FMI 2-01
November 2008

ISR Synchronization

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at Army Knowledge Online <www.us.army.mil> and the General Dennis J. Reimer Training and Doctrine Digital Library at <www.train.army.mil>.

Field Manual Interim
No. 2-01 (FM 34-2)

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 11 November 2008

Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization

Contents

***This publication supersedes FM 34-2, 8 March 1994, and FM 34-2-1, 19 June 1991.**

Figures

Tables

Preface

This FMI provides the foundation for Army intelligence, surveillance, and reconnaissance (ISR) synchronization doctrine. Since FM 34-2 was published in 1994, the Army has transformed while at war into a modular force and changed its warfighting doctrine, organizations, training, and operations to match the dangers and challenges of today's operational environments. FM 34-2 was applicable to combined arms operations, and delineated between intelligence, operations, and command responsibilities through requirements management, mission management, and asset management.

FM 34-2 was essentially doctrine specific to the Intelligence branch and units. Since 1994, the Army has issued two iterations of FM 3-0, its capstone operations manual. FM 3-0 describes the Army's view on how it conducts prompt and sustained full spectrum operations on land during a period of persistent conflict. This FMI updates Army ISR synchronization doctrine to conform to the current operational doctrine and incorporates the intelligence warfighting function concept from FM 3-0.

This FMI outlines intelligence and operations responsibilities for planning, synchronizing, integrating, and executing ISR operations. Its scope is ISR synchronization and support to ISR integration. This FMI augments doctrine set forth in FM 2-0, 3-0, 5-0, 6-0, 7-15, and FMI 5-0.1. It is divided into 7 chapters and 3 appendixes.

- The introduction summarizes doctrinal changes that have occurred since the release of FM 34-2, and expands upon the manual's purpose. Also, new terms, and definitions are defined.
- Chapter 1 summarizes key concepts within combined arms and intelligence doctrine that are directly relevant to ISR synchronization. This chapter also introduces a discussion of indicator-based ISR planning regarding support of the military decision-making process (MDMP) and rapid decision-making and synchronization process (RDSP).
- Chapter 2 outlines requirements development from the initial information requirements, through prioritization, and discusses the formulation of specific information requirements (SIRs) from which ISR tasks are derived.
- Chapter 3 describes developing the ISR synchronization strategy.
- Chapter 4 describes the role of the intelligence warfighting function in supporting ISR integration and development of the ISR plan as an integrated part of overall operations. This chapter emphasizes the operations officer's role in conducting ISR integration.
- Chapter 5 discusses the development and dissemination of intelligence and intelligence products.
- Chapter 6 discusses the ongoing assessment of ISR operations.
- Chapter 7 describes activities necessary to update ISR operations.
- Appendix A discusses the similarities and differences in terms, planning, operations, and dissemination between Army and joint, interagency, and multinational operations. This chapter will discuss considerations of ISR requirements, responsibilities, and augmentation when an Army echelon is established as a joint, interagency, or multinational headquarters.
- Appendix B discusses command pre-mission intelligence briefings and subsequent debriefings upon mission completion.
- Appendix C discusses the Distributed Common Ground Station-Army (DCGS-A) enterprise.

This FMI provides ISR synchronization guidance for Army commanders, staffs, and trainers at all echelons from battalion to Army service component command (ASCC). FMI 2-01 forms the foundation for established curriculum within the Army's educational system on ISR synchronization. Joint doctrine applies to joint organizations; Army headquarters which operate as joint headquarters must use joint ISR doctrine. The

information presented is descriptive, not prescriptive or restrictive. This presentation is a linear description and discussion of a dynamic, ongoing staff process designed to assist the commander. It provides details of the six continuous activities of ISR synchronization, depending on mission, time available, ongoing operations, and standing operating procedures (SOPs).

This FMI applies to the Active Army, the Army National Guard (ARNG)/Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR).

This manual complies with FM 2-0, 3-0, 5-0, 6-0, 7-15, and FMI 5-0.1, change 1. The term “intelligence officer” refers to the actual G-2, S-2, or other top intelligence positions within units and organizations. The term “operations officer” refers to the G-3, S-3, or other top operations positions within units and organizations. The term “G-2/S-2” or “G-3/-S3” refers generically to all members of the intelligence or operations staff sections.

Introduction

It is imperative that commanders understand the operational environment prior to taking effective action. The intelligence warfighting function provides the related tasks and systems that facilitate understanding of the enemy, terrain, weather, and civil considerations, which includes areas, structures, capabilities, organizations, people, and events (ASCOPE). A primary means of gaining knowledge of the operation environment is accomplished by executing aggressive and continuous ISR to acquire that information.

ISR supports full spectrum operations through four tasks:

- Perform ISR synchronization.
- Perform ISR integration.
- Conduct Reconnaissance.
- Conduct Surveillance.

As a critical part of the intelligence warfighting function, ISR provides answers to commanders' Information requirements and contributes significantly to the commander's situational understanding. It is crucial that all commanders and staff sections participate in ISR planning, from the identification of Information requirements through the collection and reporting of information to answer the commander's critical information requirements (CCIRs).

Since the publication of FM 34-2, ISR synchronization doctrine has changed significantly. Since the introduction of the term "ISR" in FM 3-0 in 2001, doctrinal codification of concepts, terms, and definitions changed in a number of manuals.

Changes in the Army's force structure and increasing access to and reliance upon Joint and National sensors necessitated a change in ISR synchronization doctrine. Brigade combat teams (BCTs) have a larger intelligence staff and more collection systems, as well as more robust surveillance and reconnaissance capabilities.

The Division, while possessing no organic intelligence collection assets (unless augmented by a battlefield surveillance brigade (BFSB) or task organized with assets provided by a combatant command) leverages Joint and National collectors in support of its own Information requirements as well as subordinate echelon requirements. The Army Division remains the lowest echelon that conducts long-term analysis functions, and is often the lowest echelon that representatives of national agencies will typically augment.

Many tenets of FM 34-2 carry over to FMI 2-01. However, there are significant additions and modifications from recent combined arms and intelligence doctrine. The table below shows the new or changed material from FM 34-2.

New or Changed	*Comments*
named area of interest	Added, FM 3-90, 2001
targeted area of interest	Added, FM 3-90, 2001
ISR Synchronization	Modified, FM 3-0, 2008
ISR Integration	Modified, FM 3-0, 2008
Conduct ISR Task	Added, FM 2-0, 2004
Intelligence Warfighting Function	Added, FM 3-0, 2008
Retasking	Added and defined. See glossary
Redirecting	Added and defined. See glossary.
Civil Considerations (ASCOPE)	Added, FM 6-0, 2003
Eliminated, removed, or replaced	Comments
Collection Management	Deleted
Asset Management	Deleted
Mission Management	Deleted
Specific Orders and Requests	Deleted, FM 2-0 2004, replaced by ISR tasks

Chapter 1

The Foundations of Intelligence, Surveillance, and Reconnaissance Synchronization

This chapter describes the task of Perform Intelligence, Surveillance, and Reconnaissance (see FM 7-15, ART. 1.3); its sub-task of Perform ISR synchronization (ART 1.3.1), and the relationship to the intelligence warfighting function; the principles of successful intelligence support; and how these principles are applied.

THE OPERATIONAL ENVIRONMENT

1-1. The operational environment can be defined as a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. The operational environment encompasses physical areas and factors of the air, land, maritime, space, and information domains. It also includes enemy, adversary, friendly, and neutral systems. The operational environment is described using operational and mission variables as described in FM 3-0. ISR operations are one means of developing information and knowledge leading to situational understanding of the operational environment for the commander.

RECENT INTELLIGENCE OPERATIONS

1-2. The dynamic relationship between intelligence and operations is demonstrated by recent operations. Effective intelligence drives effective operations and effective operations produce information, which in turn leads to more intelligence. In recent operations, one of the key functions of intelligence is to facilitate an understanding of the operational environment with greater emphasis on the human elements of the mission and operational variables and how those elements interact.

1-3. In today's operational environment, explaining these complex relationships and enhancing understanding requires presenting a greater level of detail for the commander and staff on cultural issues, perceptions, values, beliefs, interests, and the varied decision-making processes of different individuals and groups. These insights are critical components to the planning, preparation, execution, and assessment of successful operations, and they provide a significant challenge to effective ISR synchronization.

1-4. Closely linking ISR synchronization with all ongoing analytical efforts across an effective and collaborative staff framework is vital to success operations. ISR synchronization in support of complex stability operations should follow the fundamental doctrinal methodologies presented in this manual; however, a much greater emphasis on civil consideration is necessary, especially with regard to demographic groups and formal or informal leaders.

1-5. A thorough and detailed intelligence preparation of the battlefield (IPB) is needed to appreciate the complex operational environment we are facing today. In-depth IPB processes in recent operations have considered areas like economics, social anthropology, and the effects of governance. Therefore, the integrating staff must draw upon the experience of non-intelligence personnel and external experts with local and regional knowledge during the IPB process. A thorough IPB process facilitates a more effective and efficient ISR synchronization process.

1-6. In order to bring clarity to the broad scope of information available, all staff members work to improve the knowledge base used to develop an understanding of the area of interest (AOI) and area of

operations (AO). For example, civil affairs (CA) personnel receive training in analysis of populations, cultures, and economic development. FM 3-24, chapter 3, articulates the process to describe the unique characteristics of the operational environment within counterinsurgency operations.

1-7. Other unique considerations for ISR synchronization within stability operations include using—

- Open-source intelligence as a source of potentially important information covering aspects of civil considerations like culture, languages, history, current events, and actions of the government. Open sources include books, magazines, encyclopedias, websites, and tourist maps. Academic sources, such as articles and university personnel, can also provide critical information.
- Quick-reaction capabilities down to the lowest possible level in order to collect information and integrate the information and intelligence into the effective execution of operations. For example, unmanned ground sensors and signals intelligence (SIGINT) terminal guidance have provided unprecedented ISR capabilities and opportunities below the battalion level.
- Detainee interrogation, site exploitation, and document and media exploitation in order to cue other ISR capabilities and sometimes to "trigger" subsequent operations, branches, or sequels, as appropriate.

COMMANDER DRIVES INTELLIGENCE

1-8. Because understanding is fundamental to effective command and control, the commander drives intelligence and, in particular, the conduct of ISR. Prior to deployment and well before the execution of offensive, defensive, stability, or civil support operations, the commander and staff require knowledge about the operational environment in order to begin planning. ISR synchronization is a continuous activity from pre-mission planning through the conduct of operations until completion of operations. Continuous ISR planning (including synchronization and integration) supports enhanced battle command and the commander's situational understanding.

1-9. The commander will focus collection by stating priorities, asking questions of intelligence relevance, prioritizing reconnaissance objectives, and approving CCIRs recommended by the staff during the MDMP. The entire intelligence process facilitates the commander's situational understanding, by either directly satisfying the CCIRs requirements or satisfying staff information requirements. Intelligence acquired by ISR assets, units, and Soldiers facilitates the commander's decision making which drive operations. ISR operations concurrently satisfy the staff's information requirements, support the various staff section running estimates, and facilitate recommendations to the commander. The task "Conduct Intelligence, Surveillance, and Reconnaissance" includes four subtasks:

- Perform ISR synchronization.
- Perform ISR integration.
- Conduct reconnaissance.
- Conduct surveillance.

1-10. According to FM 3-0, ISR is a continuing activity which occurs during all operations process activities, whereas ISR synchronization is one of the five integrating processes. Together with IPB and the intelligence running estimate, ISR focuses on assessing three of the six mission variables of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). The three variables are enemy, terrain and weather, and civil considerations (ASCOPE). This assessment involves active surveillance and reconnaissance missions as part of ISR operations.

1-11. ISR synchronization supports the assessment through the ISR synchronization plan by managing assets collecting against intelligence requirements. ISR operations allow units to produce intelligence about the enemy and the operational environment necessary to make decisions. Intelligence derived from ISR assets, intelligence reach, and requests for information (RFIs) satisfies requirements developed throughout the operations process. Timely and accurate intelligence encourages audacity and can facilitate actions that may negate enemy tactics and materiel.

INTELLIGENCE WARFIGHTING FUNCTION

1-12. The intelligence warfighting function consists of the related tasks and systems that facilitate understanding of the threat, terrain and weather, and civil considerations. The four intelligence warfighting function tasks are—

- Support to force generation.
- Support to situational understanding.
- Conduct ISR.
- Provide intelligence support to targeting and information capabilities.

1-13. The intelligence warfighting function is a flexible and adjustable architecture of procedures, personnel, organizations, and equipment enabled by the DCGS-A network to provide commanders with relevant information and products relating to the AO. The intelligence warfighting function not only includes Soldiers, assets, systems, units, and sensors within the military intelligence (MI) branch but also includes those of the other warfighting functions as they conduct ISR. Every Soldier, as part of a small unit, is a potential information collector and an essential component to help answer information requirements.

1-14. The intelligence warfighting function relies upon inputs from and collaboration with the other warfighting functions. The collection and reporting of information, analysis, and dissemination of intelligence must routinely occur across the AO, across all staff sections and across the Army's branches and warfighting functions.

1-15. The intelligence warfighting function focuses on four primary intelligence tasks that facilitate the commander's visualization and situational understanding of the operational environment. These tasks are interactive and often take place simultaneously.

- Support to force generation.
- Support to situational understanding.
- Conduct ISR.
- Provide intelligence support to targeting and information capabilities.

1-16. These tasks are discussed further in FM 2-0, chapter 1, and FM 7-15. The task "Conduct ISR" supports the other three intelligence tasks as well as tasks across multiple warfighting functions.

INTELLIGENCE PROCESS

1-17. Intelligence operations generally follow five functions that constitute the intelligence process: plan, prepare, collect, process, and produce. In addition to these functions of the intelligence process, there are three common tasks: analyze, disseminate, and assess. These functions are not necessarily sequential. The intelligence process provides a common model with which to guide one's thinking, discussing, planning, and assessing the threat and operational environment.

1-18. The intelligence process generates information, products, and knowledge about the threat, the AOI, and the situation, which allows the commander and staff to develop a plan, seize and retain the initiative, build and maintain momentum, and exploit success. The execution of this process must follow all applicable policies and regulations on the collection of information and operations security (OPSEC). The ISR synchronization task complements and is embedded throughout the intelligence process and supports the operations process. Figure 1-1 illustrates the relationship between the operations and intelligence processes. (See FM 2-0 for further explanation of the intelligence process.)

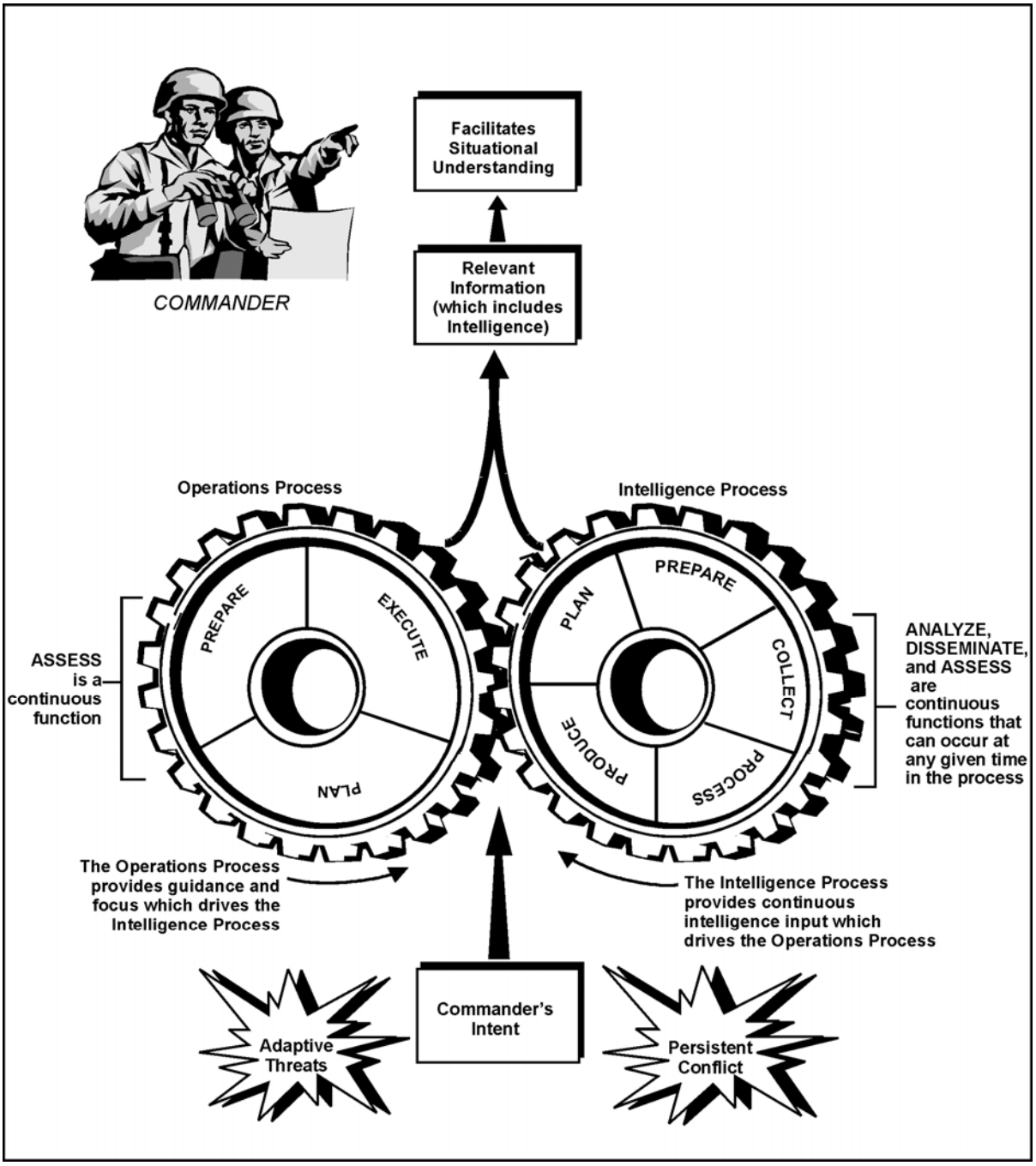

Figure 1-1. The relationship between the intelligence and the operations processes

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

1-19. **Intelligence, Surveillance, and Reconnaissance is an activity that synchronizes and integrates the planning and operation of sensors and assets, as well as processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function (JP 2-01).**

1-20. For Army forces, this activity is a combined arms operation that focuses on priority intelligence requirements (PIRs) while answering the commander's critical information requirements (CCIRs) (FM 3-0).

1-21. A PIR is an intelligence requirement, stated as a priority for intelligence support, which the commander and staff need to understand the adversary or the operational environment (JP 2-0).

1-22. CCIRs are elements of information required by the commander that directly affect decision making and dictate the successful execution of military operations.

1-23. Army doctrine recognizes the joint ISR definition. Army ISR operations complement joint ISR activities; however, Army ISR operations are unique because of the complex interaction of Army forces with indigenous population and terrain. The Army must focus its ISR operations for maximum collection by limited assets to produce the best intelligence possible. Army units contend with complex terrain considerations requiring a concerted effort between all ISR assets to include coordinated exploitation of joint and national ISR capabilities as well as Soldier surveillance and reconnaissance. Soldier surveillance and reconnaissance implements the Army initiative called every Soldier is a Sensor (ES2). ISR must be extremely flexible, allowing for re-tasking as current operations warrant. Units have unique requirements and contributions in the conduct of surveillance or reconnaissance. Many of the personnel and units that participate in ISR operations have additional missions. For more information on Soldier surveillance and reconnaissance, see FM 2-91.6, which is under development.

1-24. ISR operations are fundamental to information superiority and support friendly operations through four tasks:

- Perform ISR synchronization, which considers all assets—both internal and external to the organization— to ensure the most appropriate assets collect information, to identify the gaps in information, and to assign the most efficient means of processing and dissemination of intelligence.
- Perform ISR integration, which ensures the efficient tasking of assets to collect on requirements that cannot be satisfied by intelligence reach or RFI or which the commander considers critical.
- Conduct Surveillance.
- Conduct Reconnaissance.

1-25. Commanders integrate all assets into a single ISR plan in order to capitalize on the different capabilities. They synchronize and coordinate surveillance and reconnaissance missions; and employ other units for ISR within the scheme of maneuver. Synchronization and integration of ISR with the overall operations plan (OPLAN) positions ISR assets to continue to collect information; sustain and reconstitute for branches or sequels; or to shift priorities in accordance with the order.

1-26. Managing the ISR effort entails intelligence personnel to perform the following:

- Requirements visibility. Use procedures and information systems to monitor and display the status of information requirements.
- Asset visibility. Use procedures and information systems to monitor and display collection asset status, location, and activities.
- Assessment capability. Use procedures and information systems to assess the effectiveness of the ISR effort and the operational impact of ISR results (such as its success or gaps in collection) and to task collection assets.

1-27. Lessons learned and observations from combat training center rotations and current operations emphasize the importance of ISR planning involving full staff integration to focus ISR assets on the commander's PIRs. Successful ISR operations integrate and synchronize the collection effort across all warfighting functions using every available asset, Soldier, sensor, and unit. Effective ISR draws on all available collection assets (internal, external, and joint) enhanced by the net-centric DCGS-A enterprise.

1-28. Army Intelligence provides timely, relevant, accurate, and synchronized intelligence support to tactical, operational, and strategic commanders from force projection planning to the execution of full

spectrum operations. All intelligence operations are executed within the scope and parameters of applicable laws, policies, and regulations. These directives can be complex and require attention during ISR synchronization and ISR integration activities, which are discussed in chapters 3 and 4 of this manual.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION

1-29. ISR synchronization is the task that accomplishes the following:

- Analyzes information requirements and intelligence gaps.
- Evaluates available assets (internal and external).
- Determines gaps in the use of those assets.
- Recommends ISR assets controlled by the organization to collect on the CCIRs; and submits RFIs for adjacent and higher collection support (FM 3-0).

1-30. ISR synchronization ensures all available information is obtained through intelligence reach, RFIs, and ISR tasks resulting in successful reporting, production, and dissemination of information, combat information, and intelligence to support decision making.

1-31. ISR synchronization ensures the commander's requirements drive ISR operations and that ISR reporting responds in time to influence decisions and operations. Intelligence officers synchronize the ISR effort through coordination with operations officers with full staff participation. Synchronizing includes all assets the commander controls, assets of lateral units and higher echelon units and organizations, RFIs and intelligence reach to support intelligence production and dissemination which help answer CCIRs and other requirements.

1-32. ISR synchronization identifies the best way to satisfy information requirements concerning the operational environment. Commanders use it to assess ISR asset reporting. The operations process provides the guidance and mission focus that drives the intelligence process; the intelligence process provides the continuous intelligence input, which is essential to the operations process.

1-33. The ISR synchronization process involves six continuous activities, as depicted in figure 1-2. These activities and subordinate activities are not necessarily sequential. The ISR synchronization process supports full spectrum operations and does not dramatically change with echelon, although organization, terminology, and tools may vary.

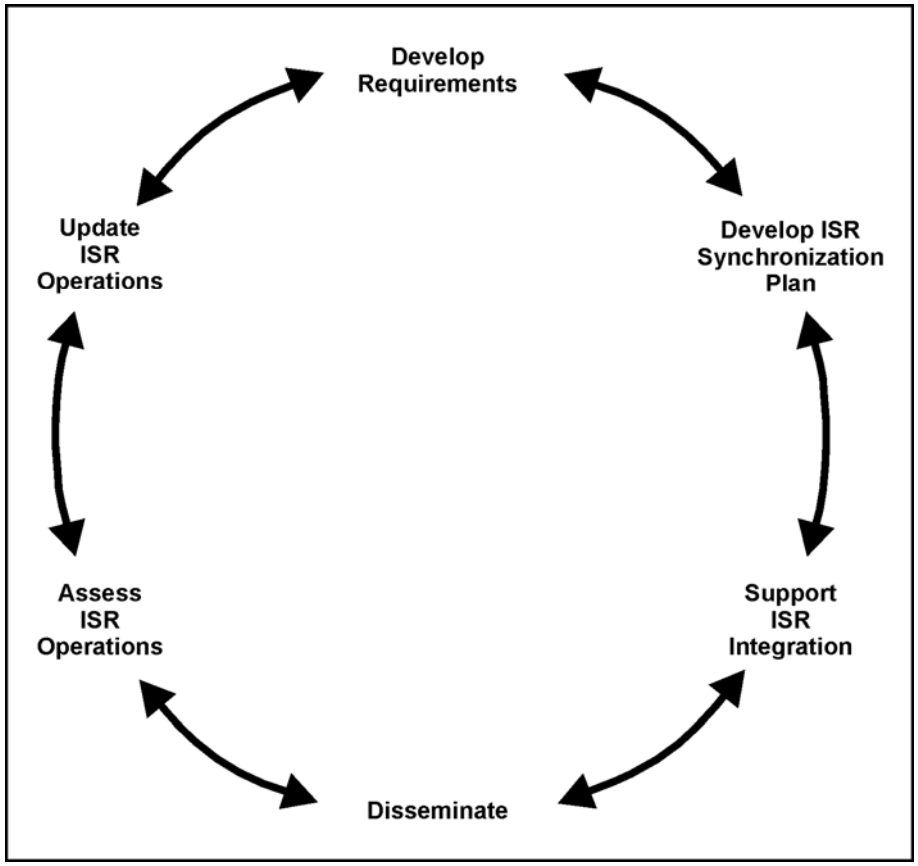

Figure 1-2. ISR synchronization activities

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION PLAN CONSIDERATIONS

1-34. The intelligence staff considers six criteria in planning ISR synchronization and ISR activities, as discussed below. These considerations are essential elements of the ISR synchronization process.

- Anticipate. The intelligence staff must recognize when and where to shift collection or identify new intelligence requirements. The intent of this principle is to identify a new or adjust an existing requirement and present it to the commander before the commander or other staff members identify the need. By participating in future operations planning, intelligence officers can best anticipate requirements.
- Integrate. The intelligence staff must collaborate and coordinate with all staff sections and with both higher headquarters and subordinate units in order to be continuously integrated and engaged in the unit's orders production and planning activities to ensure early identification of intelligence requirements. The intelligence staff must also be integrated into current operations to anticipate future branches, sequels, and new operations based on intelligence produced today. Early and continuous consideration of collection factors enhances the unit's ability to direct ISR assets in a timely manner in support of developing situations, ensures thorough planning, and increases flexibility in selecting and retasking assets.
- Prioritize. Intelligence officers prioritize each intelligence requirement based upon its importance in supporting the commander's intent and decisions and the current situation so that limited ISR assets and resources are directed against the most critical requirements.

- Balance. ISR capabilities complement each other. The intelligence staff should resist favoring or becoming too reliant on a particular unit, discipline, or system. Balance is simply ensuring an appropriate mix of ISR assets or types. The ISR synchronization matrix is useful in determining or evaluating balance. During ISR synchronization, the staff recommends cueing, redundancy, and mix as appropriate.
- Control. To ensure timely and effective responses to intelligence requirements, a unit should first use ISR assets it controls. These assets usually are more responsive to their respective commander's needs, and this decreases the reliance on the ISR assets of other units, agencies, or organizations.
- Reach. Intelligence reach and RFIs may answer a requirement without having to use assigned or attached ISR assets. However, a unit should not depend solely on intelligence reach to satisfy a PIR.

COORDINATE WITH OTHER WARFIGHTING FUNCTIONS AND STAFF SECTIONS

1-35. ISR synchronization involves the entire staff and all of the warfighting functions. (Refer to FM 3-0 for more information on the warfighting functions.) All staff sections within a command post have the responsibility to satisfy information requirements. For example, a CA unit reporting through the Civil-Military Operations Center or CA staff officer could provide answers to questions about the AO. Satisfying information requirements through staff element coordination facilitates ISR planning by eliminating the necessity to task an asset to collect information that another unit or asset already observed in the course of operations. The same can be said for other warfighting functions; Soldiers on patrol or other missions are potentially a valuable source of information. A serious effort must be made at each echelon of command to fully exploit the ES2 potential.

STAFF ROLES

1-36. ISR synchronization is the responsibility of the intelligence officer and G-2/S-2 staff. The operations officer is responsible for ISR integration with the support of the intelligence officer. All staff sections must collaborate on ISR synchronization to ensure all warfighting functions are fully integrated into the ISR plan. The commander may designate an ISR working group; however, the primary staff's responsibilities cannot be delegated.

1-37. In order for the intelligence and operations staff officers to prepare an effective ISR plan, they must completely understand the commander's intent and objectives. It is vital that the commander provide those staff officers with input and guidance during the various synchronization activities in order for the ISR plan and intelligence production to focus on the critical information and knowledge the commander needs.

1-38. The commander provides input which the staff uses to generate information requirements. Subordinate units and adjacent units generate information requirements as RFIs. Intelligence officers review these requirements and develop intelligence requirements. They also recommend PIRs to the commander, manage the commander's PIRs and request information from higher or lateral organizations.

1-39. Intelligence officers validate and recommend PIRs. Where possible, ISR synchronization satisfies IR through intelligence reach and RFIs. It recommends ISR tasks for assets the commander controls. Intelligence officers and staff develop indicators and SIRs to focus collection requirements. The intelligence staff develops collection strategies that will satisfy SIRs which support the targeting process. The intelligence officer plans for synchronized collection, focusing on the proper requirements, to include high-value targets (HVTs) at each phase of the operation. If combat assessment is required to support the operation, the G-2/S-2 plans collection to satisfy that set of SIRs as well. When appropriate, the G-2/S-2 plan and arrange direct dissemination of targeting intelligence from the collector to the fires cell or appropriate fire support element within the fires cell. In many cases, weapons intelligence teams or site exploitations may provide information which can be used for targeting or immediate operational planning. Whatever the focus and mission, ISR supports targeting as an integrated part of any operation.

1-40. Intelligence reach tasks are assigned to G-2/S-2 personnel or subordinate intelligence elements according to unit SOPs. Intelligence officers submit RFIs to higher and lateral echelons and coordinate with and assist the operations officer to refine and assign ISR tasks. ISR synchronization includes continually identifying new and partially filled intelligence gaps.

1-41. Specifically, intelligence officers—

- Evaluate ISR assets for suitability (availability, capability, vulnerability, and performance history) to execute ISR tasks and make appropriate recommendations on asset tasking to the operations officer. For further discussion on evaluating ISR assets, see chapter 3.
- Assess ISR asset reporting and intelligence production to evaluate the effectiveness of the ISR effort. They maintain situational awareness in order to identify gaps in coverage and to identify the need to cue or recommend redirecting ISR assets to the operations officer.
- Update the ISR synchronization plan as requirements are satisfied, modified, or created. They remove satisfied requirements and recommend new requirements as necessary.
- In coordination with operations staff, monitor satisfactory completion of ISR tasks from higher headquarters. Operations officers integrate the updated synchronization plan into orders tasking ISR assets, units, and Soldiers.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE INTEGRATION

1-42. **ISR integration is the task of assigning and controlling a unit's ISR assets (in terms of space, time, and purpose) to collect and report information as a concerted and integrated portion of OPLANs and operations orders (OPORDs) (FM 3-0).** ISR integration ensures assignment of the best ISR assets (internal and external including joint assets) through a deliberate and coordinated effort of the entire staff across all warfighting functions by integrating ISR into the operation.

1-43. ISR operations require constant coordination between the command and control, operations, intelligence, and plans cells within an organization. During ISR integration, the entire staff participates as the lead for ISR planning transitions from the G-2/S-2 to the G-3/S-3 because directing the ISR plan is a command and control integrating function led by the current operations cell. The ISR plan is developed and synchronized by the intelligence officer and then integrated with the overall operational plan by the operations officer.

1-44. ISR integration is vital in controlling limited ISR assets. Thoroughly integrated ISR operations add many collection sources, multiplying the potential for multi-source collection of information. ISR integration occurs during the "Support ISR Integration" and "Update ISR Operations" sub-activities of ISR synchronization. (See chapters 4 and 7 for more details on these activities.) The ongoing activities of ISR all contribute to updating the ISR plan.

1-45. The operations officer, with input from the intelligence officer, develops mission taskings based on SIRs (developed as part of ISR synchronization). SIRs facilitate tasking by matching requirements to assets. The operations officer assigns tasks in time precedence based on the latest time information is of value (LTIOV) and the capabilities and limitations of available ISR assets. **The LTIOV is the absolute latest time the information can be used by the commander in making the decision the PIR supports (FM 2-0).** The LTIOV can be linked to time, an event, or a point in the battle or operation.

1-46. During ISR integration, the G-2/S-2 satisfies as many information requirements as possible through staff coordination, intelligence reach, and RFIs; then the G-3/S-3 assigns unanswered information requirements as ISR tasks to the most suitable collector based on the recommendations of the intelligence officer. When information requirements exceed the capability of traditional ISR units to collect, maneuver and support units may be required to collect information to satisfy the commander's PIR or other staff information requirements.

1-47. The development of an integrated ISR plan requires the participation of the entire staff. Staff sections are required to determine the suitability of elements to collect information and recommend to the operations officer the appropriateness of tasking those assets.

1-48. Surveillance and reconnaissance are the primary means of collecting information used to produce intelligence. A thorough understanding of joint ISR capabilities allows commanders to prepare complementary collection plans. Surveillance and reconnaissance assets focus primarily on collecting information about the enemy and the operational environment to satisfy the PIRs.

MILITARY DECISION-MAKING PROCESS AND RAPID DECISION-MAKING AND THE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION PROCESS

1-49. ISR synchronization directly supports MDMP and RDSP, by developing information requirements and stating clear indicators of threats or other actions in the AOI. During mission analysis, the staff develops a list of information requirements. This list is based upon higher headquarters tasks, commander's guidance, staff assessments, and subordinate and adjacent unit RFIs. These information requirements identify requirements for each potential friendly course of action (COA). The intelligence staff also develops information requirements for each potential enemy at COA.

1-50. During COA development, the G-2/S-2 staff develops and recommends initial CCIRs. The commander decides what information is critical based on experience, the mission, the higher commander's intent, and the input (initial IPB, information, information requirements, intelligence, and recommendations) from the staff. After the wargaming stage of MDMP, the commander designates CCIRs to let the staff and subordinates know what information is deemed to be essential for decision making where the ISR synchronization activity begins to develop indicators and SIRs.

1-51. It is important at this point to state whether by time (LTIOV) or event, a point in the battle or operation where satisfying each PIR ceases to be critical because this focuses and prioritizes the ISR effort. ISR synchronization continues beyond MDMP or RDSP supporting the various phases of the operation until mission completion. For more information on MDMP and RDSP, see FM 3-0, FM 5-0, and Change 1 to FMI 5-0.1.

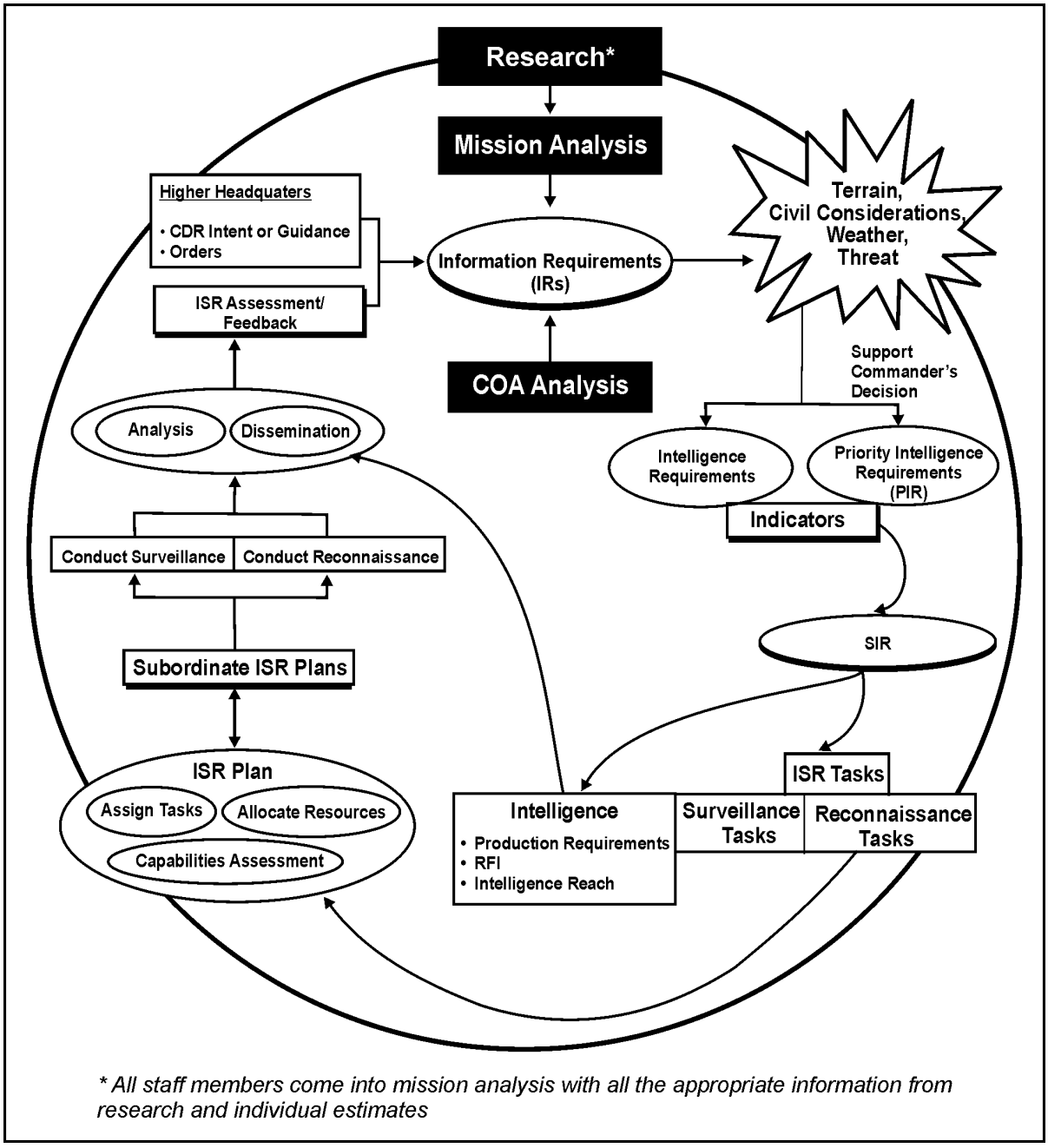

Figure 1-3. Information requirement development during MDMP

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

1-52. IPB is a continuous process. After the staff conducts the initial IPB for a mission, they must continually review and update their products to account for new information and changing situations. ISR supports IPB by actively collecting on information gaps, resulting in a more accurate intelligence product concerning the AOI. IPB facilitates the determination of requirements and collection priorities. (Refer to FM 2-01.3 and FMI 2-01.301 which is currently under development.)

INTELLIGENCE RUNNING ESTIMATE

1-53. Intelligence officers continuously consider the effects of new information and update and assess the following:

- Facts.
- Assumptions.
- Enemy COAs.
- Terrain.
- Weather.
- Threat activities and capabilities.
- Civil considerations.
- Conclusions and recommendations.
- Friendly force capabilities with respect to the adversary's capabilities.
- Threat capabilities for current operations and future plans.
- Civil considerations as they affect current operations and future plans.
- Environment's effect on current and future operations.

1-54. The intelligence running estimate is the current assessment from which planning and decisions are made. When an estimate reveals a gap then a new IR is developed and added to the ISR synchronization process. When the estimate reveals information that satisfies an IR, especially a CCIR, G-2/S-2 staff representatives immediately send that information to the sections requiring the information. Information and combat information are constantly processed and analyzed into knowledge which is disseminated to all sections requiring it. Each staff section's running estimate is one product of this effort.

1-55. Intelligence officers maintain the intelligence running estimate to identify when decisions are needed and to help commanders make them. When commanders are considering a decision, an estimate's presentation always ends with a recommendation. Sometimes the recommendation is implied. For example, when the estimate is presented as part of a situation update, the implicit recommendation is to continue operations according to the present order unless the G-2/S-2 recommends otherwise. The intelligence staff representatives to the command post cells and working groups base their assessments and recommendations on that single running estimate. The intelligence running estimate is a key component of the ISR synchronization process as it drives the current situational awareness of the intelligence officer and staff. For more information on the intelligence running estimate, see FM 2-0.

SOLDIER SURVEILLANCE AND RECONNAISSANCE

1-56. When conducting surveillance or reconnaissance, Soldiers actively observe details related to the CCIRs. Soldiers must be competent in reporting their experience, perceptions, and judgments concisely and accurately. To accommodate this task, the leadership must train Soldiers and foster an environment that encourages small-unit and individual-Soldier reporting. Therefore, ISR synchronization must account for Soldier surveillance and reconnaissance.

1-57. All Soldiers report their observations through the chain of command even when not specifically tasked to conduct surveillance or reconnaissance. The Soldier remains an indispensable source for much of the information needed by the commander. Observations and experiences of Soldiers often working with the local population provide depth and context to information collected through surveillance or reconnaissance. Commanders and staff must ensure information collected by Soldiers within their AOs integrated into the overall intelligence warfighting function. Focusing on effective integration will contribute to more detailed and accurate intelligence.

1-58. As Soldiers learn to regularly report relevant information, battalion and brigade intelligence staffs can quickly become overwhelmed with information if not sufficiently trained and prepared to handle the large volume of reports. Lessons learned collected from BCT Battalion and Brigade level S-2s who served in Operation Iraqi Freedom attest to the tremendous volume of information reported. They related that

while every Soldier and leader who encountered Iraqis was a potential information collector, it fell on the Battalion or Brigade S-2 to parse, vet, link, and package the information into useable intelligence.

1-59. SOPs must be written and Soldiers and staffs must be trained in order to be prepared to handle large volumes of information. In many cases S-2s required additional personnel to adequately support operations. At the company level, some commanders have opted to form company intelligence support teams (ad hoc) to improve timely processing and access to perishable information at the company level and to act as a conduit to the Battalion S-2 in order to improve coordination and ISR synchronization.

1-60. Appendix B describes command briefing and debriefing programs which is one method of integrating Soldier surveillance operations into overall ISR synchronization.

UNIFIED ACTION

1-61. **Unified action is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1).**

1-62. Joint operations focus and maximize the complementary and reinforcing effects and capabilities of each service. Joint force commanders (JFCs) synchronize the complementary capabilities of the service components that comprise the joint force. Consequently, the employment of MI in campaigns and major operations must be viewed from a joint perspective, and the "mud-to-space" intelligence concept must establish a fully interoperable and integrated joint intelligence capability. Army Forces intelligence assets also work with multinational and interagency partners to accomplish their missions. Ideally, multinational and interagency intelligence partners provide cultural perspectives and capabilities that reinforce and complement Army MI strengths and capabilities. At the same time, Army ISR support is a capability that complements other Services intelligence functions.

JOINT PERSISTENT SURVEILLANCE AND RELATED ARMY CONCEPTS

1-63. A critical part of current operations is the execution of the joint doctrinal concept of persistent surveillance. Joint doctrine defines persistent surveillance as:

> *A collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in real or near-real time. Persistent surveillance facilitates the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action.*

1-64. In its most simple form, the goal of the Army conceptual discussion of joint persistent surveillance is to provide the right intelligence to the right person at the right time and in the right format focused to their requirements. The latest Army intelligence concepts are based on the fundamental Army ISR construct and recognize ISR as a combined arms mission. However, these concepts focus on balancing future requirements for providing or accessing combat information and intelligence in a networked environment to support ongoing operations while also supporting long-term intelligence analysis and planning and other staff functions. Most of the concepts (and the Tactical Persistent Surveillance white paper) focus on—

- Embedded ISR synchronization capabilities.
- Improved ISR sensor capabilities and effective evaluation of ISR resources.
- Assured network communications capability.
- An enterprise approach to analysis, processing, and data or information access across units or organizations and echelons.
- Enhanced automated analytical tools to include planning and control, and analytical change detection capabilities.

1-65. As a result of implementing these tactical ISR concepts, we can expect gradual incremental improvements in—

- The number of ISR resources available.
- Phasing, cueing, and overlapping of ISR capabilities.
- Integrating and networking ISR assets and collection efforts.
- Executing the intelligence handover.

1-66. Within the latest Army intelligence concepts there is recognition that while vast improvements in ISR capabilities are possible, these new characteristics are not likely to fully develop in the near future. ISR will—

- Not provide guaranteed and uninterrupted collection on all requirements for all operations.
- Not change from inherently using a combined arms operational construct.
- Not eliminate all operational risk and uncertainty.
- Not obviate the need for operational planning.
- Not exclusively focus on sensor capability issues.

Chapter 2

Develop Requirements

Developing requirements means identifying, prioritizing, and refining gaps in data, relevant information, and knowledge concerning the operational environment that must be resolved in order for the commander to achieve situational understanding. See figure 2-1.

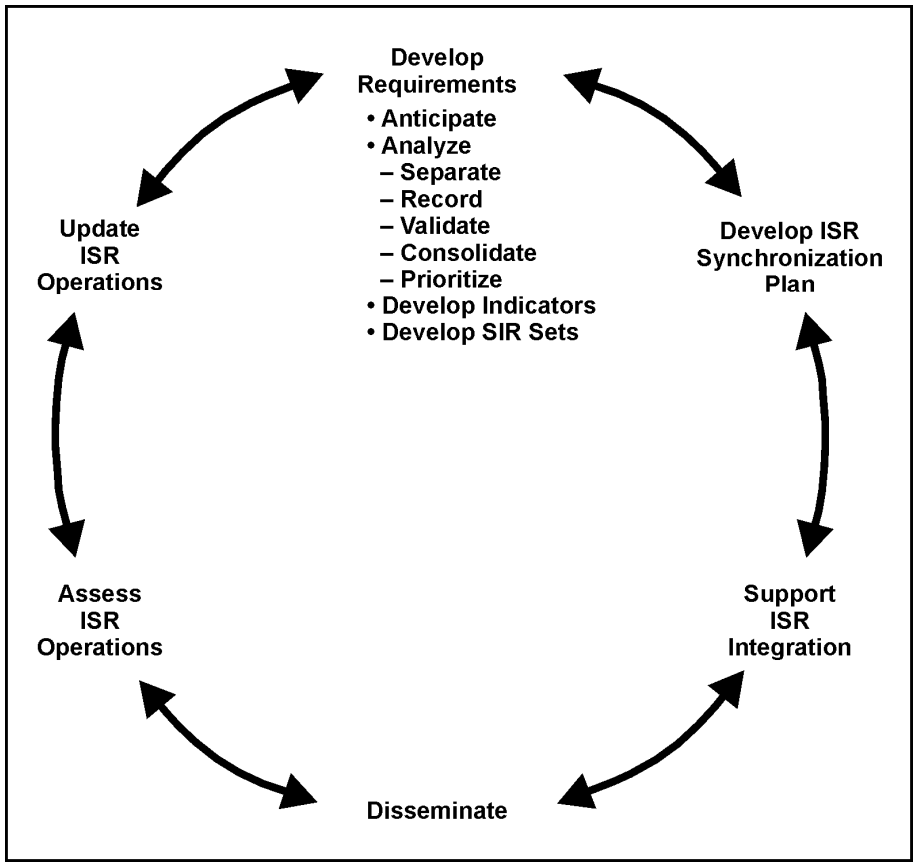

Figure 2-1. Develop requirements

GENERAL

2-1. Requirements are developed in pre-deployment, prior to a mission and during on-going operations because ISR synchronization activities are continuous and not sequential. An important element of developing requirements during on-going operations is a constant collaboration between analytical personnel and ISR planners to redefine information requirements and focus the ISR effort as the situation develops.

2-2. Developing requirements begins as early as possible, in some cases before receipt of the mission, when only partial information about the general location or category of mission are known. Requirements development continues as the intelligence staff collects initial (baseline) information and intelligence from existing sources, databases, and through intelligence reach in order to develop a preliminary intelligence and the initial staff estimate in preparation for the MDMP.

2-3. The intelligence staff continues to develop and refine requirements as the commander receives the mission and presents initial guidance to the staff. The commander's guidance includes the critical information for the AOI, expressed in later steps of the MDMP as the CCIR, which the commander must know to successfully plan, prepare, execute, and assess operations.

2-4. The commander decides what information is critical based on experience, the mission, input from the staff, the higher commander's intent, and the staff's estimate of the situation. Critical information requirements are based on events or activities that are linked directly to the current and future situation. CCIRs consist of priority intelligence requirements (PIRs) and friendly fore information requirements (FFIRs), which assist the commander in controlling the flow of critical information.

2-5. Although essential elements of friendly information (EEFIs) are not part of the CCIR, however, they may be a priority if the commander deems them to be. **EEFIs are the critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation and, therefore, must be protected from threat detection (FM 3-0).**

2-6. During staff planning and wargaming, it is important that the commander and staff look at friendly forces through the eyes of the threat force. Conducting operations in such a way as to set predictable patterns, not adhering to strict OPSEC measures, and considering the threat on purely conventional, linear terms are examples of situations in which the threat force can easily exploit weaknesses. A commander may task the intelligence staff to determine if an EEFI has been detected by the enemy. Figure 2-2 depicts the relationship of information requirements, including CCIRs (PIRs and FFIRs) and EEFIs.

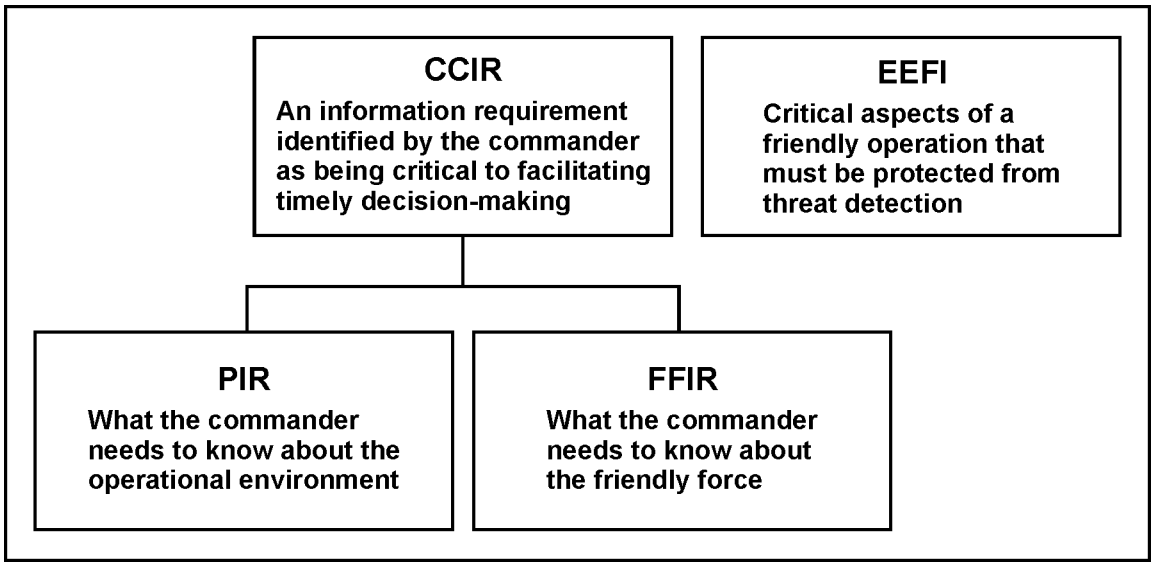

Figure 2-2. Information requirements

2-7. Because the ISR synchronization process is non-sequential and continuous, requirements are developed throughout the full spectrum of operations and at all stages or phases of operational planning, preparations, and execution. As on-going operations produce information which is analyzed into intelligence, new information requirements will be developed to drive new operations or branches and sequels of current operations. For example, intelligence derived from site exploitation conducted on today's objective could drive an operation tomorrow.

2-8. The intelligence staff generates information requirements during the mission analysis portion of the MDMP, either stated as an IR or an assumption concerning the METT-TC mission variables. The intelligence staff also consolidates and manages information requirements from other staff sections. The commander may express information requirements early in the MDMP, and may identify them specifically as PIRs. The intelligence staff refines information requirements during COA development and COA analysis (wargaming).

TYPES OF INFORMATION REQUIREMENTS

2-9. **Information requirements are all information elements the commander and staff require to successfully conduct operations; that is, all elements necessary to address METT-TC (FM 6-0).** When analyzed, information requirements concerning the threat, terrain, weather, and civil considerations (ASCOPE) become intelligence requirements or PIRs. Information requirements concerning friendly forces become FFIRs.

- **Intelligence requirements are requirements for intelligence to fill a gap in the command's knowledge and understanding of the operational environment or threat forces (JP 2-0).** Intelligence requirements are designed to reduce the uncertainties associated with successful completion of a specific friendly COA; a change in the COA usually leads to a change in intelligence requirements. Intelligence requirements that support decisions which affect the overall mission accomplishment, such as choice of a COA, branch or sequel, when approved by the commander, are designated as PIRs.
- **Friendly Force Information Requirements (FFIRs) is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0).** Although the operations staff manages the FFIR and they are part of CCIRs, the commander may require ISR assets to collect information on FFIRs. For example, personnel recovery missions may require the use of ISR assets.
- **Priority intelligence requirements are those intelligence requirements stated as a priority for intelligence support that the commander and staff need to understand the adversary or the operational environment (JP 2-0).** These are intelligence requirements for which a commander has an anticipated and stated priority during the task of planning and decision making.

2-10. Using the commander's stated requirements, upon receipt of mission, the intelligence staff develops and recommends PIRs to the commander. The commander approves PIRs, which form the basis for planning and executing operations. The goal of ISR operations is to satisfy the commander's PIRs. ISR assets are tasked to collect against these requirements, the result of which is the production of intelligence essential to the commander's situational understanding and decision making. The staff also develops the FFIRs, which provide the information that the commander and staff need about the forces available for the operations.

2-11. Although essential elements of friendly information (EEFIs) are not part of the CCIR, they may be a priority if the commander deems them to be. EEFIs are the critical aspects of a friendly operation that, if known by the threat, would subsequently compromise, lead to failure, or limit success of the operation, and therefore must be protected from threat detection (FM 3-0). During staff planning and wargaming, it is important that the commander and staff look at friendly forces through the eyes of the threat force. Conducting operations in such a way as to set predictable patterns, not adhering to strict OPSEC measures, and considering the threat on purely conventional, linear terms are examples of situations in which the threat force can easily exploit weaknesses.

2-12. PIRs should be developed for each friendly COA. Just as there are no standard situation templates or friendly COAs that will serve in all situations, there is no standard set of PIRs. Well-written PIRs meet the following criteria:

- They provide intelligence required to support a single planning task, decision, or action.
- They ask only one question.

- They focus on a specific fact, event, or activity.
- They can be satisfied using available assets or capabilities.

Example Poor PIR

"Will the threat attack? If so, where, when, and in what strength?"

2-13. The example above actually contains four significantly different questions. "Will the threat attack?" Where will the threat attack?" "When will the threat attack?" "In what strength will the threat attack?" Which of these four questions is the priority? Unless given more guidance, ISR assets must decide for themselves which part of this PIR to collect against.

2-14. It assumes the intelligence staff knows absolutely nothing about the threat situation. Actually, they probably know more about the situation than "the threat might attack sometime, somewhere, and in some strength." Using the IPB process, they can provide a more focused PIR than this.

2-15. Finally, when wargaming potential friendly and enemy COAs, the staff should find some aspects of this PIR to be irrelevant to the friendly COA. For example, the defense may be fully capable of repelling the threat regardless of when they actually attack. Perhaps the focus needs only to be on where they will attack, supporting a decision on employment of the friendly reserve.

Examples of Good PIRs

"What are the religious leaders of neighborhood X saying about friendly forces?"
"How does terror cell Y receive payments from terror financier Z?"

2-16. Each of these examples asks one question and focuses on a specific fact, event, or activity. PIRs can be used by the commander and staff to determine threat capabilities, objectives, intent, or to support (confirm or deny) a decision or hypothesis on probable enemy COAs.

2-17. Commanders and staffs may be concerned that making new intelligence requirements and PIRs will overloaded the collection system. A greater number of PIRs and information requirements which are clear and specific are more likely to be satisfied. The more specific focus makes it easier to develop SIRs, ISR tasks, and RFIs to support them. The number of ISR tasks and RFIs will remain more or less constant. The poorly written PIR that asks four questions will need about as many ISR tasks and RFIs as four specific, well-written PIRs.

2-18. As discussed earlier, the commander's decision making drives PIR development during mission analysis and wargaming (COA analysis). Indicators can also drive PIRs and intelligence requirements development, especially in stability operations where confirmed indicators could lead the commander to consider new PIRs for tomorrow's operations. Requirements development does not stop with the OPORD publication, but remains a continuous assessment process throughout operations. Requirements are refined and updated as necessary to identify precise intelligence needed to trigger a decision. As military operations develop, requirements can be re-prioritized based on many factors, to include high-payoff targets and combat assessment requirements.

2-19. Graphic aids represent aspects of the AO and facilitate situational awareness and situational understanding. These aids are developed during wargaming and continuously updated and refined to facilitate the common operational picture (COP), intelligence running estimate, or other products for the commander. For intelligence planning, the ISR synchronization plan, ISR plan, ISR matrix, and decision support template (DST) are tools to ensure ISR operations are linked to the commander's requirements and respond in time to influence decisions and operations.

2-20. After updating requirements, the intelligence staff refines ISR taskings in order to assign responsibility; eliminates satisfied requirements; and develops specific tasks and/or RFIs for specific collectors in order to refocus efforts. This must be coordinated through the other staff members, especially

the operations officer who will publish warning orders (WARNOs), fragmentary orders (FRAGOs), or OPORDs as necessary.

DEVELOPING REQUIREMENTS FOR TARGETING

2-21. Developing requirements also supports the commander's decision making regarding targeting. Well-stated requirements help the commander maneuver forces and apply lethal and nonlethal fires or effects in the AO to accomplish the mission.

2-22. **In intelligence usage, a target is a country, area, installation, agency, or person against whom intelligence operations are directed (JP 1-02).** To effectively target the threat, the staff develops named areas of interest (NAIs) and targeted areas of interest (TAIs). The staff can also develop an HVT list which could include not only geographic NAIs or TAIs but also organizations, networks, and individuals who are identified as key or critical elements of the operational environment. There is no limit to how creative or flexible the intelligence staff can be in developing and focusing requirements for targeting in support of the commander's objectives and intent. In certain circumstances, some requirements may not be focused on a certain geographic area.

NAMED AREA OF INTEREST

2-23. **A named area of interest is the geographical area where information that will satisfy a SIR can be collected (FM 3-90).** NAIs are usually selected to capture indications of enemy COAs but also may be related to battlefield and environmental conditions.

2-24. Commanders tailor the shape of the NAI symbol to the actual area they want observed, rather than using a prescribed shape. It is possible to redesignate an NAI as a TAI on confirmation of enemy activity within the area, allowing commanders to mass the effects of their combat power on that area. See FM 3-90 for more information on NAIs.

TARGETED AREA OF INTEREST

2-25. **A targeted area of interest is the geographical area or point along a mobility corridor where successful interdiction will cause the enemy to abandon a particular COA or require him to use specialized engineer support to continue. It is where the enemy can be acquired and engaged by friendly forces (FM 3-90).** Commanders designate TAIs where they believe their units can best attack high-payoff targets.

2-26. The unit staff develops TAIs during the targeting process, based on the currently available products resulting from the IPB process. These TAIs are further refined during wargaming and finally approved by the commander during COA approval. The shape of a TAI reflects the type of target and the weapon system intended to engage that target. They are normally cued by surveillance assets, which include unmanned aircraft systems (UASs), combat observation and lasing teams, long-range surveillance units, fixed-wing reconnaissance aircraft using a variety of sensors, and special operations forces. Commanders can designate a TAI for any of their organic or supporting systems, including close air support. See FM 3-90 for more information on TAIs.

2-27. TAIs are obviously associated with threat information requirements. NAIs, on the other hand, are used to gather information in order to inform the commander about threats, civil considerations (ASCOPE), or to pinpoint terrain which might be considered key or decisive terrain. Religious buildings, places of worship and shrines are an example of potential NAIs which are part of civil considerations (ASCOPE) of the METT-TC mission variables. The commander may designate them as NAIs in order to monitor conditions or activities at these locations to measure atmospherics. NAIs and TAIs focus collection efforts in order to facilitate the commander's situational understanding.

HIGH-VALUE TARGETS

2-28. **A high-value target is a target the enemy commander requires for the successful completion of the mission. The loss of an HVT would be expected to seriously degrade important enemy functions throughout the friendly commander's AOI (JP 1-02).** In the most common usage, HVTs are systems or facilities; however, in counterinsurgency or stability operations, personality targets may be the HVT for lethal or nonlethal fires and effects. For more discussion on targeting in counterinsurgency operations, see FM 3-24.

DEVELOPING REQUIREMENTS

2-29. Developing requirements includes the following steps: anticipate, analyze, develop indicators, and develop SIRs.

ANTICIPATE

2-30. Intelligence officers and G-2/S-2 staff identify new or refine existing requirements and present them to commanders for approval. They must recognize when and where to recommend to operations officers to shift collection. Anticipating and developing new requirements is based on solid situational awareness, a thorough review of IPB products and existing intelligence holdings, and an understanding of the concept of the operation to include branches, sequels, and the need to transition into follow-on operations.

2-31. The ability to anticipate requirements will give intelligence officers additional time to plan for the use of ISR assets available to them. Anticipating upcoming requirements also allows intelligence officers to communicate with higher headquarters and plan for future submissions of RFIs. The more time intelligence officers can give the units that control the Army, Theater, and National level systems the more likely it will be to obtain the required support for a specified timeframe. A good example is forecasting the additional ISR support needed during critical events such as national elections. If intelligence officers know that national elections will occur in 6 months, they can develop additional requirements and request asset support from higher headquarters in advance.

ANALYZE

2-32. Requirements are analyzed to ensure the most effective use of ISR assets. Analyze each requirement to determine how best to satisfy it. Sometimes this does not require tasking a unit, organization, or sensor for collection. Often, a newly received requirement can be satisfied by intelligence reach or by submitting an RFI. This includes separating, recording, validating, consolidating, and prioritizing each recommended requirement.

Separate

2-33. Intelligence officers categorize intelligence gaps by those that can be answered through—

- Intelligence Reach. Although usually not as responsive as a unit's own assets, intelligence reach may be the only way to satisfy an intelligence requirement. If at all possible, one should not depend solely on intelligence reach to answer a PIR.
- RFI for Collection. Submit RFIs for collection to higher and lateral echelons.
- Other collection recommendations.

Record

2-34. Intelligence officers receive requirements in the form of ISR tasks and RFIs, as well as requirements produced from mission analysis, COA analysis (wargaming), and current operations. Record requirements from higher, adjacent, and subordinate units along with the requirements produced during mission planning. This record tracks each requirement from its receipt to its eventual satisfaction, merger, or

elimination. Recording can be done using a spreadsheet, database, or other mechanism prescribed by unit SOPs.

Validate

2-35. Validate each requirement by considering its necessity, feasibility, and completeness.

- Necessity. Is this requirement really necessary or valid? If so, has it already been satisfied? Check databases to see if someone has already collected the information or produced the intelligence. If a product already exists that satisfies the requirement, refer the requester to the agency that produced it. If the requester does not have access to that agency's database, then obtain and provide the product to the requestor. Refer requests for production to the appropriate agency. In some cases, the intelligence already exists, but not in the format the requestor desires. One example of this is a unit that wants a demographics map put together from data that already exists.
- Feasibility. Does the unit have the assets with the capabilities to execute the mission in time and with the detail required to support a decision? If not, can the unit submit an RFI to the echelon that does own the ISR capability, with a reasonable expectation of getting a response in time?
- Completeness. All requirements should specify:
  - WHO (needs the results).
  - WHEN (time that the indicator is expected to occur and the latest time the commander needs to know [LTIOV]).
  - WHAT (activity or indicator).
  - WHERE (geolocation, NAI, or TAI).
  - WHY (justification).
  - Other specific instructions or information.

Consolidate

2-36. Requirements received as ISR tasks and RFIs are often similar to those generated during mission planning. Consolidation involves identifying identical and similar requirements and forming them into a single requirement. Successful consolidation results in a smaller number of requirements to track and an identification of which subordinate elements may or may not be capable of collecting on a requirement.

2-37. Simplify the collection effort by merging similar requirements. Normally, replace the more poorly written requirement with the wording of the better justified or more specific requirement. However, exercise caution when—

- Merging requirements, the intent of either of the original requirements is not lost.
- The accountability of merged requirements is maintained through accurate recordkeeping.
- Dissemination is made to every requesting headquarters when a requirement is satisfied or eliminated.

Prioritize

2-38. Prioritize each intelligence requirement based on its importance in supporting the commander's intent and decisions. Prioritization, based on the commander's guidance and the current situation, ensures limited ISR assets and resources are directed against the most critical requirements. Effective prioritization requires monitoring of the operation to respond to changing situations.

2-39. When prioritizing, consider the importance of the requirement above the echelon that generated it. A subordinate commander's requirement may well be more important to the success of the commander's mission than all the other requirements.

2-40. When prioritizing requirements, intelligence officers should consider the ability to meet the requirement as well as justification, specificity, significance, and time phasing of requirements over the course of the operation.

Justification

2-41. Requirements are justified by their linkage to decisions. Consider the following two requirements:

- Requirement 1. ISR task from higher: "Where does the terror cell obtain improvised explosive device (IED) components and precursor explosive materials?"
- Requirement 2. RFI from a subordinate: "Is the threat's reserve tank battalion assembled for counterattack in NAI 5 or NAI 6? (Triggers artillery strikes and decision to send attack helicopters to either TAI 5 or TAI 6.)"

2-42. In the above case, prioritize requirement number 2 higher than number 1, even though the first is a task from higher and the second is a request from a subordinate. Accept and plan collection to satisfy the senior command's specific order (a specified task); however, its priority is determined by the importance of the decision it supports.

Specificity

2-43. Requirements should be narrowed and refined to the most specific WHAT, WHEN, and WHERE questions possible. The WHY is the justification. Consider the following two requirements:

- Requirement 1. Specific order from higher: "Which mosques in Fallujah have been broadcasting anti-coalition messages during Friday prayers?"
- Requirement 2. Specific request from a subordinate: "When will terrorist Y return to his family's home in Sadr City?" (Triggers repositioning of other ISR assets to continue surveillance and a possible raid to capture terrorist Y.)"

2-44. Requirement number 1 is so broad that collectors have authority to collect on just about anything. These kinds of general, unfocused questions usually generate general, unfocused answers. Requirement number 2 is a thoroughly considered, focused question. The requester knows exactly what is required and stands a better chance of receiving the required answer. Once again, rank requirement number 2 higher than number 1.

Significance

2-45. What is the relative significance of the activity to the commander's intent? Some activities within the AO are more critical to your commander's intent than others. During wargaming, commanders will give guidance on what is considered most important. If not, the commander's intent is reflected in the priorities assigned to each part of the operation. Use this as a basis for establishing a prioritized list from which to make recommendations to the commander for approval.

2-46. After intelligence officers prioritize the list and make recommendations, commanders designate some of the most important requirements as PIRs and therefore declare that the effort to answer PIRs is mission essential. In other words, failure to satisfy the PIR endangers the command's mission accomplishment. The PIRs are then arranged in priority order. For maximum effectiveness intelligence officers and commanders should refine the PIRs to specific questions that are linked to operational decisions as discussed above.

Time Phasing

2-47. Time phasing influences prioritization. Time phasing of intelligence requirements, like synchronization, is a continuous process. The operation may progress more or less quickly than anticipated during staff wargaming. Consequently, the expected timelines based on the original staff wargaming may change as the operation unfolds. Monitor the conduct of the operation and stay alert for changes in the

LTIOV based on other shifts in the operational timeline. The most important requirement may have an LTIOV in a later stage of an operation.

2-48. Normally, each intelligence requirement has a time relative to a point in the operation when satisfying it will be critically important, after which the requirement may be overcome by events and it becomes no longer significant or no longer necessary to collect. Consequently, the relative priority of each requirement may change over time. Some PIRs may remain the same for the duration of the operation or entire campaign, while other PIRs change during the operation, from phase to phase or based on the sequence of events as they unfold.

2-49. The G-2/S-2 staff establishes LTIOV based on the commander's input, the priorities in each phase of the operation, and by considering the time required to deliver the finished intelligence to the commander and staff. They must be sure that they establish an LTIOV which will allow delivery of the intelligence in time for the commander to make a decision.

2-50. Once commanders approve PIRs, intelligence officers and staff begin the process of translating PIRs and other intelligence requirements into indicators and SIRs, which result in ISR tasks and RFIs for collection. Indicators and SIRs may be developed concurrently.

DEVELOPING INDICATORS

2-51. **An indicator is an item of information which reflects the intention or capability of an adversary to adopt or reject a COA (JP 2-0).** In Army intelligence usage, indicators are positive or negative evidence of threat activity or any characteristic of the AO which points toward threat vulnerabilities or the adoption or rejection by the threat of a particular capability, or which may influence the commander's selection of a COA. Indicators may result from previous actions or from threat failure to take action. Indicators are the basis for situation development. Indicators are positive or negative evidence of threat, other activity or characteristic of the AO that points toward capabilities, vulnerabilities, or intentions. Indicators show the adoption or rejection by the threat of a particular COA which may influence the commander's selection of a COA.

2-52. Indicators may also result from previous actions or from threat failure to take action. Taken together, indicators may prove or disprove a PIR. Individual indicators usually do not stand alone. Analysts on the intelligence staff develop indicators, integrating each indicator with other factors and indicators before patterns are detected and threat intentions are established.

2-53. The event template and event matrix are tools to assist in visualizing indicator development. (Refer to
FM 2-01.3 when published.) The event template depicts the NAIs where activity or lack of it will indicate which enemy COA the threat has adopted. The combination of the NAI, indicators, and time phase lines associated with each threat COA form the basis of the event template.

2-54. The event matrix complements the event template by describing indicators and activities expected to occur in each NAI. It normally cross-references each NAI and indicator with the times they are expected to occur and the COAs they will confirm or deny and its relationship to other events in the AO. The primary use of the event matrix is to plan intelligence collection; however, it serves as an aid to situation development as well.

2-55. The intelligence analyst uses indicators to correlate particular events or activities within the operational environment. These may pertain to threat or civil activities. Indicators will identify probable enemy COAs and determine what events or activities must occur for a threat to follow a particular COA. The ability to read indicators (including recognition of threat deception indicators) contributes to the success of friendly operations. The analyst integrates information from all sources to confirm indicators of threat activities. As indicators are detected and confirmed, PIRs are satisfied.

SPECIFIC INFORMATION REQUIREMENTS

2-56. SIRs describe the information required and may include both the location where and the time during which the information can be collected. Generally, each intelligence requirement generates a set of SIRs.

2-57. Ideally, each intelligence requirement will contain all the information the G-2/S-2 needs to develop supporting SIRs. In such cases, the intelligence requirement states where and when to collect; intelligence officers need to refine what to collect into specific items of information. If they receive requirements which do not contain the information needed to establish where and when to collect, they must coordinate with the originator to obtain that information. The needed information should be contained in the IPB products that helped generate the requirement.

2-58. When the intelligence staff matches indicators with the where, when, and what to collect, transition to the creation of SIRs occurs. As intelligence officers develop SIRs, they should coordinate with operations officers to get an understanding of the specificity required to support planning. A technique is to develop SIR sets while the operations officers develop the collection strategy for each requirement and the general scheme of maneuver.

2-59. SIRs may be expressed as a question or a statement. The first step is to make each indicator more specific by identifying the "where to collect," tying it to a specific point in the AO. For example, use a specific NAI to replace the general idea of "forward" in the indicator "forward deployment of artillery" and rewrite it as "artillery deployed in NAI 12." If the intelligence requirement is well written, it will contain the level of detail necessary for the intelligence staff to do this.

2-60. Use a similar technique to specify the "when to collect." If the intelligence requirement is well written, it will contain the timelines needed to establish the "when to collect." If it does not, coordinate with the intelligence section. Their situation templates depicting the enemy COA under consideration and the graphics depicting the friendly scheme of maneuver should help provide the information needed to establish collection timelines for the NAI in question.

2-61. Develop more detail in the observables by identifying the specific information which supports the indicator. For example, specific information which supports the indicator "artillery deployed in NAI 12" might include—

- Presence of artillery weapons.
- Presence of fire direction control equipment or vehicles.
- Presence of artillery associated communications equipment.
- Presence of artillery ammunition carriers.

2-62. Develop each indicator further by coordinating with the intelligence section to identify the specific types of equipment or other specifics associated with each developing SIR.

2-63. For example, replace the generic "artillery weapons" with specifics such as "M-109 or M-110 self-propelled artillery systems" if that is what should be present within the NAI. Similarly, replace "artillery associated communications" with "the digital data signal" if that is the type used by the threat force in question. This helps commanders and operations officers to optimize their collection capabilities against the target in question.

2-64. Because each intelligence requirement will generate a number of indicators which will in turn generate a number of SIRs, finalize each SIR by labeling it with an identifier that allows intelligence officers to trace it back to the original intelligence requirement. A final SIR might be written as "Are there digital data signals active in NAI 12 between 041200 and 060200 March? LTIOV: 060400 March. "

2-65. Remember that indicators and SIRs are analytical tools for the intelligence section. Intelligence officers ensure the analyst has the information that truly indicates threat actions and satisfies the original requirement.

Chapter 3

Develop Intelligence, Surveillance, and Reconnaissance Synchronization Plan

Intelligence officers use the ISR synchronization plan, with staff input, to synchronize the entire collection effort, to include all assets the commander controls, assets of lateral units and higher echelon units and organizations, and intelligence reach to answer the CCIRs. See figure 3-1.

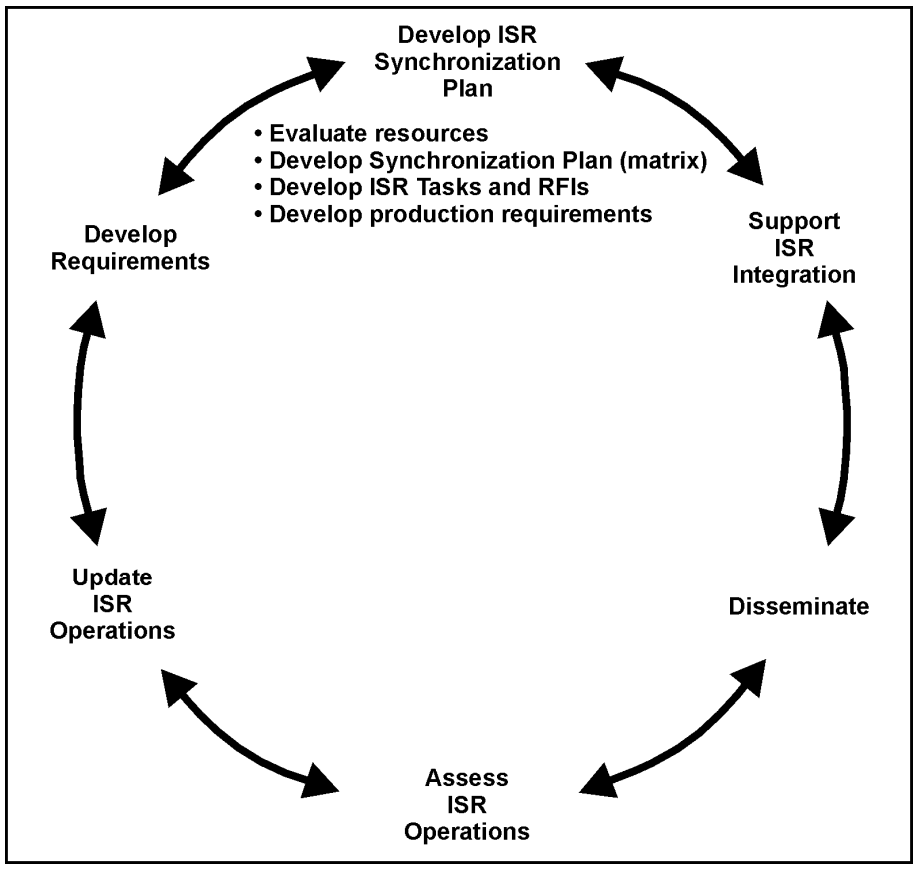

Figure 3-1. Develop ISR synchronization plan

GENERAL

3-1. The ISR synchronization plan is used to recommend potential ISR assets to collect against the CCIR (PIR, intelligence requirement), the NAI, and the period of time. The ISR synchronization plan aids in synchronizing and deconflicting the ISR effort with the overall operation and the commander's decision points.

3-2. The ISR synchronization plan can be a simple automated spreadsheet used solely by the intelligence staff or a more formal document, depending on the complexity of the ISR tasks and the needs of the unit. It will most often be in matrix format. The completed ISR synchronization plan is the intelligence staff's tool to support the development of the ISR plan and to synchronize intelligence production with reporting.

3-3. In the next activity of the process, intelligence officers must evaluate resources; develop the ISR synchronization matrix and proposed scheme of support; develop specific ISR tasks and RFIs; and develop production requirements in order for the intelligence and operations officers to provide the commander with the best recommendations regarding ISR tasks and collection.

3-4. The intelligence staff begins to identify those ISR assets best suited to conduct the collection, and those assets must include assigned and attached assets as well as other assets to which the unit has reasonable access. The intelligence officer then evaluates the suitability of each ISR asset for each requirement by assessing capability, availability, vulnerability, performance history, and reliability. This planning includes determining the appropriate balance and control of ISR assets and their potential deployment in time and space. At this point, the intelligence officer begins to develop ISR tasks for collection assets and production requirements for the staff so that collection and production satisfy the CCIRs.

EVALUATE RESOURCES (INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE ASSETS)

3-5. The intelligence officer and staff take the prioritized requirements and begin to match them with suitable ISR assets using the following criteria:

- **Availability:** The intelligence officer must know the collectors and processors available to them at their own echelon, at echelons above and below, as well as how to access those ISR assets. Aside from maintenance and operator readiness issues, the intelligence officer has influence over the availability of assigned and attached assets. Determine higher echelon and other service asset availability by reviewing various scheduling and tracking mechanisms. Human intelligence (HUMINT) assets are not tied to traditional schedules; their availability is linked to geographic access, support relationships, and workload.
- **Capability:** Intelligence officers must know and address the capabilities of all unit assets, not just of the traditional ISR assets. They must consider the capabilities of such assets as the chemical company, scout platoon, Engineer Company, transportation section, and others. Capability includes such things as—
  - Range. What is the asset's ability to move and maneuver, to include travel and support times? If the best asset is a UAS, what are its transit and dwell times?
  - Day and night effectiveness. Consider factors such as available optics and thermal crossover.
  - Technical characteristics. Can the system see through fog or smoke? Can it continue despite hostile electronic warfare? Each asset has time factors for task accomplishment which must be taken into account.
  - Reporting timeliness.
  - Geo-location accuracy.
  - Durability. Can the aircraft launch in high winds or limited visibility? Can the prime mover cross restricted terrain?

Examples

Assigning a scout platoon to conduct a zone reconnaissance is certainly within the capability of that platoon. However, a zone reconnaissance is a time-intensive mission leaving this ISR asset tied up for significant amounts of time to conduct this mission.

Another example is transit time for a UAS. When planning ISR synchronization, the intelligence officer must consider the time it takes a UAS to travel to and from its launch and recovery site or base of employment to the intended surveillance target.

In both examples, assigning one mission to an asset or unit must be balanced against other requirements because they will not be available for other missions for a period of time which might prove critical.

- **Sustainability:** Each collection asset has unique sustainment requirements; therefore, the intelligence officer must consider the collection asset's sustainability for longer duration operations. The longer the collection period on the ISR synchronization matrix, the harder it will be to find assets for continuous activity. Weather can significantly impact sustainability of certain ISR assets. Redundancy, discussed later in this chapter, is one solution to the sustainability problem.
- **Vulnerability:** The intelligence officer must evaluate the collector's vulnerability to threat forces, not only in the target area but also along the entire route of travel. For example, a helicopter's capabilities make it suitable as an ISR asset; however, its vulnerabilities make it potentially an HVT for the enemy. Therefore, it is important to evaluate the threat's ability to locate, identify, and destroy our ISR assets.
- **Performance History:** Experienced intelligence officers know which ISR assets they can rely on to meet the commander's intelligence requirements. Readiness rates, responsiveness, and accuracy over time may raise one collector's reliability factor.

Example

A collector's reported information was verified through multi-source reporting in the all-source analysis process. This increases the credibility and reliability of that particular collector's future reporting.

3-6. Certain capabilities require confirmation, especially if targeting is an issue. For example, target selection standards may require you to rely on systems capable of providing targeting accuracy, such as Advanced Synthetic Aperture Radar System (ASARS), Joint STARS, or UASs. If experience shows that ASARS is often unavailable because of local weather patterns, an experienced intelligence officer considers this in evaluating the system's performance history; perhaps leading to the selection of an alternate system.

3-7. ISR assets include:

- ISR Units. ISR units are those specialized units that have surveillance and/or reconnaissance as their primary mission. These units include but are not limited to—
  - Infantry and armor scout platoons.
  - Cavalry units.
  - BFSBs.
  - MI elements to include all HUMINT, geospatial intelligence, SIGINT, measurement and signature intelligence (MASINT), and counterintelligence (CI) assets.
  - UAS platoons.
  - Fires target acquisition sections.

- Long-range surveillance units.
- Chemical, biological, radiological, and nuclear squads.
- Reconnaissance squadrons.
- Attack and/or reconnaissance aircraft.

- ISR Capable. ISR-capable units are units that do not have surveillance and/or reconnaissance as their primary mission, but may be directed to perform these missions to complement or expand the ISR capability. Examples of these units include—
  - Combat Engineer Battalions.
  - Engineer Reconnaissance Sections.
  - Infantry Battalions.
  - Military Police.
  - BCTs.
- Additional Capabilities. Those units that are not tasked with a surveillance and/or reconnaissance mission but observe and report information incidental to their normal missions. CCIRs and unit SOPs dictate the reporting activities of these units. Their reports provide valuable information about the threat and environment that assists the intelligence staff in building an accurate picture of the threat and alerting the command to unpredicted, potentially dangerous threat activity. Examples of these units and operations include—
  - Unit leaders traveling to meet with local leaders.
  - CA teams reporting the location and condition of refugee concentrations visited while assisting non-governmental agencies. They report statistics and data on populations, essential services, and governmental functions which can be useful in answering the commander's PIR.
  - Transportation or sustainment units reporting route conditions while moving supplies throughout the AO.
  - Any element moving from point to point in the AO. **All** Soldiers are potential sources of relevant information regarding the threat and the operational environment.

3-8. Other assets which collect information to satisfy intelligence requirements include national, joint, and multinational assets.

DEVELOP INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE, SYNCHRONIZATION PLAN (MATRIX)

3-9. Intelligence staffs begin the ISR synchronization plan by establishing blank timelines for each ISR asset. The ISR synchronization plan can show timelines for ISR assets, units, or disciplines. Intelligence officers then capture the LTIOV for each SIR on the matrix. This is easy to determine since each ISR task is exactly matched to the criteria to execute a decision identified in wargaming. The earliest time information is of value (ETIOV) and LTIOV timelines on the working ISR synchronization matrix are determined by backwards planning from the commander's decision points recorded on the DST.

3-10. ETIOV is a tool used by the intelligence and operations officers to achieve synchronization and integration of ISR activities into the overall plan. ETIOV is particularly useful during wargaming to determine when ISR assets, units, and Soldiers should be moved on the battlefield and retask as mission priorities change. ETIOV will not appear on the final ISR plan as it would confuse units, assets, and Soldiers tasked with ISR missions. Figures 3-2 and 3-3 provide examples of the evolution of an ISR synchronization plan.

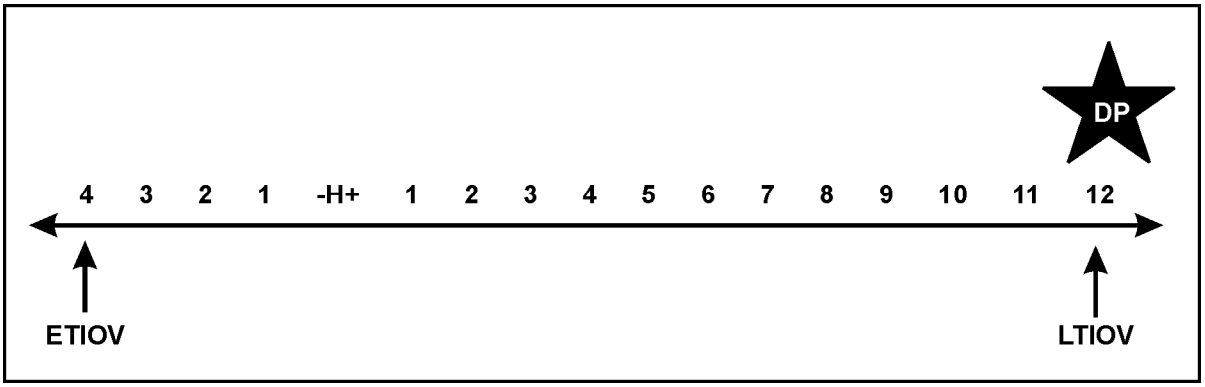

Figure 3-2. Working timeline for ISR synchronization plan

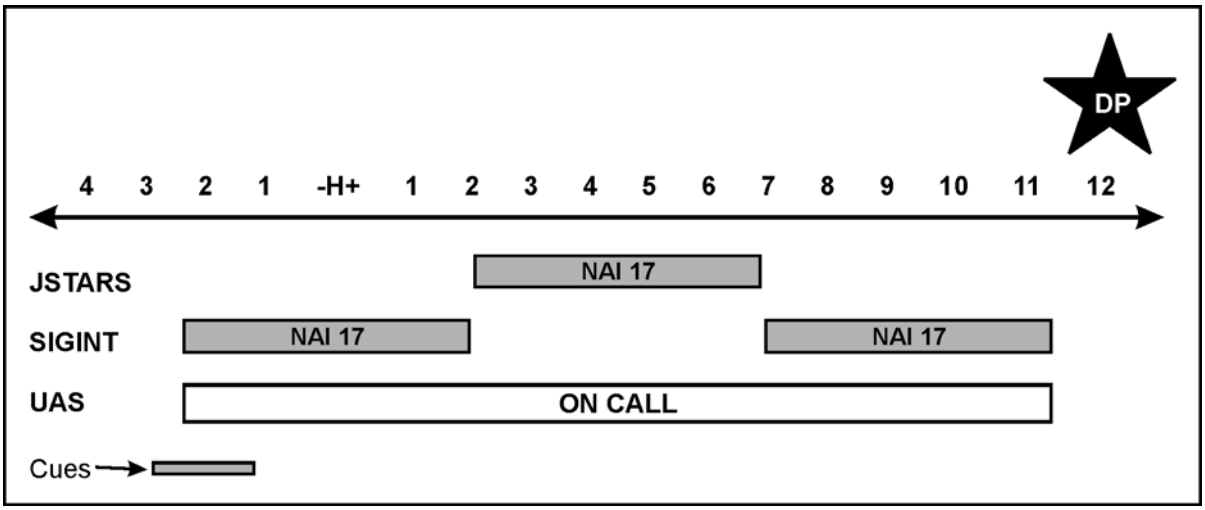

Figure 3-3. Working ISR synchronization plan and cueing strategy for one NAI

3-11. The operations and intelligence staffs should resist favoring or becoming too reliant on a particular unit, discipline, or system when recommending or employing ISR assets. Balance is planning redundancy when required, eliminating redundancy when not desired, and ensuring an appropriate mix of ISR assets or types. Additionally, the ability to cue ISR and maneuver assets allows the operations officer flexibility and capability to collect information and to see the AO more clearly. ISR capabilities complement each other. The ISR synchronization plan is useful in determining or evaluating balance.

- **Redundancy** planning as part of collection strategy development involves the use of several same type assets to cover the same NAI. Use redundant tasking when the probability of success by any one system is low. For example, if you focus several SIGINT collectors on a designated emitter at different times, the probability of intercept improves, even if the emitter operates intermittently. The chance of accurate geo-location is also improved through the use of redundancy.
- **Mix** means planning for complementary coverage by a combination of assets from multiple units. Sensor mix increases the probability of collection, reduces the risk of successful threat deception, facilitates cueing, and provides more complete reporting. For example, scouts report resupply activity within a known assembly area; SIGINT collection of the associated logistics net may provide unit identity, subordination, and indications of future activity.

- **Cue** involves the use of one or more sensor systems to provide data that directs collection by other systems. For example, sweeping the AO electronically with wide-area surveillance systems reveals activity that cues direct collection by a more accurate sensor system. Cueing maximizes the efficient use of finite ISR assets in support of multiple, often competing, intelligence collection priorities. (See figure 3-3 for an example cueing strategy.)

3-12. If a HUMINT source reports the absence of activity, the G-2/S-2 might recommend redirecting the UAS to another mission or use it to confirm the absence of activity, depending on the relative priority of requirements and the reliability of the source.

3-13. If the HUMINT source reports significant activity earlier than anticipated, the UAS launch sequence can be accelerated to collect supporting detail or the UAS asset retasked to collect against another requirement.

3-14. Cueing can also occur dynamically (outside the ISR synchronization plan) as one system or echelon tips the other off to an unexpected collection opportunity. Higher headquarters, adjacent or multinational ISR assets, also cue assets throughout all of the warfighting functions.

3-15. Displaying all the potential asset information in an initial ISR matrix allows intelligence officers to visually ensure all assets and all NAIs are covered for collection. Figure 3-4 is an example of a wargaming matrix.

270600 to 280559 (I) May																
	Infantry	Aviation	Military Police	Air Defense	Field Artillery	Signal	Sustainment	Scouts	SIGINT	HUMINT	UAS	CI Team	GEOINT	MASINT		
NAI 1																
NAI 2																
NAI 3																
NAI 4																
NAI 5																
NAI 6																
What is the effect of the sentiment of the local populace in the BDE AO?																
(Pro, neutral, anti-US?) (LTIOV: Continuous)																

Figure 3-4. Wargaming matrix

3-16. The wargaming matrix records the results of COA analysis and is used to develop the ISR synchronization plan. The ISR synchronization plan recommends assets for tasking to satisfy PIRs and intelligence requirements. This plan can be expressed as a matrix or annex. The ISR synchronization plan facilitates analysis by identifying or helping to identify critical alarms and filters, expected report times,

expected production, and directions for production and dissemination. The ISR synchronization plan generally includes—

- PIRs and information requirements.
- Indicators.
- Times and dates of the collection mission or RFI.
- LTIOV.
- NAIs.
- Available assigned, attached, supporting, and higher echelon units and organizations which possess collection assets to be tasked or requested for collection tasks.
- Tasks and RFIs.
- Other information deemed necessary to support the management of the collection effort.

3-17. Intelligence officers maintain situational awareness to identify gaps in coverage and to identify the need to redirect the tasking of assets. The G-2/S-2 synchronizes commanders' new intelligence requirements, requests from subordinate and lateral organizations, and tasks from higher headquarters into the ISR synchronization plan. The ISR synchronization plan is most often developed and published in a matrix format. Figure 3-5 is an example of an ISR synchronization plan matrix.

CCI PIR or Intelligence Requirements	SIR			LTIOV	Capable Assets					Reporting	Action Required	Remarks
	Indicators	Indicator Specifics	NAI									
INSTRUCTIONS												
List PIR and IR. Leave enought space to list indicators for each PIR and IR in column 2.	List indicators that will satisfy each PIR and IR.	If necessary, list specific information required to satisfy the indicator. Key requirements to NAI on the event template if possible. These requirements form the basis for order and requests.	Number.	Time may be specific, periodic, or as obtained.	Place an "X" under each agency that can collect the required information. Circle the "X" when an agency has been selected and tasked.					Include established communications; for example, multichannel, FM, SINCGARS, or state "by SOP." Include means of reporting; for example, via spot report format. Report precedence: Example: Flash, immediate	Examples: - Retasking of assets - Execution of branch or sequel - Call for fire - New plan or orders - Information S2 for decision - Report in INTSUM	

Figure 3-5. Sample ISR synchronization plan in matrix format

DEVELOP INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE TASKS AND REQUESTS FOR INFORMATION

3-18. Intelligence and operations officers work together to convert the SIRs into ISR tasks. The officers should first use organic ISR assets, as these assets usually are more responsive to their respective commander. These tasks are published in annex L and the specified task section of the OPORD or FRAGO.

3-19. The intelligence and operations officers can easily translate a well-written SIR into an effective ISR task by making a directive vice inquisitive statement. Tailor the reporting criteria to the capabilities of the tasked ISR asset. For example:

- SIR: Will more than 20 insurgents subordinate to the Mahdi Army or Muqtada Al-Sadr pass through NAI 8 between 041800 and 052000 March?
- ISR task: Report the presence of Mahdi Army personnel in NAI 8 between 041800 and 052000 March. Specify direction of movement, numbers, and types of vehicles. LTIOV: 060400 March.
- SIR: Is there normal activity in the city of Fallujah, NAI 10 on 21 June?
- ISR task: Report the presence of threat counter-reconnaissance activity in NAI 10 between 210900 and 211800 June. LTIOV: 211800 June.

3-20. Prioritize ISR tasks for the ISR assets. Each asset may have several ISR tasks to respond to. Prioritization affects reporting as well as collection procedures. To avoid the "first in, first out" approach to reporting, especially if communications paths are limited, specify which answers need to be transmitted first regardless of when they were received.

Note. Be specific. However, avoid overly restrictive reporting guidelines. Allow ISR assets the latitude to provide information you and the analysts had not anticipated.

3-21. Emphasis or amplification tasking supplies the specifics required without artificially restricting ISR asset capability. Include instructions for direct dissemination of combat or targeting information to the original requestor. Sometimes direct dissemination will not be possible due to communications systems or classification considerations.

3-22. Tailor the ISR task to the selected collection system or organization. For example, some imaging systems require a basic encyclopedia number rather than a geographic or universal transverse mercator coordinate for target location. Most Air Force airborne collection platforms recognize geographic coordinates only. HUMINT collectors need to have specific timeliness, reporting, and dissemination guidance. If the ISR tasks are specific enough, they can roll over into the actual tasking or request mechanism or format.

3-23. Submitting an RFI to the next higher or lateral echelon is the normal procedure for obtaining intelligence information not available through the use of available ISR assets. Users enter RFIs into an RFI management system where every other user of that system can see it. Hence, analysts several echelons above the actual requester become aware of the request and may be able to answer it.

3-24. When the unit is unable to satisfy a collection requirement through its own assets, the intelligence staff composes and submits an RFI to the next higher echelon (or lateral units) for integration within its own ISR plan. At each echelon, the requirement is validated and a determination made as to whether or not that echelon can satisfy the requirement. If that echelon cannot satisfy the requirement, it is passed to the next higher echelon.

Note. This process continues until the requirement is satisfied, the intelligence is no longer needed, or it is determined that the requirement cannot be satisfied.

3-25. Throughout the RFI process units must apprise the submitting organization of the RFI's status: accepted for action, passed to another organization for action, returned without action (invalid or infeasible request), or closed (satisfied). The intelligence staff must track all production requirements, particularly those transmitted to higher echelons. When a requirement is satisfied or determined to be overcome by events, intelligence officers must notify the higher headquarters that the requirement is closed.

DEVELOP PRODUCTION REQUIREMENTS

3-26. Intelligence officers plan and coordinate intelligence production activities to provide timely and relevant intelligence products to commanders, staff, and subordinate forces. The ISR synchronization plan is used to plan production activities and timelines to answer the CCIRs and meet the commander's need for situational understanding.

3-27. Intelligence production includes analyzing information and intelligence and presenting intelligence products, assessments, conclusions, or projections regarding the AO and threat forces in a format which aids the commander in achieving situational understanding. Production occurs in the intelligence section or separate analysis element at every echelon from the national to tactical levels. At the company level, some commanders may choose to form a company-level intelligence cell (ad hoc) to process information and produce intelligence.

3-28. The digital collaborative environment enabled by the DCGS-A enterprise allows the unit to distribute analysis and production between the intelligence officers and subordinate intelligence units maximizing intelligence analysis capabilities throughout the unit and a federated intelligence environment. Effective requirements management ensures the commander receives the intelligence products and services required to accomplish the mission. Automated intelligence processing systems provide intelligence that can be tailored to the commander's needs. The G-2/S-2 evaluates the success of production based on commanders' and staff's satisfaction with the products provided in response to the production requirement.

INTELLIGENCE REACH

3-29. Intelligence reach is a process by which military forces proactively and rapidly access information, receive support, and conduct direct collaboration and information sharing with other units and agencies both deployed in theater and outside the theater unconstrained by geographic proximity, echelon, or command. Intelligence reach is distinguishable from the normal process of providing combat information and intelligence up and down the chain of command. Intelligence reach allows a unit to obtain information or intelligence directly without submitting a formal RFI. Units can access the information and intelligence holdings of other organizations, normally via classified and unclassified Internet access.

3-30. Intelligence reach may be the only way to satisfy an intelligence requirement. Depending upon the validity of the source, one should not solely depend on intelligence reach to satisfy a SIR associated with a PIR. In the same manner that your unit may require combat information or intelligence from external ISR sources, other organizations may depend upon your unit to provide them with information or intelligence that only your unit can provide. The intelligence staff synchronizes the requirements (RFIs and intelligence reach) from external elements into the unit's ISR synchronization plan and/or ISR plan. See FM 2-0 for further details on intelligence reach.

ISSUE THE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION PLAN

3-31. When the preceding activities are accomplished, intelligence officers circulate the ISR synchronization plan. This is put together in concurrence with the operations officer who then integrates the ISR synchronization plan into the ISR plan. It is published as appendix 2, annex B (Intelligence) to the OPORD. It is most commonly presented in matrix format and will contain at least those items shown previously in figure 3-5. The plan is provided to the operations officer by the intelligence officer, and it is used during the ISR integration activities by the operations officer to publish annex L or a FRAGO.

Chapter 4

Support Intelligence, Surveillance, and Reconnaissance Integration

During ISR integration, the entire staff participates as responsibility for the ISR plan transitions from the intelligence officer to the operations officer. As stated in the introduction of this manual, ISR integration is the task of assigning and controlling a unit's ISR assets to collect and report information as a concerted and integrated portion of OPLANs and OPORDs. See figure 4-1.

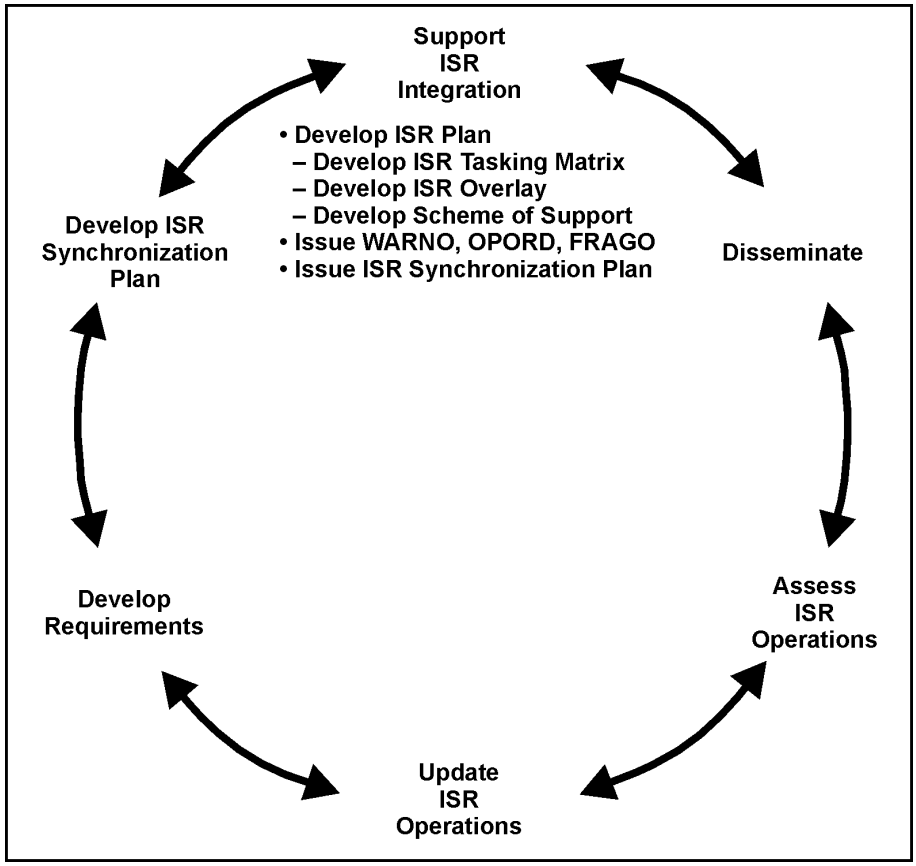

Figure 4-1. Support ISR integration

GENERAL

4-1. **The operations officer (in coordination with the intelligence officer and other staff members) tasks available ISR assets to best satisfy each requirement.** ISR integration is vital in the synchronization of the ISR plan with the scheme of maneuver. These results focus on satisfying the commander's requirements through ISR tasks translated into orders.

4-2. The intelligence officer supports integration by effectively developing requirements and the ISR synchronization plan as described in chapters 3 and 4, advising the operations officer on capabilities and limitations, as well as availability of assets. The intelligence officer does this by fully participating in the MDMP from the start and knowing the capabilities and limitations of all potential organic ISR assets and assets available from other units.

4-3. ISR integration consists of the following tasks:

- Develop the ISR plan:
  - Develop the ISR tasking matrix.
  - Develop the ISR overlay.
  - Develop the ISR scheme of support.
- Issue WARNO, OPORD, FRAGO.
- Issue ISR synchronization plan.

4-4. The entire staff must be involved and engaged in the unit's orders production and planning activities to ensure early identification of all intelligence requirements.

DEVELOP THE INTELLIGENCE, SURVEILLANCE, AND RECONNSAISSANCE PLAN

4-5. The ISR plan is an execution order and should be published in the five-paragraph OPORD format either as a WARNO, an OPORD, or a FRAGO. Operation officers of all units use the ISR plan for tasking, directing, and managing of ISR assets (both assigned and attached assets and assets external to the unit) to collect against the CCIRs. Although ISR integration is accomplished with staff participation and in coordination with the intelligence officer, the operations officer is the staff proponent for ISR integration. Intelligence officers assist the operations officer in the development of the ISR plan by providing an ISR synchronization plan (see chapter 3). Operations officers—

- Integrate the ISR synchronization plan into the scheme of maneuver.
- Publish annex L (Intelligence, Surveillance, and Reconnaissance) to the OPORD which tasks surveillance and reconnaissance assets as soon as possible to begin the collection effort. Figure 4-1 is a sample plan format which can be used as an appendix to annex L.
- Ensure the ISR plan addresses all of the commander's PIRs, that assigned and attached assets have been carefully evaluated and recommended for ISR tasks within their capabilities, and that ISR tasks outside the capabilities of assigned and attached assets have been prepared as RFIs to appropriate higher or lateral headquarters.

4-6. Figure 4-2 is a sample ISR matrix format which can be used as an appendix to annex L.

Sample ISR Matrix

Period covered from _____ to _____

PIR	SIR: Indicators	SIR: NAI	SIR: LTIOV	ISR Units: Maneuver: 1st Bn	2d Bn	3d Bn	RSTA: A Troop	B Troop	C Troop	D Troop	Intelligence: HUMINT	IMINT	MASINT	SIGINT	Force Protection: CBRN	ADA	MP	Engineer	Report to -	Remarks	
1	A	1				⊗				⊗											
		2					⊗	X													
	B	1							X		⊗										
		2		X	X						⊗										
2	A	3								⊗											
		4																			
	B	3																			

X = Sensor and unit capable of collecting information ⊗ = Sensor and unit tasked to collect information

Figure 4-2. Sample ISR matrix

4-7. The primary means of tasking ISR assets is through the use of an ISR plan. A unit could issue the ISR plan as part of the completed OPORD. However, the need to win the battle for information may impose a limited time constraint. In such cases, the unit issues ISR tasks as early as the initial WARNO; this gives the unit more time to achieve the effect of reconnaissance. FRAGOs are used to retask assets that are already conducting operations and to adjust execution as requirements and priorities change.

4-8. The operations officer may issue an OPORD to units to conduct ISR operations prior to issuing the OPORD for the main body or main effort.

DEVELOP ISR OVERLAY

4-9. The operations officer may choose to issue an ISR overlay depicting the ISR plan in graphic form as an appendix to the OPORD. Some of the control measures might have to be determined by subordinate ISR units; if so, higher headquarters must consolidate them as soon as the unit completes its planning. If the overlay is transmitted over digital systems, it might need to be broken into component parts to speed transmission and reduce clutter. Typical items on the overlay include the following:

- Friendly boundaries and phase lines.
- Reconnaissance handover lines.
- NAIs and TAIs.
- Limits of advance and limits of reconnaissance. Limits of reconnaissance are constraints derived from higher headquarters orders which may designate a limit of advance impacting reconnaissance units.
- Counter-reconnaissance areas.
- Fire support control measures.

- Graphics depicting zone, area, or route reconnaissance.
- Routes, start points, release points, infiltration lanes, and checkpoints.
- Primary and alternate observation post locations.
- Ambulance exchange points and logistics release points.
- Planned or existing obstacles.
- Scan sectors for sensors.
- UAS flight paths.
- Retransmission locations.

DEVELOP THE ISR SCHEME OF SUPPORT

4-10. The ISR scheme of support includes the planning and execution of operations and resources to support the Soldiers and units who perform ISR operations. This support includes fires, movement, protection, and sustainment (personnel, medical, maintenance, and logistics). The operations, sustainment, and other special staff officers prepare the initial scheme of support. The operations officer approves the plan and tasks units.

4-11. The scheme of support is published in annex L and addresses as a minimum those items shown in table 4-1. Commanders are then directed to provide their respective pieces of the ISR scheme of support. The scheme of support includes the coordination of surveillance and reconnaissance missions and AOIs with the joint force or higher headquarters and lateral units to satisfy the intelligence requirements within the AOI.

4-12.

Table 4-1. Scheme of support

Movement and maneuver	• Provide asset movement routes to and from mission execution location.
Fires	• Call for fire. • Request immediate attack helicopter support. • Request immediate close air support.
Protection	• Air defense.
Sustainment	• Medical evacuation request. • Casualty evacuation request. • Landing zone and pickup zone procedures for rotary-wing aircraft to perform air-ground integration, casualty evacuation, or aerial resupply. • Casualty reporting. • Reconstitution. • Postal and administrative support. • Religious support. • Resupply of Classes I, III, and V. • Field maintenance support, recovery, and evacuation of unserviceable equipment including vehicles, collection platforms, and systems

ISSUE THE WARNING ORDER, OPERATIONS ORDER, OR FRAGMENTARY ORDER

4-13. The operations officer issues the initial ISR tasks to subordinate units in the WARNO or OPORD, under paragraph 3 (Execution), subparagraph b (Tasks to maneuver units), or subparagraph c (Tasks to other combat or sustainment units).

4-14. Subsequent tasks are published as an entire ISR plan in annex L of the OPORD. See FM 5-0, figure G-22, for an example of annex L.

ISSUE THE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION PLAN

4-15. Once ISR assets receive orders and execute missions, operations and intelligence officers monitor the situation and predict changes that affect the plan. Intelligence officers maintain continuous situational awareness of all supporting ISR assets. Situation development confirms or denies enemy COAs, provides threat locations, explains what the threat is doing in relation to the friendly force commander's intent, and provides an estimate of threat combat effectiveness.

4-16. Automation tools should help intelligence officers maintain situational awareness of the ISR asset's ability to execute the mission. Weather, equipment issues, personnel losses, and other challenges may impact the asset's ability to continue the mission. Sustainment of ISR operations is an important factor to be considered as unforeseen challenges arise. Situational awareness by the staff alerts the intelligence officer and the operations officer of the need to adjust the ISR synchronization and revise or update ISR plans. Situational understanding of ISR assets helps the commander make decisions and execute appropriate branches and sequels.

Chapter 5

Disseminate

Disseminating timely, accurate, and predictive intelligence to the unit commander, staff, and subordinate commands is critical to successful operations. See figure 5-1.

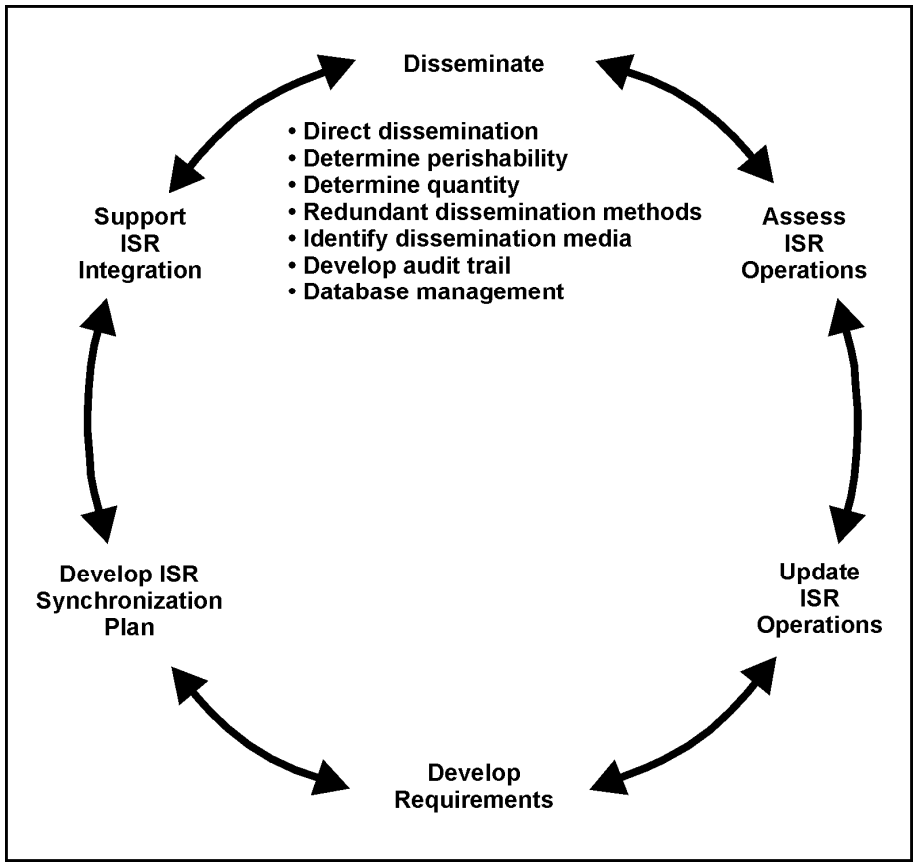

Figure 5-1. Dissemination of information and intelligence

GENERAL

5-1. The key to dissemination is providing the precise amount of information in the appropriate format to the commander or requestor in sufficient time to affect a decision or assessment. The networked environment of the DCGS-A enterprise will facilitate dissemination and improve the commander's situational understanding.

5-2. Implied in this task is the need to mitigate risk by implementing by redundant means or pathways when necessary to ensure delivery of information to the commander. Providing too much, too little, or incorrectly formatted information to the commander may hinder situational understanding. The intelligence

officer ensures commanders and staff receive combat information and intelligence products not later than the LTIOV in a format that best supports the commander's decision making.

5-3. **Dissemination is delivered as voice, text, graphic, or digital media. Posting information on a webpage is not considered dissemination until the intelligence office ensures the commander, subordinate commanders, and staff actually receive the product.** Timeliness and capability will determine the method of dissemination.

5-4. Intelligence officers must continuously coordinate with the entire staff to determine what information will bypass the normal intelligence processing functions and be sent directly to the commander based on the importance and perishability of the information and proximity to LTIOV. Determining the time sensitivity of each report allows you to make decisions about the best means of dissemination. Mission-critical information may require point-to-point dissemination depending on the overall execution timelines and planning requirements. In order to be responsive, the intelligence officer maintains awareness on the current and developing situation. Continuous coordination is essential within the intelligence section, targeting cell, and the operations staff. If the information meets the attack guidance matrix criteria, immediately disseminate it to the targeting cell before further processing or analysis.

5-5. Check the report against outstanding requirements to determine who requested the information. Ideally, this information is included in the report by way of a cross-reference to the ISR task that generated the collection.

INFORMATION PATHS AND CHANNELS

5-6. Information normally moves throughout a force along specific transmission paths or channels. Structure, in the form of command relationships, establishes these channels. Channels help streamline information dissemination by ensuring the right information passes promptly to the right people. The command and control infrastructure disseminates both COP-related information and execution information. The Army's solution to meet these challenges is the DCGS-A enterprise. As part of the DOD command, control, and communication systems and ISR transformation, the DOD Distributed Common Ground Surface System (DCGS) effort provides the defense application framework for the military services to develop a common, interoperable, family of systems to task, post, publish, subscribe and process, use, and disseminate ISR sensor data and intelligence products.

5-7. Commanders and staffs communicate through three formal channels: command, staff, and technical:

- Command channels are direct chain-of-command transmission paths. Commanders and authorized staff officers use them for command-related activities.
- Staff channels are staff-to-staff transmission paths between headquarters. They are used for control-related activities. They transmit planning information, controlling instructions, and other information to support command and control. The intelligence and administrative log nets are examples of staff channels.
- Technical channels are the transmission paths between two technically similar units or offices within a command that perform a technical function requiring special expertise. Technical channels are typically used to control performance of technical functions. They are not used for conducting operations or supporting another unit's mission. Examples include the technical support and sensitive compartmented information reporting channels of intelligence and ISR operations. The SIGINT tasking and reporting, broadcast intelligence communications, and wide area networks supporting single intelligence discipline collection, processing, and production are examples of technical channels.

5-8. Informal channels of collaboration and dissemination develop whenever analysts from different units or echelons talk directly via formal means like telephone or e-mail or through chat room conversations. Intelligence officers must be sure that unit SOPs address the procedures for formalizing information dissemination that takes place when analysts collaborate by any means to ensure the information is added to the proper product, report, or database.

5-9. Intelligence officers must ensure the staff has clear dissemination guidelines. Dissemination must be more focused during stability operations when air, ground, and sea assets may be limited, AOs may be noncontiguous, and lines of communications extended.

5-10. During planning, the intelligence staff coordinates with the rest of the staff, subordinate commands, and the next higher echelon intelligence officer to ensure specific assets, personnel, communications and support equipment, and procedures are available for disseminating intelligence and intelligence products throughout the unit. Intelligence officers must be involved during operational planning in order to understand the intelligence products needed, required timeliness, decision-maker locations, logistics, and communications assets available to support intelligence dissemination.

ADMINISTRATIVE RESPONSIBILITIES

5-11. Intelligence officers work with subordinate and higher echelon intelligence staffs or joint-level dissemination program managers to disseminate intelligence products to the user. They ensure redundant means and pathways, appropriate mailing addresses, message addresses, routing indicators, and special security office security accreditations are requested and established for the unit. This administrative information must be communicated to, and validated by, the joint-level dissemination program managers who will provide the information to Defense Intelligence Agency and other supporting national agencies.

5-12. Intelligence officers determine who needs each piece of information and the best means of transmitting that information for analysis. For example, information regarding a TAI should go to the intelligence, operations, information engagement, fires, and other sections to determine if the information meets targeting requirements. The commander's guidance should provide each staff officer with priorities for reportable information. The executive officer or chief of staff serves as the sounding board for other information reported to the commander.

5-13. The ISR plan and unit SOP should detail the procedures to properly disseminate relevant information using all appropriate means, including e-mail, web postings, FM radio, and instant messenger. These documents should also detail who needs to do what level of analysis before passing the refined information to higher headquarters. They should also address how to provide report information to the commander and staff that needs the information without the report externals. This is often referred to as tear-line reporting. The goal is to quickly analyze and satisfy CCIRs, thus enabling the commander to make informed, timely decisions.

5-14. When dealing with time-sensitive information, the intelligence officer ensures the requestor receives the best available information and intelligence before the LTIOV. Relevant information is passed by the most expeditious means to any affected unit as well as to the unit initially requesting the information. Information is passed to the appropriate intelligence organization for analysis and incorporation into intelligence products. Intelligence officers will—

- Arrange for direct dissemination (point-to-point dissemination).
- Determine perishability.
- Determine how much to disseminate.
- Arrange for redundant dissemination methods.
- Identify dissemination media.
- Develop an audit trail.
- Manage databases.

ARRANGE FOR DIRECT DISSEMINATION (POINT-TO-POINT DISSEMINATION)

5-15. Getting the required intelligence to the requester as soon as possible is essential to successful ISR operations. In point-to-point dissemination, information goes to a specific user or users because it is mission critical, time sensitive, and directly supports the commander's decision making. It then passes sequentially from one user to the next. Point-to-point dissemination has two advantages: First, information

can be tailored to the needs of each recipient. Second, information has built-in control mechanisms that broadcast dissemination lacks.

5-16. Whenever possible, write into the ISR task the requirement for point-to-point dissemination of intelligence to the original requester. If the asset reports directly to the requesting unit, the intelligence staff must ensure they receive a copy of the report. Information copies of reports already provided directly to the original requester is one technique.

5-17. Another effective technique is not only to transmit directly as stated but also to transmit simultaneously to the intelligence staff. The desired dissemination method is written into the specific ISR task order or RFI. Include the required coordinating information such as call signs, frequencies, and routing addresses.

DETERMINE PERISHABILITY

5-18. Point-to-point dissemination is for items required by higher headquarters or subordinates that are of an immediate and specific nature; it is particularly important for intelligence that supports early warning and perishability. Whenever possible, arrange for point-to-point dissemination of targeting intelligence to the targeting cells, especially when the intelligence source prompts an operation.

5-19. Even with direct dissemination, intelligence officers must arrange a system that allows for tracking the status of each request. Sometimes direct dissemination is impossible due to communications system limitations or the classification level of the intelligence. Intelligence officers must plan and arrange for dissemination that is as direct as possible. Since information already disseminated directly to requestors can often satisfy other requests, they must also apply the same procedures to information copies.

DETERMINE HOW MUCH TO DISSEMINATE

5-20. Intelligence officers must provide the precise amount of information to commanders and staffs to support their decision making while avoiding overwhelming them with unnecessary detail or compromising security techniques, means, and sources. For example, it may not be important to provide the entire text of a report to commanders if all required is a threat force location and direction of movement.

5-21. Intelligence officers must ensure that sensitive compartmented information is not disseminated to unauthorized users. Legal restrictions may also prohibit the dissemination of information to multinational forces. This is especially true during stability operations, where political considerations may dictate ISR operations.

5-22. Today's automation and communications technology will tempt analysts to try to send everything to everybody. Resist the temptation. Competition for a limited amount of bandwidth will force you to prioritize dissemination anyway. Additionally, automated filters at other headquarters will eliminate information that you should not have sent.

5-23. Evaluate each element of reported information against the decisions, requirements, and supporting SIRs and ISR tasks for the identified consumer. Disseminate information and intelligence accordingly. Accurate and timely dissemination of information and intelligence, to the right commander or staff element, is vital to successful ISR operations.

ARRANGE FOR REDUNDANT DISSEMINATION METHODS

5-24. This topic is unique to each unit and is normally specified by SOPs. As a minimum, intelligence officers should plan for primary and alternate methods of dissemination (redundant means and pathways) for intelligence or reporting that supports CCIRs and decision making. The organizational communications architecture provides a basis from which to determine appropriate dissemination channels and methods. The intelligence officer must work with operations and signal staff to determine the available dissemination methods. As with the status of ISR assets, intelligence officers must continuously monitor the status of the

dissemination means. If information and intelligence are not provided to those who need it, when they need it, and in the form they need it, it may not be useful to the current or future operations.

IDENTIFY DISSEMINATION MEDIA

5-25. Dissemination media includes radios, telephone systems, and computer systems. Web pages are an excellent method of sharing large quantities of information and intelligence.

> ***Note.*** Simply posting intelligence reports on a web page or uploading a new database is not dissemination.

5-26. The intelligence officer must ensure commanders, subordinate commanders, and staffs actually receive the product in a timely manner. In order to satisfy mission-critical and time-sensitive dissemination needs, the intelligence officer must choose the correct dissemination media to ensure timely delivery.

5-27. Voice is most useful in situations where speed in the transmission of a small amount of information is critical. It obtains instant feedback and acknowledgement, allowing for resolution of misunderstandings or ambiguity. On the other hand, when passing large amounts of information, voice systems are slow and prone to error.

5-28. Graphics and text dissemination is ideal for lengthy messages but can sometimes make information too subtle, ambiguous, and confusing. When there is an option, use the graphic solution for information on disposition, composition, and strength; use text for the other threat characteristics. The optimal mix is to send the graphics or text immediately with a notice that a voice conference will follow. This allows for verification of receipt and gives an opportunity for recipients to resolve any questions or ambiguities. The distribution list determines whether you use broadcast, limited broadcast, or point-to-point techniques.

5-29. For voice communications, use a radio net call or a conference call to transmit broadcast or limited broadcast items. Point-to-point communication is best for single distribution items. Intelligence officers ensure the use of proper radio procedures when using this means of communication and dissemination.

5-30. In terms of time required, a messenger with a hardcopy is least desirable. However, if the messenger is well briefed, this technique can be effective in terms of user understanding.

5-31. When disseminating information, the intelligence officers must ensure the staff—

- Uses the precedence coding system (FLASH, PRIORITY); be careful not to deflate the value of the highest precedence codes.
- Is proficient in terms of operating automated systems and familiarity with message formats.
- Answers questions about accuracy, source, and completeness that arise during dissemination.
- Pushes items of essential information to all appropriate commanders and staff sections and makes them aware of what else is available. Informing them of other information and intelligence available allows them to access additional information from the intelligence system.

DEVELOP AN AUDIT TRAIL

5-32. Intelligence officers coordinate with the signal officer to ensure they know who receives what information. This optimizes dissemination by ensuring that everyone who requires information actually receives it. It is not uncommon for a concerned user not to receive information, even though the intelligence staff arranged for direct dissemination and the collector has sent the information. This problem arises due to reasons such as missed broadcasts, incorrect call signs, or incorrect routing. Instant messaging and chat rooms are a challenging problem for signal officers who must try to determine the best method for recording the delivery of information by those means.

5-33. Audit trails further optimize dissemination by ensuring that all appropriate commanders and staff sections receive each report only once. It is not uncommon for a user to receive the same report multiple times, which could lead to false confirmation. An audit trail is one means to avoid false confirmation, by

ensuring that the reports received were actually different and complementary, rather than the same information from the same source.

5-34. A common technique is to provide columns on the ISR plan to record messages received that satisfy an ISR task and where messages were sent to. This technique enables the intelligence officer to record directly onto the ISR plan. A disadvantage to this technique is that it is difficult to track messages chronologically (for example, "give me all the messages that came in yesterday morning").

5-35. Another technique is to develop a matrix separate from the ISR plan, with "time received" and "sent to" on one axis and ISR tasks on the other axis. Another technique is to annotate the dissemination list directly into the remarks section of each message.

5-36. A collection and dissemination journal is a simple technique to track who has seen what messages. A disadvantage of this technique is that without automation it is difficult to efficiently link journal entries to the requirements numbering system.

5-37. This is an area where automation is especially useful. Relational databases and automated journals allow complete and thorough cross-indexing, solving many of the problems intelligence officers usually experience in relating requirements to reports and tracking dissemination.

MANAGE DATABASES

5-38. Given the amount of information that is likely to be available as a result of intelligence collection, reporting, processing, and production, database management will be a critical component in making the data accessible for analytical purposes. While database management is not strictly or solely an intelligence function, intelligence personnel will be required to perform database management functions for the unit intelligence databases.

5-39. Database management includes the requirements for format and standardization, indexing and correlation, storage, procedures for establishing new databases, security protocols, and associated applications. Database managers must address database development, management, and maintenance; data sources; information redundancy; import and export standards; data management; update and backup procedures; and data mining, query, and search protocols.

Establishing New Databases

5-40. Units must have an SOP for establishing new databases. This ensures all unit databases conform to minimum standards established by unit automation personnel and will help prevent storing of duplicate data (which uses up valuable storage space) and mixing of information that must be stored at different classification levels and with different security or access requirements.

5-41. Intelligence personnel often develop their own personal databases that are user-friendly to that particular individual because they developed the data entry standards and framework of the database themselves. While useful to that particular intelligence Soldier, this technique is not helpful to other intelligence personnel trying to access the same information for the same or similar purposes.

Data Entry

5-42. When entering data into a database, individuals tend to use formats that make sense to them. Unfortunately, what may be a "common sense" standard for data entry for one person may seem completely illogical to another individual. Thus, retrieving data from a database with no data entry standards becomes haphazard. Units must therefore set specific data entry standards for their databases. These specific formats ensure data can be easily retrieved from the database through equally standardized query criteria and that the types of information (fields) entered into the database are consistent.

5-43. At a minimum, data entry standards should include specific formats and standardized naming conventions and fields (based on the category of information being entered into the database). Standard naming conventions include determining a standard nomenclature or equipment.

Data Entry Examples:

A primary database field with a mixture of IED nomenclatures such as "VBIED," "RCIED," and "EFP" would turn a simple query of the database for "IEDs" into a complex search for all of the possible variants of IEDs.

Standardizing data entry on an improvised explosive device with a primary field of "IED" and a secondary field to specify the type of IED (such as VBIED, RCIED, or EFP) may allow the analyst to conduct a more organized search for information and intelligence.

5-44. As another example of data entry standards, a unit may want complete descriptions of captured weapons in a database. Unit intelligence officers should specify the types of information required when entering reports of captured enemy equipment into the database. This may include the type of equipment (such as truck, tank, small arms) and a complete description of the equipment (such as equipment is operational or nonoperational, serial number or vehicle identification number, or other unique identifiers that may determine the origin and manufacturer of the equipment).

5-45. Not all of the required information will be available for each data entry. But in many cases it is equally important to an analyst using the information to know that a specific type of information for that data entry is unavailable or was not collected, and not that the person entering the data simply failed to input that particular information.

5-46. Another example is setting standards for storage of photographs. Information such as the source and classification of the photograph should normally be included in the database along with the photograph itself.

Security Protocols

5-47. Automation personnel must be aware of the security requirements for their networks, systems, and databases. Protocols must be established to ensure only authorized personnel can access the network, system, or database. Additionally, appropriate protocols must be developed in order to prevent the export or import of data to unauthorized networks, systems, or databases, based on accesses or classification levels.

5-48. Protocols include establishing a set of rules so that network, system, and database users are aware of their individual requirements when accessing the network, system, or database. An example of one of these rules may be the prohibition of downloading or copying specified files onto the network or system in order to prevent security breaches.

Associated Applications

5-49. In order to process data most effectively, units must ensure the appropriate software applications are legally installed on their systems so that relevant databases can be created and accessed and that the data can be appropriately manipulated in order to support the unit's mission.

Data Sources

5-50. Units must identify data sources that they will require for use during the mission as early as possible in order to ensure the required communications and security authorizations are appropriately coordinated. As a result of security requirements, intelligence personnel may need different computer systems in order to access all the necessary data sources required for the mission.

Database Normalization

5-51. Database normalization helps to eliminate redundancy (storing the same information in multiple tables) in a database and ensures only related data is stored in any given table. Developing procedures to

minimize redundancy of data in a database will ensure effective use of limited storage space, speed up database queries, and prevent confusion over duplicate data entries.

Import and Export Standards

5-52. Units often transfer data between systems and other units. A standardization of import and export protocols will ensure transferred databases are accessible immediately upon transfer. Databases and files that are created with different standards may not be accessible nor usable to the system receiving the data. The DCGS-A enterprise open architecture should aid in the import and export of databases. (See appendix C for more information on DCGS-A overview.)

Update and Backup Procedures

5-53. Units must establish a plan for updating the software on their networks and systems to ensure that the latest changes to fix glitches or security holes in the software are repaired. Likewise, units must establish procedure for conducting backups of the data on their networks and systems to prevent an irrecoverable loss in the event of hardware or software failure. A system of archiving data must also be established.

Chapter 6

Assess ISR Operations

Assessment of ISR operations allows the staff to determine how well the system is satisfying all requirements. See figure 6-1.

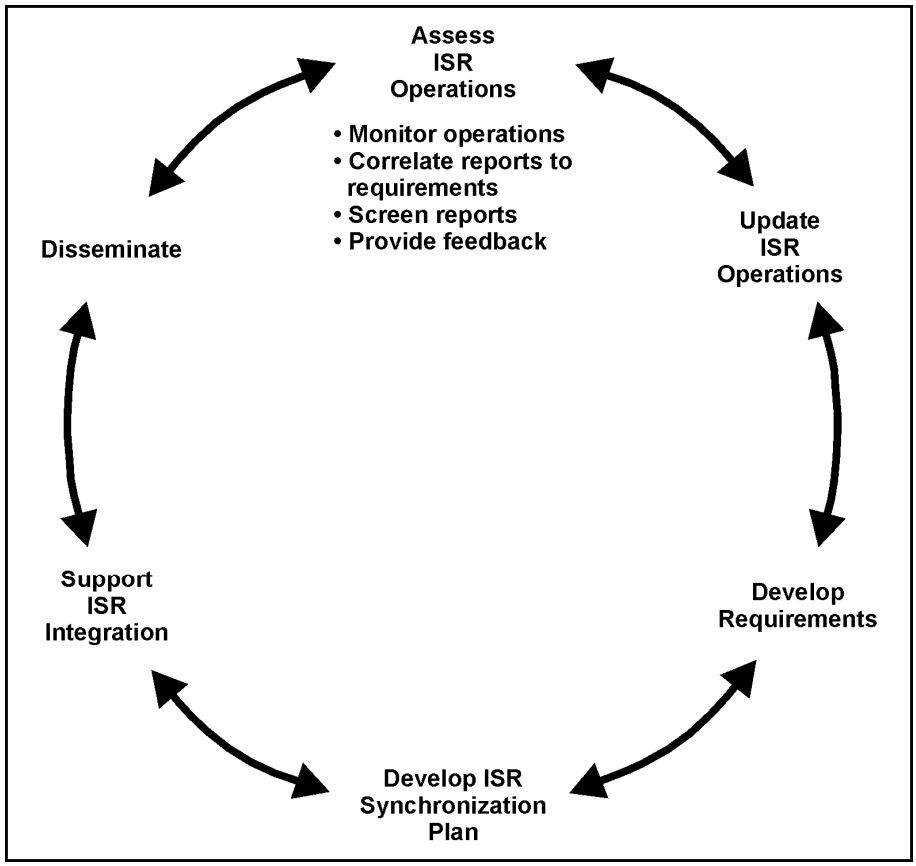

Figure 6-1. Assess ISR operations

GENERAL

6-1. **Assessment is the continuous monitoring and evaluation of the current situation, particularly the enemy, and progress of an operation (FM 3-0).** Assessing ISR operations enables the operations and intelligence officers to monitor and evaluate the current situation and progress of the operation. The desired result is to ensure all ISR tasks are completely satisfied in a timely manner, keeping the intelligence system synchronized and that intelligence officers know the status of each requirement.

6-2. Assessing ISR operations starts with monitoring and evaluating the reporting by ISR assets as they execute their missions. Reporting is the act of passing information from ISR asset to processor or operations center, and into the intelligence process. Combat information is quickly reported to the

commander or other decision maker for immediate action as well as reported into the intelligence process where it is analyzed against other intelligence and then disseminated.

6-3. Intelligence officers track reporting to determine how well the ISR effort is satisfying the PIRs. The desired result is relevant information is delivered to the commander before the LTIOV. Intelligence officers, ISR elements, and staff each ensure ISR assets are not performing tasks for intelligence requirements that have already been satisfied. The intelligence staff must perform four essential tasks to effectively evaluate reporting: monitor operations and maintain synchronization, correlate reports to requirements, screen reports, and provide feedback to ISR assets.

MONITOR OPERATIONS AND MAINTAIN SYNCHRONIZATION

6-4. Through extensive staff coordination intelligence officers determine what critical pieces of information are missing from the commander's estimate of the situation or situational understanding. The officer then uses the ISR synchronization plan to ensure synchronization with the overall operation and scheme of maneuver. The other critical tool for the intelligence staff is the DST. Intelligence officers must have a complete copy of the DST, ensuring the ISR synchronization plan contains each collection requirement.

6-5. The intelligence officer tracks the flow of the operation against the ISR synchronization plan. As necessary, the intelligence officer prompts subordinate commanders and collectors to keep their reporting synchronized with the operation and the commander’s needs.

6-6. The operation will seldom progress on the timelines assumed during planning and staff wargaming. Watch for changes in tempo that require changes in reporting times (LTIOV).

6-7. Coordinate any changes with all parties concerned, including commanders and appropriate staff sections. It is also possible that the staff’s assumptions about enemy COAs will not prove entirely correct. The usual result is a change in intelligence requirements as well as adjustments to the timelines. The staff usually initiates abbreviated versions of the IPB and decision-making processes to accommodate the changes in their assumptions. Be prepared to update ISR planning as a result.

6-8. Not all intelligence will flow through the intelligence cell; some collectors will report directly to users such as the targeting cell. Monitoring synchronization and evaluating reporting requires intelligence officers to establish some system to evaluate all reports, including those that go directly from the collector to the user.

6-9. Intelligence officers set up a system that allows the intelligence cell to monitor synchronization and evaluate how well the intelligence system is meeting requirements without unduly delaying intelligence dissemination.

CORRELATE REPORTS TO REQUIREMENTS

6-10. The intelligence staff tracks which specific ISR task originates from which intelligence requirement to ensure the collected information was provided to the original requester and to all who need the information. For efficiency and timeliness, the intelligence staff also ensures production tasks are linked to validated intelligence requirements. This also allows intelligence officers to determine which ISR tasks have been satisfied and which require more collection.

6-11. Intelligence officers must address potential challenges. For example:

- Large volumes of information that could inundate the intelligence section. The intelligence staff may have trouble finding the time to correlate each report.
- Many reports will only partially satisfy a number of ISR tasks, while other reports may have nothing to do with the tasked ISR task.
- Collectors may report information without referring to the original ISR task that drove their collection.

- Some collectors may assign their own internal numbering system which intelligence officers might confuse with the ISR task and requirements numbering system.

6-12. Units should have a tracking system in place, as part of their operational SOP that links requirements to ISR tasks. Inform attached ISR assets, so that they know and use the standard tracking system. Remember that all intelligence requirements should already be linked to commanders' decisions.

6-13. Correlating intelligence reporting to the original requirement and evaluating reports are keys to effective requirements management. This quality control effort helps the G-2/S-2 staff ensure timely satisfaction of intelligence requirements. Requirements management includes dissemination of reporting and related information to original requesters and other users. All of these functions require a recording system that allows intelligence officers to track the progress of each requirement and cross-reference incoming reports to outstanding requirements.

6-14. ISR assets must ensure they follow the SOP and tag all of their reports with the numbers of the ISR tasks they satisfy. At the same time, the SOP must ensure ISR assets understand and have a means of reporting important but unanticipated information. Intelligence officers must—

- Develop templates that will enable you to quickly match incoming reports to outstanding ISR tasks. Match the locations on the report to the event template. The report locations will naturally appear in or near the NAIs for the concerned ISR task.
- Develop key-word, key-name, and key-indicator lists that quickly index key elements of a report to the appropriate ISR task. For example, "all reports about the city of Baghdad refer to ISR task 7-y-4 or 5-a-2."

SCREEN REPORTS

6-15. After reports have been correlated and tagged to the appropriate ISR task, determine whether the ISR task has been satisfied. Screen each report for the following criteria:

- Relevance: Does the information actually address the tasked ISR task? If not, can you use this information to satisfy other requirements?
- Completeness: Is essential information missing? (Refer to the original ISR task.)
- Timeliness: Has the collector reported by the LTIOV established in the original ISR task?
- Opportunities for Cueing: Can this system or another system take advantage of the new information to increase the effectiveness and efficiency of the overall ISR effort? If the report suggests an opportunity to cue other assets, take immediate action to do so and record any new requirements into the ISR plan and audit trail.

6-16. If the report satisfies the ISR task, make the appropriate entry in the tracking log or register of intelligence requirements and disseminate the final intelligence to the requestor. Coordinate with the requestor to ensure the requestor also considers the requirement satisfied.

6-17. If the report only partially satisfies the ISR task, annotate in the audit trail or registers what has been accomplished and what remains to be done.

6-18. ISR assets should avoid submitting reports that simply state "nothing significant to report." Sometimes these reports intend to convey that collection occurred and that no activity satisfying the ISR task was observed. This may be a significant indicator in itself. On the other hand, "nothing significant to report" may have a different connotation, particularly to intelligence officers, and is by no means a reliable indicator of the absence of activity.

PROVIDE FEEDBACK

6-19. The intelligence staff should provide feedback to all ISR collection assets on their mission effectiveness and to analytic sections on their production. This is normally provided through the command and control element of that unit. Feedback reinforces whether collection or production is satisfying the

original task or request and provides guidance if it does not. Feedback is essential to maintaining ISR effectiveness and to alert leaders to deficiencies that must be corrected.

6-20. As the operation continues, the intelligence section tracks the status of each ISR task, analyzes SIRs, and ultimately satisfies requirements. Intelligence officers pay particular attention to which assets are not producing the required results, which may result in adjustments to the ISR plan. During execution, the staff assesses the value of the information from ISR assets, and develops and refines requirements to satisfy information gaps.

6-21. When reporting satisfies a requirement, intelligence officers in coordination with operations officers relieve the ISR assets of further responsibility to collect against ISR tasks related to the satisfied requirement; they provide additional tasks as appropriate to satisfy emerging requirements. Intelligence officers must—

- Notify the ISR assets and their leaders for partially satisfied requirements to continue collection against those ISR tasks that remain outstanding and explain what remains to be done.
- Notify ISR assets of new ISR tasks designed to exploit cueing and other opportunities.

6-22. By monitoring operations, correlating reports to requirements, screening reports, and providing feedback, the intelligence officers and staff ensure the most effective employment of ISR assets. Once intelligence officers assess ISR operations, they can effectively update ISR operations.

END OF PHASE AND OPERATION ASSESSMENT

6-23. After each phase or operation, the intelligence staff must conduct an assessment. They should examine the audit trail to determine what CCIRs were answered and which ones were not answered. Then the intelligence staff should assess the accuracy and effectiveness of the collection teams and analytic elements.

Chapter 7

Update Intelligence, Surveillance, and Reconnaissance Operations

Updating ISR operations is the adjustment of the overall ISR plan to keep ISR synchronized and collection and exploitation capability optimized as the current situation changes. See figure 7-1.

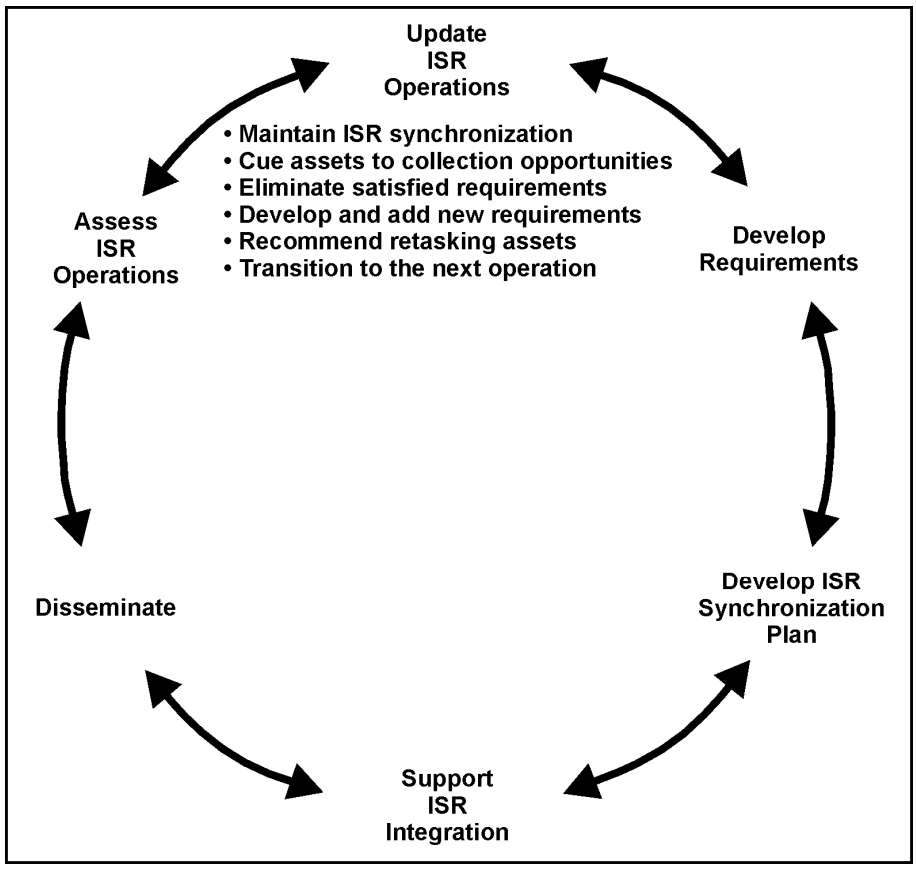

Figure 7-1. Update ISR operations

GENERAL

7-1. Evaluation of ISR reporting, production, and dissemination identifies updates for ISR operations. Intelligence offices, operations officers, and commanders determine if the CCIRs have been satisfied or are still relevant. If requirements have been satisfied or are no longer relevant, the intelligence and operations officers eliminate them from the plan. If requirements have not yet been satisfied and are still relevant, intelligence officers coordinate with the operations officers for additional assets and/or recommends adjustments to the current coverage.

7-2. Rapidly determining requirements satisfaction facilitates redirecting assets to unfulfilled requirements. As requirements are satisfied, intelligence officers in coordination with the operations officers update the ISR synchronization plan and recommends redirecting assets to satisfy other or new requirements within the constraints of METT-TC. The intelligence officer reviews all new intelligence requirements prior to including them in the ISR synchronization plan and recommends changes to the operations officer and the staff.

7-3. Intelligence officers synchronize new ISR requirements with ongoing ISR operations and recommend integration techniques to the operations officer. The intelligence staff keeps the G-2/S-2 informed of the status of all ISR tasks and requirements. The intelligence officer retains the responsibility to validate, modify, or develop intelligence requirements against targets and objectives as the situation develops or operations progress.

7-4. The intelligence staff should—

- Maintain ISR synchronization.
- Cue assets to other collection opportunities.
- Eliminate satisfied requirements.
- Develop and add new requirements.
- Recommend redirecting assets to unsatisfied requirements.
- Transition to next operation.

MAINTAIN INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION

7-5. The decision point timeline estimates are used as the basis for establishing the LTIOV. As planning or execution of the command's COA progresses, these estimates are refined. The intelligence staff must stay alert to the need for changes in the ISR plan that results from these refinements. These are usually changes to the LTIOV, but sometimes also involve other changes.

7-6. As the need for changes arise, intelligence officers must coordinate with the appropriate sections to update products required to refine the ISR plan. Depending on the situation, this may be as simple as updating the timelines on the situation templates, event templates, and event matrices. It may also require that these products be completely redone.

Scenario:

An analyst notifies the intelligence officer that the analysis and control element (ACE) solved IR-12 through analysis of previously submitted ISR tasks.

When the intelligence officer reviews the ISR synchronization plan, it is noted that ISR assets were relieved of three ISR tasks associated with IR-12 and that five ISR tasks remain outstanding. The intelligence officer, in coordination with the operations officer, relieves the BFSB from their two ISR tasks and withdraws the other three ISR tasks from the division's request list at corps.

While updating on the current situation, the intelligence officer notices that the operation appears to be progressing more rapidly than anticipated. The intelligence officer confers with the ACE and operations officer and determines that the LTIOV will have to be updated for several ISR tasks in order to keep the intelligence system synchronized with the operation. The intelligence officer coordinates with the ACE to make the needed changes to the event templates and matrices and then uses them as a basis for changing outstanding ISR tasks.

When intelligence officers identify such collection opportunities produced by cueing, they recommend appropriate redirecting or retasking of an ISR asset. The operations officer reevaluates the original synchronization plan based upon the new requirements. In particular, the operations officer looks for opportunities to improve collection strategies and retasks ISR assets appropriately.

The BCT S-2 discovers that a scout platoon conducting a patrol has received information that a particular insurgent leader is in the vicinity. The operations officer's original plan for locating this individual was to use SIGINT and HUMINT assets. Since this individual is a critical high-payoff target, the intelligence officer recommends diverting an ongoing UAS mission from a lower priority requirement to conduct reconnaissance in the vicinity of the patrol to assist in the search. The intelligence officer coordinates with the operations officer, who issues the necessary orders and then helps coordinate the changed flight track with the division's air space manager.

After the UAS identifies the precise location of the insurgent leader, the operations officer withdraws the corresponding ISR tasks from the asset, making the UAS available for additional missions. The immediacy of this dynamic retasking allowed the command to execute a successful operation.

7-7. Cueing opportunities, whether prompted through combat information or analysis, allows intelligence officers to satisfy requirements more efficiently than previously planned through collection strategies.

ELIMINATE SATISFIED REQUIREMENTS

7-8. During evaluation, the intelligence staff identified satisfied requirements. In this step, eliminate satisfied requirements and requirements that are no longer relevant, even if unsatisfied. This requires continuous coordination with the agency that generated the original requirement.

7-9. For example, a division intelligence officer would coordinate with—

- The ACE and plans section for intelligence requirements.
- Senior, subordinate, and adjacent commands for their ISR tasks.

7-10. When higher headquarters declares a requirement satisfied, eliminate it from the ISR synchronization plan and the ISR plan, and update any other logs and records.

DEVELOP AND ADD NEW REQUIREMENTS

7-11. As the operation unfolds and the threat situation develops, commanders will generate new requirements. This prompts intelligence officers to begin updating the ISR synchronization plan. As new requirements are developed, they are prioritized against the remaining requirements. Some of the previous requirements may still be valid. Consolidate the new requirements with the existing requirements, reprioritize the requirements, evaluate resources based upon the newly developed requirements and priorities, and make appropriate recommendations to the commander and the operations officer.

RECOMMEND RETASKING ASSETS

7-12. Retasking is assigning an ISR asset a new task and purpose on completion of its initial requirement, on order after LTIOV having not satisfied the original requirement, as planned to support a branch or sequel, or to respond to a variance. Adjusting LTIOV may be required.

7-13. Through situational awareness, intelligence officers determine the need to redirect ISR assets. Some assets and units can be immediately retasked by the operations officer, while other assets may require considerable amounts of time to plan, prepare, and deploy before executing a new mission. The intelligence officer must factor time requirements when recommending redirecting an asset or unit. If redirection changes an ISR asset's collection priorities, without changing its basic mission parameters, the intelligence officer may pass this information by the most expedient means to the ISR asset while keeping both the operations officer and the unit commander informed. Command or operational channels must issue changes if the redirection subsequently results in a change in mission, the movement of the asset, or its function in the operational scheme of maneuver.

7-14. Requirements can be satisfied by the ISR asset or unit to which they were tasked or as a result of successful operations elsewhere in the AO. After eliminating satisfied requirements from the ISR plan, reevaluate each ISR asset based on its capability. Based upon operations tempo and diminished capabilities, operations officers with input from the intelligence officers will redirect ISR assets and units within the AO. This will ensure coverage of ISR tasks. Focus the ISR asset to the most important unsatisfied requirements. This enables the staff to compensate for—

- Second- and third-priority requirements designated for economy of force efforts developed in the original strategies and plan.
- Unanticipated requirements that use more effort than originally planned.
- Assets that are not performing to the capability originally evaluated (for example, the threat counters one of our collection capabilities).

7-15. Redirecting an ISR asset does not change the asset's mission; instead, it updates or corrects the focus of the collection that allows the asset to more effectively execute that mission. When redirecting assets, consider the following:

- Higher headquarters new requirements received prior to the completion of the redirected missions.
- The likely priority of the new requirements relative to those remaining unsatisfied requirements.
- The command or support relationship.
- The ability of available ISR assets to respond to new missions while working on redirected missions.
- Necessary responses to second- and third-order effects and branches and sequels.

7-16. The desired outcome is that ISR tasks continuously evolve to ensure intelligence and operational synchronization.

TRANSITION TO THE NEXT OPERATION

7-17. **A transition occurs when the commander decides to change focus from one type of military operation to another (FM 3-90).** Updating ISR operations may result in change of focus for several ISR assets. ISR assets, as with any other unit, may require rest and refit, or lead time for employment in order to effectively transition from one mission or operation to another.

7-18. Refit includes all of those administrative and logistics activities that provide for the reorganization, recovery, and re-supply of units and assets.

7-19. The commander must plan for rest and refit of ISR assets in the concept of operations in order to ensure adequate ISR coverage throughout the operation, during possible branches and sequels that may occur, and when a transition to the next operation occurs.

7-20. A rest and refit plan may require coordination with higher headquarters for other surveillance and reconnaissance resources to conduct ISR operations while assigned and attached ISR assets are unavailable.

Appendix A

Joint, Interagency, and Multinational Considerations

Intelligence supports joint operations by providing critical information and finished intelligence products to the combatant command, the subordinate service and functional component commands, and subordinate joint forces. Commanders at all levels depend on timely, accurate information and intelligence on an adversary's dispositions, strategy, tactics, intent, objectives, strengths, weaknesses, values, capabilities, and critical vulnerabilities. Intelligence operations (planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback) must focus on the commander's mission and concept of operations.

SIMILARITIES

A-1. There is no standard existing joint-level ISR synchronization organization. There are joint intelligence centers (JICs), J-2 operations, and collection management sections that perform the collection requirements management (CRM) and collection operations management (COM) functions. These sections often interface with a joint reconnaissance center and joint intelligence operations center (JIOC) for the conduct of theater airborne collection.

TERMINOLOGY AND FUNCTIONS

A-2. Service specific and joint terms describing the management of collection may differ based on the respective branch of service. The standard definition of collection management is the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and re-tasking as required.

A-3. Joint terminology includes joint collection management, which has two distinct functions:

- Collection requirements management—
  - Defines what intelligence systems must collect.
  - Focuses on the requirements of the customer.
  - Is all-source (all intelligence disciplines) oriented, and advocates (provide and support) what information is necessary for collection.
- Collection operations management—
  - Specifies how to satisfy the requirement.
  - Focuses on the selection of the specific intelligence disciplines and specific systems within a discipline to collect information addressing the customer's requirement.
  - Is conducted by organizations to determine which ISR assets can best satisfy the customers' product requests. Figure A-1 illustrates these functions.

A-4. Collection requirements management and collection operations management are performed at all levels of the Intelligence Community. Each level interacts with the levels above and below, and among units, agencies, and organizations on the same level. The further up the chain, the broader the perspective and scope of responsibility; the lower, the more specific the function and narrow the scope. Organizations possessing collection assets and/or resources perform collection operations management.

JOINT DISSEMINATION PROCEDURES

A-5. The J-2, at each echelon, manages the dissemination of intelligence to the user.

A-6. Intelligence must be provided in a form that is readily understood and directly usable by the recipient in a timely manner without overloading the user and, at the same time, minimizing the load on communications capabilities. It is also important to provide for maximum possible release of appropriate classified reporting, analysis, and targeting data to multinational forces.

A-7. 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. The "pull" concept involves direct electronic access to databases, intelligence files, or other repositories by intelligence organizations at all levels.

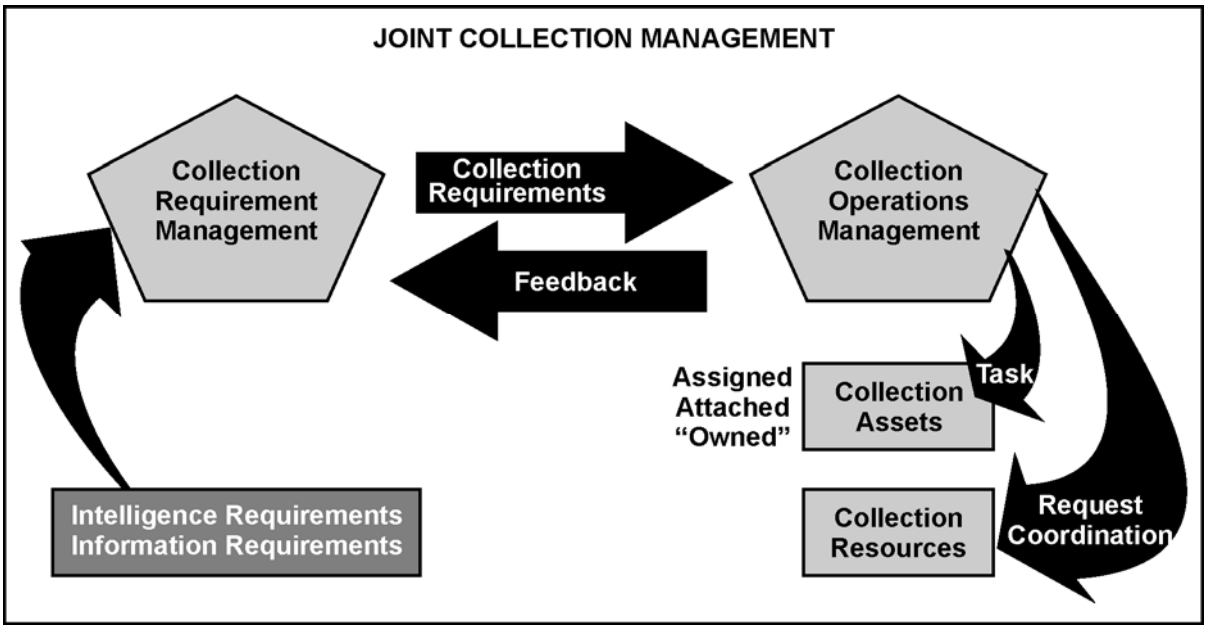

Figure A-1. Joint collection management

A-8. Common joint operations functions fall into six basic groups:

- Command and control.
- Intelligence.
- Sustainment.
- Movement and maneuver.
- Fires.
- Protection.

A-9. Some functions, such as command and control and intelligence, apply to all operations. Others such as fires apply as required by the JFC's mission. Although ISR capabilities are distinctive, and each fulfills a different purpose, they are often thought of as a collective whole.

JOINT INTELLIGENCE PROCESS

A-10. The joint intelligence process shown at figure A-2 depicts how various types of intelligence operations interact to meet the commander's intelligence needs.

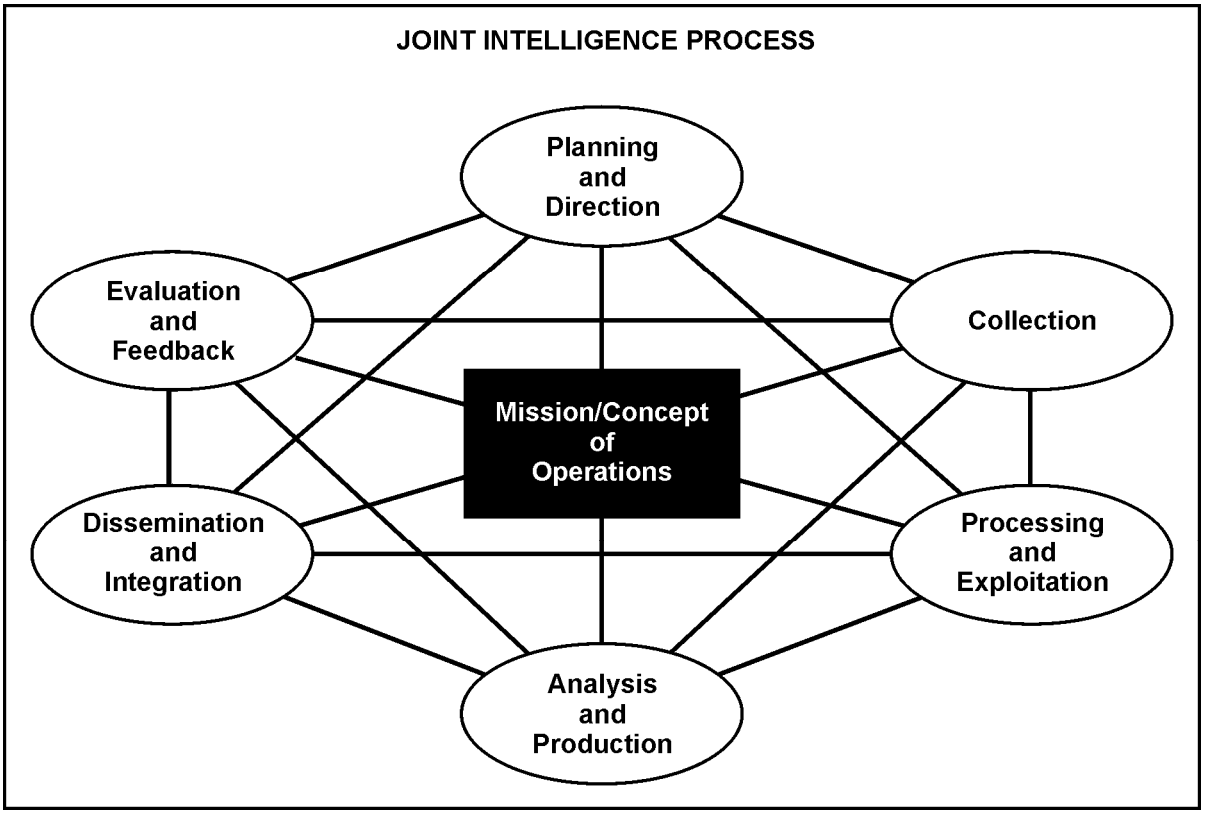

Figure A-2. Joint intelligence process

A-11. The joint process is composed of six phases: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. The intelligence process may not continue throughout the entire cycle. For example, a request for imagery will require planning and direction activity but may not involve new collection, processing, or exploitation. The request could go directly to a production facility where previously collected and exploited imagery is reviewed to determine if it will satisfy the request. Activities within each phase are conducted continuously and in conjunction with activities in other phases. For instance, planning is updated based on previous information requirements being satisfied and upon new requirements being identified as a result of analysis performed in the production phase.

A-12. There will be differences in intelligence doctrine and procedures among multinational partners. A key to effective multinational intelligence is heavy coordination, training, and extensive liaison, beginning with the highest levels of command to make the adjustments required to resolve these differences.

A-13. The following are guidelines to assist a subordinate joint force J-2 and staff (exact steps depend on the nature of the military operation):

- Establish liaison between joint and multinational force intelligence organizations.
- Ensure procedures have been established and reviewed to expedite sanitization and sharing of US-generated intelligence products with allies and multinational partners.
- Ensure friendly objectives, intentions, and plans are communicated to appropriate intelligence organizations.
- Ensure interoperability of command, control, and communication systems.

A-14. Be aware of, and remain sensitive to, cultural and/or religious differences among multinational 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.

A-15. Major differences may include how intelligence is provided to the commander (jointly or individual Services or agencies), procedures for sharing information among intelligence agencies, and the degree of security afforded by different communications systems and procedures. Administrative differences that need to be addressed may include classification levels, personnel security clearance standards, requirements for access to sensitive intelligence, and translation requirements.

A-16. Typically there is a disparity in the capabilities of US and multinational forces. Multinational forces may have greater intelligence resources within a given region, valuable and extensive HUMINT, and access to the population and open sources. US forces generally have to provide technical assistance in order to share information and intelligence.

A-17. It is imperative that combined forces commanders establish a system that optimizes each nation's contributions and provides all units reliable intelligence. US units subordinated to non-US headquarters may face unique problems in disseminating intelligence. If a direct channel is available to the next higher US headquarters, the tactical US unit may have better and more current intelligence than its controlling non-US headquarters. In that instance, liaison personnel have a responsibility to disseminate intelligence both up and down, while adhering to restrictions that deal with the release of intelligence to allied and multinational forces.

A-18. The joint operation planning process (JOPP) provides an orderly approach to planning at any point before and during joint operations. The steps of JOPP, as shown in figure A-3, provide an orderly framework for planning, both for Joint Operation Planning and Execution System requirements and for organizations that have no formal Joint Operation Planning and Execution System responsibilities. The focus of JOPP is on the interaction between an organization's commander and staff and the commanders and staffs of the next higher and lower commands. The process is continuous throughout an operation. Even during execution, the planning process produces OPLANs and OPORDs for future operations as well as FRAGOs that drive immediate adjustments to the current operation.

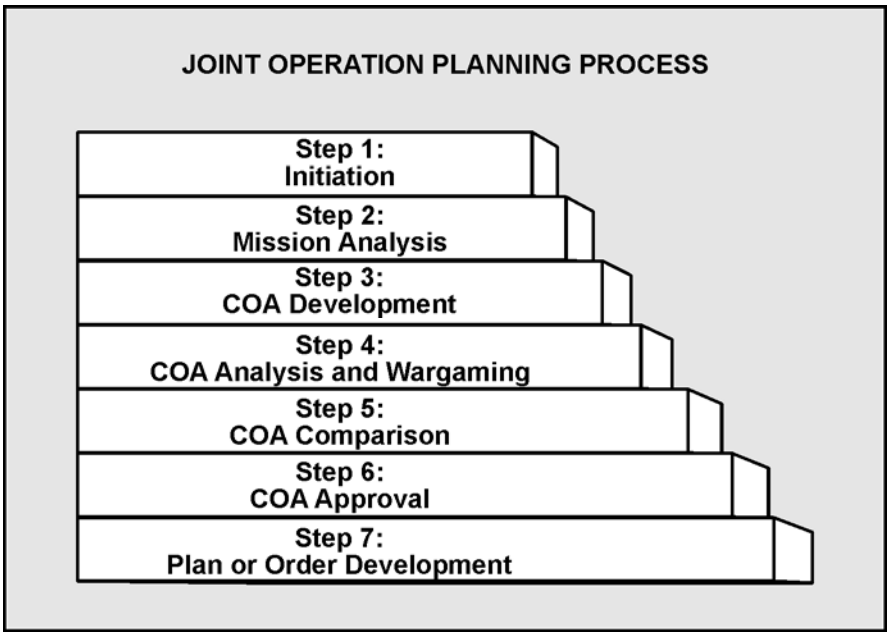

Figure A-3. Joint operation planning process

A-19. Planning early and concurrently is critical to the success of any joint or multinational operation. JFCs determine what intelligence may be shared with the forces of other nations early in the planning process. The North Atlantic Treaty Organization 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.

A-20. ISR planning activities include, but are not limited to—

- Developing requirements – This activity involves items of information regarding the threat and environment which need to be collected and processed in order to meet the intelligence requirements of the commander.
- Developing indicators and SIR sets – This activity involves activity or lack of activity that will confirm or deny the action or event specified in an intelligence requirement. Taken together, indicators may prove or disprove a PIR. They are any positive or negative evidence of activity or characteristic of the AO that points toward capabilities, vulnerabilities, or intentions. Individual indicators cannot stand alone. Each indicator is integrated with other factors and indicators before patterns are detected and threat intentions established. Indicators are developed by the intelligence analysts.
- Developing the synchronization plan – This activity bridges the CCIRs and other requirements to ISR in order to influence decisions and operations through increased situational understanding. This activity ensures that ISR, intelligence reach, and RFIs result in successful reporting, production, and dissemination of combat information and intelligence.
- Contributing to the development of the ISR plan – This activity involves a command and control function led by the current operations cell. The J-3/S-3 must take a renewed interest in the accuracy and completeness of annex L (ISR).

Note. The following paragraphs describe respective branches of the Armed Services' ISR scope and are meant to provide a basic understanding of what is expected within a joint, interagency, or multinational operation.

JOINT TASK FORCES AND MULTINATIONAL UNITS

A-21. The joint task force (JTF) is the primary organization for joint operations, especially during force projection. The JTF performs missions of short duration with specific, limited objectives. The JTF draws units from theater components and may receive out-of-theater augmentation in terms of units, intelligence capabilities, and communications. Flexibility is the operative word.

A-22. Additionally, national intelligence support teams (NISTs) are formed at the request of a deployed joint or combined task force commander. NISTs are comprised of intelligence and communications experts from Defense Intelligence Agency, Central Intelligence Agency, National Geospatial Intelligence Agency, National Security Agency, and other agencies as required to support the specific needs of the JFC. The Joint Staff J-2 is the NIST program's executive agent and has delegated the NIST mission to the Deputy Directorate for Crisis Operations (J-2O). The J-2O manages daily operations and interagency coordination for all NISTs. DIA is the executive agent for all NIST operations. Once on station, the NIST supplies a steady stream of agency intelligence on local conditions and potential threats. Needs of the mission dictate size and composition of teams.

A-23. As a rule, during multinational operations, the JFC is required to share intelligence with foreign military forces and to coordinate receiving intelligence from those forces. In some multinational operations, JFCs are able to use existing international standardization agreements (for example, North Atlantic Treaty Organization, standardization agreements) as a basis for establishing rules and policies for conducting joint intelligence operations. Since each multinational operation has its unique aspects, such standing agreements may have to be modified or amended based on the situation.

A-24. In other cases a JFC participating in a multinational force or alliance, following national and theater guidance, must develop the policy and procedures for that particular operation. Intelligence efforts of the nations must be complementary and consider the intelligence system strengths, limitations, and unique and valuable capabilities each nation will have.

A-25. The ISR synchronization organization within a JTF includes component ISR synchronization sections, the JTF headquarters collection, management, and dissemination, and JIC collection managers. Since the organization is not fixed, but is tailored to each mission, collection managers must quickly learn and become proficient at making use of the systems available to the JTF.

A-26. The desired end-state is to synchronize intelligence with operations. The J-2/Intelligence staff synchronizes all intelligence activities with the JFC's concept of operations. To achieve synchronization, the J-2 must play an active role during the wargaming and analysis of all COAs and plans. Synchronization results in the maximum use of all intelligence assets where and when those assets will make the greatest contribution to success.

A-27. The JFC may conduct operations through the Service component commanders or, at lower echelons, Service force commanders. Conducting joint operations using Service components has certain advantages, which include clear command lines. The JFC can establish functional component commands to conduct operations when forces from two or more Services must operate in the same domain or there is a need to accomplish a distinct aspect of the assigned mission. Normally, the Service component commander with the preponderance of forces to be tasked and the ability to command and control those forces will be designated as the functional component commander. However, the JFC will always consider the mission, nature, and duration of the operation, force capabilities, and the command and control capabilities in selecting a commander.

A-28. JTF service component commanders employ forces to accomplish operational tasks, including intelligence collection. There is a tasking relationship, therefore, between the JTF collection managers and Service components. JTFs also access national collection and production agencies to fill intelligence gaps. The National Military Joint Intelligence Center, the combatant command's intelligence directorates (J-2s), the JICs (or equivalents) of combatant commands, and the J-2s and joint intelligence support elements of subordinate joint forces all support the commander by minimizing the number of organizations and echelons upon which the JFC must rely in order to accomplish intelligence support missions. See JCS Publication 2.01 for additional information on Joint Intelligence Operations.

COMBINED OPERATIONS

A-29. When a multinational or alliance enters into multinational operations, command and control may remain essentially national or it may integrate. Either way, intelligence remains a national responsibility. US units subordinated to non-US headquarters may require augmentation with translators and interpreters, and a series of "front end" terminals such as a Mobile Integrated Tactical Terminal, to ensure their continued connectivity with US Theater and national collection systems. US units subordinated to non-US headquarters may also face unique problems in disseminating intelligence.

A-30. ISR synchronization operations in a combined environment are affected by the confusion factors of language, differing tasking and request channels and formats, information classification and releasibility concerns, and national sensitivities. Collection managers must be familiar with multinational collection and communications systems and the tasking and request channels they require. A proven technique is the use of intelligence liaison personnel to formulate effective collection strategy and facilitate rapid dissemination.

A-31. A combined unit commander must establish a system that optimizes each nation's contributions and provides all units high quality intelligence. If a direct channel is available to the next higher US headquarters, the tactical US unit may have better and more current intelligence than its controlling non-US headquarters. In that instance, liaison personnel have a responsibility to disseminate intelligence both up and down, while adhering to restrictions that deal with the release of intelligence to other nationals.

JOINT/INTERAGENCY

A-32. The primary consideration from an organizational and leadership standpoint is the absence of a formal command structure. Non-Department of Defense (DOD) agencies often operate with management and direction vice command, complicating any attempt at maintaining unity of effort. Each non-DOD agency—

- Will have its own collection management structure.
- May be augmented with special collection assets.
- Will likely have access to national systems.

A-33. An excellent example of a joint headquarters operating in an interagency environment is US Southern Command. The Drug Enforcement Administration, CIA, and a variety of economic development agencies exercise non-DOD elements of national power throughout the region.

A-34. Interagency operations require a robust liaison environment to make things work. Additionally, in the absence of command unity, commanders and agency chiefs should establish formal agreements to ensure all parties clearly understand their responsibilities and relationships within the system.

A-35. When conducting ISR synchronization, formal agreements should specify tasking and request relationships, timelines, formats, and who will conduct analysis. They should identify who, or which agency, has PIR and ISR synchronization strategy approval authority. The responsibility for collection platform readiness and scheduling and the elements of availability should be clearly defined.

A-36. ISR synchronization elements within joint and interagency include component ISR synchronization sections, the JTF headquarters collection management, and JIC collection managers.

ARMY SERVICE COMPONENT COMMAND

A-37. The organizational objective of the ASCC is to provide support consistent with JFC-directed missions.

A-38. The ASCC commander is the senior Army commander in a combatant commander's area of responsibility (AOR). The ASCC commander, using Administrative Control authority, is responsible for the Army Title 10 functions of preparing, maintaining, training, equipping, administering, and supporting Army forces attached to joint forces subordinate to the combatant command. The ASCC also provides theater-strategic and operational level support to combatant command campaign and major operation planning. The ASCC commander normally designates an Army unit within each joint force subordinate to the combatant command as the Army forces for that joint force. These Army forces are responsible for accomplishing operational level Army tasks within the joint force to which they are assigned.

A-39. The ASCC commander's responsibilities include—

- Recommending to the JFC or sub-unified commander the proper employment of Army component forces.
- Accomplishing operational missions as assigned.
- Selecting and nominating Army units for assignment to subordinate theater forces.
- Informing the combatant commander of Army sustainment effects on operational capabilities.
- Providing data to supporting OPLANs as requested.
- Ensuring signal interoperability.

NAVY

A-40. Naval intelligence forces have been designed as an integrated system of personnel, procedures, facilities, and equipment structured to support naval, joint, and multinational operations. To be effective, naval intelligence must be structured to ensure both top-down and bottom-up intelligence support. Top-down intelligence support leverages national or theater intelligence resources to support the tactical

commander; bottom-up support ensures organic intelligence supports operations while contributing to the larger intelligence effort.

A-41. Naval forces have unique, multidimensional intelligence requirements. Countering threats to air, surface, subsurface, and landing forces requires in-depth knowledge of the threat, weather, hydrography, terrain, ports, and airfields. The sophisticated nature of the threat in naval warfare causes naval forces to demand detailed technical intelligence on an adversary's weapon systems.

A-42. The intelligence picture is formed from all sources in the operational environment, including dedicated force intelligence collection resources, national and theater assets, liaison officers, and units in contact with the enemy. Naval forces also have unique intelligence collection capabilities, such as embedding intelligence and crypto logic personnel, equipment, and communications at the unit, afloat staff, and theater and national levels which contribute to effective intelligence support under virtually all circumstances. See Naval Doctrine Publication (NDP) 2.

A-43. Naval intelligence attempts to impart thorough knowledge of the situation through the application of certain basic intelligence functions. These intelligence functions form the foundation of required analytical support to the commander. The effective incorporation of the following functions into the intelligence process will produce the highest quality support throughout planning and execution.

A-44. To support naval forces engaged in littoral operations, the primary work of naval intelligence is conducted at the tactical level in dedicated intelligence centers afloat, such as a Carrier Intelligence Center, or deployed ashore with the Marine Air Ground Task Force (MAGTF) command element. Personnel assigned produce not only current intelligence but also other finished intelligence products that support a variety of contingency operations. Intelligence centers provide assessments of the adversary's capabilities and build and maintain threat intelligence files and databases. Depending on mission requirements, these centers may be augmented with liaison personnel from other services or national intelligence agencies.

A-45. Naval intelligence centers serve as fusion centers where information from various sources (such as crypto logic sensors, tactical airborne reconnaissance, units in contact with the enemy) is validated, correlated, analyzed, and disseminated to support operations. These centers also use links to theater and component sensors and to the JICs, to complement organic capabilities and to facilitate national, theater, and tactical intelligence support to a wide range of operations.

A-46. Because naval forces will normally operate as a component of joint forces, both afloat and ashore intelligence centers are integral parts of an intelligence architecture that connects the commander to joint and service intelligence centers, national intelligence agencies, and the intelligence centers of other nations. Interoperability, cooperation in resource management, and intelligence sharing throughout this architecture are essential to support the commander's decision making.

A-47. For more information on naval operations, see NDP 1 and NDP 2.

MARINE CORPS

A-48. Unit intelligence sections are supported by a primary MAGTF intelligence node that can perform all types of intelligence operations. The four core elements of the MAGTF are—

- The command element, a headquarters unit that directs the other elements.
- The ground combat element, usually comprising infantry, supported by armor (tanks) and artillery, but may also include special units such as scouts or force reconnaissance, snipers, and forward air controllers.
- The aviation combat element, which contributes the air power to the MAGTF. The aviation combat element includes all aircraft (both fixed wing and helicopters), their pilots and maintenance personnel, and those units necessary for aviation command and control.
- The logistics combat element.

A-49. For complete details, see Marine Corps Doctrine Publication (MCDP) 1-0 and MCDP 2.

A-50. The LCE contains all of the support units for the MAGTF: communications, combat engineers, motor transport, medical, supply units, and certain specialized groups such as air delivery and landing support teams.

A-51. The MAGTF G-2, through its combat intelligence center, provides centralized direction for the collection, production, and dissemination efforts of organic and supporting intelligence assets and ensures these efforts remain focused on satisfying the PIRs that are essential to mission success.

A-52. The MAGTF intelligence functions are planned and executed by the surveillance, reconnaissance, and intelligence group, or the surveillance, reconnaissance, and intelligence group detachment. The surveillance, reconnaissance, and intelligence group has SIGINT, HUMINT, and reconnaissance assets that provide information to the MAGTF. A key to success is the ability to gather, analyze, evaluate, and disseminate combat intelligence between the MAGTF and the brigade. Leaders and liaison officers must focus on the differences in intelligence reporting procedures and techniques, digital capabilities and integration, and the different intelligence requirements of Army combined arms forces. All the organic, adjacent, higher, and joint, interagency, and multinational collection assets help to form the COP.

A-53. Recognizing that organic intelligence capabilities may be limited in particular environments, the MAGTF can draw on the full range of national, theater, Joint, other Service, and multinational intelligence assets. When available, these capabilities will be integrated into MAGTF intelligence operations.

MARINE CORPS FORCE RECONNAISSANCE

A-54. These are special-purpose units roughly analogous to the Navy SEALs, Air Force Air Commandos, or US Army Special Forces and are widely recognized as the "special operations forces" of the United States Marine Corps. Marine Force Reconnaissance personnel, or "operators," perform highly specialized, small- scale, high-risk operations, such as amphibious and deep ground surveillance, assisting in specialized technical missions such as nuclear, biological, chemical, radio, sensors and beacons, and deep reconnaissance, and other missions.

A-55. Force Reconnaissance units have been recently integrated into the United States Special Operations Command, and are now part of Marine Special Operation Battalions East and West.

AIR FORCE

A-56. The Air Force provides airborne surveillance and reconnaissance and is DOD's executive agent for space.

A-57. The commander, Air Force Forces, is also the Joint Force Air and Space Component Commander (JFACC). Typically, the JFACC serves as the supported commander for theater airborne surveillance and reconnaissance and provides integrated ISR for the JFC.

A-58. The Air and Space Operations Center (AOC) integrates the JFC's theater-wide airborne ISR capabilities, to include reachback and distributed operations ISR support. The ISR division within the AOC is responsible for effectively and efficiently orienting the JFACC and AOC to current and emerging enemy capabilities, threats, COAs, and centers of gravity with predictive and actionable intelligence, and to provide the JFACC with ISR operations management and targeting intelligence support. Planning, tasking, and executing theater airborne ISR missions are included in this responsibility. Subtasks of this responsibility include—

- Identify and manage JFACC requirements.
- Manage JFC (theater-level) requirements in conjunction with other Service components and with validation from the JFC.
- Integrate and synchronize use of air and space assets.
- Task theater airborne ISR assets to satisfy the JFC's requirements.

A-59. For more information on Air Force doctrine, see AFFD 1 and AFDD 2-9.

JOINT SPECIAL OPERATIONS TASK FORCE

A-60. SOF operates across the spectrum of military operations and is usually employed in theaters of operations under joint special operations task forces (JSOTFs).

A-61. Special operations include a variety of offensive, defensive, stability operations, and civil support operations that help to attain force dominance across the spectrum of conflict. JSOTFs usually conduct operations that support the theater campaign and major operations of subordinate forces. Special Operations Forces (SOF) may conduct operations outside continental United States in a geographic combatant commander's AOR, either in a foreign country supporting a US Ambassador or in a joint operations area established by the designated JFC. SOF offer viable military options, particularly when the situation calls for subtle, indirect, or low-visibility approaches.

A-62. All SOF of the Army, Navy, and Air Force based in the United States are placed under Commander, United States Special Operations Command (USSOCOM). USSOCOM has three service component commands: Army Special Operations Command, Fort Bragg, NC; Naval Special Warfare Command (NAVSPECWARCOM), Coronado, CA; Air Force Special Operations Command, Hurlburt Field, FL; and one sub-unified command, Joint Special Operations Command , Fort Bragg, NC.

A-63. USSOCOM exists to provide SOF to the President and Secretary of Defense, geographic combatant commanders, and American ambassadors and their country teams for successful conduct of special operations during both peace and war. USSOCOM prepares SOF to successfully conduct special operations, including CA and psychological operations.

A-64. Each of the theater unified commands has established a separate Special Operations Command (SOC) to meet its theater-unique special operations requirements. As subordinate unified commands, the theater SOCs provide the planning, preparation, and command and control of SOF from the Army, Navy, and Air Force. They ensure SOF strategic capabilities are employed and that SOF activities are synchronized with conventional military operations when applicable.

A-65. Theater SOCs offer several advantages to geographic commanders. As peacetime elements, the SOCs are the nucleus around which a JSOTF can be structured. They provide a clear chain of command for in-theater SOF as well as the staff expertise to plan, conduct, and support joint special operations in the theater's AOR. These special operations may include General Purpose Forces under operational control to a SOC. Theater SOCs normally exercise operational control of SOF (except CA and psychological operations) within each geographic combatant commander's (GCC) AOR. Additionally, SOCs provide the nucleus for the establishment of a JSOTF, when a JTF is formed. There are six SOCs supporting GCCs worldwide:

- Special Operations Command Joint Forces Command (SOCJFCOM).
- Special Operations Command Central (SOCCENT).
- Special Operations Command Europe (SOCEUR).
- Special Operations Command Pacific (SOCPAC).
- Special Operations Command Korea (SOCKOR).
- Special Operations Command South (SOCSOUTH).

Appendix B

Command Briefing and Debriefing Program

Commanders must ensure all Soldiers, units, and assets are involved in answering CCIRs. One way to make sure this occurs is to have a command pre-mission intelligence briefing and intelligence debriefing program.

PRE-MISSION INTELLIGENCE BRIEFING AND DEBRIEFING PROGRAM

B-1. The commander must establish, support, and allocate appropriate resources for a pre-mission briefing and debriefing program. Battle updates and after-action reviews are distinct and separate tasks from the pre-mission briefing and debriefing program. The intelligence officer develops a pre-mission intelligence briefing plan and complementary debriefing plan to support the commander's program. The intelligence pre-mission briefing and debriefing generally follow the format of a mission briefing, to include a review of the patrol route, mission patrol collection objectives, and methods employed.

PRE-MISSION INTELLIGENCE BRIEFING

B-2. Intelligence officers should develop a pre-mission intelligence briefing plan. The purpose of the pre-mission intelligence briefing is to ensure all personnel conducting tactical operations, tactical movements, non-tactical movements, and operational liaison are sensitized to specific information and reporting requirements, intelligence gaps, and unique mission requirements. (For more information on operational liaison, see FM 2-91.6.)

B-3. Pre-mission intelligence briefings may be an updated intelligence assessment or a detailed intelligence brief, depending upon the nature of the mission. Missions that may occur routinely, like convoy operations or presence patrols, may be preceded by an updated intelligence assessment including indicators of activity related to the CCIR. Tactical operations, such as planned raids, combat patrols, or patrols that will likely result in tactical site exploitation, will be preceded by a more detailed intelligence brief specific to the mission. This briefing will contain indicators related to the CCIR and instructions on handling captured enemy materiel. In all instances, pre-mission briefings include reporting guidance for observed information.

DEBRIEFING

B-4. Debriefing is the process of questioning US forces and DOD personnel returning from missions and patrols for information of value. Friendly force debriefing operations are the systematic debriefing of US forces to answer ISR tasks. Predictive intelligence is enhanced by analyzing what has been occurring within an AO. Debriefing also facilitates situational understanding of the operational environment.

B-5. Intelligence officers should develop a debriefing plan. The purpose of debriefing is to identify and record data the patrol collected pertaining to assigned SIRs and ISR tasks; collect any additional information and observations the patrol made concerning the operational environment; and collect any fliers, pamphlets, media or pictures the patrol found or obtained.

B-6. The plan should include debriefing all leaders returning from operational liaison or meetings, returning patrols, HUMINT collection teams, helicopter pilots, convoy personnel, and others who may have obtained information of intelligence value. The intelligence section debriefs personnel, writes and submits reports, or reports information verbally, as appropriate. The requirement for a debriefing by the

intelligence section following each mission should be a part of the intelligence pre-mission briefing. Leaders should not consider the mission complete or release involved personnel until reporting and debriefings are completed.

B-7. Operational liaison presents an opportunity to quickly assimilate information provided by key individuals into the intelligence process. Leaders plan for debriefing, either by intelligence officers or by the command debriefing team, after completing one or more operational liaisons. This information may provide insights into the civil considerations of the AO and indicators associated with CCIRs.

B-8. Once the element (leader, patrol, convoy) returns from the mission, the intelligence staff or command debriefing team conducts a thorough debrief. This debriefing should include all members of the patrol, including the leader, unit members and any attached personnel. Since every Soldier is a potential source of information, the intelligence debriefing is one way that information collected by these Soldiers gets into the intelligence system. In the event that the returning patrol splits into different locations, the intelligence staff should visit each location in order to debrief all the patrol members.

B-9. Debriefings are oral and normally result in a written report. Information on the written report should include the following:

- Size and composition of the unit conducting the patrol.
- Mission (type, location, and purpose).
- Departure and return times.
- Routes. Use checkpoints and grid coordinates for each leg or include an overlay.
- Detailed description of terrain and enemy positions that were identified.
- Results of any contact with the local population or the enemy.
- Unit status at the conclusion of the mission, including the disposition of dead or wounded Soldiers.
- Description of materials collected during the mission, such as fliers, pamphlets, media, or pictures the patrol found or obtained.
- Conclusions or recommendations.

B-10. When company, platoon, or smaller elements deploy to remote locations, debriefings by the intelligence staff may not be possible. Platoon and company leaders conduct debriefings in accordance with battalion SOPs to ensure reports are available to the intelligence section and staff. Reporting by the most expeditious means possible ensures patrol reports and additional notes from the debriefings are available for timely intelligence analysis. A viable method of enhancing unit support to intelligence when subordinate elements are not in proximity to the battalion staff is to task organize intelligence personnel to companies and platoons. A second method is cross-training company and platoon personnel to perform basic intelligence tasks, including patrol debriefing.

B-11. The intelligence staff debriefing should follow along the lines of the mission briefing—review the route traveled, collection objectives of the patrol, and methods employed. By the time the intelligence staff does its debriefing, it should be in receipt of the patrol report. Having the patrol report will streamline the intelligence staff debriefing process, allowing the intelligence staff to concentrate on filling in gaps and following up on reported information.

B-12. A practical method for debriefing is to review all patrol or mission actions chronologically. As detailed a sketch as possible should be made for visual reference of debriefed patrol areas. It is easier to recall and record information if it is broken into smaller pieces that flow logically. For example:

- Use a map to determine segments of the route traveled. Coordination points, checkpoints, phase lines, or significant events may divide segments. Start at the beginning of the patrol route and let the patrol leader show you on the map the route traveled.
- Ask the patrol leader: “From here (CKP1) to here (CKP2), what did you see (or hear or learn about)?” The goal is to extract information of intelligence value. Avoid asking only for the PIR. Doing so will tend to limit the patrol leader’s answers, and you might miss something of significance. Instead, let him tell you everything learned while on that segment of the mission.

Use follow-up questions to get complete information, always remembering to ask "What else" or "What other" before leaving a topic.

- If the patrol had digital cameras, it is helpful to use the pictures they have taken during the debriefing.
- Once a segment of travel has been fully exploited, move on to the next segment, questioning from the second CKP to the third CKP and continuing the process until the entire route has been exploited.

Appendix C

DCGS-A OVERVIEW

The DCGS-A program was created in response to the DOD Distributed Common Ground Station (DCGS) Mission Area Initial Capabilities Document, which captured the overarching requirements for an ISR Family of Systems that will contribute to joint and combined Warfighter needs. DCGS-A facilitates "Seeing and Knowing" on the battlefield—the foundation for the understanding.

SYSTEM OBJECTIVES

C-1. DCGS-A provides a net-centric, enterprised ISR, weather, geospatial engineering, and space operations capability to maneuver, support, and sustainment organizations at all echelons from the battalion to JTFs. DCGS-A will be the ISR component of the modular and future force Battle Command System and the Army's primary system for ISR tasking, posting, processing, and using information about the threat, weather, and terrain at all echelons.

C-2. DCGS-A provides the capabilities necessary for commanders to access information from all data sources and to synchronize non-organic sensor assets with their organic assets. DCGS-A provides continuous acquisition and synthesis of data and information from joint and interagency capabilities, multinational partners and non-traditional sources that will permit modular forces to maintain an updated and accurate understanding of the operational environment. DCGS-A contributes to visualization and situational awareness, thereby enhancing tactical maneuver, maximizing combat power, and enhancing the ability to operate in an unpredictable and changing operational environment throughout full spectrum operations.

C-3. DCGS-A will facilitate the rapid planning, execution, and synchronization of all warfighting functions resulting in the current and future force's ability to operate within the enemy's decision cycle. The core functions of DCGS-A are—

- Receipt and processing of select ISR sensor data.
- Control of select Army sensor systems.
- ISR synchronization.
- Fusion of sensor information.
- Direction and distribution of relevant threat.
- Friendly and environmental (weather and terrain) information.

C-4. DCGS-A systems (starting with DCGS-A(V4) described below) will be a net-centric, web-enabled, enterprise-based, open-architecture system of systems deployed across the force in support of land component commanders. It will function as a first step toward the ability to systematically access and leverage other Service ISR datasets and build an ISR architecture that integrates and synchronizes on-scene, network-distributed, and intelligence reach activities. The DCGS-A objective (DCGS-A(V5)) architecture will be capable of supporting multiple, simultaneous, worldwide operations through scalable and modular system deployments.

OPERATIONAL DESCRIPTION

C-5. DCGS-A is the Army's ground processing system for all ISR sensors. DCGS-A integrates existing and new ISR system hardware and software that produces a common net-centric, modular, multi-security,

multi-intelligence, interoperable architecture. DCGS-A provides access to data across the Intelligence Enterprise as well as facilitates intelligence reach with knowledge centers. DCGS-A—

- Provides access to Joint Worldwide Intelligence Communications System, National Security Agency Net, Secure Internet Protocol Router Network, and Nonclassified Internet Protocol Router Network.
- Links tactical ISR sensors along with weather, space, and geospatial analysis capabilities into the Intelligence Enterprise.
- Enhances distributed operations through its net-centric capability by allowing ISR data access down to tactical units.
- Provides the analyst data mining, fusion, collaboration, and visualization tools to conduct situational awareness, ISR synchronization, targeting support, analysis, and reporting.
- Provides users access to ISR raw sensor data, reports, graphics, and web services through the DCGS-A Integration Backbone (DIB). The DIB—
  - Creates the core framework for a distributed, net-centric Intelligence Enterprise architecture.
  - Enables DCGS-A to task, process, post, and use data from Army, Joint, and National ISR sensors.
  - Provides a meta-data catalog that defines how to describe data. The meta-data allows DCGS-A to expose the required data elements to the user.

C-6. As the primary ISR processing system from the JTF down to battalion and below units, DCGS-A is the ISR component of the Battle Command System and provides the intelligence, weather, and geospatial engineering data to Battle Command. It provides threat reporting and the threat portion of the COP to the Publish and Subscribe Services for ABCS users, as well as accesses friendly unit information for DCGS-A users. DCGS-A provides the analyst data mining, fusion, collaboration, and visualization tools to quickly sort through large amounts of data to provide timely, relevant intelligence to the commander.

C-7. DCGS-A tools assist the targeting process as well as synchronize ISR collection. DCGS-A not only provides the analyst access to national and theater data sources but also serves as a ground station for organizational ISR sensors. DCGS-A facilitates distributed operations and reduces the forward physical footprint.

DCGS-A CONFIGURATIONS

C-8. There are three major DCGS-A configurations:

- Embedded.
- Mobile.
- Fixed.

EMBEDDED

C-9. The embedded configurations will be the common software baseline for all users. When connected to the DCGS-A enterprise, the embedded configuration will provide access to the enterprise of ISR sensor data, information, and intelligence. Immediate access to weather, geospatial engineering, and multi-intelligence discipline data—along with ISR synchronization, collaboration, fusion, targeting, and visualization tools provided in the DCGS-A embedded configuration—will enable users to collaboratively access, plan, task, collect, post, process, exploit, use, and employ relevant threat, non-combatant, geospatial engineering, and weather information.

C-10. Embedded DCGS-A software will enable access to the DCGS-A enterprise where users will subscribe to data services and acquire on-demand software applications to perform unique or new information processing tasks. The DCGS-A embedded configuration provides the ISR component to the Battle Command System at all echelons and within all units connected to the Future Force Network. DCGS-A will be an embedded component of the Future Combat System (FCS) Family of Systems and the

Ground Soldier System. Because it is a component of the Battle Command System, DCGS-A permeates the entire Army force structure to facilitate combat and staff functions.

MOBILE

C-11. DCGS-A mobile configurations will be organic to and directly support deployed modular brigades and Division G-2s, BFSBs, Corps G-2s, and Military Intelligence Brigades (MIBs) of the ASCCs. DCGS-A mobile capabilities will be modular and scalable to meet supported unit deployment and tactical mobility criteria. They will operate independently, but will be more capable when connected to operational and strategic level sensors, sources, and people. DCGS-A mobile brings sensor data to the deployed unit and provides a dedicated processing and analysis segment for organic sensors as well as the capability to use unexploited data from all sensors. DCGS-A mobile extends the strategic and operational level joint, interagency, and multinational ISR network into the tactical operational environment. The DCGS-A mobile will provide a wide range of ISR capabilities including direct access and control of select sensor platforms.

C-12. When not deployed, mobile assets will operate as part of the ISR network and be fully integrated into DCGS-A fixed and home station operations. Upon full fielding, the DCGS-A mobile capabilities will displace (physically) and replace (functionally) current tactical intelligence tasking, posting, processing, and using systems within the Corps G-2s/Division G-2s/BFSBs/MIBs and BCTs. The DCGS-A mobile configuration includes man-portable and vehicle-based hardware platforms.

C-13. The man-portable system is titled Multi-Function Workstation-Mobile (MFWS-M) and the vehicle transportable system is titled the Mobile Intelligence Service Provider. Each Mobile Intelligence Service Provider will contain a mixture of Multi-Security Level, Multifunction Workstations and MFWS-Ms based on the number of personnel supported and the unit's mission. The MFWS-M includes the embedded software baseline plus additional applications exclusive to MI professionals. These additional applications are required to allow MI Soldiers to perform more complicated processing tasks that require specialized training to perform. The MFWS-M will be found primarily with the S-2 sections in the maneuver battalions, separate brigades, and other areas with MI professionals where an MISP cannot be supported.

FIXED

C-14. DCGS-A fixed facilities are regionally located and provide overwatch to tactical units. The fixed configuration conducts the day-to-day "heavy lifting" support to all echelons. This configuration possesses a robust hardware processing and data storage capacity. Forward-deployed organizations collaborate with, and reach to, fixed configurations across the network to substantially expand the commander's situational awareness without increasing the forward footprint. Fixed configurations are expected to be "always on" providing general and direct ISR processing, exploitation, analysis, and production support to all echelons.

DCGS-A INCREMENTAL DEVELOPMENT

C-15. DCGS-A will follow an evolutionary acquisition strategy to develop and field capabilities incrementally throughout its life cycle. This evolutionary approach is divided into three increments and provides the ability to field the best possible capability available at any point in time. This incremental approach will be executed through a series of software releases. For the most part, delivered capabilities will be software only but could include some hardware products as necessary.

C-16. It should be noted that although there are some DCGS-A capabilities that will not be available until Increment 3 (FY 13 and beyond), Increment 2 systems will be designed to support the objective system requirements. This should allow Increment 3 upgrades to be executed as software-only modifications to fielded systems. DCGS-A fielding was accelerated and delivered incrementally based on operational requirements associated with the war on terrorism. The incremental development includes consolidation and replacement of the capabilities found in the following current force systems:

- All versions of all-source analysis system (ASAS).
- CI and Interrogation Workstation.

- Human Domain Workstation.
- All versions of the Tactical Exploitation System.
- All versions of the Guardrail common sensor ground processors (for example, the Integrated Processing Facility and the Guardrail Ground Baseline).
- Prophet Control.
- Joint Surveillance Target Attack Radar System common ground sensor (CGS).
- Digital Topographical Support System-Light (DTSS-L).
- Integrated Meteorological System (IMETS).
- Space Support Enhancement Toolset.

INCREMENT 1

C-17. Increment 1 includes initial efforts to improve interoperability between current force systems and related modification to program of record (POR) systems to provide a capability like and early DCGS-A. Increment 1 also includes the integration of the Joint Intelligence Operations Capability-Iraq quick reaction capability. Responsibility for all JIOC capabilities transitioned to the program manager DCGS-A. At that time JIOC systems were redesignated DCGS-A(V2). This product was fielded to Operation Iraqi Freedom and Operation Enduring Freedom units in FY 06-07 and provides access to over 200 data sources.

C-18. Version 3.0 hardware and software upgrades added the DIB as well as two-way battle command interoperability. Version 3.1 will add the DCGS-A architecture framework. Increment 1 supports the migration of functionality and capabilities from existing POR systems, providing a means to support replacement of ASAS-Light with V3.1 software.

INCREMENT 2

C-19. DCGS-A Increment 2 provides ongoing development, through successive DCGS-A software baseline releases, and integration of echelon above corps to battalion fixed and mobile systems that provide for full net-centric operations. This increment includes DCGS-A enabling of current POR systems at the BCT in FY09, at division and above in FY10, and the DCGS-A mobile test article development and follow-on production.

C-20. Increment 2 includes the DCGS-A enabling of BCT POR systems (Analysis and Control Team-Enclave, DTSS-L, IMETS, CGS, and Prophet Control). When the DCGS-A capability is hosted on fielded POR systems, these systems are termed “DCGS-A enabled.”

INCREMENT 3

C-21. Increment 3 (“Objective” DCGS-A) includes the embedded ISR toolset for ABCS and FCS and the delivery of capabilities requiring the maturity of technology or developments from complementary systems such as FCS and future Aerial Common Sensor not available during the previous increments. For additional information on DCGS-A, see Military Intelligence Handbook 2-50.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

ACE	analysis and control element
AO	area of operations
AOC	Air and Space Center
AOI	area of interest
AOR	area of responsibility
ARNG	Army National Guard
ARNGUS	Arny National Guard of the United States
ART	Article (Army Universal Task List)
ASARS	Advanced Synthetic Aperture Radar System
ASAS	all-source analysis system
ASCC	Army Service Component Command
ASCOPE	areas, structures, capabilities, organizations, people, and events
BCT	brigade combat team
BE	basic encyclopedia
BFSB	battlefield surveillance brigade
CA	Civil Affairs
CCIR	commander's critical information requirements
CKP1	Checkpoint 1
CKP2	Checkpoint 2
CGS	common ground sensor
CI	counterintelligence
COA	course of action
COM	collection operations management
COP	common operational picture
CRM	collection requirements management
DCGS	Distributed Common Ground Station
DCGS-A	Distributed Common Ground Station-Army
DIB	Distributed Common Ground Station-Army Integration Backbone
DOD	Department of Defense
DST	decision support template
DTSS	Digital Topographical Support System-Light
EEFI	essential elements of friendly information
ETIOV	earliest time information is of value
ES2	every Soldier is a sensor
FCS	Future Combat System
FFIR	friendly force information requirement

FRAGO	fragmentary order
FY	fiscal year
GCC	geographic combatant commander
HUMINT	human intelligence
HVT	high-value target
IED	improvised explosive device
IMETS	Integrated Meteorological System
IPB	intelligence preparation of the battlefield
IR	information requirement
ISR	intelligence, surveillance, and reconnaissance
JFACC	Joint Force Air Component Commander
JFC	joint force commander
JIC	Joint Intelligence Center
JIOC	joint intelligence operations center
Joint STARS	Joint Surveillance Target Attack Radar System
JOPP	joint operation planning process
JSOTF	joint special operations task force
JTF	joint task force
LNO	liaison officer
LTIOV	latest time information is of value
MAGTF	Marine Corps Air Ground Task Force
MASINT	measurement and signature intelligence
MCDP	Marine Corps Doctrine Publication
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MFWS-M	Multi-Function Workstation-Mobile
MI	military intelligence
MIB	military intelligence brigade
NAI	named area of interest
NDP	Naval Doctrine Publication
NIST	National Intelligence Support Team
OCONUS	outside continental United States
OPLAN	operations plan
OPORD	operations order
PIR	priority intelligence requirement
POR	program of record
RCIED	radio-controlled improvided explosive device
RDSP	rapid decision-making and synchronization process

RFI	request for information
SIGINT	signals intelligence
SIR	specific information requirement
SOC	Special Operations Command
TAI	targeted area of interest
UAS	unmanned aircraft system
USAR	United States Army Reserve
USSOCOM	United States Special Operations Command
VBIED	vehicle-borne improvised explosive device
WARNO	warning order

SECTION II – TERMS

basic encyclopedia

A compilation of identified installations and physical areas of potential significance as objectives for attacks (JP 1-02).

cueing

The use of one or more systems to provide data that directs collection by other systems (FM 2-0).

intelligence, surveillance, and reconnaissance

An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function (JP 1-02). For Army forces, this activity is a combined arms operation that focuses on priority intelligence requirements while answering the commander's critical information requirements.

intelligence, surveillance, and reconnaissance integration

The task of assigning and controlling a unit's intelligence, surveillance, and reconnaissance assets (in terms of space, time, and purpose) to collect and report information as a concerted and integrated portion of operation plans and orders. This task ensures assignment of the best intelligence, surveillance, and reconnaissance assets through a deliberate and coordinated effort of the entire staff across all warfighting functions by integrating intelligence, surveillance, and reconnaissance into the operation (JP 2-0).

intelligence, surveillance, and reconnaissance synchronization

The task that accomplishes the following: analyzes information requirements and intelligence gaps; evaluates available assets internal and external to the organization; determines gaps in the use of those assets; recommends intelligence, surveillance, and reconnaissance assets controlled by the organization to collect on the commander's critical information requirements; and submits requests for information for adjacent and higher collection support. This task ensures that intelligence, surveillance, and reconnaissance, intelligence reach, and requests for information result in successful reporting, production, and dissemination of information, combat information, and intelligence to support decision making (JP 2-0).

latest time information is of value

The absolute latest time the information can be used by the commander in making the decision the priority intelligence requirement supports. The latest time information is of value can be linked to time, an event, or a point in the battle or operation (FM 2-0).

named area of interest

The geographical area where information that will satisfy a specific information requirement can be collected. NAIs are usually selected to capture indications of enemy courses of action but also may be related to battlefield and environment conditions. It is possible to redesignate a named area of interest as a targeted area of interest on confirmation of enemy activity within the area, allowing a commander to mass the effects of his combat power on that area (FM 3-90).

reconnaissance handover line

A designated phase line on the ground where reconnaissance responsibility transitions from one element to another (FM 3-20.96).

redirecting

Updating or correcting information that allows an ISR asset to more effectively execute its mission. Redirecting an ISR asset does not change its mission

retasking

Assigning an ISR asset a new task and purpose on completion of its initial requirement, on order after latest time information is of value having not satisfied the original requirement, as planned to support a branch or sequel, or to respond to a variance.

targeted area of interest

The geographical area or point along a mobility corridor where successful interdiction will cause the enemy to abandon a particular course of action or requires him to use specialized engineer support to continue. It is where the enemy can be acquired and engaged by friendly forces. The commander designates target areas of interset where he believes his unit can best attack high-payoff targets (FM 3-90).

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

Note. Field manuals and selected joint publications are listed by new number followed by the old number.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

ARMY PUBLICATIONS

AR 381-10, *US Army Intelligence Activities*, 3 May 2007
DODD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 25 April 1988
FM 1-02 (101-5-1), *Operational Terms and Graphics*, 21 September 2004
FM 2-0 (34-1), *Intelligence*, 17 May 2004, with Change 1, dated September 2008
FM 3-0, *Operational Terms and Graphics*, 27 February 2008
FM 3-90, *Tactics*, 4 July 2001
FM 5-0 (101-5), A*rmy Planning and Orders Production*, 20 January 2005
FM 6-0, *Mission Command: Command and Control of Army Forces*, 11 August 2003
FM 7-15, *The Army Universal Task List (AUTL)*, 31 August 2003.
FM 34-2-1, *Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance*, 19 June 1991
FMI 5-0.1, The *Operations Process*, 31 March 2006
JP 2-0, *Joint Intelligence*, 22 June 2007
JP 2-01, *Joint and National Intelligence Support to Military Operations*, 7 October 2004
JP 3-60, *Joint Targeting*. 13 April 2007

AIR FORCE PUBLICATIONS

AFFD 1, *Air Force Basic Doctrine*
AFFD 2-9, *Intelligence, Surveillance, and Reconnaissance*, July 2007

NAVY PUBLICATIONS

NDP 1, *Naval Warfare*, March 1994
NDP 2, *Naval Intelligence*

MARINE CORPS PUBLICATIONS

MCDP 1-0, *Marine Corps Operations*, September 2001
MCDP 2, *Intelligence*, June 1997.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/jpcapstonepubs.htm.

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (as amended through 4 March 2008)
JP 2-03, *Geospatial Intelligence Support to Joint Operations*, 22 March 2007

JP 3-0, *Joint Operations*. 17 September 2006
JP 3-06, *Doctrine for Joint Urban Operations*, 16 September 2002
JP 3-55, *Doctrine for Reconnaissance, Surveillance, and Target Acquisition Support for Joint Operations (RSTA)*, 14 April 1993
JP 3-60, *Joint Doctrine for Targeting*, 17 January 2002
JP 5-0, *Joint Operational Planning*, 26 December 2006

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://akocomm.us.army.mil/usapa/doctrine/.
Army regulations are produced only in electronic media. Most are available online:
https://akocomm.us.army.mil/usapa/epubs/index.html

FM 2-22.3, *Human Intelligence Collector Operation*, 6 September 2006
FM 2-91.4, *Intelligence Support to Urban Operations*, 20 March 2008
FM 2-91.6, *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*, 10 October 2007
FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aircraft Systems*, 3 August 2006
FM 3-06, *Urban Operations*, 26 October 2006
FM 3-07, *Stability Operations*, 06 October 2008
FM 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, 28 November 2003
FM 3-19.1, *Military Police Operations*, 22 March 2001
FM 3-19.50, *Police Intelligence Operations*, 21 July 2006
FM 3-20.96, *Reconnaissance Squadron*, 20 September 2006
FM 3-20.98, *Reconnaissance Platoon*, 02 December 2002
FM 3-20.971, *Reconnaissance Troop, Reconnaissance Troop and Brigade Reconnaissance Troop*, 2 December 2002
FM 3-24, *Counterinsurgency*, 15 December 2006
FM 3-34.170, *Engineer Reconnaissance*, 25 March 2008
FM 3-50.1, *Army Personnel Recovery*, 10 August 2005
FM 3-90.15, *Sensitive Site Operations*, 25 April 2007
FM 3-90.119, *Combined Arms Improvised Explosive Device Defeat Operations*, 21 September 2007
FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process*, 8 May 1996
FM 7-92, *The Infantry Reconnaissance Platoon and Squad (Airborne, Air Assault, Light Infantry)*, 23 December 1992
FM 7-93, *Long-Range Surveillance Unit Operations*, 3 October 1995
FM 17-95, *Cavalry Operations*, 24 December 1996
FM 17-97, *Cavalry Troop*, 3 October 1995
FM 34-3, *Intelligence Analysis*, 15 March 1990
FM 34-10, *Division Intelligence and Electronic Warfare Operations*, 25 November 1986
FM 34-37, *Echelons above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations*, 15 January 1991
FM 34-54, *Technical Intelligence*, 30 January 1998
FM 34-80, *Brigade and Battalion Intelligence and Electronic Warfare Operations*, 15 April 1986
FM 34-81, *Weather Support for Army Tactical Operations*, 31 August 1989
FM 34-130, *Intelligence Preparation of the Battlefield*, 8 July 1994
FMI 2-22.9, *Open Source Intelligence*, 5 December 2006
ST 2-19.402, *STRYKER Brigade Combat Team Intelligence Operations*. 1 March 2003
ST 2-19.602, *Surveillance Troop*, 1 March 2003

READINGS RECOMMENDED

These sources contain relevant supplemental information.

Scouts Out! The Development of Reconnaissance Units in Modern Armies, John J. McGrath, U.S. Army Combat Studies Institute, Fort Leavenworth, KS, 2008

Index

FMI 2-01
November 2008

By order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0829501

DISTRIBUTION:

Active Army, the Army National Guard (ARNG)/Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR). Not to be distributed. Electronic media only.

FOR OFFICIAL USE ONLY

PIN: 085222-000

FOR OFFICIAL USE ONLY