FM 2-01

ISR SYNCHRONIZATION

HEADQUARTERS, DEPARTMENT OF THE ARMY

15 MARCH 2009

Field Manual
No. 2-01 (FMI 2-01)

Headquarters
Department of the Army
Washington, DC, (Initial Draft)

Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization

Contents

***This publication supersedes FMI 2-01, 11 November 2008**

Figures

Tables

Preface

This FM provides the foundation for Army intelligence, surveillance, and reconnaissance (ISR) synchronization doctrine and supersedes FMI 2-01 published in 2008. Its scope is ISR synchronization and intelligence support to ISR integration, and ISR during the planning and operations processes. Readers must understand FM 3-55 (when published) which describes the overarching doctrinal concepts for ISR as well as this FM to grasp the true importance of combined arms ISR operations.

The Army's warfighting doctrine, organizations, training, and operations continue to change in order to match the dangers and challenges of today's operational environment. Therefore, FM 2-01 updates Army ISR synchronization doctrine to conform to the most current operational and intelligence doctrine. This FM complies with doctrine set forth in FM 2-0, 3-0, 5-0, 6-0, and FM 5-1 (when published).

While applicable to all Army leaders, the primary audience for FM 2-01 is the intelligence and operations staff officers, who must work together to develop the ISR plan, and commanders, who must understand the importance of ISR synchronization as part of ISR planning and the operations process.

This FM outlines intelligence responsibilities during planning and on-going operations, propagation of ISR information and intelligence, assessing, and updating ISR operations. There are four chapters and four appendixes.

- The introduction summarizes doctrinal changes that have occurred since the release of FMI 2-01, lays out the doctrinal framework and expands upon the manual's purpose.
- Chapter 1 explains how ISR synchronization supports the full spectrum of operations; its role in the operations process; and how it relates to the intelligence warfighting function.
- Chapter 2 summarizes and defines key ISR synchronization terms and concepts within combined arms and intelligence doctrine and directly links them to battle command.
- Chapter 3 describes intelligence support and ISR planning during the military decision-making process (MDMP).
- Chapter 4 details the ISR synchronization process after the completion of planning when operations are underway.
- Appendix A explains the requirements development process from the initial information requirements, through prioritization process, to the formulation of specific information requirements (SIRs), to the development of ISR tasks that are used to direct ISR operations.
- Appendix B describes ISR synchronization training and resources available at the US Army Intelligence Center.
- Appendix C discusses Joint, national, and multinational ISR planning considerations.
- Appendix D describes DCGS-A enabled ISR planning and operations.

FM 2-01 provides ISR synchronization guidance for Army commanders, staffs, and trainers at all echelons from company to Army service component command (ASCC). This FM forms the foundation for established curriculum within the Army's educational system on ISR synchronization. The information presented is descriptive, not prescriptive or restrictive.

FM 2-01 provides details on the six continuing activities of ISR synchronization; one of the most important staff activities performed to aid the commander with visualization and battle command. Although the discussion and descriptions in this manual may seem linear, ISR synchronization is a dynamic, continuous, and interactive staff process requiring constant coordination between the intelligence and operations officers. Depending on

mission, time available, ongoing operations, and standing operating procedures (SOPs), units may develop abbreviated ISR planning techniques to meet the commander's needs, however, this manual describes the optimal process.

This FM 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). Joint doctrine applies to joint organizations; Army headquarters that operate as joint headquarters must use joint ISR doctrine.

The term "intelligence officer" refers to the actual G-2, S-2, or other top ISR 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 and weather, and civil considerations, which includes areas, structures, capabilities, organizations, people, and events. Continuous and aggressive ISR operations are the primary means of gaining knowledge of the operation environment.

ISR supports the full spectrum of operations through five tasks:

- Perform ISR synchronization.
- Perform ISR integration.
- Conduct Reconnaissance.
- Conduct Surveillance.
- Conduct Related Missions and Operations.

As a critical combined arms operation, ISR provides answers to commanders' and staffs' 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) to the assessment of ISR operations and updating of ISR plans.

It is also crucial that commanders and staffs understand that ISR is not synonymous with Intelligence, which is one supporting effort to ISR requiring total staff involvement and careful planning to answer the commander's critical information requirements (CCIR).

How the Army performs ISR is continuously changing. The Army's evolving force structure, newly developed systems and increased reliance upon Joint and National sensors necessitates the weaving of ISR doctrine into every aspect of combined arms doctrine. It must also be current, relevant, and usable at all echelons.

As the result of force structure developments, Brigade combat teams (BCTs) have a larger intelligence staff and more collection systems, as well as more robust surveillance and reconnaissance capabilities. The Army brigade combat team (BCT) is now the lowest echelon that conducts long-term analysis functions and often receives representatives of national agencies. At Corps and ASCC, intelligence staffs rely more heavily on Joint, National and Multinational ISR resources and information requirements cover operational and strategic matters.

The Army Division possessing no organic intelligence collection assets, however, it can be augmented by a battlefield surveillance brigade (BFSB) or task organized with assets provided by a combatant command. Therefore, it must leverage Joint and National collectors in support of its own information requirements as well as those of its subordinate echelons.

The ISR synchronization process laid out in FMI 2-01 carries over to this FM. However, the approach taken in this FM will directly connect ISR synchronization to staff functions, the planning and operations processes, and it includes significant additions and modifications from recent updates to combined arms and intelligence doctrine. The table below shows the new or changed material in FM 2-01 compared to FMI 2-01.

Some of the terms used this manual require clarification because misusage is common. For example, an ISR asset is subordinate to the requesting unit or echelon, while an ISR resource is not. In other words, higher echelons own and control ISR resources, while an asset is organic or under the command and

control of the supported organization. This distinction becomes tricky when ISR resources take direction from the supported commander, but are managed and controlled by a different organization. Higher echelons apportion limited ISR resources against the competing requirements of lower echelons. The owning echelon allocates ISR assets against its own requirements and apportions ISR resources against those of subordinate and supported commanders.

New or Changed	***Comments***
Intelligence Warfighting Function	Modified, FM 2-0, 2009
RSTA/ISR definition	Added, FM 2-0, chg 1, 2008
Generate Intelligence Knowledge	Added, FM 2-0, 2009
Conduct Related Missions and Operations	Added, FM 2-0, 2009
ISR synchronization plan	Deleted, replaced by ISR synchronization tools
ISR synchronization tools	Added to decrease confusion with the ISR plan; tools include ISR synchronization matrix, requirements matrix, and ISR overlay
Apportionment	Added, JP 2-01
Allocation	Added, JP 2-01
ASCOPE	Deleted, pending new civil consideration memory aid

Chapter 1

Intelligence, Surveillance, and Reconnaissance Synchronization and Full Spectrum Operations

Army operations occur within a complex framework of environmental factors that shape their nature and affect their outcomes. The Commander uses ISR operations and Intelligence to understand that complex framework of environmental factors. This chapter describes the operational environment, the operational concept, and the full spectrum of operations and the intelligence warfighting function.

THE OPERATIONAL ENVIRONMENT

1-1. The *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). While they include all enemy, adversary, friendly, and neutral systems across the spectrum of conflict, they also include an understanding of the environment, the state of governance, technology, local resources, and the culture of the local population (FM 3-0).

1-2. Today's operational environments are complex and require continuous learning and adaptation. The operational environment is different for each campaign or major operation. The operational environment evolves as the campaign or operations progress. The changes in Operation Iraqi Freedom from 2003 to the present provide a good example of the environment evolving over time.

1-3. Observations from senior Army leaders during Operation Desert Storm, Operation Iraqi Freedom, and Operation Enduring Freedom regarding intelligence operations show that military intelligence analysts at the tactical level were not familiar with the operational environment at the outset of these conflicts. Those observations further suggest that it took analysts a significant amount of time to gain enough of an understanding to assist the staff in improving its situational awareness. This shortfall negatively affected the commander's ability to gain situational understanding.

1-4. Successful mission accomplishment requires understanding of the operational environment. ISR operations are one of the best means for the commander to achieve that understanding, but understanding truly begins well before the execution of operations. Intelligence officers assist the commander in achieving a full understanding prior to operations by remaining connected to the global information grid (GIG) throughout the Army Force Generation (ARFORGEN) cycle.

INSTABILITY AND PERSISTENT CONFLICT

1-5. Complex local, regional, and global changes shape today's operational environments leading to both opportunities and risks for our country. The risk component of these changes manifests in certain trends that drive instability and persistent conflict. Some of those trends are:

- Globalization.
- Technology.
- Demographic changes.
- Urbanization.
- Resource demand.

- Climate change and natural disasters.
- Proliferation of weapons of mass destructions and effects.
- Failed or failing states.

1-6. Properly synchronized and integrated ISR operations help reduce risk and uncertainty for the Commander. For further discussion on these trends, see FM 3-0.

THE THREAT

1-7. FM 3-0 defines threats as nation-states, organizations, people, groups, conditions, or natural phenomena able to damage or destroy life, vital resources, or institutions. There are four major threat categories the intelligence officer must assist the commander and staff in understanding—

- Traditional threats posed by states employing recognized military capabilities and forces in understood forms of military competition and conflict.
- Irregular threats from those employing unconventional, asymmetric methods and means to counter traditional U.S. advantages.
- Catastrophic threats involving the acquisition, possession, and use of nuclear, biological, chemical, and radiological weapons (also called weapons of mass destruction) and effects.
- Disruptive threats from enemies who develop and use new technologies to reduce U.S. advantages in key operational domains.

1-8. These threats increase the possibility of state failures, humanitarian disasters, and ungoverned areas becoming enemy safe havens. The rise of transnational terrorist networks, religious radicalism, ethnic genocide, sectarian violence, and large criminal networks coupled with failing nation-states create perils for United States and its national interests.

1-9. By combining traditional, disruptive, catastrophic, and irregular capabilities, adversaries will seek to create advantageous conditions by quickly changing the nature of the conflict and moving to employ capabilities for which the United States is least prepared. Threats use the environment to their advantage and they rapidly adapt to changes in the environment. Extremist organizations will seek to take on state-like qualities using the media and technology and their position within a state's political, military, and social infrastructures to their advantage.

1-10. ISR operations and intelligence, in addition to experience and applied judgment, are the best tools a commander has available to gain situational understanding of the threat and the operational environment. See FM 3-0 for further discussion on the changing nature of the threat.

OPERATIONAL VARIABLES

1-11. Commanders and staffs use operational variables to understand and analyze the characteristics of the operational environment. The operational variables are directly relevant to campaign planning; however, they may be too broad for tactical planning. Planners at the tactical level should carefully consider whether PMESII-PT is valuable in their particular case.

1-12. Military planners describe the operational environment in terms of the operation variables. Joint military planners use six interrelated variables: **P**olitical, **M**ilitary, **E**conomic, **S**ocial, **I**nformation, **I**nfrastructure (PMESII). Army doctrine adds two additional variables: ***P***hysical environment and **T**ime (PMESII-PT). Operational variables describe not only the military aspects of an operational environment, but also human aspects such as the population and its influences on the operational environment. Before the receipt of the mission, the operational variables help the commander understand the problem and lead the unit through its training, planning and preparations.

1-13. Prior to receipt of mission, commanders and staffs generate intelligence knowledge to answer information gaps in the operational variables. Upon receipt of a mission (which may only be a warning

order), Commanders focus their mission analysis what is relevant to their mission using mission variables. Table 1-1 illustrates the relationship between operational and mission variables.

MISSION VARIABLES

1-14. Once a warning order or mission is received, commanders narrow their focus to six mission variables to analyze the operational environment. The mission variables are Mission, Enemy, Terrain and weather, Troops and support available, Time available, and Civil considerations (METT-TC). The mission variables help the commander understand the nature of the mission, design the operation, and visualize the end state. The mission variables are the major variables considered during mission analysis.

1-15. *Civil considerations* reflect how the man-made infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, population, and organizations with an area of operations influence the conduct of military operations (FM 6-0).

Table 1-1. Operational and mission variable comparison

Operational Variables PMESII-PT	***Mission Variables (METT-TC)***					
	Mission	***Enemy***	***Terrain and weather***	***Troops and support***	***Time available***	***Civil considerations***
Political						√
Military		√		√		
Economic						√
Social						√
Information		√		√		√
Infrastructure						√
Physical environment			√			
Time					√	

1-16. Commanders use ISR operations to develop information and intelligence on three mission variables: enemy, terrain and weather, and civil considerations. ISR synchronization supports the commander's needs through the ISR synchronization tools used to manage 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.

1-17. ISR operations and intelligence reach should begin as soon as possible after receipt of the mission in order to begin gathering data to answer information and intelligence gaps on the operational environment. Timely and accurate intelligence encourages audacity and can facilitate actions that may negate enemy tactics and materiel.

THE OPERATIONAL CONCEPT

1-18. The Army's operational concept describes the full spectrum of operations where Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment. Mission command that conveys intent and appreciation of all aspects of the situation guides the adaptive use of Army forces (for more detail, see FM 3-0).

THE SPECTRUM OF CONFLICT

1-19. The general nature of military operations can be described as a point along an ascending scale of violence ranging from stable peace to general war called the spectrum of conflict. Total war and perfect peace are rare and cannot coexist. Between these extremes are variations of conflict involving the application of military force needed to restore order or overturn the existing order within a society or the struggle between two societies. Conflict intensity varies over time and among locations; therefore, it is difficult to describe an operations character because it is likely to evolve over time.

OPERATIONAL THEMES

1-20. The Army's operational concept uses operational themes to describe the character of the dominant major operation. The operational themes group types of military operations according to common characteristics and establish the taxonomy for understanding the many kinds of joint operations and the relationships among them.

1-21. The Army's uses the following operational themes to characterize its major operations:

- Peacetime military engagement.
- Limited intervention.
- Peace Operations.
- Irregular warfare.
- Major combat operations.

1-22. Operational themes have implications for task-organization, resource allocation, protection, and tactical task assignment. Therefore, the operational theme influences the commander's decisions with regard to ISR operations. Intelligence officers must guide the Commander through the planning process on the unique ISR considerations for each major operational theme. Several examples in the following paragraphs will guide the intelligence officer when preparing an ISR strategy and intelligence architectures for each type of operation. Figure 1-1 depicts the spectrum of conflict and operational themes.

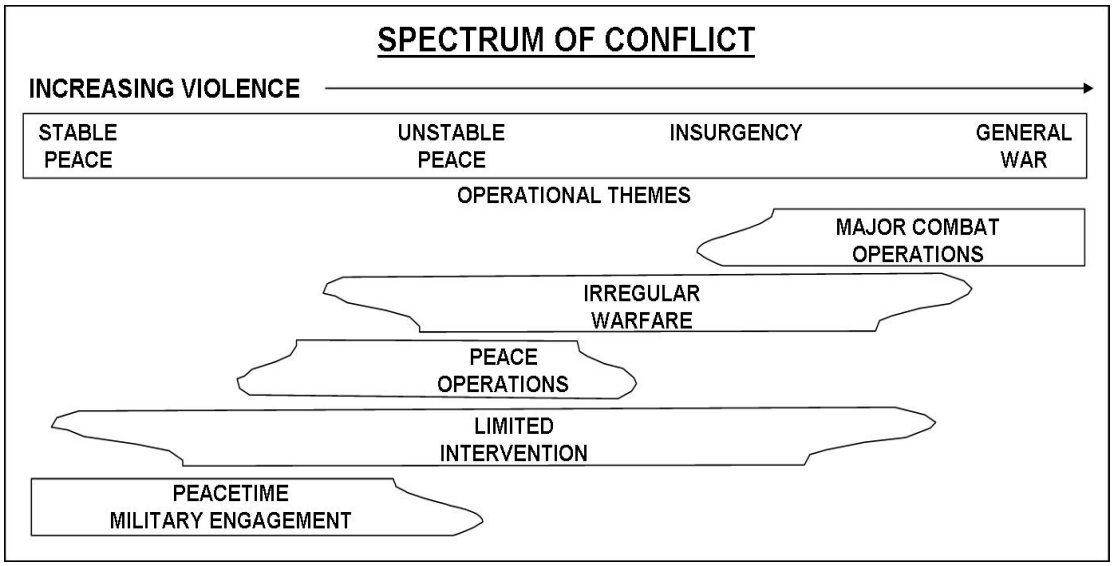

Figure 1-1. The spectrum of conflict and operational themes

Peacetime Military Engagement

1-23. Peacetime military engagement comprises all military activities involving other nations intended to shape the security environment in peacetime. Examples include multinational training exercises, security assistance, joint combined exchange training, recovery operations, arms control, and counterdrug operations.

1-24. Combat is not likely during these operations, but terrorist attacks against Army forces are always possible. Nonetheless, commanders will require intelligence support for force protection planning and for operations security concerns. U.S. National and Theater intelligence agencies will provide the primary ISR support to units these missions. Army units may receive also limited support from host nation agencies. Intelligence officers should consider both sources of information when developing intelligence plans. During peacetime military engagements, legal constraints or political concerns may limit ISR options.

Limited Intervention

1-25. Commanders use limited interventions to achieve a clearly defined and limited scope end state. Joint task forces normally conduct limited interventions. Examples of limited interventions the brigade may participate in are noncombatant evacuation, raids, show of force, foreign humanitarian assistance, consequence management, sanction enforcement, and elimination of weapons of mass destruction.

1-26. Like peacetime military engagement, combat is not likely during limited interventions. However, the threat of terrorist attacks is possible as are attacks from the general population. The Commander will be primarily concerned with targeting operations, force protection, and operations security.

1-27. The threat usually consists of terrorist, guerilla, paramilitary, political, or religious groups opposing an established government supported by the U.S. government. These groups may not well defined at the tactical level and are probably un-located. National, theater, and host nation agencies will generally not provide all of the information the Commander requires. Instead, those agencies generally provide enough information initially to focus tactical ISR operations. During limited interventions, legal constraints or political concerns may limit ISR options.

Peace Operations

1-28. Peace operation is a broad term that encompasses multiagency and multinational crisis response and limited contingency operations. The primary purpose of peace operations is to create a safe and secure environment, deter adversaries from overt actions against each other, and provide time for civilian agencies to generate a self-sustaining peace. Peace operations include peacekeeping, peace building, peacemaking, peace enforcement, and conflict prevention.

1-29. Peace operations normally occur in complex environments characterized by asymmetric threats, a failing government, little or no rule of law, terrorism, human rights abuses, collapse of civil infrastructure, and the presence of dislocated civilians. Attacks by insurgent and terrorist groups are likely and US forces may conduct limited offensive operations against these groups during peace operations.

1-30. Enemy forces will try to mitigate the US ISR capabilities by adopting tactics, techniques, and procedures (TTP) that reduce vulnerability to observation and collection systems. When developing ISR plans at every echelon, intelligence officers must consider the enemy's ability to develop low technology, low-cost counter-ISR solutions including deception techniques designed to spoof collection systems.

1-31. Peace operations often occur under the mandate of international organizations such as the United Nations. They are also likely to be multinational operations involving forces from many nations. See appendix C for multinational ISR considerations.

Irregular Warfare

1-32. Irregular warfare is a violent struggle among state and non-state actors for legitimacy and influence over a population. It differs from conventional operations in two aspects. First, it is warfare among and within the people. Secondly, it emphasizes an indirect approach by avoiding direct military confrontation. Instead, it combines irregular forces and indirect unconventional methods to exhaust the opponent. To counter irregular warfare, the Army employs its forces in foreign internal defense, support to insurgency, counterinsurgency, combating terrorism, and unconventional warfare types of operations.

1-33. Traditionally, special operations forces conduct these types of operations. Conventional forces may be involved either in support of special operations forces or they may be involved in separate operations in the same area of operations. During Operation Enduring Freedom (OEF) special operations forces and conventional forces work together on different problem sets in the same type of operation.

1-34. Just as in limited interventions and peace operations, US forces generally oppose an undefined and un-located enemy that operates within complex terrain. The tactics and operational art employed by these forces will vary from conflict to conflict as will the structure of the threats themselves.

1-35. In irregular warfare operations, the traditional mix of ISR assets used in conventional operations may not satisfy the commander's information requirements. Irregular warfare operations sometimes require unconventional thinking in terms of ISR planning.

Major Combat Operations

1-36. Major combat operations occur in circumstances usually characterized by general war and combat between large formations. During major combat operations, Army forces are normally involved in offensive or defensive operations as part of a larger joint force. ISR operations during major combat operations will be very complex and fast-paced requiring constant coordination and synchronization.

FULL SPECTRUM OPERATIONS

1-37. Full spectrum operations require continuous, simultaneous combinations of offensive, defensive, and stability or civil support tasks. Modern conflict involves more than combat between opposing nations. Current and future conflicts are likely to be conducted "among the people" instead of "around the people." Therefore, operations will likely consist of a complicated mixture of lethal and nonlethal actions designed to change political, military, economic, social, and other conditions within an area of operations.

1-38. While defeating the enemy, the Army may simultaneously be conducting stability operations and could be engaged in civil support tasks for homeland security purposes. This was the case in late 2001 with offensive and stability operations in Afghanistan happening concurrently with infrastructure security missions in the US.

1-39. Army Intelligence provides timely, relevant, accurate, and synchronized intelligence support to tactical and operational commanders during the full spectrum of operations. ISR operations facilitate the commander's understanding of the mission variables of enemy, terrain and weather, and civil considerations. This understanding allows the commander to conduct operations at a time and place of our choosing rather than reacting to enemy operations. When the enemy is not a foe, but rather the factors influencing instability or a natural disaster, ISR operations are still able to aid the commander in understanding the operational environment in order to make prudent decisions about the application of military resources.

1-40. All intelligence operations must be executed within the scope and parameters of applicable laws, policies, and regulations. To ensure compliance with these directives, intelligence and operations officers must give them detailed consideration during ISR planning.

1-41. Full details on the full spectrum of operations appear in FM 3-0 and FM 3-90 describes the tactics used in these operations.

OFFENSIVE OPERATIONS

1-42. *Offensive operations* are combat operations conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers (FM 3-0). Offensive operations at all levels require effective intelligence to help the commander avoid the enemy's main strength and to deceive and surprise the enemy. During offensive operations, intelligence must provide the commander with an intelligence running estimate in a timely manner for the commander to affect the enemy significantly. The intelligence running estimate ensures commanders have the intelligence they need to conduct offensive operations with minimum risk of surprise.

1-43. The primary purpose of ISR during offensive operations is to locate, identify, and track the enemy. Intelligence derived from ISR operations then creates an opportunity for the commander to allocate sufficient combat power at the point of the enemy's greatest vulnerability. Intelligence also identifies where and when the commander can most decisively defeat the enemy's counterattack or exploit additional enemy vulnerabilities.

1-44. Intelligence officers must understand the tenets of offensive operations and the tactics performed during offensive operations in order to synchronize ISR operations to complement maneuver operations. ISR synchronization is especially important during offensive operations because sequencing and timing of movement and maneuver events can change quickly. Airborne ISR assets are well suited to offensive operations because they can rapidly respond to friendly forces location changes. Centralized planning and execution of ISR operations may provide the control necessary to keep collection synchronized with maneuver.

DEFENSIVE OPERATIONS

1-45. *Defensive operations* are combat operations conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations (FM 3-0). The immediate purpose of defensive operations is to defeat an enemy attack. Commanders defend to buy time, hold key terrain, hold the enemy in one place while attacking in another, or destroy enemy combat power while reinforcing friendly forces.

1-46. ISR operations and intelligence analysis should determine the enemy's strength, COAs, and location of enemy follow-on forces. Defending commanders can then decide where to arrange their forces in an economy-of-force role to defend and shape the battlefield. Intelligence support and ISR provide time for commanders to commit the striking force precisely.

1-47. ISR operations and the intelligence effort in defensive operations identifies, locates, and tracks the enemy's main attack and provides the commander time to allocate sufficient combat power to strengthen the defense at the point of the enemy's main effort. Intelligence should also identify where and when the commander can most decisively counterattack the enemy's main effort or exploit enemy vulnerabilities.

1-48. Intelligence officers must understand the tenets of defensive operations and the tactics performed during defensive operations in order to synchronize ISR operations to complement maneuver. Ground-based ISR assets can play a key role in defensive operations. However, the intelligence officer must consider the risk to the asset when considering its ISR task and positioning.

STABILITY OPERATIONS

1-49. *Stability operations* encompass various military missions, tasks, and activities conducted outside the US in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (JP 3-0). Current Army thinking considers the tasks required for stability operations equally as important as the full combat with the enemy.

1-50. Information is currency during stability operations. Commanders require the appropriate intelligence and IPB products in order to determine how best to influence the environment and enhance regional

stability. The identification and analysis of the threat, terrain, weather, and civil considerations are important in conducting stability operations. A lack of knowledge concerning insurgent activities, issues creating tension between factions, local politics, customs, and culture could lead to US actions that potentially offend or create mistrust among popular leaders or the population.

1-51. The operational environment is frequently more complex during stability operations and as a result, ISR operations are often equally as complex. Commanders must be closely involved in and knowledgeable of ISR during stability operations. For example, commanders may have to deal with multiple lines of operations within one major campaign, each one with competing requirements for ISR operations. The commander must decide how to prioritize his ISR operations when there are more requirements than he has collection capabilities. In addition, legal or political considerations may constrain the commander's ISR operations.

1-52. During stability operations, ISR operations controlled at higher echelons are much more difficult to synchronize with the other aspects of the lower echelon's operations. In Operation Iraqi Freedom (OIF), centralized planning and decentralized execution of ISR seems to be a successful strategy. By giving control to the supported ground tactical commander, all enablers and maneuver elements are synchronized with the organic ISR assets and allocated ISR resources from higher echelons. In addition, pushing the ISR assets down to the lowest level possible flattens the architecture so those commanders can pull data directly from the asset and not have to wait for higher echelons to push the data down. For more information on intelligence support to stability operations, see FM 2-91.1 when published.

Company Intelligence Support Team

1-53. Many commanders have found it useful to designate a company intelligence support team during stability operations. When properly resourced, it can increase the company Commander's situational understanding and provide bottom-up intelligence to battalion and BCT improving battle command at those echelons as well.

1-54. The mission of a company intelligence support team is to describe the enemy, terrain and weather, and civil considerations in the company's area of operation in order to reduce the commander's uncertainty and aid his decision-making.

CIVIL SUPPORT OPERATIONS

1-55. *Civil support* is the Department of Defense support to U.S. civil authorities for domestic emergencies, and for designated law enforcement and other activities (JP 1-02). Civil support includes operations that address the consequences of natural or manmade disasters, accidents, terrorist attacks, and incidents within the United States and its territories. Army forces conduct civil support operations when the size and scope of events exceed the capabilities or capacities of domestic civilian agencies.

1-56. The Army National Guard (ARNG) often acts as a first military responder for civil support operations on behalf of State authorities while serving in State active duty status or when functioning under Title 32 U.S. Code authority. State active duty status refers to ARNG forces and State defense force personnel under State control. In State active duty status, the State Governor commands the ARNG and the State defense force (if applicable). ARNG civil support missions are planned and executed in accordance with the needs of the State and within the guidelines of State laws and statutes. ARNG forces in State active duty status can perform civil law enforcement missions in accordance with the laws and statutes of their State. Once placed in Title 32 or Title 10 status, ARNG units must adhere to the same laws governing active Army and Army Reserve operations.

1-57. Intelligence support in civil support operations is conducted strictly within the guidelines of U.S. law and focused on the specific missions directed by the Secretary of Defense. ISR operations must be planned to they adhere to the law and still answer the CCIR. Careful planning of ISR operations with detailed instructions to the units and Soldiers involved will ensure collection operations do not violate U.S. laws.

1-58. ISR assets can provide imagery and video products of the incident location or affected areas for federal agencies, first responders, and local law enforcement to use. ISR systems that provide real time data and images from ISR assets can be positioned in incident command posts to provide video or imagery to the incident commander. ISR can be a valuable asset for assessing damage to infrastructure, locating populations at risk, and determining passable routes for first responders to provide aid.

1-59. For more information on Civil Support see FM 3-28.1 and for intelligence support to civil support operations, see FMI 2-91.501 when published.

THE OPERATIONS PROCESS

1-60. The *operations process* consists of the major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation. The commander drives the operational process (FM 3-0). ISR synchronization is one of five integrating processes that occur during all operations process activities. Figure 1-2 illustrates the operations process.

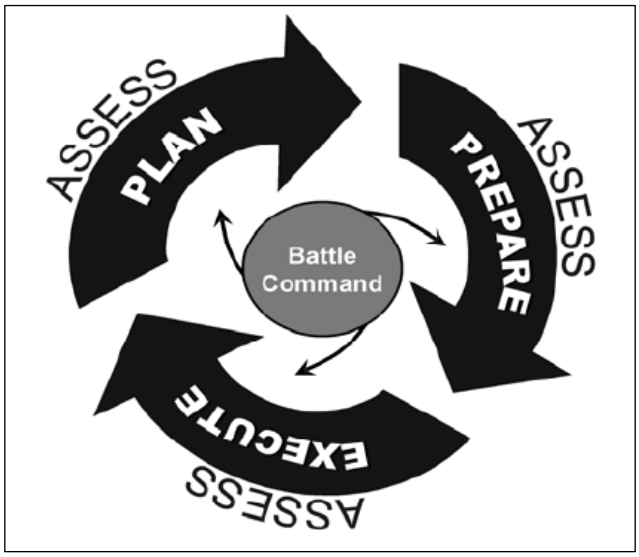

Figure 1-2. The operations process

1-61. A *plan* is a design for a future or anticipated operation (FM 5-0). A plan is a continuous, evolving framework of anticipated actions, which guides subordinates through each phase of the operation. Planning begins at receipt of mission. The commander and staff translate the commander's visualization into a specific course of action for execution using the operations process. Planning does not end when the plan is published as operations plans (OPLAN), operations orders (OPORD), or fragmentary orders (FRAGO). Planning continues throughout the operation to anticipate and prepare for changes in the situation.

1-62. One of the most important aspects of ISR synchronization planning is the intelligence and opeations officers make sure the ISR plan nests within the overall plan to ensure ISR operations provide timely critical information that answer the CCIR and tie directly to decision points. The best way for this to happen is for the intelligence officer and staff to be involved in every step of the decision making process.

1-63. *Prepare* consists of activities performed by units to improve their ability to execute an operation. Preparation includes, but is not limited to, plan refinement; rehearsals; intelligence, surveillance, and reconnaissance; coordination; inspections; and movement (FM 3-0). This definition mentions ISR because of its importance to the execution phase of the operations process. The prepare phase of the operations process is where the commander refines his plan based on information obtained through surveillance and reconnaissance operations.

1-64. *Execution* is putting a plan into action by applying combat power to accomplish the mission and using situational understanding to assess progress and make execution and adjustment decisions (FM 3-0). It focuses on concerted action to seize, retain, and exploit the initiative. Commanders assess the situation throughout execution. They base assessments on their personal observations, the common operational picture, running estimates and assessments from the staff, and input from subordinate commanders and others. ISR operations are vital to keeping the common operational picture, running estimates and staff assessments up to date and focused.

1-65. *Assessment* is the continuous monitoring and evaluation of the current situation, particularly the enemy, and progress of an operation (FM 3-0). Assessment ties directly to the commander's decisions throughout planning, preparation, and execution. Critical to effective assessment is developing criteria to evaluate progress toward task accomplishment, achievement of objectives, and attainment of the end state conditions. The commander expresses assessment criteria in terms of measures of effectiveness (MOEs) or measures of performance (MOPs).

1-66. Assessment is continuous throughout planning, preparation, and execution. However, the focus of assessment differs for each of these activities. ISR operations are typically used to gather the measurements used to assess the efficacy of current operations.

INTELLIGENCE WARFIGHTING FUNCTION

1-67. The *intelligence warfighting function* consists of the related tasks and systems that facilitate understanding of the threat, terrain and weather, and civil considerations (FM 2-0). The four intelligence warfighting function tasks are—

- Support to force generation.
- Support to situational understanding.
- Perform ISR.
- Support to targeting and information superiority.

1-68. The intelligence warfighting function is a flexible and adjustable architecture of procedures, personnel, organizations, and equipment enabled by the DCGS-A network providing 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 resources from the other warfighting functions if they conduct intelligence, surveillance or reconnaissance missions. Every Soldier, as part of a small unit, is a potential information collector and an essential component to help answer information requirements.

1-69. The intelligence warfighting function is a continuous process and 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, components and warfighting functions.

1-70. The collective task "Perform ISR" supports the other three intelligence tasks listed above well as collective tasks across many other warfighting functions by collecting the information necessary to facilitate force generation, situational understanding and lethal and non-lethal targeting.

1-71. According to FM 2-0, the Army's tactical collective task "Perform Intelligence, Surveillance, and Reconnaissance" is an integrated operations and intelligence function that includes five subtasks:

- Perform ISR synchronization.
- Perform ISR integration.
- Conduct reconnaissance.
- Conduct surveillance.
- Conduct related missions and operations.

1-72. Perform ISR synchronization is described in detail in later this chapter. The other ISR collective tasks are discussed further in FM 3-55.

INTELLIGENCE PROCESS

1-73. Intelligence operations are executed by performing five steps that constitute the intelligence process: generate intelligence knowledge, plan, prepare, collect, and produce. Additionally, there are four functions that occur across the five steps of the intelligence process: analyze, commander's input, assess, and propagate. The four functions can occur at any time during the process.

1-74. The *intelligence process* provides a common model with which to guide one's thoughts, discussions, plans, and assessments (FM 2-0). The intelligence process generates information, products, and knowledge about the threat, the AOI, and the situation, which supports the commander and staff in developing a plan, seizing and retaining the initiative, building and maintaining momentum, and exploiting success. Figure 1-3 depicts the intelligence process. See FM 2-0 for further explanation of the intelligence process.

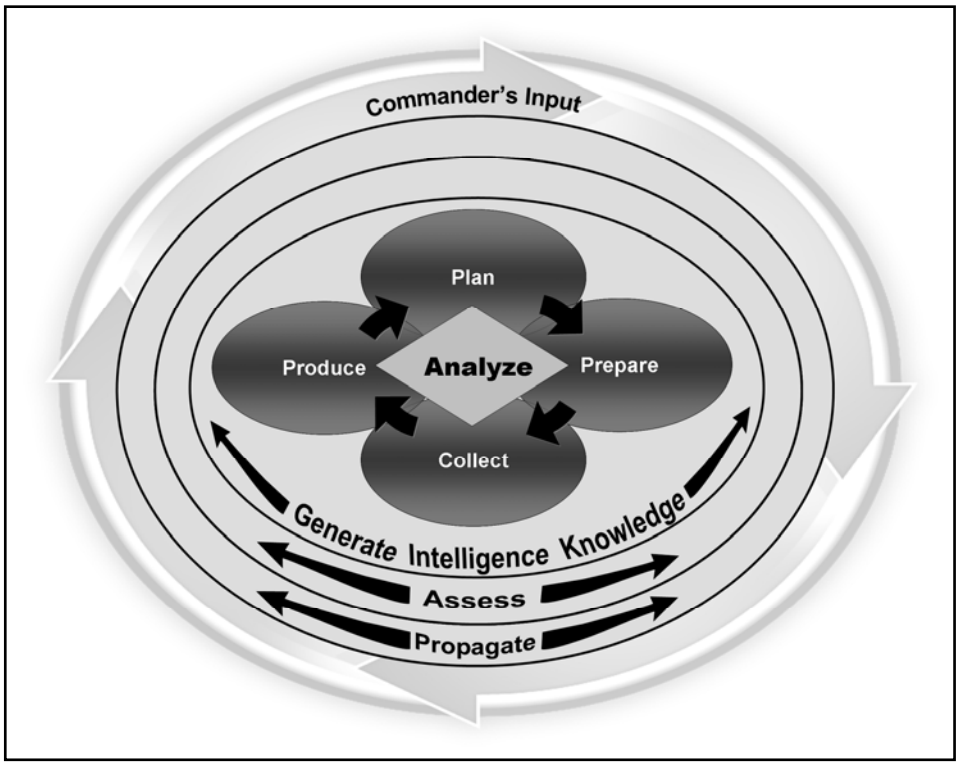

Figure 1-3. The intelligence process

GENERATE INTELLIGENCE KNOWLEDGE

1-75. *Generate intelligence knowledge* is a continuous and user-defined step driven by the commander that begins prior to mission receipt and provides the basic knowledge required concerning the operational environment before conducting mission analysis, IPB, planning, and operations (FM 2-0). Generate intelligence knowledge begins as early as possible, in some cases when the commander knows only the general location or theme for a projected operation, and continues throughout the operations process. The unit determines what information they will need (based on the commander's guidance), what information they already and what information they need to collect.

1-76. Knowledge is obtained through intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; OSINT; or other information sources that support operations, planning, battle-focused training, execution, and commander's decisions for the operational environment. When conducting the generate intelligence knowledge step, units and personnel must follow all applicable policies and regulations on the collection of information and OPSEC. Generate intelligence knowledge is an integral part of the intelligence process.

1-77. Generate intelligence knowledge is the precursor for conducting IPB and mission analysis. Generate intelligence knowledge is also the basis for developing a unit's initial intelligence survey. When published, see TC 2-33.401 and FM 3-0.2.

Initial Database Development

1-78. The initial result of the generate intelligence knowledge step is the creation and population of data files as directed by the commander that are compatible with the technical information architecture. When generating intelligence knowledge, unit intelligence personnel should begin by determining what information they need to collect based on the primary components of the operational environment for which the intelligence staff is responsible in order to support the command, IPB, and answer the CCIRs. As G-2/S-2 and other staff sections begin to collect data on the projected AO, baseline data files are organized per the commander's guidance.

1-79. Generally, the tactical echelons create primary data files, based on the threat, terrain and weather, and civil considerations. After creating the data files the data, information, intelligence, products, and material obtained are organized and refined to support mission analysis and the entire military decision-making process (MDMP) through functional analysis.

1-80. Chapter 4 of this FM discusses database management.

Intelligence Survey

1-81. The intelligence survey is a tool that assists the intelligence officer in identifying ISR asset collection capabilities and limitations within the projected AO for potential employment. The intelligence survey consists of five steps:

- Developing a comprehensive information baseline, collection capability baseline, and analytical baseline for the projected AO.
- Determining key intelligence gaps which begins the process of determining and validating ISR collection requirements.
- Determine key gaps in analytical ability.
- Developing an understanding of the information and intelligence that can be collected with unit intelligence assets and, when appropriate, ISR assets in the projected AO and how and where it may best be collected. This becomes the initial ISR plan developed in the MDMP.
- Determining a method of understanding when changes to the information baseline, collection capability baseline, or analytical baseline occur that are of intelligence interest.

1-82. The intelligence survey is a key element used during ISR synchronization. Developed over time and continuously updated, the intelligence survey provides the unit intelligence officer with an initial assessment for recommending intelligence asset apportionment within the projected AO and how best to use the unit's intelligence assets within the projected AO, taking into account technical and tactical considerations across all disciplines.

PLAN

1-83. The plan task consists of the activities that identify pertinent IRs and develop the means for satisfying those requirements. The CCIRs (PIRs and FFIRs) drive the ISR effort. The intelligence officer

supports the operations officer in arranging the ISR effort, based on staff planning, to achieve the desired collection effects. Planning activities include, but are not limited to—

- Conducting IPB.
- Submitting RFIs and using intelligence reach to fill information gaps.
- Establishing the intelligence communications and dissemination architecture.
- Managing requirements for ISR operations.
- Developing, managing, and revising the ISR synchronization tools and the ISR plan as mission requirements change.
- Evaluating reported information.
- Supporting the end state of the plan step, the preparation of annex B, Intelligence, and assisting the operations officer in completing annex L, ISR.

PREPARE

1-84. Preparation is the key to successful intelligence analysis and collection. Intelligence analysts must use the previous steps to prepare products for the commander and staff for orders production and the conduct of operations. Failure to prepare properly for intelligence collection and the publication of finished intelligence products can cause an operation to be focused on an entirely wrong location, force, or objective. Thorough preparation allows the operations staff to develop a plan that fights the threat and focuses the greatest amount of combat power at the right spot on the battlefield to achieve victory. The intelligence officer and the G-2/S-2 staff must develop these products during the prepare step of the intelligence process:

- IPB products and overlays.
- Initial PIRs.
- The ISR synchronization tools including matrices and overlays.
- Initial running intelligence estimates or briefings (usually as part of the Mission Analysis Briefing), which should include initial PIRs as well as threat strengths and vulnerabilities that friendly forces should avoid or exploit.

1-85. The prepare step includes those staff and leader activities which take place upon receiving the OPORD, OPLAN, WARNO, or commander's intent in order to improve the unit's ability to execute tasks or missions.

COLLECT

1-86. The collect task involves collecting, processing, and reporting information based on ISR tasks. ISR assets collect information and data about the threat, terrain, weather, and civil considerations for a particular AO and area of influence. A successful ISR effort results in the timely collection and reporting of relevant and accurate information that supports the commander's situational understanding.

1-87. This collected information forms the foundation of intelligence databases, intelligence production, and the situational awareness of the staff. The intelligence officer evaluates the reported information for its responsiveness to the CCIRs (PIRs and FFIRs).

PRODUCE

1-88. The produce task involves combining analyzed information and intelligence from single or multiple sources into intelligence or intelligence products in support of known or anticipated requirements. Production also involves combining new information and intelligence with existing intelligence in order to produce intelligence in a form that the commander and staff can apply to planning and situational understanding. During the produce task, the intelligence staff exploits information by—

- Analyzing the information to isolate significant elements.

- Evaluating the information to determine accuracy, timeliness, usability, completeness, precision, and reliability.
- Combining the information with other relevant information and previously developed intelligence.
- Applying the information to estimate possible outcomes.
- Presenting the information in a format that will be most useful to its user.

1-89. The intelligence staff deals with numerous and varied production requirements based on PIRs and other intelligence requirements; diverse missions, environments, and situations; and user format requirements. Through analysis, collaboration, and intelligence reach, the intelligence officer and G-2/S-2 staff use the collective intelligence production capability of higher, lateral, and subordinate echelons to meet the production requirements.

THE INTELLIGENCE FUNCTIONS

1-90. The three functions discussed below can occur at any time throughout the intelligence process.

COMMANDER'S INPUT

1-91. Input is a commander's responsibility and is provided at the commander's discretion. It provides the primary mechanism for the commander to focus the intelligence warfighting function and. Through the planning process and assessment functions, the intelligence officer is obliged to consult the commander for input. The commander's input directly influences the unit's ISR effort.

1-92. Each commander determines which intelligence products are developed, as well as the format of the products. The commander's input for ISR operations is described further in Chapter 2 under the role of the commander. Assessment of ISR operations and dissemination of ISR information are also important and those two concepts are discussed in chapter 4.

ANALYZE

1-93. *Analysis* is the process by which collected information is evaluated and integrated with existing information to produce intelligence that describes the current—and attempts to predict the future—impact of the threat and environment on operations (FM 2-33.4). The intelligence staff analyzes intelligence and information about the threat's capabilities, friendly vulnerabilities, and the AO to determine their nature, origin, and interrelationships. The intelligence staff must also analyze and identify issues and problems that occur while conducting the unit's intelligence process. One example of this could be focusing on the wrong priority or assets that are inadequately placed to collect required information.

1-94. This analysis enables commanders, staffs, and leaders to determine the appropriate action or reaction and to focus or redirect assets and resources to fill information gaps, mitigate collection limitations, or alleviate pitfalls. It is also within the analyze function that intelligence analysts evaluate large amounts of collected information and intelligence to obtain only that information which pertains to the CCIRs (PIRs and FFIRs), updating the intelligence running estimate, maintaining intelligence input to the common operational picture (COP), and facilitating the commander's situational understanding.

ASSESS

1-95. Assess plays a critical role in evaluating the information collected during the intelligence process. The continual assessment of ISR operations, available information and intelligence, and what is known about the various aspects of METT-TC are critical to ensure the intelligence staff:

- Answers the commander's CCIRs.
- Provides the operations staff with input to redirect ISR assets in support of changing requirements.

- The effective use of information and intelligence.

1-96. Assessment of ISR operations is described in chapter 4.

PROPAGATE

1-97. The propagate function includes all aspects of dissemination including intelligence sharing and granting access to databases, information or intelligence for others to conduct intelligence reach. It also encompasses posting information to unit web pages and the intelligence and ISR data needed to update the COP.

1-98. Dissemination is the act of communicating relevant information of any kind from one person or place to another in a usable form by any means to improve understanding or to initiate or govern action. Dissemination entails delivering timely, relevant, accurate, predictive, and tailored intelligence to the commander.

1-99. Chapter 4 describes the dissemination of ISR data as part of the propagate intelligence function.

Intelligence Reach

1-100. *Intelligence reach* is a process by which military forces proactively and rapidly access information from, receive support from, 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 (TC 2-33.5). Intelligence reach allows intelligence analysts to retrieve existing information, intelligence products, and data that can support answering the CCIRs from outside the unit in a timely manner without having to wait for an answer to an RFI or an ISR task. The information, intelligence products, or data retrieved can then be evaluated against other data and information obtained through ISR operations for use in the unit's intelligence products or analysis.

1-101. Intelligence reach is distinguishable from the normal process of providing combat information and intelligence up and down the chain of command because it involves a unit obtaining the information or intelligence directly from the source without necessarily using the formal RFI process.

1-102. Intelligence reach does not replace the traditional echeloned RFI system. The purpose of intelligence reach is to obtain information proactively or intelligence to prepare for a mission without tying up intelligence personnel at various echelons or having to wait for the traditional RFI process to deliver an answer. Instead, it enhances a unit's ability to obtain intelligence data that is already collected and intelligence products containing analyzed information. The intelligence staff synchronizes the requirements (RFIs and intelligence reach) from external elements into the unit's ISR plan.

1-103. Intelligence reach may be the only way to satisfy an intelligence requirement. In the same manner that your unit may require combat information or intelligence from external sources to independently confirm or deny assessments or enemy courses of action, other organizations may depend upon your unit to provide them with information or intelligence that only your unit can provide.

1-104. Units can access the information and intelligence holdings of other organizations, normally via classified networks, unclassified government networks and the Internet. Access to other unit's common databases usually requires prior permission. It is important that intelligence officers determine where they may need permissions and obtain them as early as possible before ad hoc requirements become urgent.

1-105. When access through intelligence reach is not possible, then intelligence personnel must initiate a formal RFI to the appropriate echelon, who will either answer it or formally pass that request to the next echelon to obtain an answer. When the information or data required does not exist and the command or its subordinate units do not possess the means to collect it through ISR operations, the intelligence officer then submits a request for collection or support to another echelon where the capability exists.

1-106. Units should not solely depend on intelligence reach to satisfy a PIR. Intelligence reach supplements and clarifies what was obtained through ISR operations. Intelligence reach can be used

answer other information requirements which are not high enough in priority to warrant ISR task. See FM 2-0 and TC 2-33.5 for further details on intelligence reach.

ARMY INTELLIGENCE ENTERPRISE

1-107. Within the framework of the intelligence warfighting function, the intelligence tasks and the intelligence process, intelligence personnel further focus on conducting intelligence from a fundamental, enterprise perspective.

1-108. The Army intelligence enterprise is the sum total of the networked and federated systems, and efforts of the military intelligence personnel (to include, collectors and analysts), sensors, organizations, information, and processes that allows the focus necessary to use the power of the entire intelligence community. The purpose of the Army intelligence enterprise is to provide technical support and guidance as well as an information and intelligence architecture that efficiently and effectively synchronizes intelligence, surveillance, and reconnaissance (ISR) operations and intelligence analysis and production to drive intelligence production in support of the commander's situational awareness.

1-109. It is important to note at this point that ISR is not synonymous with intelligence. ISR operations are intended to gather information and data that can be processed into information and intelligence for immediate application by the commander and his staff. The intelligence enterprise provides the commander with architecture containing personnel, sensors, organizations, information and processes that collect relevant information to support decision-making.

Chapter 2

Intelligence, Surveillance, and Reconnaissance Synchronization Fundamentals

This chapter describes ISR, surveillance, reconnaissance, the ISR synchronization process, and the role of the commander, the intelligence officer and the operations officer in the planning, preparation, execution and assessment of ISR operations.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

2-1. ISR is more than just the sum of its parts—intelligence, surveillance and reconnaissance. It is the composite of all activities and operations intended to gather data and information that in turn are used to create knowledge and support the commander's information needs facilitating battle command and visualization.

2-2. *Intelligence, surveillance, and reconnaissance (ISR)* is 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. ISR is an integrated intelligence and operations function. 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).

2-3. Army doctrine recognizes the joint ISR definition and 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. Army ISR operations directly support the tactical commander. The Army must focus its ISR operations for maximum collection by a limited number of assets and resources to produce the best intelligence possible. Army units contend with complex terrain considerations requiring a concerted effort between all ISR assets from coordinated exploitation of joint and national ISR capabilities down to Soldier surveillance and reconnaissance at the company or platoon level. Soldier surveillance and reconnaissance implements the Army initiative called every Soldier is a Sensor (ES2). For more information on Soldier surveillance and reconnaissance, see FM 2-91.6 Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection.

2-4. According to FM 7-15, Army Universal Task List, 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 Reconnaissance.
- Conduct Surveillance.
- Conduct Related Missions and Operations.

2-5. Synchronization and integration of the ISR effort places all ISR assets and resources into a single plan in order to capitalize on the different capabilities; synchronizes and coordinates surveillance and

reconnaissance missions; and employs other units for ISR tasks within the overall scheme of maneuver. A good ISR plan fits into the overall operations plan or order and it positions ISR assets so they can collect the right information; sustain and reconstitute for branches or sequels; or shift priorities as the situation develops.

INTELLIGENCE

2-6. According to Joint Publication 2-0, *intelligence* is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations (JP 2-0). The term is also applied to the activity that results in the product and to the organizations engaged in such activity.

2-7. For the purposes of ISR discussions in this field manual, the term intelligence has a much broader meaning, which is described under the intelligence warfighting function in chapter 1.

RECONNAISSANCE

2-8. *Reconnaissance* is a mission to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (FM 3-0).

2-9. Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about activities and resources of an enemy or potential enemy. This mission also secures data concerning the meteorological, hydrographic, or geographic characteristics and the local population of a particular area. Other detection methods include signals, imagery, measurement of signature, or other technical characteristics. This task includes performing chemical, biological, radiological, and nuclear (CBRN) reconnaissance; and the tactical aspects of special operations forces reconnaissance.

2-10. Reconnaissance operations are normally short-term and generally designed to collect information actively against specific targets for a specified time by a collector that does not dwell over the target or in the area. A time constraint is generally associated with the tasking. A reconnaissance mission may include periods of surveillance.

SURVEILLANCE

2-11. *Surveillance* is the systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means (FM 3-0). Other means may include but are not limited to space-based systems, and using special CBRN, artillery, engineer, special operations forces, and air defense equipment. Surveillance involves observing an area to collect information.

2-12. Surveillance is often passive and not oriented to a specific target, unless the surveillance takes place as part of a reconnaissance mission. Surveillance is normally a sustained process, particularly when conducted by technical means.

Joint Persistent Surveillance and Related Army Concepts

2-13. 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.*

2-14. 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.

2-15. 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.

2-16. 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 develop fully 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.

RELATED MISSIONS AND OPERATIONS

2-17. Within the context of the intelligence warfighting function, ISR related missions and operations are the activities and tasks associated with support to the conduct of ISR operations or providing ISR support to specialized missions. This task has four subtasks:

- Establish a mission intelligence briefing and debriefing program.
- Conduct intelligence coordination.
- Support Sensitive Site Exploitation.
- Intelligence Support to Personnel Recovery.

2-18. Related missions and operations are described in FM 2-0 in further detail.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION

2-19. *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).

2-20. ISR synchronization ensures the commander's requirements drive ISR operations and 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 available from 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.

2-21. ISR synchronization identifies the best way to satisfy information requirements concerning the operational environment. Commanders use the ISR synchronization process to assess ISR asset reporting and adjust ISR operations. 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.

THE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION PROCESS

2-22. The ISR synchronization process involves six continuous, non-discrete activities, as depicted in figure 2-1. These activities and subordinate steps are not necessarily sequential and often overlap. The ISR synchronization process supports the staff planning and operations processes throughout the full spectrum of operations. The process does not dramatically change with echelon, although organization, terminology, and tools may vary. In the joint environment, for example, there are differences in terminology and procedures which may require adjustments to unit SOPs.

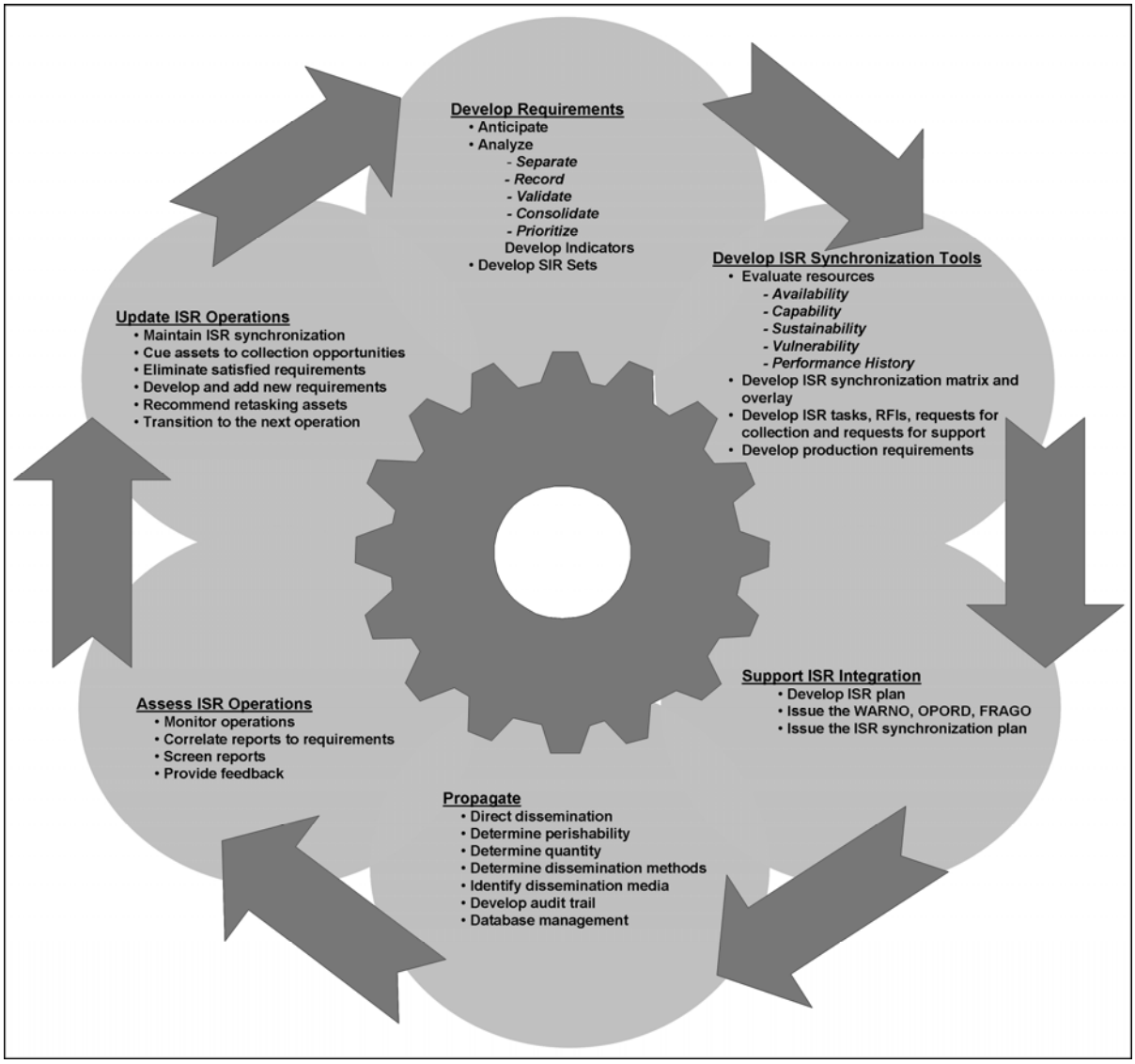

Figure 2-1. Intelligence, surveillance, and reconnaissance synchronization process

2-23. The steps, sub-steps and considerations listed in figure 2-1 are discussed further in chapters 3 and 4 in the context of the MDMP and the operations process. Appendix C describes Joint ISR synchronization considerations.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION ACTIVITIES

2-24. Intelligence officers synchronize the intelligence staff tasks of production and dissemination with the collection tasks for reconnaissance and surveillance assets, resources, and units to maintain their focus on answering the CCIR. ISR synchronization requires the development of the following products and tools used in ISR planning:

- Threat characteristics (to include a complete enemy order of battle).
- Enemy situational templates and course of action statements.
- Enemy event template and matrix.

- High payoff target list.
- Requirements management matrix.
- ISR synchronization matrix.
- ISR overlay.

2-25. Threat characteristics, enemy situational templates, enemy event templates, high payoff target list and the initial collection requirements are all products of IPB developed by the G-2/S-2 staff during the MDMP. The ISR synchronization matrix and overlay are initially developed during mission analysis and are later refined as friendly courses of action are developed and analyzed.

Note: The term "collection management" still exists on Army organizational tables at higher echelons, but the doctrinal actions taken in those sections are the ISR synchronization activities. Collection management is the Joint doctrinal term for what the Army calls ISR synchronization.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION PLANNING CONSIDERATIONS

2-26. When planning, preparing, conducting and assessing ISR operations, the intelligence officer should strive to achieve efficiency and effectiveness. These following actions describe the concerns that intelligence officers must consider to reach the optimal solution for synchronization:

- Anticipate.
- Coordinate.
- Prioritize.
- Balance.
- Control.
- Reach.

2-27. Each of these planning considerations will be discussed in detail in chapter 2.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE INTEGRATION

2-28. *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.

2-29. 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 intelligence officer develops the ISR synchronization tools, which are then integrated with the ISR plan by the operations officer.

2-30. ISR integration is vital in controlling limited ISR assets and resources. 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 3 and 4 for more details on these activities.) The ongoing activities of ISR all contribute to updating the ISR plan.

2-31. The operations officer, with input from the intelligence officer, develops mission taskings based on the SIRs and ISR tasks developed in the ISR synchronization tools (see appendix A for discussion of SIR and ISR tasks). During ISR integration, the intelligence officer satisfies as many information requirements as possible through staff coordination, intelligence reach, and RFIs; then the operations officer 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 CCIRs or other staff information requirements.

2-32. 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.

2-33. 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 ISR plans that use Army, Joint and National resources. Surveillance and reconnaissance assets focus primarily on collecting information about the enemy, terrain and weather and civil considerations aspects of the operational environment to satisfy the Commander's PIR.

THE ROLE OF THE COMMANDER, INTELLIGENCE OFFICER, AND OPERATIONS OFFICER

2-34. In order to understand the role of the commander, the intelligence officer, the operations officer and other staff in ISR synchronization and integration, the reader must first understand how ISR operations support battle command, the commander's situational understanding, and the commander's visualization.

2-35. The commander uses integrating processes and continuing activities to synchronize operations during all operations process activities. ISR is a continuing activity that occurs during all operations process activities. ISR synchronization, together with the intelligence preparation of the battlefield (IPB) and the intelligence running estimate, directly support the commander's visualization and understanding.

BATTLE COMMAND

2-36. *Battle command* is the art and science of understanding, visualizing, describing, directing, leading, and assessing forces to impose the commander's will on a hostile, thinking, and adaptive enemy. Battle command applies leadership to translate decisions into actions—by synchronizing forces and warfighting functions in time, space, and purpose—to accomplish mission (FM 3-0). Command during operations requires understanding the complex, dynamic relationships among friendly forces, enemies, and the environment, including the populace.

2-37. Commanders drive the operations process through battle command. The operations process centers on the commander as they lead the staff and subordinates throughout the operations process. The commander's need for relevant information to support his situational understanding, visualization, and decision making drives the ISR planning process (synchronization and integration). Figure 2-2 illustrates how ISR supports the commander's situational understanding and visualization in battle command.

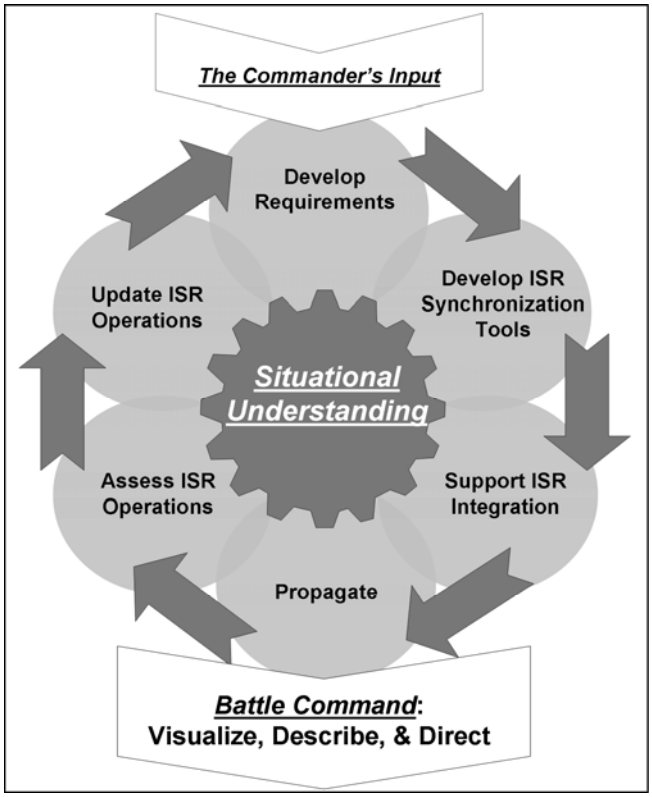

Figure 2-2. ISR supports battle command

SITUATIONAL UNDERSTANDING

2-38. The commander's understanding of the situation is fundamental to battle command. Understanding is knowledge that has been synthesized and had judgment applied to it in a specific situation to comprehend the situation's inner relationships. *Situational understanding* is the product of applying analysis and judgment to relevant information to determine the relationships among the mission variables to facilitate decision-making (FM 3-0). Situational understanding helps commanders visualize and describe the commander's intent and develop focused planning guidance for the staff.

2-39. ISR operations directly support the commander's situational understanding by providing the relevant information and intelligence needed to make informed decisions. Therefore, the commander must be involved with the staff and subordinates throughout the ISR planning process.

COMMANDER'S VISUALIZATION

2-40. *Commander's visualization* is the mental process of developing situational understanding, determining a desired end state, and envisioning the broad sequence of events by which the force will achieve that end state (FM 3-0). Continuous ISR planning (synchronization and integration) supports enhanced battle command and the commander's visualization.

2-41. Intelligence supports the commander's visualization during the full spectrum of operations and helps the commander decide when and where to concentrate sufficient combat power to overwhelm the enemy. ISR is essential for the commander to achieve surprise against the enemy, preclude surprise from the enemy, maintain the initiative on the battlefield, and win battles. Commanders and staffs at all levels

synchronize intelligence with the other warfighting functions to maximize their ability to see and strike the enemy simultaneously throughout the AO.

COMMANDER DRIVES INTELLIGENCE

2-42. Prior to deployment and well before the execution of offensive, defensive, stability, or support operations, the commander and staff require knowledge about the operational environment in order to begin the planning process and create their initial estimates. ISR synchronization is a commander-driven, continuous activity occurring from pre-mission planning through the conduct of operations until completion of operations.

2-43. 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 or satisfying other intelligence requirements for the staff and subordinate commanders. Intelligence acquired by ISR assets, units, and Soldiers facilitates the commander's decision making which drive operations. ISR operations concurrently satisfy the staff's intelligence requirements, support the various staff section running estimates, and enable options for the commander.

THE COMMANDER'S INPUT

2-44. The commander's choice of information requirements drive ISR operations; therefore, the commander is responsible for ISR operations. The commander must ensure PIR are tied directly to the scheme of maneuver and foreseen decisions. The commander should clearly articulate his intent for intelligence operations as well as reconnaissance and surveillance operations.

2-45. 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. The commander must tell the staff *what* information is needed and *when* it is required. Commanders provide this information to staff officers during the various staff planning activities, briefings and meetings that occur during the MDMP and throughout the unit's normal battle rhythm during on-going operations. In order for the ISR plan and intelligence analysis and production effort to be properly focused on the information deemed critical by the commander, the entire staff must work together and completely understand what the commander needs.

The Role of the Commander in ISR Operations

The following list was developed by General William W. Hartzog and used by the Army's Battle Command Training Program (BCTP) when teaching ISR operations concisely details the commander's role in ISR operations:

- To defeat the enemy, you must tell your intelligence officer what you must know and when you must know it.
- You must tell your operations officer that every plan must be coordinated with your intelligence officer.
- You must know what intelligence systems are available to support you and what their capabilities are.
- You and your staff must participate in the IPB process. Do not let your intelligence officer do IPB by himself/herself.
- You must decide who is responsible for controlling your recon effort and assign them the assets and mission.

Additionally, these additional step support successful ISR operations:

- Limit PIR and constantly check to be sure they are being collected on. Ensure your intelligence and operations officer are not diffusing the collection effort. A unit generally will not have enough assets to cover all intelligence gaps.
- Synchronize ISR operations with higher headquarters and make sure subordinate commanders have synchronized their plans with yours.

2-46. The staff uses the commander's input to generate information requirements. Subordinate units and adjacent units also generate information requirements and submit them to adjacent or higher units as requests for information (RFI). Where possible, ISR synchronization satisfies information requirements through intelligence reach and RFIs. When RFIs and intelligence reach do not provide answers to information requirements, the intelligence officer recommends ISR tasks for all assets the commander controls. Figure 2-3 illustrates how the commander's input drives ISR operations.

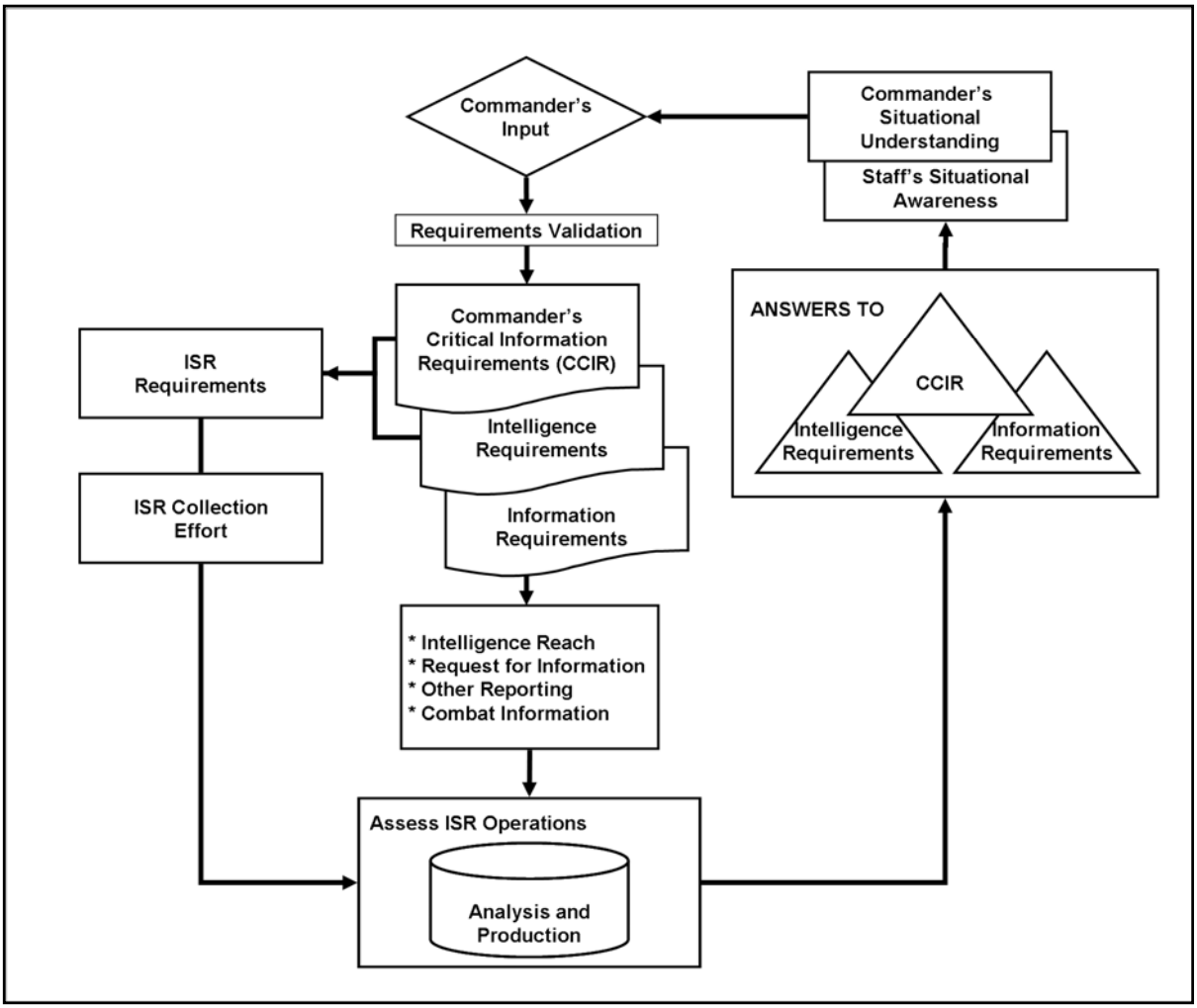

Figure 2-3. The commander's input to ISR operations

THE INTELLIGENCE OFFICER AND THE INTELLIGENCE TEAM

2-47. To execute missions effectively across the full spectrum of operations, the commander requires intelligence about the enemy and other conditions of his area of operations (AO) prior to and during operations. The commander must understand the critical elements of the operational environment that could affect the mission. As stated previously, the operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. This includes the battlefield effects of threat, terrain, weather, and civil considerations. The intelligence officer is the principal staff officer responsible for gathering data and information and turning them into intelligence for the commander.

2-48. The intelligence officer is responsible for aiding how commanders understand current and potential enemies as well as how they organize, equip, recruit, train, employ, and control their forces. The intelligence officer also aids the commander's understanding of the terrain and weather effects upon both friendly and enemy operations.

2-49. The intelligence officer and the G-2/S-2 staff develop the most accurate analysis of enemy disposition and intent possible using information and data gathered through intelligence reach, RFIs, and ISR operations. The intelligence officer must be able to:

- Describe threat characteristics.
- Project where and how the enemy is deployed on the battlefield
- Describe where and how the enemy will maneuver
- Identify high-value and high-payoff targets
- Assist the operations officer in developing and executing an ISR plan that helps the commander develop situational understanding and conduct decisive maneuver to accomplish his objectives.

2-50. Once forces are committed, the intelligence officer must continually assess effects and recommend modifications to the commander's targeting priorities and ISR operations. The intelligence officer is responsible for ensuring that the intelligence warfighting function operates smoothly and efficiently so that the commander receives accurate, timely, and relevant information.

2-51. The intelligence officer is the primary advisor to the commander on ISR synchronization and supports the commander with intelligence analysis and production to create products derived from ISR operations. Intelligence officers perform the following functions during ISR synchronization—

- 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 the associated intelligence analysis and production effort to determine the effectiveness of the ISR effort. Intelligence officers maintain situational awareness in order to identify gaps in coverage and to identify the need to cue additional resources or recommend redirecting ISR assets to the operations officer.
- Update the ISR synchronization tools as requirements are satisfied, modified, or created. Intelligence officers remove satisfied requirements and recommend new requirements as necessary.
- In coordination with operations staff, monitor and assess satisfactory completion of ISR tasks assigned by higher headquarters. Operations officers integrate the updated synchronization plan into orders tasking ISR assets, systems, units, and Soldiers.

2-52. The intelligence team, comprised of all intelligence personnel within the command and supporting the command, aids the intelligence officer.

THE OPERATIONS OFFICER

2-53. The operations officer is responsible for assigning and controlling ISR assets in terms of time, space, and purpose to collect and report information as a concerted and integrated portion of the operation. The ISR integration task ensures assignment of the appropriate ISR tasks to assets through a deliberate effort supported by the intelligence officer and the entire staff across all warfighting functions. In other words, the operations officer is responsible for "troops to task" including the ISR assets and resources made available by higher headquarters.

2-54. ISR synchronization and integration is a focused team effort to answer the commander's requirements. The operations officer, with input from the intelligence officer, translates tasks developed during ISR synchronization for specific information requirements into orders. The operations officer assigns tasks based on latest time/event that information is of value and the capabilities and limitations of available ISR assets and resources. The intelligence officer assists the operations officer in ensuring intelligence requirements are identified, prioritized, and validated so that the operations officer creates an ISR plan that is synchronized and integrated within the overall operation.

2-55. ISR integration is vital in controlling limited ISR assets against numerous tasks. The intelligence officer helps the operations officer coordinate for and integrate ISR resources from higher echelons. The

operations officer works with the intelligence officer by developing orders based on the ISR synchronization tools, monitoring the current situation to predict changes to the enemy situation, and by implementing recommended changes to the ISR plan. All changes made to the ISR plan subsequent to the first order are approved by the operations officer and issued in a FRAGO. Dynamic re-tasking and ad-hoc mission changes that may occur so quickly, they may be issued by the operations officer under verbal orders from the commander. During regular operations updates, the intelligence officer assists the operations officer in briefing the status of ISR operations.

ISR WORKING GROUPS

2-56. At division and higher echelons, there are intelligence duty positions which are responsible for ISR planning and operations. At battalion and brigade, there are no specific duty positions for ISR planning other than the S-2 and staff. Depending on the availability of personnel, the commander may choose to designate an ISR working group. The primary staff officers' (G-2/S-2 and G-3/S-3) responsibilities, however, cannot be delegated and they should direct and manage the efforts of this working group to achieve a fully synchronized and integrated ISR plan.

2-57. Unit SOP, battle rhythm and operational tempo will determine how frequently an ISR working group needs to meet. This working group should be closely aligned with both the current operations and future operations (or plans) sections to ensure ISR synchronization tools are properly integrated into the overall operational plan and they are nested in the concepts for future plans. Further discussion on working groups can be found in Chapter 4.

SOLDIER SURVEILLANCE AND RECONNAISSANCE

2-58. ISR planners must consider Soldier surveillance and reconnaissance. Unit leadership must train Soldiers and foster an environment that encourages small-unit and individual-Soldier reporting. While conducting operations, Soldiers must know the CCIRs, so that they can be actively observing for relevant information or conditions that could contribute to answering a CCIR. Soldiers must be competent in reporting their experience, perceptions, and judgments concisely and accurately. Even when not specifically tasked to conduct surveillance or reconnaissance missions, all Soldiers report their observations through the chain of command.

2-59. 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 ISR. Commanders and staff must ensure the information collected by Soldiers within their AOs is integrated into the overall intelligence warfighting function in order to yield more detailed and accurate intelligence.

2-60. As Soldiers learn to report relevant information regularly, battalion and brigade intelligence staffs can quickly become overwhelmed with information during certain types of operations if they are 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.

2-61. 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 support operations adequately. At the company level, some commanders have opted to form company intelligence support teams (CIST) 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.

2-62. For more information, see FM 2-91.6 Soldier Surveillance and Reconnaissance.

Chapter 3

Intelligence Support to the Planning Process

To plan ISR operations effectively, it is important to appreciate the fundamentals of planning and how the intelligence warfighting function supports the planning process. This chapter will discuss the actions intelligence officers take during the plan and prepare phases of the operations process. It includes a step-by-step analysis of the ISR synchronization contribution to the military decision making process (MDMP) including the specific products and deliverables that intelligence officers must prepare and use.

GENERAL

3-1. ISR synchronization planning is a fundamental part of doctrinal command and control procedures and planning processes. It should also be closely linked to the intelligence preparation of the battlefield (IPB) prepared by the intelligence section during the MDMP. The ISR collection and intelligence analytical efforts are complimentary and should be carefully synchronized and integrated to afford the commander the best possible intelligence support for his information needs.

THE PLANNING PROCESS

3-2. Planning is inherent to command. Planning is the process by which commanders (and the staff, if available) translate the commander's visualization into a specific course of action for preparation and execution, focusing on the expected results (FM 3-0). It involves understanding the situation, envisioning a desired future, and arranging a configuration of potential actions in time, space, and purpose to realize an end state.

3-3. A plan is a design for future operations. A plan should guide subordinates through execution. Commanders issue plans to communicate a visualization of an operation, to state their intent, to articulate decisions, and to describe the end state that leads to a shared vision throughout the command.

3-4. Planning does not stop with an order. During the preparation and execution phases of the operations process, plans are continuously refined based on the assessed progress of the operation and new information as it emerges. Planning is conducted for both short- and long-range time horizons. The ISR synchronization involves both short-range planning for certain assets like UAS and longer term planning for assets such as HUMINT units.

3-5. Planning orients the commander and staff on available options and familiarizes the commander with the conditions surrounding the operation. Planning and plans help—

- Build situational understanding and reduces uncertainty.
- Prioritize effort.
- Direct, coordinate, and synchronize action.
- Anticipate events and adapt to changing circumstances.

3-6. Planning should provide the basis for unity of effort while leaving enough room for the exercise of initiative during execution. Commanders use plans to designate task-organization, the main effort and the priority of support. In ISR planning, intelligence and operations officers consider these same factors to

apportion ISR resources to lower echelons, to prioritize requests for support and to designate when ISR priorities might change during an operation.

THE TIME ELEMENT IN PLANNING INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

3-7. Time is a critical factor in operations and even more critical when considering that ISR operations are some of the first events that must be decided and set into motion during the planning process. In addition, ISR operations must be timely in order to deliver timely and relevant information to the commander. Effective execution of operations requires issuing plans in a timely manner to subordinates. This makes planning ISR operations the most time sensitive aspect of the MDMP.

3-8. In ISR synchronization planning, the intelligence officer must contemplate the time it takes to ISR resources and assets to collect information and then for the organization's analytical element to process, analyze, and disseminate intelligence information. The intelligence officer should calculate the total time from beginning to end in order to synchronize the collection effort realistically.

3-9. Every ISR asset or resource will have a different planning timeline depending on its specific operational characteristics, time-related limitations, and planning factors. Figure 3-1 depicts the ISR planning timeline that intelligence officers use to backwards plan to achieve ISR synchronization.

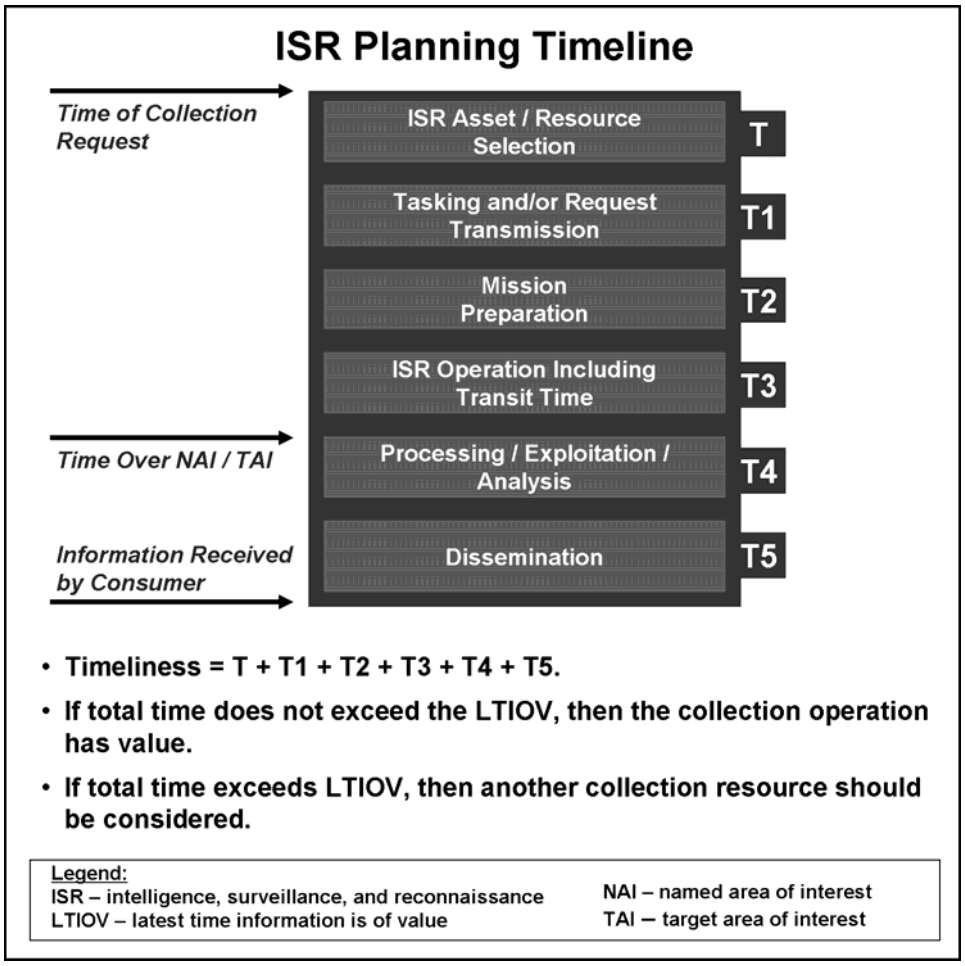

Figure 3-1. The ISR planning timeline

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE PLANNING CONSIDERATIONS

3-10. When planning, preparing, conducting and assessing ISR operations, the intelligence officer must consider the following concerns in order to reach the optimal solution for synchronization:

- **Anticipate**. The intelligence officer 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 the decision-making, planning, and operations processes, intelligence officers can best anticipate requirements.
- **Coordinate**. The intelligence staff must coordinate and collaborate with all staff sections and with both higher headquarters, subordinate, and adjacent units in order for ISR operations to be synchronized continuously. The intelligence staff must be engaged in the unit's planning and orders production activities to ensure early identification of intelligence requirements. The intelligence staff must also be integrated into the combat information reporting and battle tracking of current operations to anticipate the need for dynamic or ad-hoc ISR taskings. Early and continuous consideration of ISR planning 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**. The priority for ISR operations begins with the CCIR. Then intelligence officers prioritize each validated intelligence requirement based upon its importance in supporting the commander's intent and decisions as well as the current situation so that low-density/high-demand ISR assets and resources are directed against the most critical requirements.
- **Balance**. Balance involves using a combination of redundancy, mix and cueing of a variety of ISR capabilities to complement each other. *Redundancy* is using several same-type ISR assets to cover the same NAI. *Mix* means planning for complementary coverage by a combination of assets from multiple units and intelligence disciplines designed to increase the probability of collection success and reduce the chances of successful threat deception. Cueing involves the use of one or more sensor to provide data that result in another system to conducting collection. *Balance* also means that the intelligence staff should resist favoring or becoming too reliant on one particular unit, discipline, or system. Balance is simply achieving maximum efficiency using an appropriate mix of disciplines, ISR assets and resources to satisfy as many competing intelligence requirements as possible.
- **Control**. Units should first use organic and allocated ISR assets to ensure timely and effective collection as well as overall synchronization. These assets are more responsive to the commander's needs and can be balanced with other resources. ISR assets belonging other units, agencies, or organizations may have limited availability and are likely to receive differing priorities from their respective commanders. Information gathered by other ISR resources is harder to verify and correlate with information collected by organic assets.
- **Reach**. Units can use intelligence reach and RFIs to answer initial information requirements without having to use precious ISR assets. Intelligence, which is confirmed by more than one intelligence discipline, is generally preferred over single-source reporting. Therefore, a unit should not depend solely on intelligence reach to satisfy a PIR.

ESSENTIAL STEPS FOR INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE PLANNING

INTELLIGENCE SURVEY

3-11. The intelligence survey provides the intelligence officer with an initial assessment for recommending intelligence asset apportionment within the AO and how best to use the unit's intelligence assets within the AO. The survey is developed over time from initial planning through mission execution and is updated

continuously. It takes into account technical and tactical considerations across all intelligence disciplines. For example, one portion of the AO may be unsuited for unit SIGINT asset collection due to terrain or lack of threat transmitters, but it may be well suited for HUMINT collection teams (HCTs). The intelligence officer may recommend to the commander that unit SIGINT collection assets not be deployed to that area, but that additional HCTs would be a valuable source of intelligence collection in that same area.

3-12. The intelligence survey consists of four steps:

- Developing a comprehensive baseline database for the AO.
- Determining key intelligence gaps.
- Developing an understanding of the information and intelligence that can be collected with unit intelligence assets and, when appropriate, ISR assets in the AO and how and where it may best be collected.
- Determining a method of understanding when changes to the baseline occur that are of intelligence interest.

3-13. Using the intelligence survey, intelligence officers determine what their communications needs for deployed intelligence operations. The survey is the basis for determining what additional or specialized intelligence assets the unit may require for mission accomplishment. Based on the assessment in the survey, intelligence officers submit requests for support to obtain additional ISR asset support or requests for forces (RFF) to obtain additional ISR assets, resources units or Soldiers.

3-14. The intelligence survey is the first tool used by the intelligence officer while conducting ISR synchronization during the MDMP process.

REQUIREMENTS MANAGEMENT

3-15. Based on the initial assessment of intelligence gaps made in the intelligence survey, the commander and staff begin considering requirements for intelligence reach, requests for information and ISR operations.

3-16. *Information requirements* are all information elements the commander and staff require to conduct operations successfully; that is, all elements necessary to address METT-TC (FM 6-0).

- *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.
- *Commander's critical information requirements (CCIR)* are information requirements identified by the commander as being critical to facilitating timely decision-making. The two key elements are friendly force information requirements and priority intelligence requirements (JP 3-0). A CCIR directly influences decision-making and facilitates the successful execution of military operations. Commanders decide whether to designate an information requirement as a CCIR based on likely decisions and their visualization of the course of the operation. A CCIR may support one or more decisions. The list of CCIRs constantly changes as commanders add and delete individual requirements throughout an operation based on the information needed for specific decisions. CCIR protect subordinate headquarters from receiving excessive requests for information. For more information on how CCIR are developed into requirements for ISR operations, see Appendix A.
- *Friendly force information requirements (FFIRs)* are 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, 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.

3-17. 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 intelligence-drive operations. The staff also develops the FFIRs, which provide the information that the commander and staff need about the forces available for the operation.

3-18. The goal of ISR operations is to satisfy the CCIRs. 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.

3-19. 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.

3-20. A detailed discussion on developing requirements can be found in Appendix A.

REQUESTS FOR INFORMATION (RFI)

3-21. A *request for information (RFI)* is any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the combatant command's procedures (JP 2-0). **For the purposes of Army ISR operations, an RFI is used to determine if another entity has already collected the information needed. When information requirements cannot be answered through organic ISR operations, intelligence reach or combat information reporting, units request information by sending an RFI to higher, lower, or adjacent units using the RFI procedures prescribed by Standing Operating Procedures (SOP).**

3-22. If the information already exists, the RFI will be returned with an answer. If the information does not exist, higher echelons return the RFI with a negative response.

3-23. Units establish RFI procedures to provide a systematic method for requestors to obtain information from higher, lower and adjacent units. This procedure should provide visibility to the rest of the organization on the questions and the answers received. Procedures for and management of RFIs is determined by unit SOP. The G-2 staff should monitor and track these intelligence RFIs in concert with the command's RFI manager.

3-24. When the ISR planning process identifies an intelligence requirement that cannot be answered through the RFI process, by the current ISR collection effort, tasked to a subordinate unit (if the means to collect it resides at a lower echelon), or answered through intelligence reach, then a request for collection is generated. Requests for collection by subordinate units are sent as tasks to subordinate units through the orders process.

REQUESTS FOR COLLECTION

3-25. Requests for collection are those ISR collection requirements that can only be answered by ISR resources controlled, apportioned, allocated and/or tasked at higher echelons. Depending on the organization of higher echelon headquarters, the request may be submitted through Army systems, such as the ISR Synchronization Tool (IST) (see Appendix D for more information on IST). At higher echelon units, requests for collection are typically submitted through joint and national level requirements systems such as Collection Management Mission Applications (CMMA) and Requirements Management System (RMS). For more discussion on Joint, National and Multinational ISR synchronization considerations, see appendix C.

3-26. A request for collection to a subordinate unit is actually an ISR task that can be specified through the ISR synchronization and integration processes and issued as part of tasks to subordinate units and the ISR plan.

3-27. A request for collection should not specify a particular collection system (unless that system has a unique capability that is not available on another system). Instead, it should specify a required capability such as full-motion video (FMV), imagery, MASINT, radar imaging, etc. The ISR planners at higher echelons know the capabilities and limitations of every system available to them and they will assign the requests to a collection system according to priority of effort, availability, capability, and capacity.

3-28. Requests for collection should include detailed instructions on where to collect, when to collect and what essential elements of information the requestor is looking for (see the discussion on indicators and SIRs in Appendix A). These details permit the collector, mission manager, or mission commander to collect with precision and efficiency, increasing the likelihood that the data or product returned to the requestor will answer their information requirement.

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

3-29. ISR planning is embedded in the MDMP and depends extensively on a thorough intelligence preparation of the battlefield process (IPB). While synchronization is a continuous process, ISR synchronization starts with receipt of the mission (which could be merely a warning order).

3-30. ISR synchronization directly supports the development of intelligence and operations products used throughout the decision making process. At each step in the MDMP, the intelligence officer must prepare certain products that are used in the plan and prepare phases of the operations process.

3-31. ISR synchronization and integration activities are continuous, collaborative and interactive. Several of the outputs from the various MDMP steps require the intelligence officer and operations officer to collaborate. The ISR plan cannot be developed without constant coordination between the intelligence and operations and among the entire staff. At every step in the MDMP, the intelligence officer must rely on input from the staff and cooperation with the operations officer in order to develop ISR products that support the commander's intent and maximize ISR efficiency for each course of action being considered.

3-32. The MDMP is detailed, deliberate, sequential, and time-consuming. When decision-making occurs during the execution of a mission, planning is typically constrained by time and an order already exists, therefore commanders use the rapid decision-making process (RDSP). ISR synchronization during on-going operations appears in chapter 4.

3-33. Figure 3-2 lists the MDMP steps and the corresponding ISR-specific outputs that intelligence officers are involved in or directly prepare during the planning process.

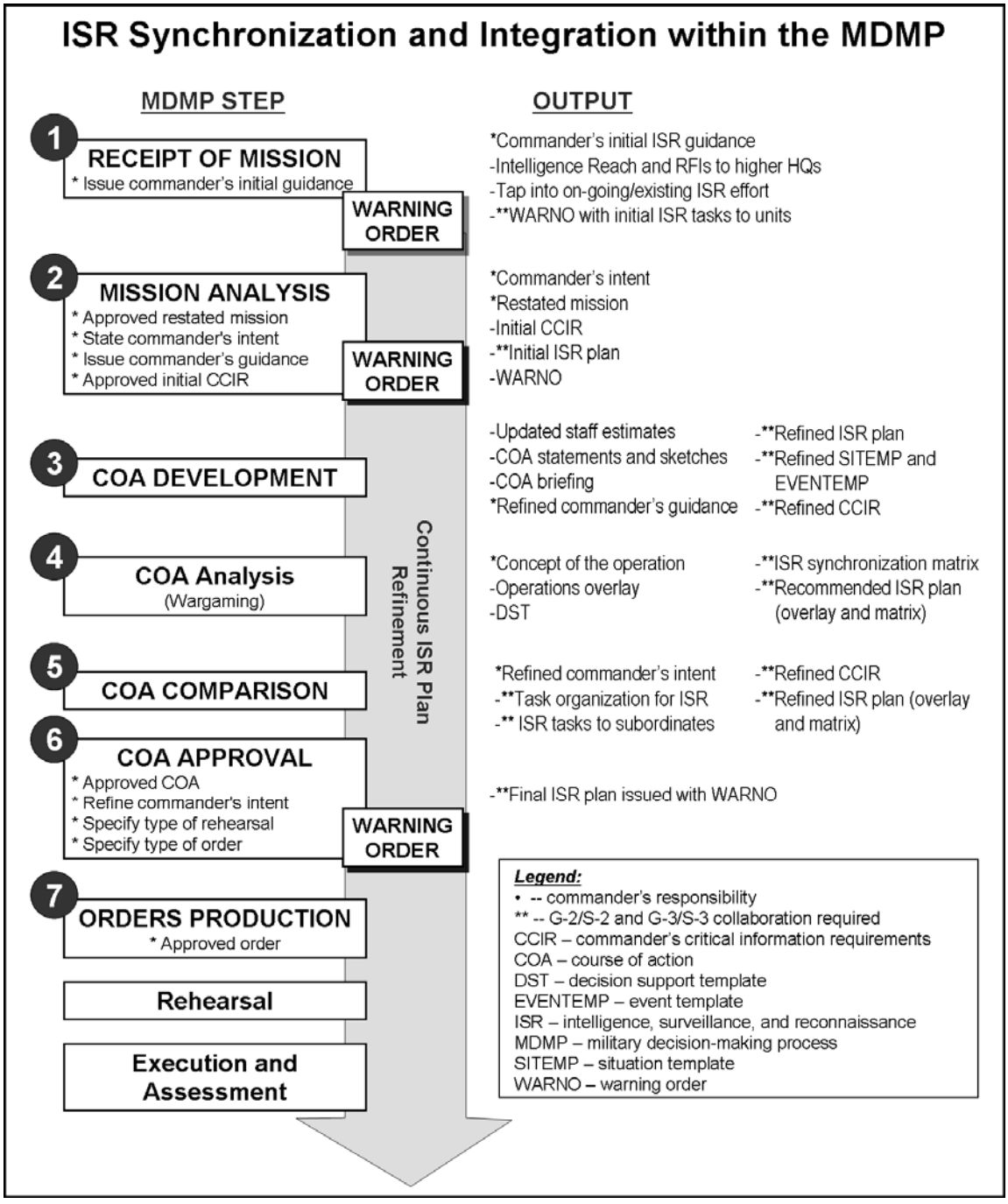

Figure 3-2. ISR synchronization and integration within the MDMP

RECEIPT OF MISSION

3-34. When a mission is received, the commander and staff shift their efforts to describing the operational environment using the METT-TC mission variables (depending on echelon) and begin preparations for

MDMP. The commander provides his initial ISR guidance to the staff that is used to generate the initial ISR tasks to units and will be transmitted as part of the first WARNO.

3-35. Prior to receipt of the mission, the G-2/S-2 staff has been generating intelligence knowledge in anticipation of the mission. In addition, the knowledge already available, the G-2/S-2 use intelligence reach and RFIs to higher headquarters to begin filling in the information gaps in the initial intelligence estimate. The intelligence officer should identify and tap into any on-going or existing ISR collection effort that may offer relevant information to fill gaps. For more information on generating intelligence knowledge, see FM 2-0.

3-36. During this step of the MDMP, the G-2/S-2 staff must gather the tools needed for the MDMP, begin the intelligence estimate, and perform an initial assessment of the time available versus the time allotted to subordinate ISR elements for planning, preparation and execution. Since surveillance and reconnaissance units, assets and resources are required as early as possible, they require earlier notification and must have sufficient preparation time to begin sending information that the commander needs. See the discussion on ISR timeliness at the beginning of this chapter and figure 3-1 on the ISR planning timeline for more details.

3-37. The intelligence officer should get access to reporting from whatever on-going ISR effort may already be in progress, whether it is being conducted by units already in place, higher echelons, or by national-level agencies. Chances are a Department of Defense organization is already looking at the operational environment and has accumulated information that will be of value to the MDMP and the commander's information requirements.

3-38. The operations and intelligence officers must agree on the initial ISR tasks to units and an initial ISR concept or focus. Then they must allocate sufficient time for those assets to plan, prepare and execute. The initial ISR tasks may be detailed and complex or they may be rather simple and temporary plans until the ISR effort is refined during the MDMP.

3-39. The ISR outputs from this MDMP step are:

- The commander's initial ISR guidance.
- Intelligence reach tasks for the analytical staff.
- ISR RFIs to higher headquarters.
- WARNO #1 with initial ISR tasks.

MISSION ANALYSIS

3-40. When mission analysis begins, the intelligence officer should have the higher headquarters' plan or order and available IPB products. The staff adds their updated estimates to the process also. The initial ISR tasks issued with WARNO #1 may begin to yield information that should be analyzed and evaluated for relevance to mission analysis. The commander provides his initial guidance, which the staff uses to capture the commander's intent and develop the restated the mission.

Step 1. Analyze the Higher Headquarters Order

3-41. During mission analysis, the G-2/S-2 staff analyzes the higher headquarters to extract ISR tasks and constraints such as limits of reconnaissance (LOR). The order will also contain details on availability of ISR resources from higher echelons and how much of those resources will be allocated to the unit. For example, a higher headquarters order might contain several full motion video (FMV) resources that are apportioned by the priority of effort or support designated in the ISR Annex.

Step 2. Perform Intelligence Preparation of the Battlefield

3-42. IPB is the most important prerequisite to ISR planning. During IPB, several key products are developed which aid ISR planning. Those products include:

- Threat characteristics.

- Enemy situational templates and course of action statements.
- Enemy event template and matrix.
- High-payoff target list.
- Updated intelligence estimate including identified information gaps.

3-43. These products aid the intelligence officer in:

- Identification of information gaps that can be answered by existing ISR operations, intelligence reach and RFIs to higher echelons. The remaining information gaps are used to develop requirements for ISR operations.
- Threat considerations that may affect ISR planning.
- Terrain effects that may benefit, constrain, or limit the capabilities of ISR assets and resources.
- Weather effects that may benefit, constrain, or negatively influence the capabilities of ISR assets and resources.
- Civil considerations that might affect ISR planning.

Note: When considering terrain effects, ISR planners can use the military topography team to develop line of sight products.

3-44. As the staff completes mission analysis and finalizes the initial IPB products, the intelligence officer and G-2/S-2 staff should have developed the initial collection requirements. These collection requirements are be the basis of both the initial ISR plan, requests for collection, and RFIs to higher and lateral units conducting ISR operations. By this time, intelligence gaps are identified and ISR planners have an initial strategy on how to answer those gaps. Additionally, the operations officer and the remainder of the staff should have a thorough understanding of the unit missions, tasks and purposes.

3-45. The IPB process continues through mission execution in the sense that IPB products are continuously updated and refined as the mission evolves.

3-46. Refer to FM 2-01.3 and FMI 2-01.301 for more specific information on IPB.

Step 3. Determine Specified, Implied, and Essential Tasks

3-47. The intelligence officer must also identify specified, implied, and essential ISR tasks. Specified tasks can be directed toward subordinate units, systems, sensors, and Soldiers. Specified tasks for resources from higher headquarters should be built into the requirements developed using the techniques in Appendix A. It is important not to forget the implied tasks because those tasks may determine how a system or sensor is set up for collection.

Step 4. Review Available Assets

3-48. In addition, the intelligence officer must review all available assets and resources, effectively creating an inventory of capabilities to be applied against collection requirements. Building the inventory of assets and resources begins with Annexes A and L of the higher headquarters order. The intelligence officer takes those assets attached or OPCON to the unit and adds those resources available from higher echelons by request and those belonging to adjacent units that might be of assistance. The higher headquarters order should specify beddown locations and air tasking order (ATO) details for airborne assets that will be needed later in course of action (COA) development.

Step 5. Determine Constraints

3-49. During the determine constraints step of mission analysis, the intelligence officer must consider legal, political, operational and rules of engagement constraints which might constrain ISR operations.

Limits of reconnaissance, earliest time information is of value and not earlier than times are examples of planning constraints that must be considered by the intelligence officer.

3-50. In some cases, the commander may impose constraints on the use of certain systems or assets. In addition, the intelligence officer must consider the system-specific constraints such as operating, weather, and crew rest or maintenance cycle limitations.

Step 6. Identify Critical Facts and Assumptions

3-51. During this step, the intelligence officer must identify critical facts and assumptions pertinent to ISR planning which will be used later in COA development. For example, a critical fact might be that imagery requests may take 72 to 96 hours to fulfill or the human intelligence (HUMINT) effort requires a significant amount of time before a good source network is fully developed.

3-52. Critical assumptions for planning ISR include the availability and responsiveness of organic assets and ISR resources from higher echelons. For example, the intelligence officer might use a certain percentage (representing hours) of UAS support available on a daily basis weather and maintenance permitting.

Step7. Perform Risk Assessment

3-53. When performing a risk assessment, the intelligence officer must consider the asset's effectiveness versus the force protection or security risk to the asset. For example, placing a sensor forward enough on the battlefield that it will be able to return valuable data and information may put the asset at high risk of being compromised, captured or destroyed. The calculus of payoff versus loss will always be determined by METT-TC and the commander's decision.

3-54. In some cases, friendly forces may reveal a collection capability by taking certain actions. If it is important to keep a collection capability concealed, then intelligence officers gives careful consideration to every lethal or non-lethal action being contemplated based on intelligence derived from that capability.

Step 8. Determine Initial Commander's Critical Information Requirements and Essential Elements of Friendly Information

3-55. This is the second most important prerequisite for ISR planning. During MDMP, the staff refines the list of information requirements that are derived from the initial analysis of information available and from intelligence gaps identified during IPB. This list is based upon higher headquarters tasks, commander's guidance, staff assessments, and subordinate and adjacent unit RFIs.

3-56. The staff then nominates these requirements to the commander to be CCIR and EEFI. The commander alone decides what information is critical, based on his experience, the mission, the higher commander's intent, and input from the staff.

3-57. CCIR are the primary focus for ISR operations. Developing requirements includes the following steps: anticipate, analyze, develop indicators, and develop SIRs. Appendix A provides a detailed discussion on the development of requirements for ISR collection.

Step 9. Determine the Initial Intelligence, Surveillance, and Reconnaissance Plan

3-58. ISR assets are tasked by the operations officer and resources requested by the intelligence officer as soon as possible in the mission analysis step of the MDMP. This is especially true for organic reconnaissance and surveillance units who need time to plan and prepare their operations.

3-59. The operations officer is responsible for the ISR plan, however, the intelligence officer and G-2/S-2 staff must create the ISR synchronization tools first. During this step of mission analysis, it is important that the operations and intelligence officers work very closely together to ensure ISR operations are

synchronization and integrated fully into the overall plan. Figure 3-3 lists the steps that the intelligence officer follows during the development of the initial ISR plan.

Figure 3-3. Develop intelligence, surveillance, and reconnaissance synchronization tools

3-60. At this point in the MDMP, the initial ISR plan has to be generic because friendly courses of action have not been developed. The basis for the plan is the commander's initial ISR guidance, the primary information gaps identified by the staff during mission analysis, and the enemy SITEMP developed during IPB.

3-61. The operations officer issues the initial ISR plan as a WARNO or a fragmentary order (FRAGO). Later, as the plan is refined and finalized, it should be issued as Annex L to the OPORD.

3-62. In order to create the initial ISR plan, the intelligence officer, operations officer, and staff must go through several important activities, several steps, and considerations to achieve a fully synchronized, efficient and effective plan. A portion of the ISR synchronization proce`ss is described below as it would occur during the MDMP, but it is also applicable to RDSP and updating ISR operations during the execution and assessment phases of the operations process.

Evaluate Resources

3-63. The intelligence officer and staff take the prioritized initial 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 and resources. Theater and Joint echelons will apportion ISR resources to subordinate echelons. Corps and divisions will allocate support from the apportioned amount they receive to BCTs and below. The intelligence officer must understand the system of apportionment and allocation to determine what is available and what can be requested by analyzing the higher headquarters order and reviewing the various scheduling or tracking mechanisms.

Note: Human intelligence (HUMINT) collectors some of the best sensors for counterinsurgency and stability operations when they are properly focused by detailed collection requirements and supported by all-source analysis. However, HUMINT source operations take time to establish operations and cultivate sources. When considered during the ISR planning, remember that HUMINT collection availability and responsiveness is linked to geographic access, support relationships, force protection restrictions, and workload. The G-2X/S-2X work for the G-2/S-2 and are the focal point for planning and managing HUMINT operations. For more information on synchronizing HUMINT operations, refer to FM 2-22.3 and TC 2-22.303.

- **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 that 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 that 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.

3-64. 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 Surveillance Target Attack Radar System (JTARS), 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.

3-65. 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.
  - Battlefield Surveillance Brigade units.
  - MI elements to include all HUMINT, geospatial intelligence, SIGINT, imagery intelligence (IMINT), measurement and signature intelligence (MASINT), and counterintelligence (CI) assets.
  - UAS platoons.
  - Fires target acquisition sections.
  - Long-range surveillance units.
  - Chemical defense units.
  - 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 engineers.
  - Infantry battalions.
  - Military police (combat MP).
  - Logistical convoys (during the course of their normal movements).
- **Additional Capabilities**. Those units that are not tasked with a surveillance and/or reconnaissance mission but can 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 meeting with host nation leaders (information engagements).
  - 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 that can be useful in answering the CCIR.
  - 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.

3-66. Other assets that collect information to satisfy intelligence requirements include national, joint, and multinational resources available through requests for collection and requests for support.

Develop Intelligence, Surveillance, and Reconnaissance, Synchronization Tools (Matrices and Overlays)

3-67. Intelligence officers begin ISR synchronization planning by establishing blank timelines for each asset and resource. The ISR synchronization matrix is a compilation of these timelines for ISR assets, resources, units, and sensors along with requirements details (indicators, SIRs, and ISR tasks).

3-68. Intelligence officers capture the latest time information of value (LTIOV) for each ISR task on the matrix. LTIOV is predicated on the ISR planning timeline (see figure 3-1). This ties the collection effort to the commander's decisions and information requirements. 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 decision support template (DST) using the ISR planning timeline. The relationship between the ISR planning timeline, the collection effort, and the decision point must be tested later during the COA analysis (wargaming) step of the MDMP.

3-69. 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. Figure 3-4 provides examples of the evolution of an ISR timeline for a single asset or resource.

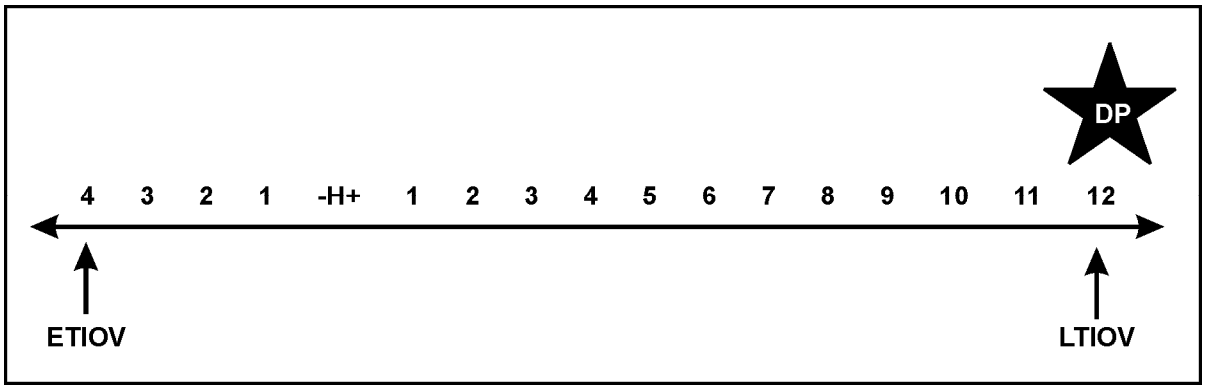

Figure 3-4. Working timeline for a single ISR asset or resource

3-70. The operations and intelligence staffs should resist favoring or becoming too reliant on a particular unit, discipline, or system when recommending to the G-3/S-3 how to employ 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 matrix 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 using redundancy.
- **Mix** means planning for complementary coverage by a combination of assets from multiple units and intelligence disciplines. 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.

- **Cueing** 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.

3-71. Figure 3-5 illustrates how a redundancy, mix and cueing work together as part of an ISR collection combining several working timelines for a single NAI in a conventional combat operation. Stability operations and other types of operations may or may not require the same redundancy, mix and cueing.

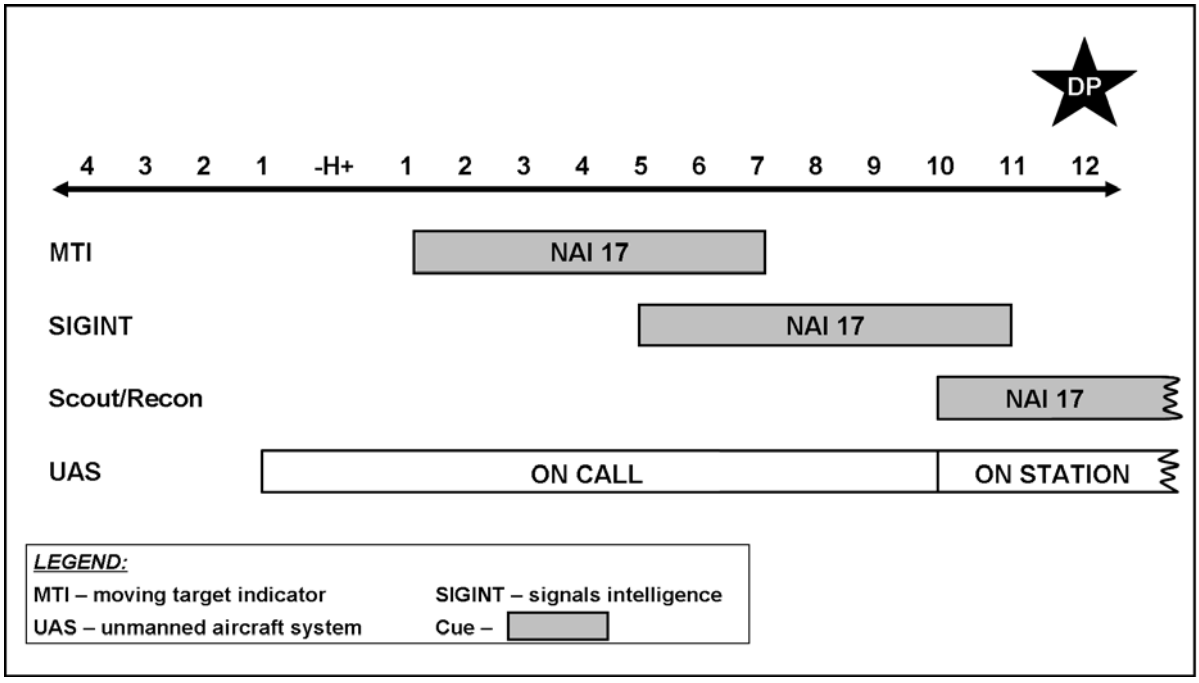

Figure 3-5. Example of redundancy, cueing, and mix for a single NAI

3-72. If JSTARS reports the absence of activity, the intelligence officer might recommend to the operations officer redirecting the UAS to another mission or use it to confirm the absence of activity, depending on the relative priority of requirements and the criticality of the decision point associated with this NAI. If JSTARS reports significant activity earlier than anticipated, the UAS launch sequence and deployment of other collectors can be accelerated to collect data and information relevant to the commander's decision. The results of this effort illustrated in Figure 3-5 might be that the decision point moves to the left on the timeline if enemy activity dictates an earlier decision.

3-73. Cueing can also occur dynamically (outside the ISR 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. Displaying all the potential asset information in an initial ISR matrix allows intelligence officers to ensure visually all assets and all NAIs are covered for collection.

3-74. Intelligence officers maintain situational awareness on all ISR operations to identify gaps in coverage and to anticipate the need to redirect the tasking of assets. The G-2/S-2 staff manages commander's PIR, requests from subordinate and lateral organizations, and tasks from higher headquarters,

which are integrated into the ISR plan by the operations officer. Requirements needed for COA development and analysis can be developed in a simple matrix as shown in Table 3-1.

Table 3-1. Sample requirements management matrix

CCIR, PIR or other intelligence requirements	*SIR*			*LTIOV*	*Assets*	*Reporting*	*Action Required*	*Action Taken*
	Indicators	*EEI*	*NAI*					
INSTRUCTIONS								
List CCIR, PIR or other requirement. Leave enough space for each to have several indicators and SIR in columns 2 and 3	List all indicators that will satisfy each item in column 1	These essential elements of info which form the basis for the ISR Task	No.	Time or Event specific	Prioritize assets by priority of effort or support against items in column 1	Include established communication requirements, reporting methods, formats, and report precedence	Examples: -Retasking -Update ISR plan -Call for Fire -Inform G-2 or S-2 -Cue another asset -Report in INTSUM	Record outcome of action taken and status of requirement

Note. Joint collection management terminology uses essential elements of information (EEIs) in a fashion similar to the Army's use of SIR. The key to writing good ISR tasks is to be sure that all the "essential elements of information" are included in a directive statement that becomes the ISR task in the ISR plan and subsequent order or FRAGO.

Develop Intelligence, Surveillance, and Reconnaissance Tasks, Requests for Information, and Requests for Collection or Support.

3-75. Intelligence and operations officers must work together to develop and assign ISR tasks. Organic ISR assets should be used first, as they are typically more responsive to the commander. Resources available to the unit are used next with the understanding that allocations, attachments, and OPCON relationships can change in the course of an operation due to changes in the higher commander's priorities. These tasks will be published in annex L and the tasks to subordinate units section of the OPORD or FRAGO.

3-76. The intelligence and operations officers can easily translate a well-written SIR into an effective ISR task by making a directive statement (inquisitive statements are less specific). Tailor the reporting criteria to the capabilities of the tasked ISR asset. For example:

- **SIR**: Will more than 20 Mahdi Army insurgents 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.

3-77. 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. Planners should allow ISR assets the latitude to provide information you and the analysts had not anticipated.

3-78. 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.

3-79. 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.

3-80. Submitting an RFI to the next higher or lateral echelon is the normal procedure for obtaining intelligence information not available with organic 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.

3-81. 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.

3-82. Throughout the RFI process units must apprise the submitting organization on the status of their RFI as either 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 and Synchronize Production Requirements

3-83. Intelligence officers coordinate and plan intelligence analysis and production activities to provide timely and relevant intelligence products to commanders, staff, and subordinate forces. The ISR synchronization matrix should be used as one basis for planning and scheduling the analytical and production activities and timelines. The unit's battle rhythm is also used as a basis for determining the daily/weekly/monthly analytical products. The intelligence officer then designs an analytical and production effort to answer the CCIRs and meet the commander's need for situational understanding and the staff's need for situational awareness.

3-84. Intelligence production includes analyzing information and intelligence and presenting intelligence products, assessments, conclusions, or projections regarding the AO and threat forces in a format that aids the commander in achieving situational understanding. The remainder of the analytical effort should be devoted to processing, analyzing and disseminating ISR data and information.

3-85. Production occurs in the intelligence section or separate analysis element, such as an ACE at every echelon from the tactical to ASCC. At the company level, some commanders may choose to form a company intelligence support team (CIST) to process information and produce intelligence.

3-86. 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.

3-87. Success of the analytical and production effort is measured by commanders' and staffs' satisfaction with the products provided and the ability to answer or satisfy the CCIR, intelligence requirements, and information requirements.

COURSE OF ACTION DEVELOPMENT

3-88. Returning to the MDMP steps, the next event is course of action development. Using the IPB products and the enemy SITEMP, the intelligence officer and staff must identify an ISR COA for each friendly force COA. In many cases, the ISR COAs will be very similar to each other depending on the characteristics of the friendly force COAs.

3-89. The next time the operations and intelligence officers must collaborate on the aspects of ISR is during step four of COA development, "develop the scheme of maneuver". Here the staff works to integrate its available resources into an integrated plan. For the intelligence officer, the focus is on the relationship of ISR assets to other friendly forces, the terrain and weather, and the enemy.

3-90. The development of NAIs and TAIs based upon suspected enemy locations will drive the arrayal of ISR collection assets. The intelligence officer must also consider how asset mix, asset redundancy, and asset cueing are used to offset the capabilities of the various ISR collection assets.

3-91. During COA development, the intelligence refines and tailors the initial PIRs to each COA. Technically, these are initial information requirements for each COA. Later in the MDMP, once a COA is approved, then the final CCIR will be approved by the commander and published by the staff. ISR synchronization continues beyond MDMP or RDSP supporting the various phases of the operation until mission completion.

COURSE OF ACTION ANALYSIS (WARGAMING)

3-92. The intelligence officer must record the results of COA analysis and use that information to develop the ISR synchronization tools. The staff uses the action-reaction-counteraction process to move logically through the wargaming process. Most of these events will have bearing on how the intelligence officer recommends assets for tasking.

3-93. The intelligence officer must remember that CCIR cease to be critical either by time (LTIOV) or event (LEIOV) because this helps focus and prioritize the ISR effort. Latest event information is of value (LEIOV) is tied to a maneuver event; for example "prior to lead element establishing the outer cordon", or "prior to Alpha Troop crossing PL Buick". Time and event-based expirations assist the intelligence officer in the synchronizing ISR with the maneuver timeline. It is only then that friendly decision points can be directly tied to PIRs, NAIs, indicators, SIRs and ISR tasks.

3-94. In addition to a synchronization plan, the ISR plan is usually accompanied by an ISR overlay. Figure 3-6 is one example of an ISR overlay.

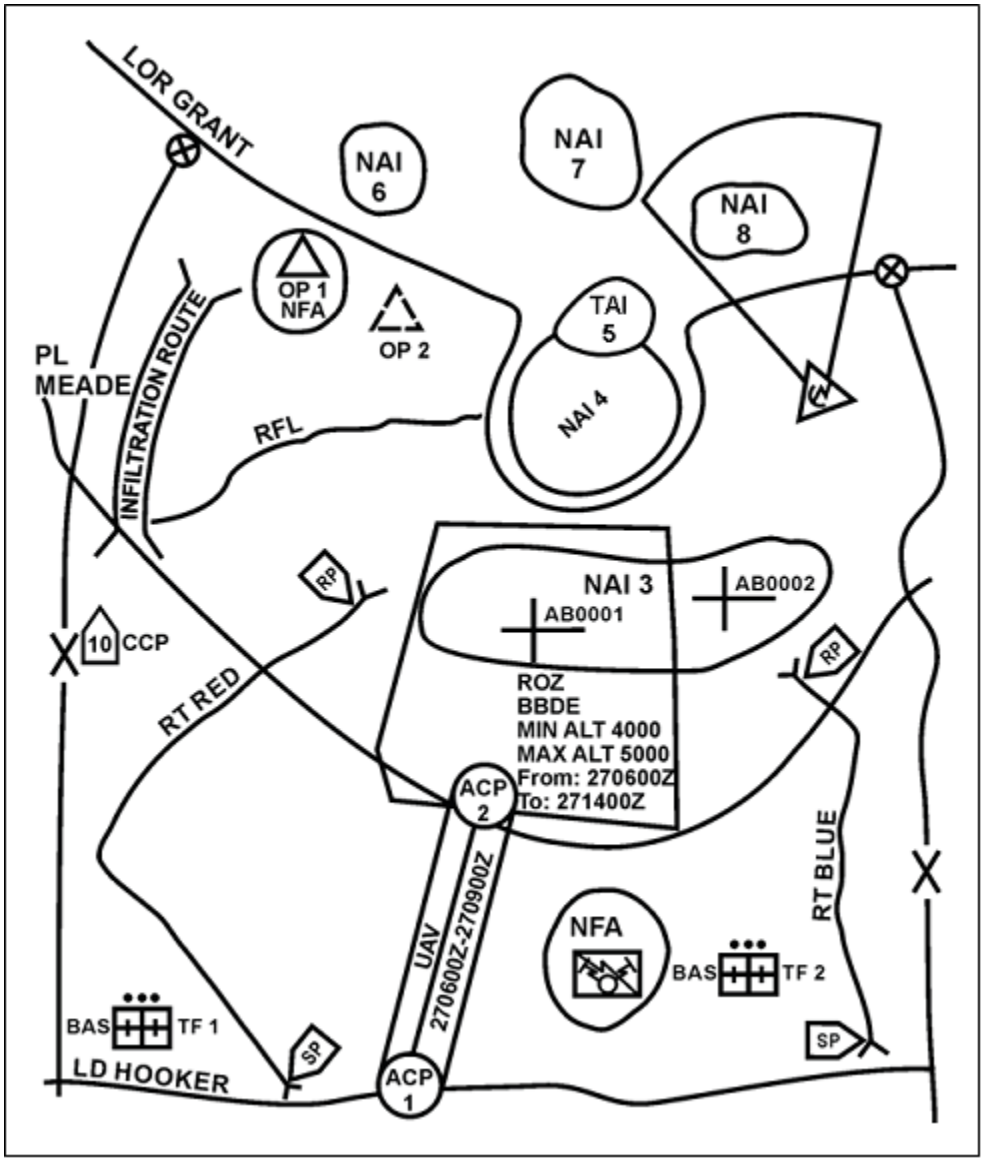

Figure 3-6. ISR overlay example

3-95. The ISR synchronization matrix 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 matrix generally includes—

- PIRs and information requirements.
- Indicators.
- Times and dates of the collection mission or RFI.
- LTIOV (or LEIOV).
- NAIs.
- Available assigned, attached, supporting, and higher echelon units and organizations that 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.

3-96. Figure 3-7 shows an example of a simple ISR synchronization matrix that can be used during wargaming to record the instances where certain collection assets would be needed for each NAI. The matrix is specific to one PIR and allows the intelligence officer to mark an "X" where an asset is available and capable of collecting on an NAI. As the wargaming continues, the intelligence officer can circle the "X" to show that a tasking for that asset is required. The details for collection can be added to a full ISR matrix after wargaming is concluded and the commander approves a friendly force COA.

ISR Wargaming Tool

Period Covered / Phase of Operation_____

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 3-7. ISR synchronization wargaming matrix used in COA analysis

COURSE OF ACTION COMPARISON/APPROVAL/ORDERS PRODUCTION

3-97. After the wargaming stage of MDMP, the commander selects a COA based on the comparative analysis made by the staff. When that COA is approved, the commander approves the final CCIRs to let the staff and subordinates know what information is deemed essential for decision-making. The commander decides what information is critical based on experience, the mission, the higher commander's intent, and the input (IPB, information, information requirements, intelligence, and recommendations) from the staff.

3-98. With the commander's approval of a COA and CCIRs, the operations officer issues the third and final warning order to include the ISR plan and accompanying overlay. The intelligence and operations officers must collaborate again to ensure the plan is fully synchronized and integrated during orders production. The ISR plan is published as an appendix to annex L (ISR) in the OPORD. It is most commonly presented in matrix format and should contain the information needed by the intelligence and operations officers to manage ISR operations as the operation unfolds. Many units use Microsoft Excel™

or PowerPoint™ to display the ISR plan in timeline or graphical form. Figure 3-8 is one example of a matrix format. Units typically develop whatever format best works for them.

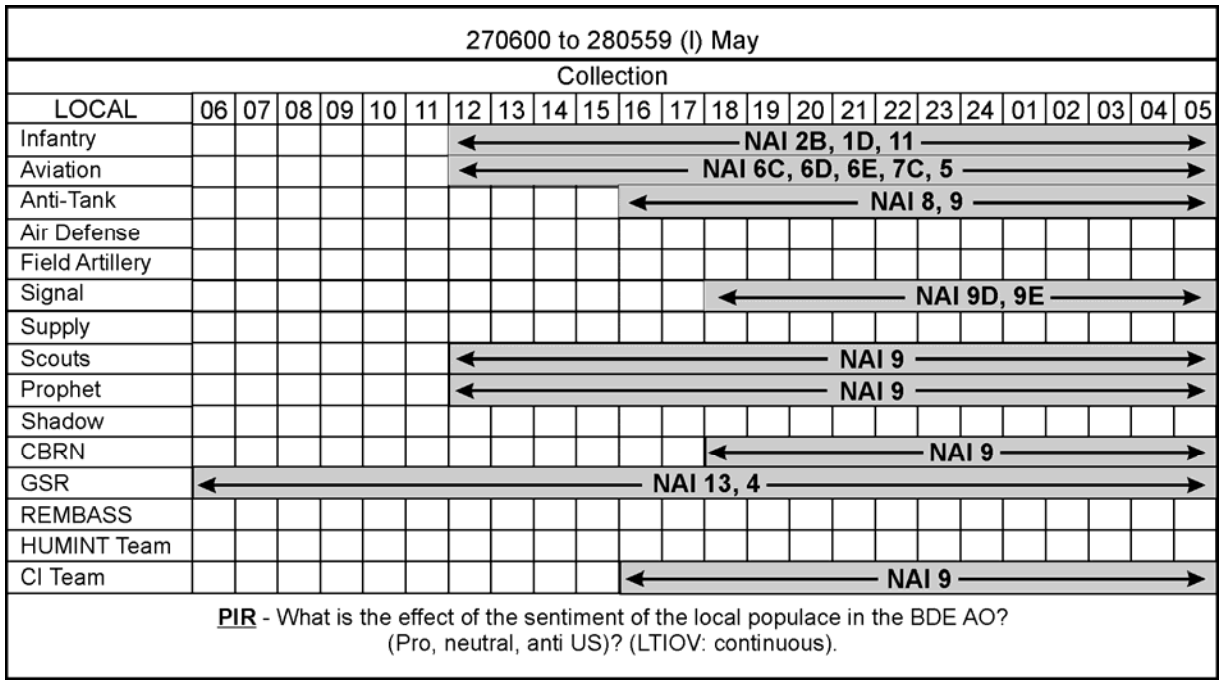

Figure 3-8. ISR plan in matrix format

Chapter 4

Intelligence, Surveillance, and Reconnaissance Synchronization Operations

This chapter describes the ISR synchronization process during the execution and assessment phases of the operations process. It describes the actions intelligence officers take during the Propagate, Assess ISR operations, and Update ISR operations activities in a time-constrained situation to maintain synchronization and aid in integration, disseminate data, information and intelligence products, assess ISR operations and update them to support the commander.

GENERAL

4-1. The previous chapter described the ISR synchronization process and the MDMP. To serve the commanders needs once operations begin, the ISR synchronization process needs to be dynamic and updated continuously. To understand ISR synchronization during on-going operations, one must understand how a command post functions, how staffs interact, and how abbreviated planning processes are conducted.

4-2. The same six ISR synchronization activities are conducted while ISR operations are on going and the intelligence and operations officers must work very closely together to revise the ISR plan continually. Figure 4-1 illustrates the ISR collection effort in terms of the operations process phases: plan, prepare, execute and assess.

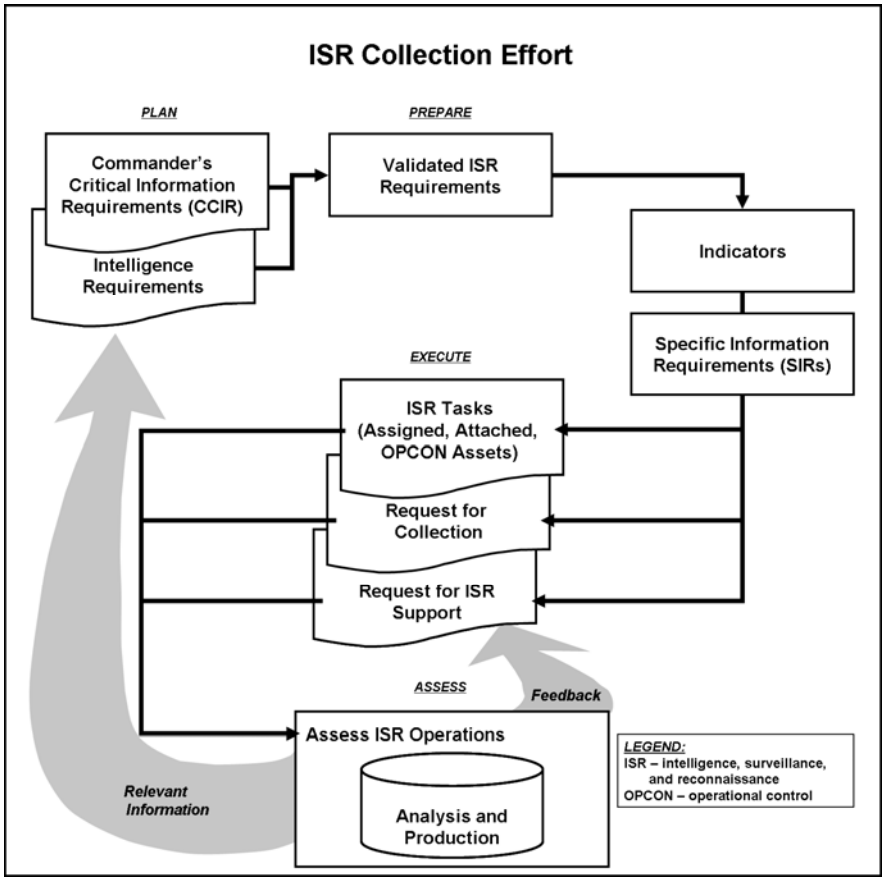

Figure 4-1. The intelligence, surveillance, and reconnaissance collection effort

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

4-3. IPB is a continuous process. Even after the staff conducts the initial IPB for a mission during the MDMP, they must continually review, refine, 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. The continuous updating of IPB products facilitates the assessment and updating of ISR operations.

4-4. ISR operations collect the data and information needed to improve IPB products and increase the commander's situational awareness as well as answer the CCIR.

INTELLIGENCE RUNNING ESTIMATE

4-5. 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.

4-6. 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 disseminated to all sections requiring it. Each staff section's running estimate is one product of this effort.

4-7. 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 intelligence officer 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.

STAFF SYNCHRONIZATION AND INTEGRATION ACTIVITIES

4-8. *Synchronization* is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. In the intelligence context, application of intelligence sources and methods in concert with the operation plan (JP 2-0).

4-9. *Integration* is the combining actions into a unified whole. Commanders and staffs use several integrating processes to accomplish this. These integrating processes combine members from across the staff to help synchronize operations.

4-10. The five staff integrating processes are:

- Intelligence preparation of the battlefield.
- ISR synchronization and ISR integration.
- Targeting.
- Composite risk management.
- Knowledge management.

4-11. Commanders and staffs also integrate the warfighting functions through command post cells, working groups, and boards. For more information on integrating processes, see FM 5-0, The Operations Process.

COMMAND POST FUNCTIONS

4-12. A command post (CP) is a unit headquarters where the commander exercises command and control and staff perform activities to support the commander's intent. Therefore, commanders organize CPs to meet changing situations and requirements of different operations. CP functions include—

- Developing and disseminating orders.

- Information management.
- Maintaining staff running estimates.
- Controlling operations including directing actions and performing critical on-going functions of execution.
- Assessing operations.
- CP administration.

4-13. 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 a commander's questions about the AO. ISR planning must begin with the military decision making process (MDMP) and all staff officers must be aware of major changes in the ISR plan as they are developed to support on-going operations.

4-14. Mission, resources and time determine how the commander organizes his command post and staff. The type of operation often dictates the need for alternative organization strategies. For example, during stability operations, the staff may be organized around the major lines of operation such as governance, security, economics, and infrastructure. In a different operation, the commander may choose to organize around the warfighting functions such as movement and maneuver, intelligence, fires, sustainment, protection and network operations.

4-15. Just as the organization of the CP and staff is often determined by the characteristics of the operation, so too are the requirements which the commander uses to drive ISR operations. In stability operations where non-lethal operations dominate, the commander may organize his information requirements around those lines of operation.

INTEGRATING CELLS

4-16. During operations, the commander may designate integrating cells to coordinate and synchronize all warfighting functions into specific short-range (current operations), mid-range (future operations), and long-range (plans) planning horizons. Since ISR operations are important to all three planning horizons, it is vitally important that the intelligence officer be represented in the current operations, future operations, and plans cells by an experienced Soldier who understands ISR.

4-17. Satisfying information requirements through staff element coordination facilitates better 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. Through continuous involvement in the integrating cells, the intelligence officer and G-2/S-2 staff maintain situational awareness and support ISR integration.

BATTLE RHYTHMS

4-18. *Battle rhythm* is a deliberate daily cycle of command, staff, and unit activities intended to synchronize current and future operations (JP 3-33). A headquarters' battle rhythm consists of a series of meetings among working groups and boards, report requirements, and other activities. The battle rhythm forces collaboration.

4-19. Working groups, boards, reports and other activities may occur daily, weekly, monthly, or quarterly; they may also be "on call" or at the whim of the Chief of Staff. During stable operational situations, these meetings may be scheduled regular recurring basis. When operational conditions are highly dynamic, working groups will occur whenever the Chief of Staff requires, or they may even be deferred. Battle rhythm during execution is critical for the staff to control time, deliverables and activities.

4-20. Battle rhythm establishes the time, frequency, and type of meetings and other events as well as who attends them. Reports, briefings, and meetings all require input and preparation. Additionally, the outputs of certain working groups are inputs for other working groups and boards. Battle rhythms must remain flexible and will change as the operation progresses. As the situation changes, the commander may require meetings or briefings less frequently than before.

4-21. ISR working group or ISR synchronization meetings must occur daily as long as ISR operations are on-going. This means that the intelligence officer, operations officer and primary staff must meet to discuss the next day's inputs for requests for collection and requests for ISR support, in addition to the current and future tasks for organic assets. The outputs from these meetings are vital to the operations synchronization meeting. The ISR synchronization tools are the basis from which the operations officer begins the integration process during operations synchronization meetings.

4-22. Due to the nature of ISR operations and the timelines required to plan and prepare them, the ISR synchronization meeting is one battle rhythm item that should not be reduced in frequency unless operations have culminated.

ISR PLANNING CYCLES

4-23. When the battle rhythm for a command post is determined, the intelligence officer synchronizes the ISR planning cycles with the other staff planning cycles. There are several cycles that must be considered:

- The ATO cycle (see appendix C).
- Higher echelons' ISR planning cycle.
- Analysis and production (sometimes called fusion) meetings.
- Intelligence product delivery schedules.
- The ISR working group or synchronization meeting frequency.

Note: Analysis and production timelines and delivery schedules must match ISR plans so the intelligence effort is synchronized properly.

4-24. The three staff meetings, working groups, or boards that require detailed intelligence input are the operations synchronization meeting, the targeting working group or board, and the effects working group or board.

MANAGING ISR OPERATIONS

4-25. Managing any echelon's ISR effort entails intelligence personnel performing the following implied tasks:

- **Requirements visibility** using procedures and information systems to develop, task, monitor, and display the status of information requirements.
- **Asset visibility** using procedures and information systems to monitor and display collection asset status, location, and current activities as well as future location and activities. Units must also know the status, location, and current activities of ISR resources performing ISR tasks under their command and control or in direct support of their requirements.
- **Assessment capability** using procedures and information systems to assess the effectiveness of the ISR effort, the ISR results (such as its success in answering CCIR or failure resulting in collection gaps) and to task (or retask) collection assets.
- **Mission management** using procedures and information systems to assign requirements within technical channels to available specialized intelligence assets, units, and resources in order to provide timely answers to those requirements. Mission management determines how to employ intelligence assets, units, and resources and synchronizes the exploitation effort to ensure intelligence products answer CCIR in a timely fashion.

4-26. The intelligence officer assists the operations officer by synchronizing ISR assets, resources, and sensors using mission management techniques to ensure maximum efficiency is achieved and maximum benefit is derived from them.

PROPAGATE

4-27. 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.

KNOWLEDGE MANAGEMENT

4-28. *Knowledge management* (KM) is the art of creating, organizing, applying, and transferring knowledge to facilitate situational understanding and decision-making. Knowledge management supports improving organizational learning, innovation, and performance. Knowledge management processes ensure knowledge products and services are relevant, accurate, timely, and useable to commanders and decision makers. (FM 3-0) Intelligence officers must be sure that delivery of ISR data and intelligence products are disseminated using KM best practices.

4-29. Effective KM supports commanders to make informed, timely decisions and reduces the fog of operations. It also links the various organizations and personnel requiring knowledge to enable effective collaboration. KM enhances rapid adaptation in a dynamic operational environment, especially when faced with a hostile, thinking, and adaptive enemy.

4-30. CCIRs focus the development of knowledge management practices and products. All leaders need to understand the processes and procedures associated with the intelligence enterprise and unit information systems in order to share information and knowledge efficiently. Commanders and staffs assess the effectiveness of ISR operations by determining if CCIRs and other information requirements have been answered or fulfilled. KM narrows the gap between relevant information that commanders require and the relevant information they receive.

4-31. Knowledge management processes include:

- Content management and associated techniques of—
  - Process analysis.
  - Report analysis.
  - Technical systems analysis.
  - Online collaborative spaces.
  - Knowledge networks development.

4-32. The G/S2 staff must work very closely with knowledge managers to leverage their expertise into efficient and collaborative dissemination of ISR data, information and intelligence products. Knowledge networks, such as a tactical web portal that integrates various ISR data files and facilitates online collaboration for ISR synchronization, can benefit the producer and consumers of intelligence and knowledge.

PROPAGATE INFORMATION AND INTELLIGENCE

4-33. 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.

DIRECT DISSEMINATION

4-34. 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.

4-35. 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.

DETERMINE PERISHABILITY

4-36. When dealing with time-sensitive information, the intelligence officer ensures the requestor receives the best available information and intelligence before the LTIOV. 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.

4-37. 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.

4-38. 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

4-39. 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.

4-40. 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.

4-41. 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.

4-42. 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.

4-43. 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 which intelligence products are needed, what is the required timeliness, where is the decision-maker (consumer), and what logistical and communications assets available to support intelligence dissemination.

DETERMINE QUANTITY

4-44. The intelligence officer must know how much information is enough information. This is no simple task because the volume and velocity of information continues to increase with every new technological innovation. The flow of data and information from multiple sensors, collectors and units can easily overwhelm the analytical capabilities of a unit. Close coordination between the analytical and ISR operations planners will help guide the intelligence officer to meter the flow of information.

4-45. 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.

4-46. Planning factors such as ETIOV can also help limit the amount of information sent by sensors and collectors. Using the enemy SITEMP and EVENTEMP from IPB, the intelligence officer can determine when to begin collection operations on a timeline or geographical basis. In the case of steady state operations, such as the stability operations in Iraq and Afghanistan, the intelligence officer and G-2/S-2 staff must determine what reporting is relevant or not before devoting a significant effort to analyzing that data or information.

4-47. Intelligence officers must also ensure only users who have the proper "need to know" receive sensitive compartmented information as opposed 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 be a constraint to ISR operations.

4-48. 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.

4-49. 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.

DETERMINE DISSEMINATION METHODS

4-50. 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.

4-51. 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 no later than the LTIOV in a format that best supports the commander's decision-making.

4-52. 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 are one of the determinants the method of dissemination.

Arrange for Direct Dissemination (Point-to-Point Dissemination)

4-53. 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.

4-54. 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.

4-55. 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.

4-56. 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.

4-57. 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.

Arrange for Redundant Dissemination Methods

4-58. 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

4-59. 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.

4-60. 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.

4-61. 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.

4-62. 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.

4-63. 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.

4-64. 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.

4-65. 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

4-66. 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.

4-67. Audit trails further optimize dissemination by ensuring that all appropriate commanders and staff sections receive each report only once. Users receiving the same report multiple times might interpret them as 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.

4-68. 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. 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").

4-69. 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.

4-70. 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 link journal entries to the requirements numbering system efficiently.

4-71. 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.

DATABASE MANAGEMENT

4-72. 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.

4-73. 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

4-74. 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.

4-75. 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

4-76. 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.

4-77. 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.

4-78. 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, or 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).

4-79. Not all of the required information will be available for each data entry. However, 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.

4-80. 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

4-81. 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.

4-82. 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

4-83. 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

4-84. 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

4-85. 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 facilitates effective use of limited storage space, speeds up database queries, and prevents confusion over duplicate data entries.

Import and Export Standards

4-86. 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 or 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

4-87. 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.

ASSESSING ISR OPERATIONS

4-88. 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.

4-89. 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.

4-90. Intelligence officers track reporting to determine how well the ISR effort is satisfying the CCIR. 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 evaluate reporting effectively: monitor operations and maintain synchronization, correlate reports to requirements, screen reports, and provide feedback to ISR assets.

MONITOR OPERATIONS

4-91. 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 matrix 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 matrix contains each collection requirement.

4-92. The intelligence officer tracks the flow of the operation against the requirements and ISR synchronization matrices. As necessary, the intelligence officer prompts subordinate commanders and collectors to keep their reporting synchronized with the operation and the commander's needs.

4-93. 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).

4-94. 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.

4-95. 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.

4-96. Intelligence officers set up a system that allows the intelligence section to monitor synchronization and evaluate how well the intelligence system is meeting requirements without unduly delaying intelligence dissemination.

CORRELATE REPORTS TO REQUIREMENTS

4-97. 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.

4-98. 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.
- Circular reporting and so-called "spam" or unnecessary message traffic can cause a great deal of consternation and wastes valuable time.

4-99. 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.

4-100. 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.

4-101. 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

4-102. 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.

4-103. 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.

4-104. 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.

4-105. 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

4-106. 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.

4-107. 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.

4-108. 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—

4-109. 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.

4-110. Notify ISR assets of new ISR tasks designed to exploit cueing and other opportunities.

4-111. 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

4-112. 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. For more information on operational assessment, see FM 5-0 chapter 6.

UPDATE ISR OPERATIONS

4-113. 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.

4-114. 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 tools 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 matrix and recommends changes to the operations officer and the staff.

4-115. Intelligence officers synchronize new ISR requirements with ongoing ISR operations and recommend integration techniques to the operations officer. The G-2/S-2 staff keeps the intelligence officer 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.

4-116. 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

4-117. 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.

Dynamic and Ad-Hoc Tasking of ISR Assets

4-118. Unforeseen events can disrupt an ISR plan or cause a new requirement to arise. Minor variances in the ISR plan can be adjusted for automatically by the staff and may not require modification of the plan. Branches and sequels to the operational plan should have already been factored into the ISR plan during the plan and prepare phases of the operations process. Dynamic re-tasking of ISR assets is accomplished more easily if the branches and sequels were considered in the original plan.

4-119. Unanticipated situations, such as a friendly force aircraft crash or shoot down or loss of a UAS asset to enemy fire, mechanical failure, or loss of signal, not only disrupt the collection operation, but may require ad-hoc tasking of additional assets to try to locate the aircraft. The best method of preparing for ad-hoc tasking is to prepare battle drills in the command post SOP.

4-120. These drills can be developed by asking "what if" and then walking step by step through the logical procedures that should follow. Obviously, there are many variables that cannot be anticipated in advance, but the G-2/S-2 and G-3/S-3 staff can be better prepared by developing drills which cover the most common occurrences expected to require ISR re-tasking of ISR assets.

4-121. For example, a troops-in-contact report from a patrol, aircraft or convoy is frequently followed by a request for ISR support (either from the unit itself or the commander who wants to see for himself what is happening on the ground). The command post battle drill for troops in contact should include ISR actions steps so that assets can be redirected.

4-122. 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. The following two examples illustrate the need for maintaining ISR synchronization.

Scenario One:

An analyst from the division analysis and control element (ACE) notifies the G-2 that PIR #2 was answered through analysis of data from current ISR operations.

The intelligence officer reviews the ISR synchronization tools and notes that ISR assets can be relieved of three ISR tasks associated with PIR #2. The G-2, in coordination with the G-3, relieves the BFSB from their two ISR tasks and withdraws the other ISR task from the division's requests for collection at corps.

While updating on the current situation, the G-2 notices that the operation appears to be progressing more rapidly than anticipated. The G-2 confers with the ACE and G-3 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 G-2 coordinates with the G-3 to make the needed changes to the event templates and synchronization matrices. The G-3 uses these changes as a basis for changing outstanding ISR tasks on the ISR plan.

When the G-2 identifies ad hoc collection opportunities through cueing, a recommendation is made to the G-3 for redirecting or retasking of a BFSB ISR asset.

The G-3 reevaluates the ISR plan based upon those recommendations. In particular, the G-3 looks for opportunities to improve reconnaissance and surveillance operations and retasks ISR assets appropriately.

Scenario Two:

A BCT's original plan for locating a high-value target (individual) called for cross-cueing by SIGINT and HUMINT assets. When S-2 learns that a scout platoon conducting a patrol received information that the HVT (a particular insurgent leader) is in their vicinity, the S-2 recommends diverting a UAS from an ongoing mission from a lower priority requirement to conduct reconnaissance in the vicinity of the patrol and to assist in the platoon's search operation. The S-2 coordinates with the S-3, who issues the necessary orders and coordinates the changed flight track with the division's airspace manager.

The combined ground and UAS operation captures the insurgent leader and the S-3 retasks the UAS to the next priority mission. The ability for the S-2 and S-3 to coordinate and dynamically retask the BCT's UAS provide the commander with flexibility and responsiveness leading to mission success.

CUEING ASSETS TO COLLECTION OPPORTUNITIES

4-123. Cueing opportunities, whether prompted through combat information or analysis, allows intelligence officers to satisfy requirements more efficiently than previously planned. The key to developing cueing opportunities is the intelligence officer and staff maintaining situational awareness throughout the operation and anticipating opportunities as they arise.

4-124. Cueing, redundancy and mix are discussed further in chapter 3.

ELIMINATE SATISFIED REQUIREMENTS

4-125. 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.

4-126. 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.

4-127. When higher headquarters declares a requirement satisfied, eliminate it from the ISR synchronization matrix and the ISR plan, and update any other logs and records.

DEVELOP AND ADD NEW REQUIREMENTS

4-128. As the operation unfolds and the threat situation develops, commanders will generate new requirements. This prompts intelligence officers to begin updating the ISR synchronization tools. 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

4-129. 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.

4-130. 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.

4-131. 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).

4-132. 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.

4-133. The desired outcome is that ISR tasks continuously evolve to ensure intelligence and operational synchronization.

TRANSITION TO THE NEXT OPERATION

4-134. 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.

4-135. Refit includes all of those administrative and logistics activities that provide for the reorganization, recovery, and re-supply of units and assets.

4-136. 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.

4-137. 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.

RECENT INTELLIGENCE OPERATIONS

4-138. 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. Another example of the key intelligence role plays in facilitating the commander's understanding of the operational environment through a greater emphasis on the human elements of the mission and how they interact with the operational variables

4-139. In today's operational environment, explaining 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.

4-140. Commanders must resource G-2/S-2 sections with appropriate manpower in order to obtain sufficient information and intelligence from the ISR effort. During counterinsurgency operations such as recent operations in Iraq and Afghanistan, the volume and velocity of information can overwhelm a traditionally staffed S-2 section. For example, many commanders have found it useful to create company intelligence support teams to resource company commanders with intelligence collection and analysis capabilities during counterinsurgency operations.

4-141. Closely linking ISR synchronization with all ongoing analytical and production efforts across a collaborative and flexible staff framework is vital to successful ISR operations. ISR synchronization in support of the full spectrum of operations should follow the fundamental doctrinal methodologies presented in this manual; however, for stability and counterinsurgency operations a much greater emphasis on civil considerations are necessary, especially with regard to varied demographic groups and formal or informal networks and leaders.

COIN ISR Planning

2nd BCT, 1st Cavalry Division was deployed to Operation Iraqi Freedom 06-08. 2nd BCT was responsible for the Karkh security district of Baghdad, one of the most difficult BCT sectors in multinational division-Baghdad's (MND-B) AOR.

Using effects-based planning techniques and unconventional thinking, the S-2 reoriented the BCT's ISR efforts into a COIN-based plan that provided the best solution for that BCT's counterinsurgency problem set.

Key lessons learned by 2/1CD:

1. Align PIR around the lines of operation so they correlate with the brigade's campaign objectives.

2. PIR and supporting IRs should start with WHY as opposed to WHAT or WHO or WHERE.

3. Link PIR to desired effects (which serve as decision points in COIN operations).

4. Work backwards from what you know to learn what you do not know.

5. Alter your planning cycle to fit the problem set because effects take longer to assess than lethal operations.

6. Detailed reporting is the key to answering highly specific nonlethal PIRs; make it simple for Soldiers to report everything.

7. Give the collector the background so collection will have more context as it is collected.

8. Manage ISR collection by using an ISR synchronization meeting to engage collectors and consumers all at once.

9. Knowledge management is critical to making the information work for the commander and staff.

10. Focus the analytical effort around COIN collection effort and leverage the entire staff's expertise in analysis.

4-142. FM 3-24, chapter 3, articulates the process to describe the unique characteristics of the operational environment during counterinsurgency operations. For more information on stability operations, see FM 3-07.

4-143. 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. This type information can prove quite useful in answering CCIR and supporting the staff's situational awareness.

4-144. 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) sensors have provided unprecedented ISR capabilities and opportunities below the battalion level.
- Detainee interrogation, site exploitation, and document and media exploitation are key intelligence activities used to cue other ISR capabilities and sometimes to "trigger" subsequent operations, branches, or sequels, as appropriate.
- The increased situational awareness that Soldiers develop through personal contact and observation is a critical element of that unit's ability to more fully understand the battlefield. However, Soldiers collect combat information that is then processed into intelligence by unit intelligence analysts. Company intelligence support teams are one technique that commanders use to collect and leverage relevant information from patrol debriefings and Soldier observations.
- While medical personnel cannot be assigned ISR tasks due to their Geneva Convention category status, medical personnel who gain information through casual observation of activities in plain view while discharging their humanitarian duties will report the information to their supporting intelligence element.

4-145. Observations from combat training center rotations and lessons learned from current combat operations emphasize the importance of ISR planning involving full staff participation and synergy to properly focus ISR assets on the CCIRs. Successful ISR planning ties the ISR synchronization and integration activities into the entire staff planning and operations processes. In addition to the operations officer, the following staff officers must be closely involved with ISR planning:

- Knowledge management officers who aid in the dissemination function and archiving of ISR data for future reference.
- G-6/S-6 personnel to integrate ISR needs into the overall communications plan.
- G-4/S-4 personnel to prepare sustainment plans for ISR units and resources that require might unique support.
- Civil affairs, information operations and special staff officers in order to integrate ISR into their plans and estimates.

4-146. Successful ISR operations integrate and synchronize the collection effort across all warfighting functions using every available asset, sensors, units, and Soldier as well as all available intelligence collection assets (internal, external, and joint/national); all enhanced by the net-centric DCGS-A enterprise.

4-147. In recent OIF counterinsurgency operations, lessons learned suggest that the requirements development process must be closely tied to the assessment process for measures of effectiveness and measures of performance. For more discussion on effects-based planning, see FM 5-0.

Appendix A

Developing Requirements for ISR Planning

The methodology used for developing requirements for ISR operations is probably the most important aspect of ISR planning. If ISR assets, units and Soldiers do not understand when, where, and what they are supposed to collect, then it is likely that the information gathered will not answer the CCIR. This appendix describes the process of developing requirements which ultimately become ISR tasks for collection by all the assets, units and Soldiers under the commander's control.

GENERAL

A-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. These steps are not discrete and may often overlap. 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.

A-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 is 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.

A-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.

A-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. Intelligence officers review the commander's requirements and develop intelligence requirements. Intelligence officers validate and recommend PIRs to the commander, manage the commander's PIRs and request information from higher or lateral organizations.

A-5. 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 A-1 depicts the relationship of information requirements, including CCIRs (PIRs and FFIRs) and EEFIs.

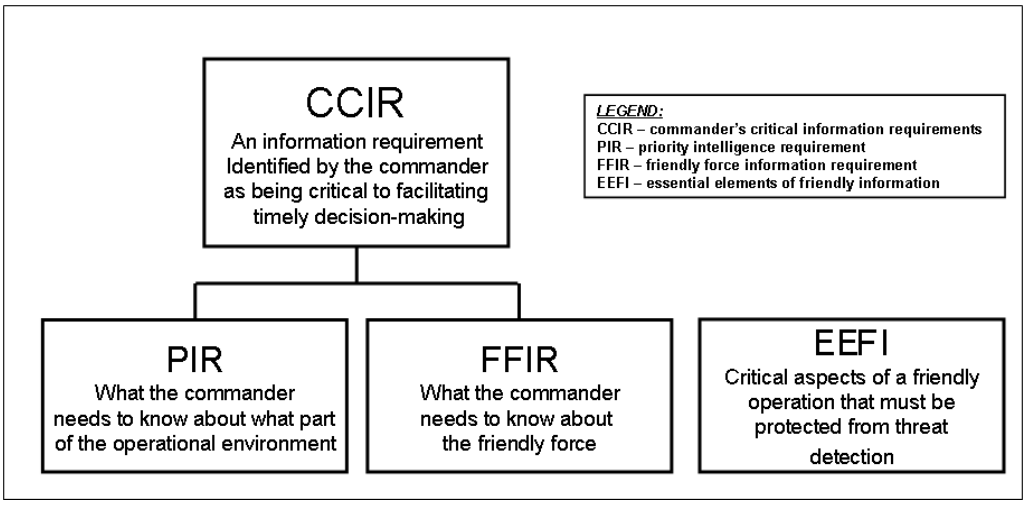

Figure A-1. Information requirements

A-6. 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.

A-7. The intelligence staff generates information requirements during the mission analysis portion of the MDMP, stated either as an IR or as 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). Figure A-2 illustrates the process of developing ISR requirements.

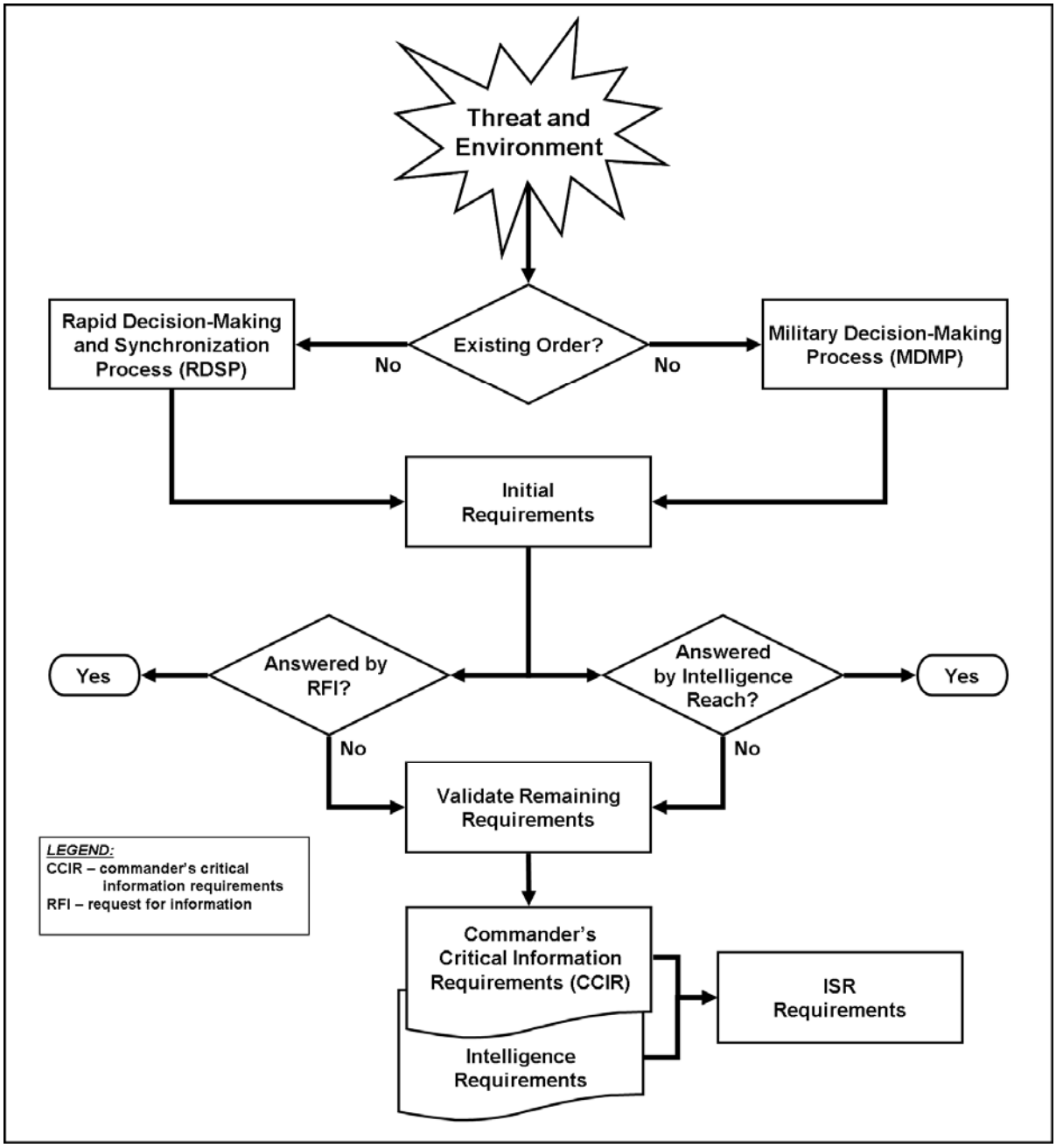

Figure A-2. Requirements development for ISR operations

TYPES OF INFORMATION REQUIREMENTS

PRIORITY INTELLIGENCE REQUIREMENTS

A-8. 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?"

A-9. 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.

A-10. 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.

A-11. 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?"

A-12. 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.

A-13. 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.

A-14. 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.

A-15. 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 requirements matrix, ISR synchronization matrix, ISR plan, 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.

A-16. 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

A-17. 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. Appendix D describes the targeting process and special ISR considerations.

A-18. In intelligence usage, a target is a country, area, installation, agency, or person against whom intelligence operations are directed (JP 1-02). To target the threat effectively, the staff develops named areas of interest (NAIs) and targeted areas of interest (TAIs). The staff can also develop an HVT list that 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. For example, requirements may not be focused on a certain geographic area, but instead on a network or a person.

NAMED AREA OF INTEREST

A-19. 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.

A-20. 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

A-21. 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.

A-22. 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.

A-23. 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, or to pinpoint terrain that might be considered key or decisive terrain. Religious buildings, places of worship and shrines are an example of potential NAIs that are part of civil considerations 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

A-24. 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

A-25. Developing requirements includes the following steps: anticipate, analyze, develop indicators, and develop SIRs.

ANTICIPATE

A-26. 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.

A-27. 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

A-28. 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

A-29. 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

A-30. 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

A-31. 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

A-32. 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.

A-33. 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

A-34. 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

low-density/high-demand ISR assets and resources are directed against the most critical requirements. Effective prioritization requires monitoring of the operation to respond to changing situations.

A-35. 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.

A-36. 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

A-37. 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.)"

A-38. 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

A-39. 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.)"

A-40. 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

A-41. 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. 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.

A-42. 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

A-43. 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.

A-44. 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.

A-45. 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.

A-46. 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

A-47. An indicator is an item of information that 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 that may influence the commander's selection of a COA.

A-48. 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.

A-49. 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.

A-50. 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.

A-51. 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 (SIR)

A-52. 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.

A-53. 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.

A-54. 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 that 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.

A-55. 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.

A-56. 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.

A-57. 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.

A-58. Develop more detail in the observables by identifying the specific information or signatures that 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.

A-59. 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.

A-60. 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.

A-61. Because each intelligence requirement will generate a number of indicators that 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. "

A-62. 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.

DEVELOPING ISR TASKS

A-63. Developing requirements ends with SIR development because the development of ISR tasks must occur as the synchronization plan is being developed. The intelligence officer must consider whether to task an asset or request support from higher (a resource) or to request collection by Joint or National systems.

Appendix B

Intelligence, Surveillance, and Reconnaissance Synchronization Training and Resources

This appendix outlines the ISR synchronization training available through US Army sources and the ISR synchronization information resources available to Soldiers.

GENERAL

B-1. ISR synchronization duties at any echelon should not be handed to the least experienced staff member. The intelligence officer must be involved and must direct the efforts of those personnel assigned to work on ISR synchronization. Ideally, the intelligence officer and select G-2/S-2 staff members would be trained specifically in ISR. At division and higher echelons, the single-discipline warrant officers on the G-2/S-2 staff will be of great help to the intelligence officer because of their subject matter expertise on the collection systems.

B-2. The various ISR training opportunities discussed in this appendix are designed to Soldiers with a solid foundation on the wide variety of Army, Joint and National ISR collection systems, platforms and sensors. A detailed understanding of ISR doctrine combined with knowledge of the capabilities, limitations and planning factors for each system, platform or sensor is the key to successful ISR planning and execution.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION TRAINING

ISR SYNCHRONIZATION MANAGER COURSE

B-3. The ISR Synchronization Manager course is an ASI/SI producing course focused on training military intelligence officers and non-commissioned officers (NCOs) to master the skills of a Brigade/Division/Corps ISR Planner/Manager. MI NCOs in the career field of 35F skill levels 2-4 and 35N skill level 2 will receive the ASI Q7 upon successful completion of the course. MI (35 career field) officers in the rank of Captain and Major will receive the SI Q7 upon successful completion of the course.

B-4. The course consists of three modules:

- In the **first module**, students will learn the capabilities and limitations of ISR assets from BCT through theater, joint, and national levels. The course includes manned and unmanned airborne systems, unattended ground sensors systems, HUMINT operations, SIGINT operations and current ISR organizations such as Task Force ODIN.
- In the **second module**, students learn the doctrinal ISR synchronization process along with how it relates to the IPB and the MDMP. Students will also receive training on the Intelligence Synchronization Tool (IST), Joint ISR operations, PRISM and COLISEUM. See appendix D for further discussion of PRISM, COLISEUM and joint ISR considerations.
- In the **final module**, students participate in a joint intelligence combat training center (JICTC) rotation acting as the ISR planners at the Division, Brigade and Battalion command posts.

B-5. The ISR Synchronization Manager course is a three-week course taught at the US Army Intelligence Center at Fort Huachuca, Arizona (USIAC/FH). It is available through the Army Training Requirements

and Resources System (ATRRS) as course number 3A-SIQ7/243-ASIQ7. A TS-SCI security clearance is required for students attending the course.

ISR Synchronization Course Mobile Training Team

B-6. In addition to the resident course, a mobile training team (MTT) ISR synchronization course is also available to meet the needs of units preparing for deployment. The ISR MTT is provided by USAIC/FH at no cost to the unit. The curriculum is tailored to the needs of the unit and is designed to be more cost effective when a number of students from one command require ISR synchronization training.

B-7. The course managers can be contacted via e-mail at isrsynchteam@conus.army.mil or by phone at 520-533-6351.

ISR TOPOFF

B-8. ISR TOPOFF is a joint mobile training team course sponsored by the Training and Doctrine Command (TRADOC) G-2 ISR Integration office, US Air Force Air Combat Command, and US Joint Forces Command. It is tailored for deploying Army BCT Commanders and staffs at their home station locations. The TOPOFF training event should be scheduled into the ARFORGEN process prior to any mission readiness exercise or combat training center rotation. This training is funded by the INSCOM Foundry program.

B-9. The course includes—

- A three hour senior leader joint seminar for BCT and battalion commanders and senior staff.
- A three to four day MTT for the S-2, S-3, S-6, effects, engineer, and military intelligence company (MICO) personnel targeted at the brigade-level ISR problem set.
- A team of US Army and US Air Force subject matter experts.
- Hands-on training with applications, portals and websites.

B-10. The ISR TOPOFF training objectives are to—

- Train collection managers to effectively employ ISR capabilities, especially non-organic, theater and joint ISR resources.
- Inform BCT personnel on the processes, platforms, sensors and reach capabilities that exist to support them in their mission.
- Familiarize and develop an understanding of the OIF and OEF mission-specific products that are already available.

B-11. The program manager for ISR TOPOFF is the TRADOC G-2 ISR Integration office at (cml) 757-788-2937 or DSN

Training Counter-IED Operations Integration Center (TCOIC)

B-12. The TCOIC is an individual and collective training resource for reachback support, modeling and simulation services to deploying and deployed units. Their capabilities and tools are focused on enhancing Soldiers' abilities to attack and defeat IED networks.

B-13. The TCOIC offers a mobile training team at no cost to the unit for commanders, staffs, and intelligence analysts. For more information, go to www.us.army.mil/suite/page/458271 on NIPRnet or http://hqinscom.portal.inscom.army.smil.mil/tcoic on SIPRnet.

Other Training

B-14. Several collection management courses are available at joint and DOD level organizations for intelligence personnel destined for higher echelon assignments.

B-15. The Defense Intelligence Agency offers a collection management course (details on SIPRNET at www.dia.smil.mil/homepage/hc/LCD/JMITC/collection.html).

ISR RESOURCES

B-16. US Army Strategic Command (ARSTRAT) provides an ISR Smartbook available at http://portal.smdc.smil.mil/C6/G2PLEX/default.aspx on SIPRnet.

B-17. The US Joint Forces Command (USJFCOM) Joint Fires Integration and Interoperability Team (JFIIT) was established to improve integration, interoperability, and effectiveness of Joint fires, focusing on the tactical level. JFIIT publishes the JFIIT Tactical Leaders Handbook (TS-06-02) is an excellent reference on Joint ISR resources. The pocket-sized FOUO version is available at https://www.jec.jfcom.mil/jfiit/. A classified version is available at http://jfiit.eglin.af.smil.mil.

FOUNDRY

B-18. The Army's Intelligence and Security Command (INSCOM) created Project FOUNDRY in 2006 to provide BCT and Division Commanders with "single hub" access to advanced skills training, certifications, and live environment training opportunities weighted towards "next deploying" units. FOUNDRY is designed specifically to improve MI wartime readiness across all intelligence disciplines and Army Components, and enables "reach-forward" opportunities to gain contact with the enemy before deployment from home station. INSCOM and USAIC have partnered with TRADOC to integrate DCGS-A and other advanced skills training capabilities into our Combat Training Centers (CTC) to enable deploying units to work against realistic battlefield complexity, reinforce combat lessons learned, and integrate emerging technologies into unit tactics, techniques and procedures.

B-19. FOUNDRY provides both funding and coordination needed to fully leverage Joint and National Intelligence training opportunities to meet ARFORGEN deployment demands. INSCOM is building several FOUNDRY training platforms at major installations to facilitate database access, virtual training programs, and tactical overwatch support.

Appendix C

Joint, National, and Multinational Intelligence, Surveillance, and Reconnaissance Planning Considerations

This appendix describes the specific considerations that Army intelligence officers must be aware of to effectively and efficiently leverage joint, national and multinational ISR assets in their ISR synchronization planning. Unique systems characteristics will not be discussed here as they are often classified and are much too varied to cover in this manual. Instead, the focus of this appendix is to present the planning considerations which are relevant to ISR synchronization.

JOINT INTELLIGENCE OPERATIONS

C-1. Joint 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

C-2. Current intelligence, surveillance, and reconnaissance operations are inherently joint, sometimes even down to BCT or battalion-level. ISR assets such as the US Navy's P-3 Orion aircraft, originally designed for anti-submarine and anti-surface warfare maritime patrol operations, are being used to provide full motion video (FMV) and signals intelligence support of ground Commanders in Operations Iraqi and Enduring Freedom. P-3s are also used by the U.S. Department of Homeland Security for counter-smuggling and counter-drug operations.

C-3. Air Force UAV systems such as Predator and Reaper, which were at one time in the purview of Commanders at echelons above corps, are now available to ground commanders at division and BCT. Air Force ISR liaison officers are posted to corps and division headquarters and planned for availability at BCTs in the near future. These are a few examples why Army intelligence officers must understand the specific planning considerations for joint, national and multinational operations.

JOINT INTELLIGENCE PROCESS

C-4. The Joint intelligence process describes how the various types of intelligence operations interact to meet the commander's intelligence needs. The process includes the following intelligence operations:

- Planning and direction.
- Collection.
- Processing and exploitation.
- Analysis and production.
- Dissemination and integration.
- Evaluation and feedback.

C-5. Figure C-1 illustrates how the Army's intelligence process relates to the Joint intelligence process. For more information on the Joint intelligence process, see JP 2-01 and FM 2-0 chapter 2.

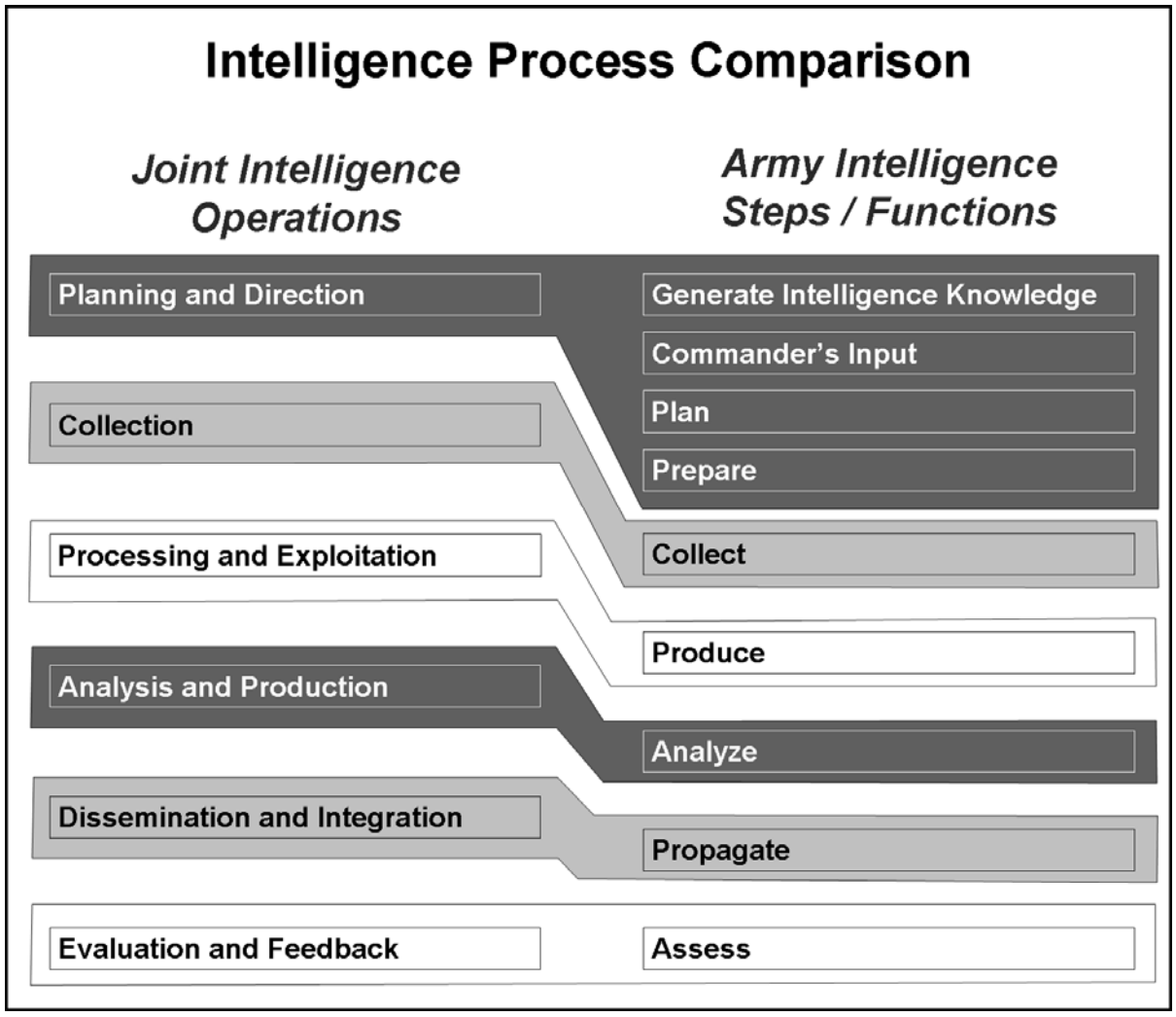

Figure C-1. Joint and Army intelligence processes

JOINT TERMINOLOGY

C-6. 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.

C-7. In the Joint lexicon, *collection management* is a process that 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 C-2 illustrates these functions.

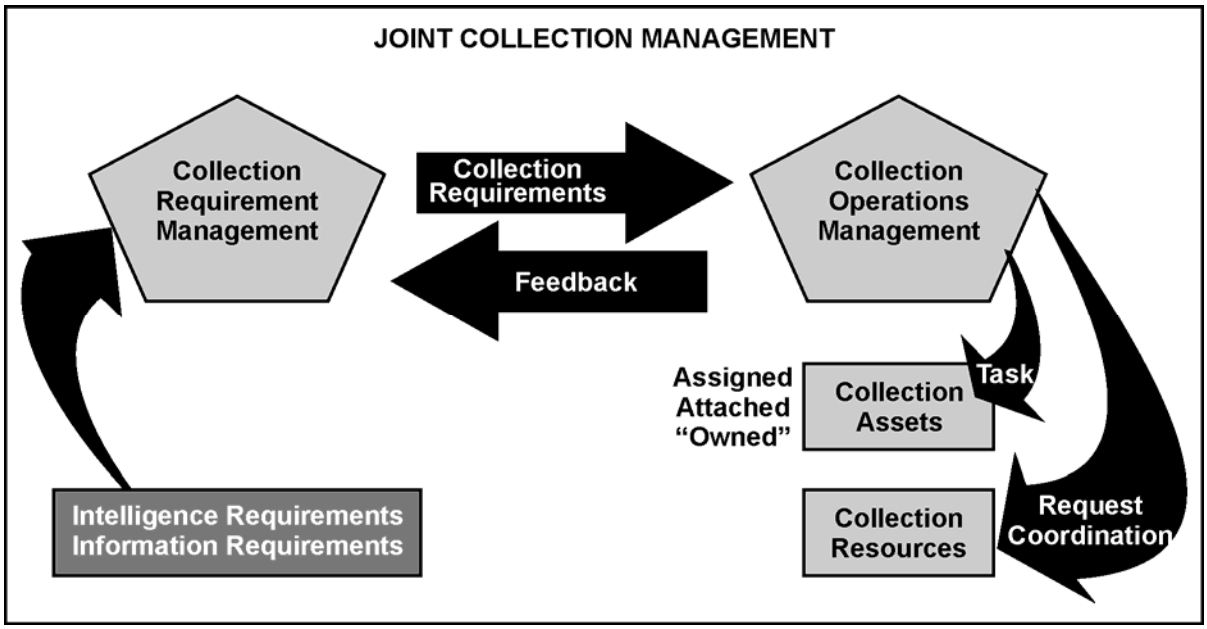

Figure C-2. Joint collection management

C-8. 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 of command, 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.

C-9. Tasking, processing, exploitation, and dissemination (TPED) is the joint term used to describe the associated activities which support the JTF commander's collection strategy and subsequent ISR operations. In a similar fashion, Army intelligence officers must consider the analysis, production, and dissemination effort as part and parcel to ISR synchronization planning. Much of TPED occurs outside the theater via reachback (what the Army calls intelligence reach) and distributed through the intelligence architecture so that requirements do not overwhelm in-theater assets. Service organizations like the National Ground Intelligence Center (NGIC), National Maritime Intelligence Center (NMIC), Marine Corps Intelligence Agency (MICA), and the Air Force ISR Agency which includes the National Air and Space Intelligence Center (NASIC) and joint organizations like the Defense Intelligence Agency (DIA) and the National Center for Medical Intelligence (NCMI) provide reach back capabilities to forward deployed joint commands.

C-10. In Joint terms, a *collection asset* or a *collection resource* is a collection system, platform, or capability. A collection asset is subordinate to the requesting unit or echelon, while a collection resource is not (JP 2-01.3).

C-11. In Joint collection management, all requests for collection are called target nominations. From the perspective of the joint collection resource, the NAI or TAI is a target for collection. Target nomination

boards are responsible to prioritizing collection requests and allocating resources against those requirements.

JOINT INTELLIGENCE ORGANIZATIONS

C-12. When Army forces operate under a Joint or combined headquarters for unified action, several organizations in the joint intelligence architecture can assist intelligence officers at lower echelons with their ISR plans. For example, in a typical joint task force (JTF) J-2 headquarters, a joint intelligence operations center (JIOC) is created. In the JIOC, the collection management (CM) and RFI sections will be most useful to Army intelligence officers as they plan ISR operations. In some cases, the collection management and dissemination sections are combined by the J-2 into one section which is referred to as collection management and dissemination (CM&D).

C-13. The joint force collection manager ensures all requests for additional ISR resources are based on validated needs as established by the command's formal intelligence requirements.

C-14. Subordinate Army commanders submit their RFIs through echelon channels and if they cannot be answered at the intermediate echelons, they are passed to the JTF RFI section for research and response. Once an RFI is returned without answer, subordinate commanders can submit a request for collection or request for ISR support to the JIOC who will apportion assets and allocate resources in order of priority as defined by the JTF commander. Collection requirements which cannot be satisfied by assets controlled or apportioned by the JTF are translated into the National intelligence system for collection.

Joint Intelligence Support Element

C-15. The Joint intelligence support element (JISE) is created at the discretion of the joint force commander to augment the J-2 element of a JTF. For Army ISR planners, the collection management operations branch section will be the interface where subordinate Army commanders' receive their ISR support from the JTF. The collection management operations branch is responsible for the JTF's ISR operations. Dynamic retasking of joint resources must be coordinated with the JISE CM operations branch.

JOINT ISR PLANNING CONSIDERATIONS

C-16. In joint collection management operations, the collection manager, in coordination with the operations directorate, forwards collection requirements to the component commander exercising tactical control over the theater reconnaissance and surveillance assets. A mission tasking order goes to the unit selected to be responsible for the collection operation. The selected unit, sometimes called the mission manager, makes the final choice of specific platforms, equipment and personnel required for the collection operations based on operational considerations such as maintenance, schedules, training and experience.

C-17. Any ISR plan involving airborne assets or resources must consider the joint air planning process. The combatant commander's air component has an Air Operations Center (AOC) that controls the airspace in AOR and all air activity above the coordinating altitude determined by the combatant commander. Therefore, the AOC must be informed of everything that is going to fly above the coordinating altitude. The AOC also "racks and stacks" ISR requirements for the assets that the Air Force Component Command controls and apportions.

C-18. Joint air planning products produced by the AOC include the air tasking order (ATO), airspace control order (ACO) and special instructions (SPINS). The ATO, ACO and SPINS provide operational and tactical direction at the appropriate levels of detail. For airborne ISR assets and resources, these products are important for ISR planners as well as mission managers and operators (i.e. UAS operators and aircraft pilots).

C-19. Army ISR planners must coordinate with the AOC through an Army unit called a battlefield coordination detachment (BCD). The BCD is the ASCC's liaison at the AOC and the BCD communicates

the land component commander's issues to the air component commander. ISR collection requests and requests for ISR support will flow through the BCD to the AOC for consideration.

C-20. The AOC sends a liaison element to the called the air component command element (ACCE) in order to communicate the air component commander's issues to the land component commander.

AIR TASKING ORDER

C-21. *Air Tasking Order* (ATO) is method used to task and disseminate to components, subordinate units, and command and control agencies projected sorties, capabilities and/or forces to targets and specific missions. Normally provides specific instructions to include call signs, targets, controlling agencies, etc., as well as general instructions (JP 3-30).

C-22. The ATO tasks aircraft to fly particular missions under specific parameters. UAS and manned airborne collection systems flying above the coordinating altitude must be in the ATO in order to fly their mission. The ATO specifies the tasking of air operations for a specific time period, normally 24 hours. The ATO planning cycle normally begins 24 hours before the period, so the total cycle is referred to as the 72-hour ATO cycle.

AIRSPACE CONTROL ORDER

C-23. *Airspace Control Order* (ACO) is an order implementing the airspace control plan that provides the details of the approved requests for airspace coordinating measures. It is published either as part of the ATO or as a separate document (JP 3-30). The ACO provides direction to de-conflict airspace and air defense plans in order to avoid mutual interference (collisions and near-miss situations), to facilitate air defense identification, to safely accommodate and expedite airflow, and prevent fratricide.

C-24. The ACO describes positive control or procedural control measures to be used in the joint operations area, designates airspace control measures, altitude restrictions, and identification procedures. For example, UAS operations require the designation of restricted operating zones (ROZ) to prohibit manned aircraft from conflicting with unmanned aircraft.

SPECIAL INSTRUCTIONS

C-25. *Special Instructions* (SPINS) are instructions issued to aviators which describe detailed procedures for loss of communications, escape and evasion, and search and rescue operations (JP 3-30). SPINS may be part of the ATO or issued as a separate document.

C-26. It is important for ISR planners to be aware of SPINS in the event that they must react to a downed aircraft or isolated Soldier incident. The SPINS can be used to anticipate the actions of Soldiers on the ground when ad-hoc ISR collection requirements arise.

ATO PLANNING CYCLES AND ISR SYNCHRONIZATION

C-27. The ATO planning cycle typically consists of three 24-hour periods:

- The 24-hour period currently being executed.
- The 24-hour period when the next order is being developed, produced, and disseminated.
- The 24-hours period when the order after next is being planned.

C-28. Submission of air mission requests or UAS mission inputs are usually required before the 72-hour ATO cycle begins. Army units having problems with an ATO or requiring an emergency change to the ATO should coordinate through the BCD. Precise timeframes for ATO planning and submission of air mission requests will be specified in the AOC SOP or OPLAN.

C-29. ISR planners may use different planning horizons for ground-based assets, however, planning for airborne ISR resources must be tied to the 72-hour ATO cycle and planned well enough in advance to get loaded into the ATO to support the commander's needs.

JOINT ISR PLANNING SYSTEMS

COLLECTION MANAGEMENT MISSION APPLICATIONS

C-30. Collection Management Mission Applications (CMMA) is a web-centric information systems architecture that incorporates existing programs sponsored by several commands, services, and agencies providing tools for recording, gathering, organizing, and tracking intelligence collection requirements for all disciplines. It facilitates the rapid and secure exchange of Collection Management (CM) data and applications and provides around-the-clock mission support to thousands of DOD personnel and end-systems operating throughout the world at multiple levels as consumers of CM information.

C-31. CMMA is used by the Air Force and is comprised of the following subsystems:

- **Battlespace Visualization Initiative** (BVI) which is a 3D graphical visualization system used to plan IMINT, SIGINT and MASINT collection by National Technical Means.
- **WEB BVI**, which is the non-3D version of BVI for lower-end workstations.
- **Flight Control®** a commercial tool providing a geospatial interface used to develop ISR situational awareness in near real-time.
- **Planning tool for Resource Integration, Synchronization and Management** (PRISM) is a collection requirement and ISR management and collaboration tool. The Army's ISR Synchronization Tool (IST) is being designed to communicate with PRISM and pass collection requirements to PRISM and approval or disapproval data back to the requestor.
- **Joint Collaborative Environment** (JCE) uses a commercial software application called InfoWorkSpace (IWS) allowing users to collaborate online in conferences and one on one chats. JCE provides far-flung users with the ability to collaborate on ISR conflicts and synchronize the collection effort.
- **Multi Asset Synchronizer** (MAS) provides critical planning and execution tools to the Air Operations Center (AOC).
- **ISR Gateway** uses CMWS applications along with data feeds from ISR assets within theater to provide situational awareness for critical ISR planning, management, tasking and reporting.

C-32. PRISM is a web-based management and synchronization tool used to maximize the efficiency and effectiveness of theater operations. PRISM creates a collaborative environment for resource managers, collection mangers, exploitation managers and customers. PRISM provides traceability throughout the intelligence cycle from planning through exploitation and production. Additionally, its synchronization matrix ensures the timely arrangement of assets (people, hardware and processes) in time and space to ensure critical intelligence is available to the commander during crisis operations. First developed for use on JWICS, it is also now being used on SIPRNET.

NATIONAL CONSIDERATIONS

C-33. Army intelligence personnel must be familiar with the various organizations in the Intelligence Community (IC) and the support they can provide to Army commanders. Chapter 2 of FM 2-0 describes the intelligence community and joint considerations.

C-34. National collection resources are leveraged against national priorities. Intelligence officers must remember that these assets are scarce and have a multitude of high priority requirements.

NATIONAL INTELLIGENCE SUPPORT TEAMS

C-35. 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. The needs of the mission dictate size and composition of NISTs.

C-36. Depending on the situation, NIST personnel are most often sent to support corps or division-level organizations. However, during recent operations in OIF and OEF, national agencies placed personnel at BCT level in some cases.

NATIONAL ISR PLANNING AND RFI SYSTEMS

C-37. The following national databases and Intelink sites contain information applicable to the IPB process and ISR planning. They should be reviewed and evaluated to determine the availability of current data, information, and intelligence products which might answer intelligence or information requirements.

- **Modernized Integrated Data Base** (MIDB) is accessible via Intelink and contains current, worldwide order of battle (OB) data organized by country, unit, facility, and equipment.
- **National Geospatial Intelligence Agency's** (NGA) **National Exploitation System** (NES) is accessible via Intelink. NES permits users to research the availability of imagery coverage over targets of interest and to access historical national imagery archives and imagery intelligence reports.
- **Country Knowledge Bases** and **Crisis Home Pages**. Many combatant command and joint force commands have Intelink websites containing the best and most up-to-date intelligence products available from the Intelligence Community.
- **Signals Intelligence** (SIGINT) **On-line Information System** (SOLIS). The SOLIS database contains current and historical finished SIGINT products.
- **Secure Analyst File Environment** (SAFE) Structured Data Files. The following databases are accessible via SAFE:
  - **Intelligence Report Index Summary File** (IRISA) contains index records and the full text of current and historical intelligence information reports.
  - **All Source Document Index** (ASDIA) contains index records and abstracts for hardcopy all-source intelligence documents produced by Defense Intelligence Agency (DIA).
- **Intelligence Collection Requirements** (ICR) is a registry of all validated human intelligence (HUMINT) requirements and taskings.
- **Modernized Defense Intelligence Threat Data System** (MDITDS). MDITDS is a collection of analytic tools that support the retrieval and analysis of information and intelligence related to counterintelligence, indications and warning, and counterterrorism.
- **Community On-Line Intelligence System for End Users and Managers** (COLISEUM). This data base application allows the user to identify and track the status of all validated crisis and non-crisis intelligence production requirements.

REQUIREMENTS MANAGEMENT SYSTEM

C-38. Requirements Management System (RMS) provides the national and DOD imagery communities with a uniform automated collection management system. RMS manages intelligence requirements for the National and DOD user community in support of the USIGS. RMS is a National Geospatial Intelligence

Agency (NGA) managed system that provides end-to-end management of national and strategic imagery collection, exploitation and dissemination. RMS enables creation, review, and approval of imagery requests; tasks requirements for collection, production, and exploitation of imagery to appropriate locations; determines satisfaction of imagery requests; can modify imagery requests based on input form other sources of intelligence and provide a suite of analytical tools for the users to exploit.

C-39. The RMS generated messages are dispatched for approval and subsequent collection and exploitation tasking. The system is central to current and future integrated imagery and geospatial information management architectures supporting national, military, and civil customers.

C-40. Nominations management services provide the coordination necessary to accept user requirements for new information; aggregate, assign, and prioritize these requirements; and track requirement satisfaction.

NATIONAL SIGINT REQUIREMENTS PROCESS

C-41. The national SIGINT requirements process (NSRP) is an integrated and responsive system of the policies, procedures and technology used by the Intelligence Community to manage requests for national-level SIGINT products and services. The NSRP replaced the previous system called national SIGINT requirement system (NSRS).

C-42. The NSRP establishes an end-to-end cryptologic mission management tracking system using information needs (INs). SIGINT collectors satisfy tactical through national level consumers information needs based on NSRP guidance. The NSRP improves the consumer's ability to communicate with the collector by adding focus and creating a mechanism for accountability and feedback

C-43. Information needs (IN) are used in NSRP to relay the collection requirements to SIGINT collectors and systems. INs are prioritized and classified according to standardized time categories. Research IN priorities involve limited efforts and only exist for a defined period of time using existing data (no new collection is required). Limited duration INs require collection and production over a period of 0-90 days. Standing INs require sustained collection over periods exceeding 90 days and up to two years.

C-44. INs are further prioritized based on how quickly the SIGINT community must react to the request for collection.

- Routine INs require action in 30 or more days.
- Time sensitive INs require actions within 4 to 29 days after submission.
- Time critical INs must be acted upon within the first 3 days after submission.

C-45. Requests for national SIGINT collection must be sponsored at the national level, validated by the Intelligence Community, and prioritized among all the other competing requirements.

MULTINATIONAL INTELLIGENCE OPERATIONS

C-46. There is no single intelligence doctrine for multinational operations. Each coalition or alliance must develop its own unique procedures.

C-47. In multinational operations, the multinational force commander exercises command authority over a military force composed of elements from two or more nations. Therefore, in most multinational operations, the JTF must share intelligence, as necessary, for mission accomplishment with foreign military forces and coordinate the exchange of intelligence liaisons with those forces.

C-48. Command and control of ISR resources may remain essentially national or they may be integrated into a combined command and control structure. Either way, intelligence remains a national responsibility and most nations with a significant presence in the combined force will establish a national intelligence cell (NIC).

C-49. US units subordinated to non-US headquarters may require augmentation with linguists or bilingual liaison officers, 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. Connectivity to US networks is critical to success in a coalition environment.

C-50. Intelligence officers should 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.

ALLIANCES

C-51. Army units frequently perform intelligence operations in a multinational environment within the structure of an alliance or coalition, which presents many additional challenges for intelligence personnel. North Atlantic Treaty Organization (NATO) and the UN Command in the Republic of Korea are examples of highly structured and enduring alliances. Intelligence architectures, organizations and procedures are well defined in alliances. Therefore, U.S. Army intelligence officers must learn to operate within the parameters of an alliance, maintaining SOPs and standards in accordance with their unit policies, but also complying with the alliance's standardized agreements.

C-52. The advantage to an alliance is existing international standardization agreements (for example, North Atlantic Treaty Organization standardization agreements or STANAGs). These arrangements establish 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.

COALITIONS

C-53. Other multinational military organizations, such as the coalitions formed during the Gulf War and the global war on terrorism (GWOT), are temporary or ad hoc organizations formed for a particular mission. Coalitions require a great deal more adaptation and improvisation in order to achieve success. Often times, the coalition comes together on a short notice basis and the arrangements for collaboration and intelligence sharing must be hammered out while the planning process is underway.

C-54. In some stability and support operations, the JTF might require the authority to go outside the usual military channels in order to provide information to non-governmental organizations (NGO) or other governments and agencies in order to achieve the commander's intent. The JTF must tailor its intelligence policies and dissemination guidance to each multinational operation because they are all unique.

INTELLIGENCE COLLABORATION

C-55. ISR synchronization operations in a combined environment can be confounded by language issues, differing tasking and request channels and formats, information classification and foreign disclosure concerns, and national sensitivities. Troop contributing nations may have political or rules of engagement constraints, which limit their ability to perform certain missions.

C-56. 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.

C-57. 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.
- Develop procedures for review to expedite sanitization and sharing of US-generated intelligence products with allies and multinational partners.
- Communicate friendly objectives, intentions, and plans to appropriate intelligence organizations.

- Ensure interoperability of command, control, and communication systems. This is achieved by placing a common coalition intelligence system, such as CENTRIX-S, in all the headquarters and subordinate units to facilitate communications.

Similarities and Differences

C-58. 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.

C-59. 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.

C-60. 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.

Foreign Disclosure Considerations

C-61. It is imperative that combined forces commanders establish a system that optimizes each nation's contributions and strengths. All units under the multinational headquarters are entitled to reliable intelligence. U.S. 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.

C-62. In ISR operations, there are always constraints to foreign disclosure due to the technical nature of the data, imagery, or intelligence product disseminated after ISR operations. Practices such as "write for release" become very important in facilitate intelligence sharing. Whenever possible tear line reports and releasable imagery should be obtained in order to share with coalition or alliance partners.

C-63. Likewise, the other nations in the multinational headquarters must be encouraged to share their intelligence information for the benefit of everyone involved. Many nations have a long tradition of "stove-piping" intelligence and will find it difficult to learn different methods of dissemination.

SYSTEMS COMPATIBILITY

C-64. Many instances in recent intelligence operations in OIF and OEF illustrate the fact that compatibility is always as issue to be considered in ISR planning. For example, in OIF the Romanian Intelligence Group at Multinational Division-Central South operated a Shadow UAS. However, their model was different than the Shadow UAS operated by the U.S. Army. Therefore, when spare parts became a problem for Romanian forces, a rapid analysis was completed to determine if there were common parts between the two different models. (See figure C-3)

C-65. Connectivity is another ISR related issue that must be considered in multinational environments. Even though many U.S. airborne collection platforms use a common data link can connect to several ground station systems such as one system remote video terminal (OS-RVT) and remote optical video enhanced receiver (ROVER), many foreign airborne systems cannot and must use their own unique ground station systems.

C-66. Coalitions may have multiple communications systems that do not connect. Each nation in a coalition will bring its own internal systems, but most nations rely on the United States to provide a

common communications system. The importance of placing American liaison officers at the coalition countries' headquarters cannot be understated because of the systems compatibility issues that frequently arise.

Figure C-3. The Romanian Intelligence Group UAV in OIF

MULTINATIONAL ISR SYNCHRONIZATION

C-67. When a multinational commander and staff consider their ISR plan, they must contemplate all of the unique and varied resources in the coalition units under their command. This may require an exchange of information on performance characteristics, capabilities, limitations, range, dwell time, sustainment requirements, and data conversion capabilities.

C-68. Frequently, coalition unit commanders who do not have a robust ISR capability will ask for U.S. support. Policies and procedures for establishing requirements, requesting collection or support, and transmitting the data or finished intelligence to the coalition partner have to be worked out by the higher headquarters J-2/G-2/S-2.

C-69. To the extent that ISR synchronization is a process that contemplates all organic and non-organic assets or resources available to the commander, the coalition contribution is important to understand so that it can be effectively and efficiently employed toward answering the CCIR.

Appendix D

DCGS-A Enabled Intelligence, Surveillance, and Reconnaissance Planning and Operations

BACKGROUND

D-1. The DCGS-A program was created in response to the DOD Distributed Common Ground/Surface System (DCGS) Mission Area Initial Capabilities Document, which captured the overarching requirements for ISR that will contribute to joint and combined Warfighter needs. DCGS-A facilitates "Seeing and Knowing" on the battlefield—the fundamental precursor to the understanding that underpins the Army's battle command.

SYSTEM OBJECTIVES

D-2. DCGS-A provides a net-centric, enterprised ISR, weather, geospatial engineering, and space operations capability to maneuver, maneuver support and maneuver sustainment support 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.

D-3. DCGS-A provides the capabilities necessary for commanders to access information from all data sources and to synchronize organic and non-organic sensors. DCGS-A provides continuous acquisition and synthesis of data and information from joint and interagency capabilities, multinational partners, and nontraditional 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 the full spectrum of operations.

D-4. 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.
- Reconnaissance and surveillance integration.
- Fusion of sensor information.
- Distribution of relevant threat data and information.
- Friendly and environmental (weather and terrain) information.

D-5. The currently fielded version is v3.1. Future iterations of DCGS-A will be a net-centric, web-enabled, enterprise-based, open-architecture system of systems deployed across the force in support of ground forces 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 reach activities. The DCGS-A objective architecture will be capable of supporting multiple, simultaneous, worldwide operations through scalable and modular system deployments.

OPERATIONAL DESCRIPTION

D-6. DCGS-A is the Army's ground processing system for 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 facilitating Reach Operations with Knowledge Centers.

D-7. DCGS-A provides access to JWICS, NSANet, SIPRNET, and NIPRNET. DCGS-A links tactical ISR sensors along with weather, space, and geospatial analysis capabilities into the Intelligence Enterprise. The DCGS-A net-centric capability enhances distributed operations by allowing ISR data access down to tactical units. Additionally, it provides the analyst data mining, fusion, collaboration, and visualization tools to conduct situational awareness, ISR synchronization, targeting support, analysis, and reporting.

D-8. DCGS-A 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. The DIB enables DCGS-A to task, process, post, and use data from Army, Joint, and National ISR sensors. The DIB provides a meta-data catalog that defines how you describe data. The meta-data allows DCGS-A to expose the required data elements to the user.

D-9. DCGS-A is 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.

D-10. DCGS-A tools support the targeting process as well as synchronize ISR collection. DCGS-A provides the analyst access to national theater data sources and serves as a ground station processor for ISR sensors. DCGS-A facilitates distributed operations and reduces the forward physical footprint.

DCGS-A CONFIGURATIONS

D-11. There are three major DCGS-A configurations: embedded, mobile, and fixed.

EMBEDDED

D-12. 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-INT 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. 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.

D-13. 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 Battle Command, DCGS-A permeates the entire Army force structure to facilitate combat and staff functions.

DCGS-A MOBILE

D-14. 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 can 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.

D-15. 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 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.

D-16. The man-portable system is the Multi-Function Workstation-Mobile (MFWS-M) and the vehicle transportable system is titled the Mobile Intelligence Service Provider (MISP). Each MISP will contain a mixture of Multi-Security Level-Multi-Function Workstations (ML-MFWSs) 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. 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

D-17. 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 ISR processing, exploitation, analysis, and production support to all echelons.

DCGS-A INCREMENTAL DEVELOPMENT

D-18. 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. Increment 2 systems will be designed to support the threshold system requirements. This should allow Increment 3 upgrades to be executed as software modifications to fielded systems. DCGS-A fielding was accelerated and delivered incrementally based on operational requirements associated with the war on terrorism.

D-19. The incremental development includes consolidation and replacement of the capabilities found in the following current force systems:

- All versions of ASAS.
- CI & Interrogation Workstation.
- All versions of the Tactical Exploitation System.

- All versions of the GRCS ground processors (for example, the Integrated Processing Facility and the Guardrail Ground Baseline).
- Incorporation of the ISR synchronization tool (formerly known as Collection Management Tool).
- PROPHET Control.
- JSTARS CGS.
- Digital Topographical Support System-Light (DTSS-L).
- IMETS.
- Space Support Enhancement Toolset.

ISR SYNCHRONIZATION TOOL (IST)

D-20. The ISR Synchronization Tool (IST) (formerly known as Collection Management Tool or CMT) allows commanders to visualize and direct ISR operations using organic and non-organic assets and resources.

D-21. IST will aid intelligence officers across the force in performing the following functions:

- Development and tracking of indicators, SIR, and ISR tasks.
- Matching ISR tasks to assets, resources, and sensors ensuring the right sensor with the right priority is placed on the right NAI, TAI, or target.
- Providing a set of automated tools to assist in ISR planning including simultaneous integration and synchronization ISR assets, resources, and sensors at all echelons
- Providing 100% ISR planning and execution visibility to all users on the network with access to IST or the IST-enabled web pages for asset visibility.
- Correlating NAIs and TAIs with IST tasks and assets using a mapping software toolset built into the IST application.
- Dynamically submitting and managing requests for collection or requests for intelligence information with feedback to the requestor from higher echelons.
- Alerting ISR planners of changes or significant events during execution of the ISR plan for asset visibility.
- Facilitating ISR planning in support of COA analysis (wargaming).
- Enabling Commanders and staffs to manage the collection effort at multiple echelons (battalion through Joint) to ensure integration with operational plan.
- Providing the intelligence officer with an overall view of the collection effort, including his higher headquarters' and adjacent units' plans.
- Exportable formats using Microsoft Excel for coordination and collaboration with non-IST users.

D-22. Some of the features of IST are shown in figures D-1 and D-2.

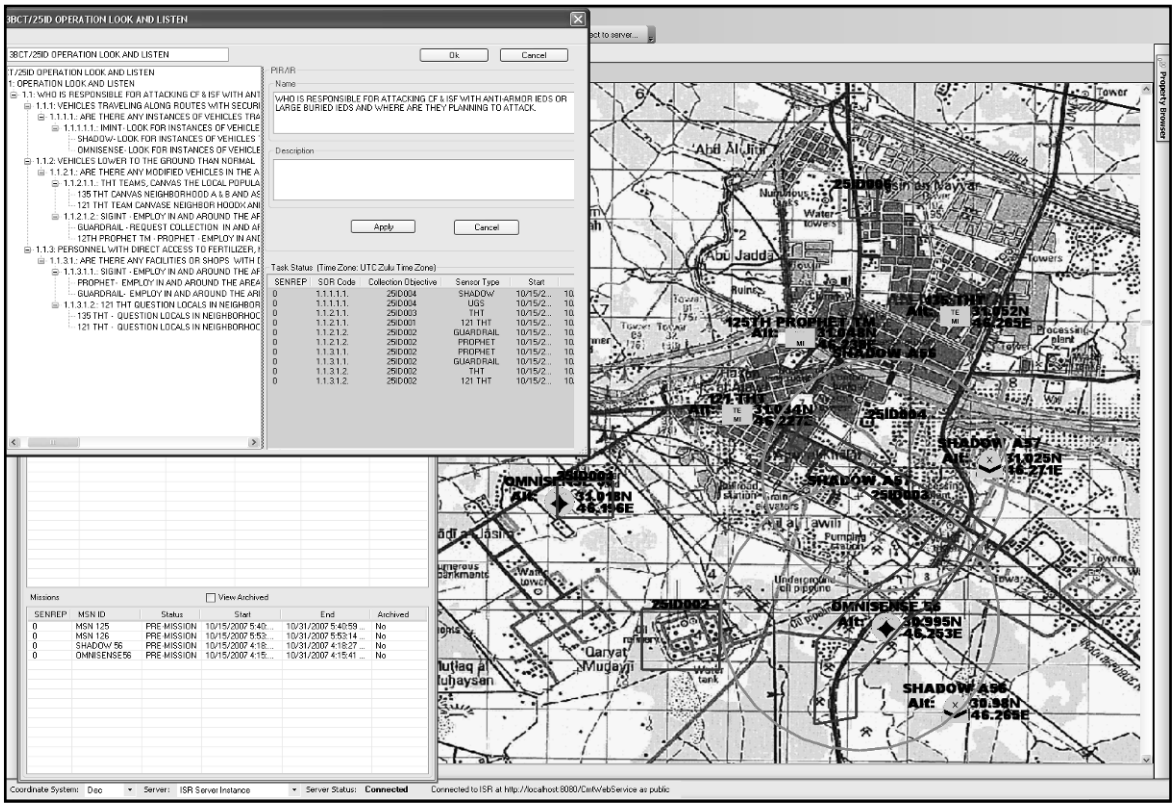

Figure D-1. IST requirements management and overlay capabilities

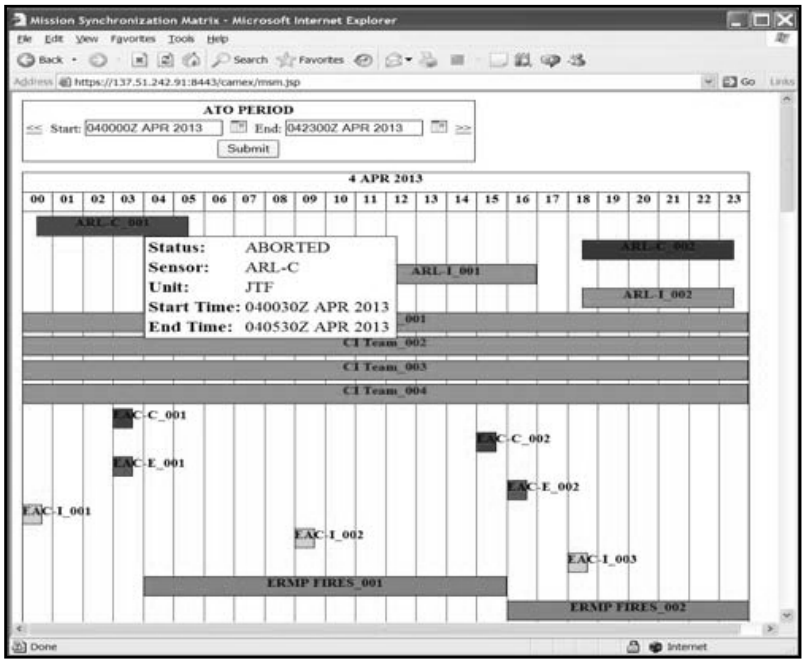

Figure D-2. ISR synchronization matrix produced using IST

BACKGROUND

D-23. CMT was originally designed by the Battle Command Battle Lab at Fort Huachuca (BCBL-H) to support a battle command experiment. The Soldiers who used CMT liked it so much that they requested a "live" version for their use in Afghanistan.

D-24. The first CMT version (v 1.08) was fielded in Operation Enduring Freedom with the 10th Mountain Division in 2006. Although the architecture underlying CMT was not robust enough to handle the large number of real world users in that theater of operations, it was proven that the software was capable of fulfilling the users needs for ISR synchronization planning and ISR mission management functions.

D-25. Based on user inputs, real world operational needs and DCGS-A developmental requirements, the BCBL-H rapidly re-engineered CMT to be fully integrated into DCGS-A as well as maintain a stand-alone capability that could handle a large numbers of users. Additionally, BCBL-H in conjunction with TCM Sensor Processing (TCM-SP) expanded the scope of user requirements based off a Military User Assessment (MUA) conducted in OIF in August/September of 07.

D-26. During 2008, the latest version of CMT was renamed Intelligence Synchronization Tool (IST) in accordance with doctrinal changes promulgated in FMI 2-01. All future versions of this application will bear the name IST.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

ACE	analysis and control element
ACO	airspace control order
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
ATO	air tasking order
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
CIST	company intelligence support team
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
IMINT	imagery intelligence
IPB	intelligence preparation of the battlefield
IR	information requirement
ISR	intelligence, surveillance, and reconnaissance
JFACC	Joint Force Air Component Commander
JFLCC	Joint Force Land Component Commander
JFC	joint force commander
JIC	Joint Intelligence Center
JIOC	joint intelligence operations center
JISE	joint intelligence support element
Joint STARS	Joint Surveillance Target Attack Radar System
JOPP	joint operation planning process
JTF	joint task force
LNO	liaison officer
LEIOV	latest event information is of value
LTIOV	latest time information is of value
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
SPINS	special instructions
TAI	targeted area of interest
UAS	unmanned aircraft system
USAR	United States Army Reserve
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.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

DODD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 25 April 1988

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

ARMY PUBLICATIONS

AR 380-10, *US Army Intelligence Activities*, 25 April 2007

FM 1-02 (101-5-1), *Operational Terms and Graphics*, 21 September 2004

FM 2-0, *Intelligence* (when published in 2009)

FM 3-0, Operational Terms and Graphics, 27 February 2008

FM 3-55, *Intelligence, Surveillance, and Reconnaissance*, (when published in 2009)

FM 3-90, *Tactics*, 4 July 2001

FM 5-0, *The Operations Process*, (when published in 2009)

FM 5-1, *The Planning Process*, (when published in 2009)

FM 6-0, *Mission Command: Command and Control of Army Forces*, 11 August 2003

FM 7-15, *The Army Universal Task List (AUTL),* (when published in 2009)

FMI 5-0.1, *The Operations Process*, 31 March 2006, with *Change 1*, dated 14 March 2008

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.

DOCUMENTS NEEDED

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

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 and support Operations*, 20 February 2003, with Change 1 dated 30 April 2003

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*, 12 February 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*, 13 December 2001

FM 7-93, *Long-Range Reconnaissance 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*, 25 November 1996

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, with Change 1, dated 7 May 2008

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

DOCUMENTS UNDER DEVELOPMENT

These sources are documents that are in some stage of development and projected to be finalized in 2009

FM 2-01.3, *Intelligence Preparation of the Battlefield*

FM 2-19.4, *Brigade Combat Team Intelligence Operations*

FMI 2-01.301, *Tactics, Techniques, and Procedures for Intelligence Preparation of the Battlefield*

FMI 2-01.501, *Intelligence Support to Civil Support Operations*

Index