, target list management, and BDA.

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

(15) CMO (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) METOC officer.

(21) Blue force SA and combat identification requirements (J-3).

(22) Civilian environment team.

(23) Analysis of the OE.

(24) Space domain awareness (USSPACECOM LNO, J-3/J-5).

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 planning and analysis and may hinder operations during execution. 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) Appoint a single GI&S POC per CJCSI 3901.01, *Requirements for Geospatial Information and Services*. 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 GI to multinational forces.

(5) Verify and/or submit GI&S requirements detailed in appendix 7 (Geospatial Intelligence) 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 (e.g., assisting in collection management, helping to anticipate enemy 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/established to support the subordinate joint force. Establishment of a JIOC/JISE is theater and/or situation dependent.

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

b. 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 coordination board, information cell, collection management board, provisional reconstruction team, and CMO 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, information, cyberspace, space, EMS, missile, and terrorism analysis.

3. Regional/sociocultural/psychological subject matter experts.

4. JIPOE production cell.

5. Collection management liaison.

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

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 CRs are identified as early as possible.

b. Develop and publish intelligence CRs. 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 CRs 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 all assigned and attached HUMINT and CI collection capabilities, within the operational area.

(2) Determine the need for a JIDC to conduct joint interrogation operations, a JCMEC, and JDEC (see Appendix D, "Intelligence Applications") 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) Request 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 coordinate requirements via echelon CRM/COM. Refine key intelligence questions and EEIs for which collection should resolve.

(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. To satisfy the intelligence need, NGA source strategies analysts collaborate with customers to develop comprehensive collection strategies utilizing all available GEOINT sensors. This strategic approach includes the use of automation techniques in intelligence data modeling through coordination with automated strategy managers.

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 SSTO.

(2) Establish the need for and request further MASINT collection augmentation and support from the Services and the DIA Science and Technology 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 and should be linked to actual or anticipated commander's decisions.

(1) As needed, in concert with J-3 and theater JIOC, tailor PIRs for the current situation, synchronizing them in time and ensuring they align with anticipated commander's decisions.

(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 the *Joint Guide for 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, to include a network analysis, 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) 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 CT plans.

b. The counterintelligence coordinating authority (CICA), through the J-2X, should recommend to the J-2, or JFC, appointment of the task force CICA 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 to provide critical threat/vulnerability assessments as necessary.

Additional information on CI can be found in classified Appendix C, "(U) Classified Appendix on Joint Intelligence (Counterintelligence and Human Intelligence/Department of Defense Cover)."

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.

Intentionally Blank

APPENDIX J
REFERENCES

The development of JP 2-0 is based upon the following primary references.

1. General

a. National Security Act of 1947, as amended.

b. The Privacy Act (Title 5, USC, Section 552a).

c. Title 10, USC.

d. Title 18, USC.

e. Title 50, USC.

f. *Intelligence Reform and Terrorism Prevention Act of 2004, as amended.*

g. *2017 National Security Strategy of the United States of America.*

h. *National Military Strategy of the United States of America, 2018.*

i. *National Strategy to Combat Weapons of Mass Destruction.*

j. *National Strategy for Homeland Security.*

k. *National Strategy for Counterterrorism of the United States.*

l. *National Intelligence Strategy of the United States of America, 2019.*

m. *Defense Intelligence Strategy.*

n. Executive Order 12333, *United States Intelligence Activities,* as amended.

o. Executive Order 12958, *Classified National Security Information.*

p. NDP-1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations.*

q. ICD 203, *Analytic Standards.*

r. ICD 302, *Document and Media Exploitation.*

s. ICD 403, *Foreign Disclosure and Release of Classified National Intelligence.*

t. ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*

u. ICD 705, *Sensitive Compartmented Information Facilities.*

v. ICS 705-1, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities.*

w. ICS 705-2, *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information.*

x. National Security Presidential Directive (NSPD)-59/Homeland Security Presidential Directive (HSPD)-24, *Biometrics for Identification and Screening to Enhance National Security*.

y. HSPD-6, *Integration and Use of Screening Information to Protect Against Terrorism.*

z. NSPD-33/HSPD-10, *Biodefense for the 21st Century.*

2. Department of Defense Publications

a. DoDD 2311.01, *DoD Law of War Program.*

b. DoDD 3000.06, *Combat Support Agencies (CSAs).*

c. DoDD 3000.07, *Irregular Warfare (IW).*

d. DoDD 3025.18, *Defense Support of Civil Authorities (DSCA)*.

e. DoDD 3115.09, *(U) DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning.*

f. DoDD 3300.03, *DoD Document and Media Exploitation (DOMEX).*

g. DoDD S-3325.09, *(U) Oversight Management, and Execution of Defense Clandestine Source Operations.*

h. DoDD 3600.01, *Information Operations (IO).*

i. DoDD 5100.01, *Functions of the Department of Defense and Its Major Components.*

j. DoDD 5100.03, *Support of the Headquarters of Combatant and Subordinate Unified Commands.*

k. DoDD 5100.20, *National Security Agency/Central Security Service (NSA/CSS).*

l. DoDD 5105.21, *Defense Intelligence Agency (DIA).*

m. DoDD 5105.23, *National Reconnaissance Office.*

n. DoDD 5105.60, *National Geospatial-Intelligence Agency (NGA).*

o. DoDD 5143.01, *Undersecretary of Defense for Intelligence and Security (USD[I&S]).*

p. DoDD 5148.13, *Intelligence Oversight.*

q. DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense.*

r. DoDD S-5200.37, *(U) Management and Execution of Defense HUMINT.*

s. DoDD 5205.12, *Military Intelligence Program (MIP).*

t. DoDD 5205.14, *DoD Counter Threat Finance (CTF) Policy.*

u. DoDD 5205.15E, *DoD Forensic Enterprise (DFE).*

v. DoDD S-5210.36, *(U) Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the United States Government.*

w. DoDD 5240.01, *DoD Intelligence Activities.*

x. DoDD 5240.02, *Counterintelligence (CI).*

y. DoDD 8521.01E, *DoD Biometrics.*

z. DoDI 3000.17, *Civilian Harm Mitigation and Response.*

aa. DoDI 3025.21, *Defense Support of Civilian Law Enforcement Agencies*.

bb. DoDI O-3115.07, *Signals Intelligence (SIGINT).*

cc. DoDI 3115.10E, *Intelligence Support to Personnel Recovery.*

dd. DoDI 3115.17, *Management and Oversight of DoD All-Source Analysis.*

ee. DoDI O-3300.04, *Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI).*

ff. DoDI 5105.58, *Measurement and Signature Intelligence (MASINT).*

gg. DoDI 5200.48, *Controlled Unclassified Information (CUI).*

hh. DoDI S-5205.01, *(U) DoD Foreign Military Intelligence Collection Activities (FORMICA).*

ii. DoDI O-5240.10, *Counterintelligence (CI) in the DoD Components.*

jj. DoDI, 5505.14, *Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, Law Enforcement, Corrections, and Commanders.*

kk. DoDI 5525.18, *Law Enforcement Criminal Intelligence (CRIMINT) in DoD.*

ll. DoDI 6420.01, *National Center for Medical Intelligence (NMCI).*

mm. DoDI 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD.*

nn. DoDM 5105.21, *Volume 1, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security.*

oo. DoDM 5105.21, *Volume 2, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security.*

pp. DoDM 5105.21, *Volume 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities.*

qq. DoDM 5200.01, *DoD Information Security Program, Volumes 1-3.*

rr. DoDM 5200.02, *Procedures for the DoD Personnel Security Program (PSP).*

ss. DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities.*

tt. DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*.

uu. DoD 5400.11-R, *Department of Defense Privacy Program.*

vv. DHE-M 3301.001, *(U) Defense Human Intelligence (HUMINT) Enterprise Manual, Volume I: Collection Requirements, Reporting, and Evaluation Procedures*.

ww. DHE-M 3301.002, *(U) Defense Human Intelligence (HUMNINT) Enterprise Manual, Volume II: Collection Operations.*

3. Chairman of the Joint Chiefs of Staff Publications

a. JP 1, Volume 1, *Joint Warfighting.*

b. JP 1-0, *Joint Personnel Support.*

c. JP 3-0, *Joint Campaigns and Operations.*

d. JP 3-05, *Joint Doctrine for Special Operations.*

e. JP 3-06, *Joint Urban Operations.*

f. JP 3-08, *Interorganizational Cooperation.*

g. JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments.*

h. JP 3-12, *Cyberspace Operations.*

i. JP 3-13.2, *Military Information Support Operations.*

j. JP 3-14, *Space Operations.*

k. JP 3-16, *Multinational Operations.*

l. JP 3-24, *Counterinsurgency.*

m. JP 3-27, *Homeland Defense.*

n. JP 3-28, *Defense Support of Civil Authorities.*

o. JP 3-29, *Foreign Humanitarian Assistance.*

p. JP 3-33, *Joint Force Headquarters.*

q. JP 3-40, *Joint Countering Weapons of Mass Destruction.*

r. JP 3-50, *Personnel Recovery.*

s. JP 3-57, *Civil-Military Operations.*

t. JP 3-59, *Meteorological and Oceanographic Operations.*

u. JP 3-60, *Joint Targeting.*

v. JP 3-85, *Joint Electromagnetic Spectrum Operations.*

w. JP 5-0, *Joint Planning.*

x. JP 6-0, *Joint Communications System.*

y. CJCSI 1301.01F, *Joint Individual Augmentation Procedures.*

z. CJCSI 3110.01K, *(U) 2018 Joint Strategic Capabilities Plan (JSCP).*

aa. CJCSI 3110.02H, *Intelligence Planning, Objectives, Guidance, and Tasks.*

bb. CJCSI 3150.25G, *Joint Lessons Learned Program.*

cc. CJCSI 3162.02, *Methodology for Combat Assessment.*

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

ee. CJCSI 3340.02B, *Joint Enterprise Integration of Warfighter Intelligence.*

ff. CJCSI 3370.01C, *Target Development Standards.*

gg. CJCSI 3505.01D, *Target Coordinate Mensuration Certification and Program Accreditation.*

hh. CJCSI 5120.02E, *Joint Doctrine Development System.*

ii. CJCSI 5221.01E, *Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations.*

jj. CJCSM 3130.03A, *Planning and Execution Formats and Guidance.*

kk. CJCSM 3150.25B, *Joint Lessons Learned Program.*

ll. CJCSM 3314.01A, *Intelligence Planning.*

4. Multi-Service Publication

ATP 3-55.3/MCRP 2-10A/NTTP 2-01.3/AFTTP 3-2.88, *Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization.*

APPENDIX K
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication using the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

a. The lead agent and the Joint Staff doctrine sponsor for this publication is the Director for Intelligence (J-2).

b. The following staff, in conjunction with the joint doctrine development community, made a valuable contribution to the revision of this joint publication: lead agent, Mr. Sean Murphy, Joint Staff J-2; Joint Staff doctrine sponsor, Mr. Sean Murphy, Joint Staff J-2; Mr. Alan Armistead and Mr. Mark Brown, Joint Doctrine Analysis Branch; and LTC Joshua Darling and Mr. George Katsos, Joint Staff J-7, Joint Doctrine Branch.

3. Supersession

This publication supersedes JP 2-0, *Joint Intelligence,* 26 May 2022; JP 2-01, *Joint and National Intelligence Support to Military Operations,* 06 April 2016; JP 2-01.2, *(U) Counterintelligence and Human Intelligence in Joint Operation,* 06 April 2016; JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment,* 21 May 2014; and JP 2-03, *Geospatial Intelligence in Joint Operations*, 5 July 2017.

4. Change Recommendations

a. To provide recommendations for urgent and/or routine changes to this publication, please complete the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil.

b. 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 observations, best practices, and 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 insights and lessons learned derived from operations, exercises, war games, and other events. As these inputs are incorporated into joint doctrine, they become institutionalized for future use, a major goal of the JLLP. Insights and lessons learned are routinely sought and incorporated into draft JPs throughout formal staffing of the development process. The JLLIS Web site can be found at https://www.jllis.mil (NIPRNET) or https://www.jllis.smil.mil (SIPRNET).

6. Releasability

LIMITED. This JP is approved for limited release. The authors of this publication have concluded that information in this publication should be disseminated on an as-needed basis and is limited to common access cardholders. Requests for distribution to noncommon access cardholders should be directed to the Joint Staff J-7.

7. Printing and Distribution

Before distributing this JP, please e-mail the Joint Staff J-7, Joint Doctrine Branch, at js.pentagon.j7.mbx.jedd-support@mail.mil, or call 703-692-7273/DSN 692-7273, or contact the lead agent or Joint Staff doctrine sponsor.

a. The Joint Staff does not print hard copies of JPs for distribution. An electronic version of this JP is available on:

(1) NIPRNET Joint Electronic Library Plus (JEL+) at https://jdeis.js.mil/jdeis/index.jsp (limited to .mil and .gov users with a DoD common access card) and

(2) SIPRNET JEL+ at https://jdeis.js.smil.mil/jdeis/index.jsp.

b. Access to this unclassified publication is limited. This JP can be locally reproduced for use within the combatant commands, Services, National Guard Bureau, Joint Staff, and combat support agencies. However, reproduction authorization for this JP must be IAW lead agent/Joint Staff doctrine sponsor guidance.

GLOSSARY

PART I—SHORTENED WORD FORMS (ABBREVIATIONS, ACRONYMS, AND INITIALISMS)

ABIS	Department of Defense Automated Biometric Identification System
AF/A2/6	Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance and Cyber Effects Operations
AFTTP	Air Force tactics, techniques, and procedures
AOI	area of interest
AOR	area of responsibility
ATP	Army techniques publication
ATSD(IO)	Assistant to the Secretary of Defense for Intelligence Oversight
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
C5ISR	command, control, communications, computers, cyber, intelligence, surveillance, and reconnaissance
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
CCP	combatant command campaign plan
CDA	collateral damage assessment
CDE	collateral damage estimation
CEM	collected exploitable material
CENTRIXS	Combined Enterprise Regional Information Exchange System
CEXC	combined explosives exploitation cell
CI	counterintelligence
CIA	Central Intelligence Agency
CIP	common intelligence picture
CIPCS	common intelligence picture correlation site
CIPFC	common intelligence picture fusion cell
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
CJTF	commander, joint task force
C-JWICS	Containerized Joint Worldwide Intelligence Communications System
CMA	collection management authority
CMO	civil-military operations
CO	cyberspace operations
COA	course of action
COG	center of gravity
COIN	counterinsurgency
COLISEUM	community on-line intelligence system for end-users and managers
COM	collection operations management
COMINT	communications intelligence
CONOPS	concept of operations
COP	common operational picture
CR	collection requirement
CRM	collection requirements management
CRMx	collection requirements matrix
CSA	combat support agency
CT	counterterrorism
CTP	common tactical picture

DCGS	distributed common ground/surface system
DCME	Defense Collection Management Enterprise
DCO	defense coordinating officer
DEA	Drug Enforcement Administration (DOJ)
DFBA	Defense Forensics and Biometrics Agency
DFSC	Defense Forensics Science Center
DHE-M	Defense Human Intelligence Enterprise manual
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
DNA	deoxyribonucleic acid
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
DONISIS	Department of the Navy Identification and Screening Information System

DOS	Department of State
DPM	dissemination program manager
DSCA	defense support of civil authorities
DTA	dynamic threat assessment
DTRA	Defense Threat Reduction Agency

EAC	exploitation analysis center
EEI	essential element of information
ELINT	electronic intelligence
EMS	electromagnetic spectrum
EO	electro-optical
EOC	emergency operations center
EPW	enemy prisoner of war
ETF	electronic target folder
EXU-1	Expeditionary Exploitation Unit One (USN)

F3EAD	find, fix, finish, exploit, analyze, and disseminate
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
FRAGORD	fragmentary order
FXT	forensic exploitation team

GCCS	Global Command and Control System
GCCS-I3	Global Command and Control System-Integrated Imagery and Intelligence
GCCS-J	Global Command and Control System-Joint
GCP	global campaign plan
GEOINT	geospatial intelligence
GFM	global force management
GI	geospatial information
GI&S	geospatial information and services
GIMS	Geospatial Intelligence Information Management Services
GMI	general military intelligence

HD	homeland defense
HQ	headquarters
HQMC	Headquarters, United States Marine Corps
HSI	hyperspectral imagery
HSIN	Homeland Security Information Network (DHS)
HSPD	homeland security Presidential directive
HUMINT	human intelligence
HVT	high-value target

I2	identity intelligence
I2D	Identity Intelligence Division (USD[I&S])
I2SP	identity intelligence support packet
I2WD	Intelligence and Information Warfare Directorate (USA)
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
ICPO-INTERPOL	International Criminal Police Organization-International Police
ICS	intelligence community standard
IDENT	Automated Biometric Identification System (DHS)
IDS	Identity Dominance System (USN)
IDS-MC	Identity Dominance System-Marine Corps
IE	information environment
IED	improvised explosive device
IET	intelligence exploitation team
IIR	intelligence information report
IMINT	imagery intelligence
INSCOM	United States Army Intelligence and Security Command
IP	intelligence planning
IPT	intelligence planning team
IR	intelligence requirement
ISM	intelligence synchronization matrix
ISP	intelligence support plan
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
ITF	intelligence task force
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
JCS	Joint Chiefs of Staff
JCSE	Joint Communications Support Element (USTRANSCOM)
JDEC	joint document exploitation center

JDIS	Joint Deoxyribonucleic Acid Index System
JDISS	joint deployable intelligence support system
JEMSO	joint electromagnetic spectrum operations
JEMSOC	joint electromagnetic spectrum operations cell
JFC	joint force commander
JFO	joint field office
JIACG	joint interagency coordination group
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
JPG	joint planning group
JPP	joint planning process
JRC	joint reconnaissance center
JSPS	Joint Strategic Planning System
JTCB	joint targeting coordination board
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

MAGTF	Marine air-ground task force (USMC)
MARS	Machine-assisted Analytic Rapid-repository System (DIA)
MASINT	measurement and signature intelligence
MCRP	Marine Corps reference publication
MEA	munitions effectiveness assessment
MEF	Marine expeditionary force
METOC	meteorological and oceanographic
MIDB	modernized integrated database
MIP	military intelligence program
MOE	measure of effectiveness
MOP	measure of performance
MSI	multispectral imagery
MTO	mission-type order

NATO	North Atlantic Treaty Organization

NCB	national central bureau
NCIS	Naval Criminal Investigative Service
NCR	National Security Agency/Central Security Service representative
NDIS	National Deoxyribonucleic Acid Index System (FBI)
NDP	national disclosure policy
NG	National Guard
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
NGI	Next Generation Identification (FBI)
NGIC	National Ground Intelligence Center
NG JFHQ-State	National Guard joint force headquarters-state
NGO	nongovernmental organization
NIA	Navy Intelligence Activity
NIM	national intelligence manager
NIP	National Intelligence Program
NIPF	National Intelligence Priorities Framework
NIPRNET	Nonclassified Internet Protocol Router Network
NISP	national intelligence support plan
NJOIC	National Joint Operations and Intelligence Center
NMEC	National Media Exploitation Center
NMRS	National Measurement and Signature Intelligence Requirements System
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
NSPD	national security Presidential directive
NST	National Geospatial-Intelligence Agency support team
NTTP	Navy tactics, techniques, and procedures
OB	order of battle
OBP	object-based production
ODNI	Office of the Director of National Intelligence
OE	operational environment
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSCAR-MS	Open-Source Collection Acquisition Requirements Management System
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
PR	production requirement
PRMx	production requirements matrix
R&S	reconnaissance and surveillance
RATE	refine, adapt, terminate, execute
RF	radio frequency
RFF	request for forces
RFI	request for information
RR	reattack recommendation
S&T	scientific and technical
S&TI	scientific and technical intelligence
SA	situational awareness
SAR	synthetic aperture radar
SBU	sensitive but unclassified
SCA	sociocultural analysis
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SecDef	Secretary of Defense
SIGINT	signals intelligence
SIO	senior intelligence officer
SIOC	Strategic Information and Operations Center (FBI)
SIPRNET	SECRET Internet Protocol Router Network
SIR	specific information requirement
SOF	special operations forces
SOFEX	special operations forces exploitation
SOM	structured observation management
SSTO	senior science and technology officer
STA	sensor tasking authority
TASKORD	tasking order
TECHINT	technical intelligence
TEDAC	Terrorist Explosive Device Analytical Center (FBI)
TM	target materials
TSA	target system analysis
TTP	tactics, techniques, and procedures
UN	United Nations
US	United States
USAF	United States Air Force
US BICES	United States Battlefield Information Collection and Exploitation System

US BICES-X	United States Battlefield Information Collection and Exploitation System Extended
USC	United States Code
USCENTCOM	United States Central Command
USCG	United States Coast Guard
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USG	United States Government
USINDOPACOM	United States Indo-Pacific Command
USNORTHCOM	United States Northern Command
USSF	United States Space Force
USSOCOM	United States Special Operations Command
VTC	video teleconferencing
WAN	wide-area network
WMD	weapons of mass destruction
xCIE	xcampaign intelligence estimate

PART II—TERMS AND DEFINITIONS

1. JP 2-0, *Joint Intelligence,* 26 May 2022, Active Terms and Definitions

all-source intelligence. 1. Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that, in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (DoD Dictionary. Source: JP 2-0)

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 2-0)

application. 1. The system or problem to which a computer is applied. 2. In the intelligence context, the direct extraction and tailoring of information from an existing foundation of intelligence and near real time reporting. (DoD Dictionary. Source: JP 2-0)

backstop. An arrangement made to support a cover so inquiries about the cover will elicit responses that make the cover appear true. (DoD Dictionary. Source: JP 2-0)

basic encyclopedia. A compilation of identified installations and physical areas of potential significance as objectives for attack. (DoD Dictionary. Source: JP 2-0)

biometrics. The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (DoD Dictionary. Source: JP 2-0)

biometrics-enabled intelligence. The intelligence derived from the processing of biologic identity data and other all-source information concerning persons of interest. Also called **BEI.** (DoD Dictionary. Source: JP 2-0)

clandestine. Any activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy and concealment. (DoD Dictionary. Source: JP 2-0)

classification. The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. (DoD Dictionary. Source: JP 2-0)

classified information. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (DoD Dictionary. Source: JP 2-0)

collected exploitable material. All material and materiel in the possession of the Department of Defense, regardless of its classification or how it was obtained, that can be exploited in support of the Department of Defense and national interests. Also called **CEM.** (DoD Dictionary. Source: JP 2-0)

collection. In intelligence usage, the acquisition of information and the provision of this information to processing elements. (DoD Dictionary. Source: JP 2-0)

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 2-0)

collection asset. A collection system, platform, or capability that is supporting, assigned to, or attached to a particular commander. (DoD Dictionary. Source: JP 2-0)

collection management. In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (DoD Dictionary. Source: JP 2-0)

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 2-0)

collection operations management. The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. Also called **COM.** (DoD Dictionary. Source: JP 2-0)

collection plan. A systematic scheme to optimize the employment of all available collection capabilities and associated processing, exploitation, and dissemination resources to satisfy specific information requirements. (DoD Dictionary. Source: JP 2-0)

collection planning. A continuous process that coordinates and integrates the efforts of all collection units and agencies. (DoD Dictionary. Source: JP 2-0)

collection requirement. A valid need to close a specific gap in intelligence holdings in direct response to a request for information. (DoD Dictionary. Source: JP 2-0)

collection requirements management. The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in the direct tasking of requirements to units over which the commander has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. Also called **CRM.** (DoD Dictionary. Source: JP 2-0)

collection strategy. An analytical approach used by intelligence personnel to determine which intelligence disciplines can be applied to satisfy information requirements. (DoD Dictionary. Source: JP 2-0)

common intelligence picture. A single, identical display of relevant, instructive, and contextual intelligence information regarding enemy, adversary, and neutral force disposition, and supporting infrastructures derived from all sources at any level of classification, shared by more than one command, that facilitates collaborative planning and assists all echelons to enhance situational awareness and decision making. Also called **CIP.** (DoD Dictionary. Source: JP 2-0)

communications intelligence. Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called **COMINT.** (DoD Dictionary. Source: JP 2-0)

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, Vol 2) 2. In mapping, charting, and photogrammetry, a collective term for a system of marks or objects on the Earth, a map, or a photograph, whose positions or elevations (or both) have been or will be determined. (JP 2-0) 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. (DoD Dictionary. Source: JP 2-0)

counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. Also called **CI.** (DoD Dictionary. Source: JP 2-0)

counterintelligence operations. Proactive activities designed to identify, exploit, neutralize, or deter foreign intelligence collection and terrorist activities directed against the United States. (DoD Dictionary. Source: JP 2-0)

cover. In intelligence usage, the concealment of true identity or organizational affiliation with assertion of false information as part of, or in support of, official duties to carry out authorized activities and lawful operations. (DoD Dictionary. Source: JP 2-0)

critical information. Specific facts about friendly intentions, capabilities, and activities needed by an enemy or adversary for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (DoD Dictionary. Source: JP 2-0)

critical intelligence. Intelligence that is crucial and requires the immediate attention of the commander. (DoD Dictionary. Source: JP 2-0)

decision support template. A combined intelligence and operations graphic based on the results of wargaming that depicts decision points, timelines associated with movement of forces and the flow of the operation, and other key items of information required to execute a specific friendly course of action. Also called **DST.** (DoD Dictionary. Source: JP 2-0)

defense human intelligence executor. The senior Department of Defense intelligence official as designated by the head of each of the Department of Defense components who are authorized to conduct human intelligence and related intelligence activities. Also called **DHE.** (DoD Dictionary P. Source: JP 2-0)

Department of Defense Intelligence Information System. The combination of Department of Defense personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national-level decision makers. Also called **DoDIIS.** (DoD Dictionary. Source: JP 2-0)

detainee debriefing. The process of using direct questions to elicit intelligence information from a cooperative detainee to satisfy intelligence requirements. (DoD Dictionary. Source: JP 2-0)

dissemination. In intelligence usage, the delivery of intelligence to users in a suitable form. (DoD Dictionary. Source: JP 2-0)

dynamic threat assessment. A defense strategic intelligence assessment developed by the Defense Intelligence Agency to support combatant command planning. Also called **DTA.** (DoD Dictionary. Source: JP 2-0)

essential elements of information. The most critical information requirements regarding the enemy and/or adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence to assist in reaching a logical decision. Also called **EEIs.** (DoD Dictionary. Source: JP 2-0)

estimative intelligence. Intelligence that identifies and describes adversary capabilities and intentions, and forecasts the full range of alternative future situations in relative order of probability that may have implications for the development of national and military strategy, and planning and executing military operations. (DoD Dictionary. Source: JP 2-0)

event template. A guide for collection planning that depicts the named areas of interest where activity, or lack of activity, will indicate which course of action the enemy and/or adversary has adopted. (DoD Dictionary. Source: JP 2-0)

exploitation. 1. Taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already created. 2. Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. 3. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. (DoD Dictionary. Source: JP 2-0)

focused surveillance. Intelligence, surveillance, and reconnaissance coverage designed with overlapping sensors so as to give particular emphasis to a specific target. (DoD Dictionary. Source: JP 2-0)

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 aerospace, surface, and subsurface systems. Also called **FISINT.** (DoD Dictionary. Source: JP 2-0)

forensic-enabled intelligence. The intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest. Also called **FEI.** (DoD Dictionary. Source: JP 2-0)

general military intelligence. Intelligence concerning the military capabilities of foreign countries or organizations, or topics affecting potential United States or multinational military operations. Also called **GMI.** (DoD Dictionary. Source: JP 2-0)

geospatial information. Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on or about the Earth, including: data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geomatics data, and related products and services. Also called **GI.** (DoD Dictionary. Source: JP 2-0)

geospatial information and services. The collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the surface of the Earth. Also called **GI&S.** (DoD Dictionary. Source: JP 2-0)

geospatial intelligence. The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on or about the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. Also called **GEOINT.** (DoD Dictionary. Source: JP 2-0)

human factors. The physical, cultural, psychological, and behavioral attributes of an individual or group that influence perceptions, understanding, and interactions. (DoD Dictionary. Source: JP 2-0)

human intelligence. A category of intelligence derived from information collected and provided by human sources. Also called **HUMINT.** (DoD Dictionary. Source: JP 2-0)

hyperspectral imagery. Term used to describe the imagery derived from subdividing the electromagnetic spectrum into very narrow bandwidths allowing images useful in precise terrain or target analysis to be formed. Also called **HSI.** (DoD Dictionary. Source: JP 2-0)

identity intelligence. The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. Also called **I2.** (DoD Dictionary. Source: JP 2-0)

imagery. A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (DoD Dictionary. Source: JP 2-0)

imagery exploitation. The cycle of processing, using, interpreting, mensuration, and/or manipulating imagery, and any assembly or consolidation of the results for dissemination. (DoD Dictionary. Source: JP 2-0)

imagery intelligence. The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. Also called **IMINT.** (DoD Dictionary. Source: JP 2-0)

indications. In intelligence usage, information in various degrees of evaluation, all of which bear on the intention of an adversary or enemy to adopt or reject a course of action. (DoD Dictionary. Source: JP 2-0)

indicator. 1. In intelligence usage, an item of information that reflects the intention or capability of an enemy and/or adversary to adopt or reject a course of action. (JP 2-0) 2. In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (JP 3-13.3) 3. In the context of assessment, a specific piece of information that infers the condition, state, or existence of something, and provides a reliable means to ascertain performance or effectiveness. (JP 5-0) (DoD Dictionary. Source: JP 2-0)

information requirements. Those items of information regarding the relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (DoD Dictionary. Source: JP 2-0)

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. (DoD Dictionary. Source: JP 2-0)

intelligence. 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations conducting such activities. (DoD Dictionary. Source: JP 2-0)

intelligence asset. Any resource utilized by an intelligence organization for an operational support role. (DoD Dictionary. Source: JP 2-0)

intelligence community. All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. Also called **IC.** (DoD Dictionary. Source: JP 2-0)

intelligence discipline. A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. (DoD Dictionary. Source: JP 2-0)

intelligence estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (DoD Dictionary. Source: JP 2-0)

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. (DoD Dictionary. Source: JP 2-0)

intelligence information report. A formatted message utilized as the primary vehicle for providing human intelligence information to the customer via automated intelligence community databases. Also called **IIR.** (DoD Dictionary. Source: JP 2-0)

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 2-0)

intelligence planning. The intelligence component of the joint planning process that coordinates and integrates all available Defense Intelligence and Security Enterprise capabilities to meet combatant commander intelligence requirements. Also called **IP.** (DoD Dictionary. Source: JP 2-0)

intelligence process. The process by which information is converted into intelligence and made available to users. (DoD Dictionary. Source: JP 2-0)

intelligence production. The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements. (DoD Dictionary. Source: JP 2-0)

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 2-0)

intelligence requirement. 1. Any subject, general or specific, upon which there is a need for the collection of information or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. Also called **IR.** (DoD Dictionary. Source: JP 2-0)

intelligence source. The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. (DoD Dictionary. Source: JP 2-0)

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.** (DoD Dictionary. Source: JP 2-0)

intelligence, surveillance, and reconnaissance visualization. The capability to graphically display the current and future locations of collection platforms; their projected 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 2-0)

joint captured materiel exploitation center. An element responsible for deriving intelligence information from captured enemy materiel. Also called **JCMEC.** (DoD Dictionary. Source: JP 2-0)

joint deployable intelligence support system. A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called **JDISS.** (DoD Dictionary. Source: JP 2-0)

joint document exploitation center. An element 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. Source: JP 2-0)

joint intelligence. Intelligence produced by elements of more than one Service of the same nation. (DoD Dictionary. Source: JP 2-0)

joint intelligence architecture. A dynamic, flexible structure that consists of the Defense Joint Intelligence Operations Center, combatant command joint intelligence operations centers, and subordinate joint task force intelligence operations centers or joint intelligence support elements to provide national, theater, and tactical commanders with the full range of intelligence required for planning and conducting operations. (DoD Dictionary. Source: JP 2-0)

joint intelligence operations center. An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level that is integrated with national intelligence centers and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. Also called **JIOC.** (DoD Dictionary. Source: JP 2-0)

joint intelligence preparation of the operational environment. The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. Also called **JIPOE.** (DoD Dictionary. Source: JP 2-0)

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.** (DoD Dictionary. Source: JP 2-0)

joint interrogation and debriefing center. Physical location for the exploitation of intelligence information from detainees and other sources. Also called **JIDC.** (DoD Dictionary. Source: JP 2-0)

Joint Worldwide Intelligence Communications System. The sensitive compartmented information portion of the Defense Information Systems Network. Also called **JWICS.** (DoD Dictionary. Source: JP 2-0)

key terrain. Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant. (DoD Dictionary. Source: JP 2-0)

measurement and signature intelligence. Information produced by quantitative and qualitative analysis of physical attributes of targets and events to detect, characterize, locate, and identify targets and events; and derived from specialized, technically derived measurements and signatures of physical phenomenon intrinsic to an object or event. Also called **MASINT.** (DoD Dictionary. Source: JP 2-0)

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. (DoD Dictionary. Source: JP 2-0)

Military Intelligence Board. A decision-making forum which formulates Department of Defense intelligence policy and programming priorities. (DoD Dictionary. Source: JP 2-0)

Modernized Integrated Database. The national-level repository for the general military intelligence for 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 2-0)

modified combined obstacle overlay. A joint intelligence preparation of the operational environment product used to portray the militarily significant aspects of the operational environment, such as obstacles restricting military movement, key geography, and military objectives. Also called **MCOO.** (DoD Dictionary. Source: JP 2-0)

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.** (DoD Dictionary. Source: JP 2-0)

named area of interest. The geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected, usually to capture indications of enemy and adversary courses of action. Also called **NAI.** (DoD Dictionary. Source: JP 2-0)

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. (DoD Dictionary. Source: JP 2-0)

National 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 **NMRS.** (DoD Dictionary. Source: JP 2-0)

National System for Geospatial Intelligence. The combination of technology, policies, capabilities, doctrine, activities, people, data, and organizations necessary to produce geospatial intelligence in an integrated, multi-intelligence environment. Also called **NSG.** (DoD Dictionary. Source: JP 2-0)

need to know. A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties. (DoD Dictionary. Source: JP 2-0)

object-based production. The intelligence communities' framework for organizing and sharing information, relating data from all sources to known objects (e.g., units, people, locations, or events). Also called **OBP.** (DoD Dictionary. Source: JP 2-0)

open-source intelligence. Publicly available information collected, exploited, and disseminated to address a specific requirement. Also called **OSINT.** (DoD Dictionary. Source: JP 2-0)

operations support element. A group who supports the counterintelligence and human intelligence staff. Also called **OSE.** (DoD Dictionary. Source: JP 2-0)

order of battle. The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called **OB.** (DoD Dictionary. Source: JP 2-0)

overhead persistent infrared. 1. Those systems originally developed to detect and track foreign intercontinental ballistic missile systems. (JP 3-14) 2. Within geospatial intelligence, a capability that provides on-demand, persistent, global, and/or localized coverage of high- to low-intensity infrared events to detect energy radiation from various tactical to strategic objects. Also called **OPIR.** (DoD Dictionary. Source: JP 2-0)

planning and direction. In intelligence usage, the determination and prioritization of intelligence requirements, preparation of collection and production plans, development of appropriate intelligence architecture, and issuance of orders and requests to information collection agencies or intelligence production centers. (DoD Dictionary. Source: JP 2-0)

priority intelligence requirement. The intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support. Also called **PIR.** (DoD Dictionary. Source: JP 2-0)

processing. A system of operations designed to convert raw data into useful information. (DoD Dictionary. Source: JP 2-0)

processing and exploitation. In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (DoD Dictionary. Source: JP 2-0)

production requirement. A tasking to produce a new analytical product in response to an intelligence requirement. Also called **PR.** (DoD Dictionary. Source: JP 2-0)

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.** (DoD Dictionary. Source: JP 2-0)

reconnaissance. A mission undertaken to obtain information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, geographic, or other characteristics of a particular area, by visual observation or other detection methods. (DoD Dictionary. Source: JP 2-0)

red team. An ad hoc organizational element that provides an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. (DoD Dictionary. Source: JP 2-0)

request for information. Any specific, time-sensitive, ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. Also called **RFI.** (DoD Dictionary. Source: JP 2-0)

scientific and technical intelligence. Foundational all-source intelligence that covers: a. foreign developments in basic and applied research and 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 2-0)

security. 1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 3-10) 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JP 3-10) 3. Measures taken to prevent unauthorized persons from having access to information safeguarded in the interest of the nation. (DoD Dictionary. Source: JP 2-0)

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 2-0)

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.** (DoD Dictionary. Source: JP 2-0)

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, whereby 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 that facility. Also called **SCIF.** (DoD Dictionary. Source: JP 2-0)

signals intelligence. 1. A category of intelligence comprising all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted, individually or in combination. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT.** (DoD Dictionary. Source: JP 2-0)

signals intelligence operational tasking authority. A military commander's authority to operationally direct and levy signals intelligence requirements on designated signals intelligence resources. Also called **SOTA.** (DoD Dictionary. Source: JP 2-0)

situation template. A depiction of assumed enemy dispositions, based on that enemy's preferred method of operations and the impact of the operational environment if the adversary should adopt a particular course of action. (DoD Dictionary. Source: JP 2-0)

sociocultural analysis. The analysis of enemies, adversaries, and other relevant actors that integrates cultural norms and beliefs of societies, populations, and other groups of people, including their activities, informal and formal power structures, laws and policies, access to resources, and decision making across time and space at varying scales. Also called **SCA.** (DoD Dictionary. Source: JP 2-0)

sociocultural factors. The social, cultural, and behavioral factors characterizing the relationships and activities, informal and formal power structures, laws and policies, access to resources, and decision making of the population of a specific region or operational environment. (DoD Dictionary. Source: JP 2-0)

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 2-0)

source management. The process to register and monitor the use of human sources to protect the security of the operations and avoid conflicts. (DoD Dictionary. Source: JP 2-0)

source operations. The collection, from, by, and/or via humans, of foreign and military and military-related intelligence. (DoD Dictionary. Source: JP 2-0)

source registry. A source record or catalogue of leads and sources acquired by collectors and centralized for management, coordination, and deconfliction of source operations. (DoD Dictionary. Source: JP 2-0)

strategic intelligence. Intelligence required for the formation of policy and military plans at national and international levels. (DoD Dictionary. Source: JP 2-0)

structured observation management. The framework for standardizing how geospatial intelligence observations are captured, organized, and shared. Also called **SOM.** (DoD Dictionary. Source: JP 2-0)

synchronization. 1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In intelligence usage, application of intelligence sources and methods in concert with the operation plan to answer intelligence requirements in time to influence the decisions they support. (DoD Dictionary. Source: JP 2-0)

Tactical Exploitation of National Capabilities. A program exploiting national capabilities and integrating those capabilities into the tactical decision-making process. Also called **TENCAP.** (DoD Dictionary. Source: JP 2-0)

tactical intelligence. Intelligence required for the planning and conduct of tactical operations. (DoD Dictionary. Source: JP 2-0)

target area of interest. The geographical area where high-value targets can be acquired and engaged by friendly forces. Also called **TAI.** (Approved for incorporation into the DoD Dictionary. Source: JP 2-0)

task force counterintelligence coordinating authority. An individual in a joint force intelligence directorate, counterintelligence and human intelligence staff element, joint task force configuration that coordinates counterintelligence activities with other supporting counterintelligence organizations and agencies to ensure full counterintelligence coverage of the task force operational area. (DoD Dictionary. Source: JP 2-0)

tear line. A visible line on an intelligence message separating categories of information that have been approved for foreign disclosure and release. (DoD Dictionary. Source: JP 2-0)

technical intelligence. Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an enemy’s technological advantages. Also called **TECHINT.** (DoD Dictionary. Source: JP 2-0)

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 2-0)

United States person. A United States citizen; an alien known by the concerned intelligence agency to be a permanent resident alien; an unincorporated association substantially composed of United States citizens or permanent resident aliens; or a corporation incorporated in the United States, except for those directed and controlled by a foreign government or governments. (DoD Dictionary. Source: JP 2-0)

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 2-0) 2. In the context of time-phased force and deployment data validation, it is an execution procedure whereby all the information records in the time-phased force and deployment data are confirmed error-free and accurately reflect the current status, attributes, and availability of units and requirements. (JP 3-35) 3. A global force management procedure for assessing combatant command requirements to determine viability, for sourcing, with respect to risk and prioritization between competing needs and the nature of the requirement. (JP 3-35) (Definition #1 approved for incorporation into the DoD Dictionary. Source: JP 2-0)

warning intelligence. Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. (DoD Dictionary. Source: JP 2-0)

2. Terms Removed from the DoD Dictionary

- **Supersession of JP 2-0, *Joint Intelligence,* 22 October 2013:** acoustic intelligence; collection posture; concept of intelligence operations; elicitation; foreign intelligence; fusion; open-source information; operational intelligence; synthesis

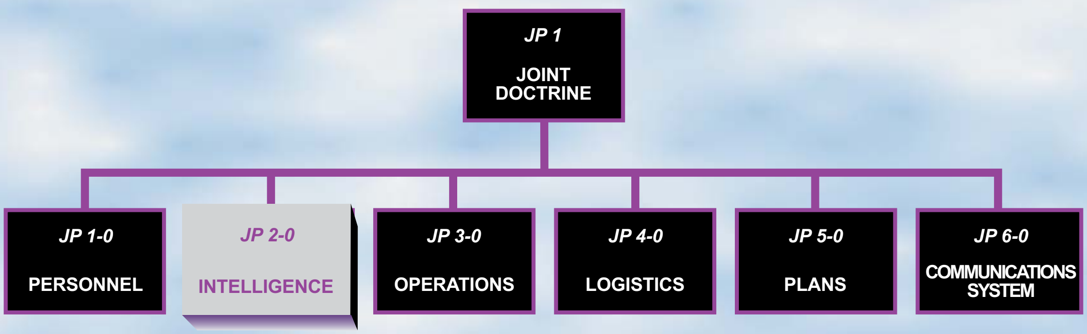
- **Cancellation of JP 2-01, *Joint and National Intelligence Support to Military Operations,* 5 July 2017:** agency; collection requirements matrix; collection resource; combat information; consumer; courier; evaluation; evaluation and feedback; information report; intelligence mission management; intelligence system; interpretation; joint interrogation operations; originator

- **Cancellation JP 2-01.2, *(U) Counterintelligence and Human Intelligence Support to Joint Operations,* 6 April 2016:** access; agent; asset validation; bona fides; case officer; compromise; controlled information; controlled technical services; counterespionage; counterintelligence activities; counterintelligence investigations; counterintelligence operational tasking authority; counterintelligence production; counterintelligence support; double agent; force protection detachment; foreign intelligence entity; intelligence interrogation; intelligence reporting; joint counterintelligence unit; lead; offensive counterintelligence operation; overt; overt operation; placement; screening; security service; technical surveillance countermeasures; tradecraft; walk-in; witting

- **Cancellation of JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment,* 21 May 2014:** adversary template; avenue of approach; begin morning civil twilight; end evening civil twilight; end of evening nautical twilight; event matrix; intelligence preparation of the battlespace; line of communications; littoral; mobility corridor

- **Cancellation of JP 2-03, *Geospatial Intelligence in Joint Operations,* 5 July 2017:** activity-based intelligence; Allied System for Geospatial Intelligence; change detection; datum (geodetic); foundation geospatial intelligence data; geographic coordinates; geospatial intelligence operations; infrared imagery; planning factors database; technical analysis; terrain analysis; topographic map; unified geospatial-intelligence operations

JOINT DOCTRINE PUBLICATIONS HIERARCHY



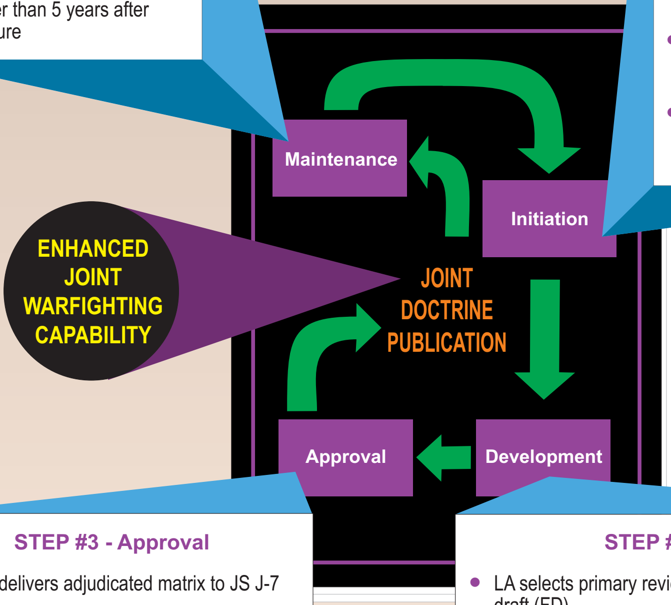
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 2-0** is in the **Intelligence** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

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)


Maintenance
Initiation
ENHANCED JOINT WARFIGHTING CAPABILITY
JOINT DOCTRINE PUBLICATION
Approval
Development

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