FM 3-05.102
(FM 34-36)

ARMY SPECIAL OPERATIONS FORCES INTELLIGENCE

July 2001

DISTRIBUTION RESTRICTION:
Distribution authorized to U.S. Government agencies and their contractors only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This determination was made on 5 December 2003. Other requests for this document must be referred to Commander, United States Army John F. Kennedy Special Warfare Center and School, ATTN: AOJK-DT-JAA, Fort Bragg, North Carolina 28310-5000.

DESTRUCTION NOTICE:
Destroy by any method that must prevent disclosure of contents or reconstruction of the document.

Headquarters, Department of the Army

***FM 3-05.102**

Field Manual
No. 3-05.102

Headquarters
Department of the Army
Washington, DC, 31 August 2001

Army Special Operations Forces Intelligence

Contents

Page

PREFACE v

Chapter 1 **OPERATIONS AND ARSOF** 1-1

Introduction 1-1
Range of Military Operations 1-1
Army Special Operations Forces 1-7
Army Special Operations Characteristics 1-10
ARSOF Truths 1-11
Special Operations Mission Criteria 1-11
Army Special Operations Imperatives 1-12
ARSOF Missions 1-15
ARSOF Collateral Activities 1-18
Targeting and Mission Planning 1-19

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies and their contractors only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This determination was made on 5 December 2003. Other requests for this document must be referred to Commander, United States Army John F. Kennedy Special Warfare Center and School, ATTN: AOJK-DT-JAA, Fort Bragg, North Carolina 28310-5000.

DESTRUCTION NOTICE: Destroy by any method that must prevent disclosure of contents or reconstruction of the document.

---

*This publication supersedes FM 34-36, 30 September 1991.

Page

Chapter 2 ARSOF AND THE INTELLIGENCE AND ELECTRONIC WARFARE SYSTEM ...2-1
Introduction 2-1
ARSOF IEW Characteristics 2-3
Integrating IEW With Operations 2-5
Intelligence in the Military Decision-Making Process 2-7
Intelligence Cycle 2-9
Characteristics of Effective Intelligence 2-13
Intelligence Disciplines 2-14
ARSOF Intelligence Tasks 2-17

Chapter 3 IEW SUPPORT TO SPECIAL FORCES OPERATIONS 3-1
Introduction 3-1
SF Missions 3-1
SF Intelligence Organization 3-5
Deployed SF 3-15
SF IEW Roles and Functions 3-17
Other Organic Intelligence Assets 3-23
Nonorganic IEW Support to SF 3-23
IEW Support From Higher Headquarters 3-23

Chapter 4 IEW SUPPORT TO RANGER OPERATIONS 4-1
Introduction 4-1
Ranger Missions 4-1
Ranger Intelligence Organization 4-2
Other Organic Support 4-5
Nonorganic IEW Support to Ranger Regiment 4-6
Ranger Support to IEW System 4-7

Chapter 5 IEW SUPPORT TO ARSOA 5-1
Introduction 5-1
Missions and Organization 5-1
Organic Intelligence Assets 5-2
ARSOA Intelligence Operations 5-4
External IEW Support 5-5
Other Nonorganic Support 5-7

Chapter 6 IEW SUPPORT TO PSYOP 6-1
Introduction 6-1

Page

Missions 6-1
Organization 6-2
PSYOP Intelligence Organization 6-3
Other Organic Support 6-4
PSYOP Analysis Process 6-6
Nonorganic IEW Support to PSYOP 6-6
Intelligence Disciplines Supporting PSYOP 6-8
Other Nonorganic Support 6-9
PSYOP Support to IEW 6-10
Information Operations 6-11

Chapter 7 IEW SUPPORT TO CIVIL AFFAIRS 7-1
Introduction 7-1
Missions 7-1
Organization 7-2
Intelligence Requirements 7-8
CA Intelligence Organization 7-9
CMO Preparation of the Battlespace 7-10
Nonorganic IEW Support to CA 7-11
Other Nonorganic Support 7-12
CA Support to IEW System 7-13

Chapter 8 ARSOF IEW SUPPORT SYSTEMS AND ARCHITECTURE 8-1
Introduction 8-1
Connectivity, Architecture, and Systems 8-1
ARSOF IEW Systems 8-4
ARSOF Databases 8-9
ARSOTF IEW Architecture and Support Channels 8-10
MACOM IEW Support 8-11
Department of the Army IEW Support 8-21
Joint and Theater-Level IEW Support 8-22
National-Level IEW Support 8-28

Appendix A MULTINATIONAL AND INTERAGENCY INTELLIGENCE A-1
Doctrine for Multinational Operations A-1
Multinational Intelligence Architecture A-1
Joint and Multinational Doctrine Relationship A-1
Multinational Intelligence Principles A-2

Page

Interagency Intelligence A-4

Appendix B **SPECIAL OPERATIONS MISSION PLANNING FOLDER FORMAT** B-1
Part 1: Mission Tasking Package B-1
Part 2: Feasibility Assessment B-2
Part 3: Target Intelligence Package B-2
Part 4: Plan of Execution B-5
Part 5: Mission Support Plans B-6

Appendix C **SPECIAL OPERATIONS FORCES TARGET INTELLIGENCE PACKAGE** C-1
DA and SR Missions C-1
FID and UW Missions C-3

GLOSSARY Glossary-1
BIBLIOGRAPHY Bibliography-1
INDEX Index-1

Preface

Field Manual (FM) 3-05.102 provides the United States (U.S.) Army special operations forces (ARSOF) commander and his staff a broad understanding of intelligence support to ARSOF. This manual also provides guidance for ARSOF commanders who determine the force structure, budget, training, materiel, and operational requirements needed to prepare organic military intelligence (MI) assets to conduct their missions and collateral activities. This Service doctrine is consistent with joint doctrine. ARSOF need relevant, accurate, predictive, and timely intelligence and information to—

- Identify and develop targets.
- Plan missions.
- Secure the element of surprise.
- Protect the force.
- Protect friendly command, control, communications, computers, and intelligence (C4I).

These actions take place across the full range of military operations, including war and military operations other than war (MOOTW).

FM 3-05.102 is the integrating manual for intelligence support to ARSOF. The acronym "ARSOF" represents Special Forces (SF), Ranger, Army special operations aviation (ARSOA), Psychological Operations (PSYOP), and Civil Affairs (CA). FM 3-05.102 is an ARSOF subordinate doctrine publication and expands upon the doctrine in FM 3-05, *Army Special Operations Forces Doctrine* (currently published as FM 100-25, *Doctrine for Army Special Operations Forces*). It should be used with FM 3-05 and not independently. (Figure Preface-1, page vii, depicts the ARSOF doctrinal and training publication architecture.)

FM 3-05.102 describes the missions and functions of intelligence elements and organizations that provide intelligence and electronic warfare (IEW) support to ARSOF organizations. It provides an overview of ARSOF IEW capabilities, including the organization, missions, and functions of ARSOF MI assets, and connectivity from the level of the ARSOF battalion S2 section to national-level intelligence organizations. It shows how organic and nonorganic IEW assets meet ARSOF operational needs within the IEW system. It is authoritative doctrine for use by Active Army and Reserve Component (RC) ARSOF units and any other units or personnel operating with or supporting them.

This manual is unclassified to ensure ARSOF-wide dissemination and to facilitate the integration of intelligence in the planning, execution, and coordination of major operations. For a thorough understanding of intelligence support within the joint and land component environment, readers must also reference the following joint publications (JPs) and Army FMs:

- JP 2-0, *Doctrine for Intelligence Support to Joint Operations.*
- JP 2-01, *Joint Intelligence Support to Military Operations.*

- JP 2-02, *National Intelligence Support to Joint Operations*.
- FM 34-1, *Intelligence and Electronic Warfare Operations*.
- FM 34-2, *Collection Management and Synchronization Planning*.
- FM 34-8, Combat Commander's Handbook on Intelligence.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

The proponent of this publication is the U.S. Army John F. Kennedy Special Warfare Center and School (USAJFKSWCS). Submit comments and recommended changes to Commander, USAJFKSWCS, ATTN: AOJK-DT-JAA, Fort Bragg, North Carolina 28310-5000.

This manual does not implement any International Standardization Agreements (ISAs).

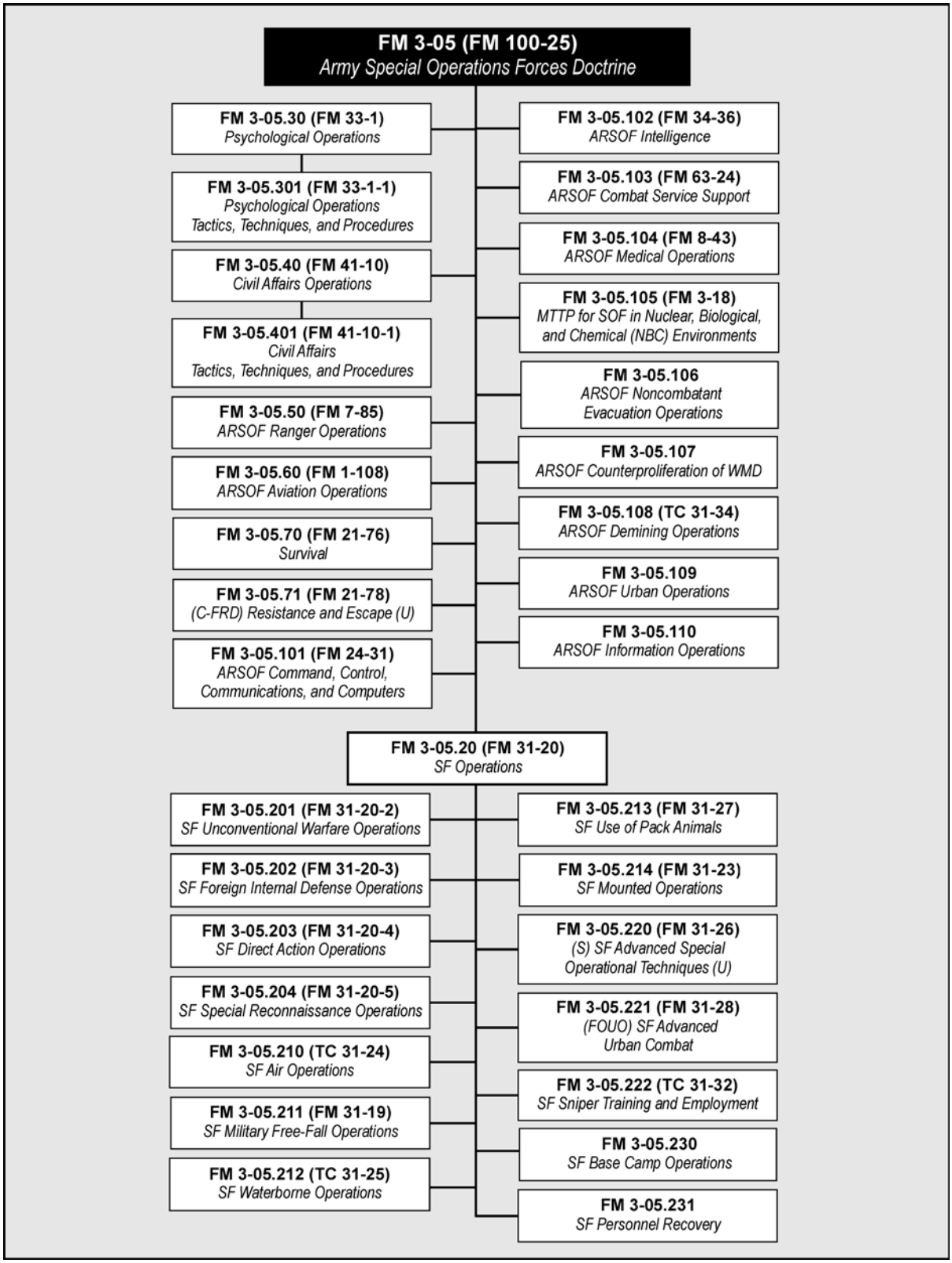


Figure Preface-1. ARSOF Doctrinal and Training Publications Architecture

Chapter 1

Operations and ARSOF

This chapter describes the range of military operations, characteristics of ARSOF units and their missions, and considerations for their employment. It provides an overview of concepts addressed in FM 3-05 (FM 100-25). The fundamental purpose of ARSOF intelligence operations is to provide the commander with the information required to visualize the adversary and the environment. This support will enable ARSOF to successfully conduct worldwide special operations (SO) throughout the range of military operations supporting the geographic combatant commanders, American ambassadors and their country teams, and other government agencies.

INTRODUCTION

1-1. ARSOF are specifically organized, trained, and equipped to conduct SO independently or in conjunction with the operations of Army conventional forces, joint forces, and/or combined forces. ARSOF support the national security strategy by—

- Enhancing security with their unique military capabilities.
- Promoting prosperity by supporting global and domestic stability.
- Promoting security through the development and preservation of democracy.

RANGE OF MILITARY OPERATIONS

1-2. ARSOF conduct operations throughout the range of military operations (war and MOOTW). ARSOF provide geographic combatant commanders additional means to shape the environment and respond to crises, while preparing for future requirements (Figure 1-1, page 1-2). ARSOF can support the joint force commander (JFC) at all levels—strategic, operational, or tactical—as follows:

- The *strategic level* concerns the broadest aspects of national and theater policy. Decisions at this level reflect national and multinational goals, integrate all the instruments of national power, provide forces, and determine constraints and restraints on their use. The National Command Authorities (NCA) and the geographic combatant commanders determine the strategic-national and strategic-theater objectives and the manner of use of military means to achieve them. The NCA or the geographic combatant commanders may directly or indirectly (through subordinate commanders) employ ARSOF in pursuit of these objectives.

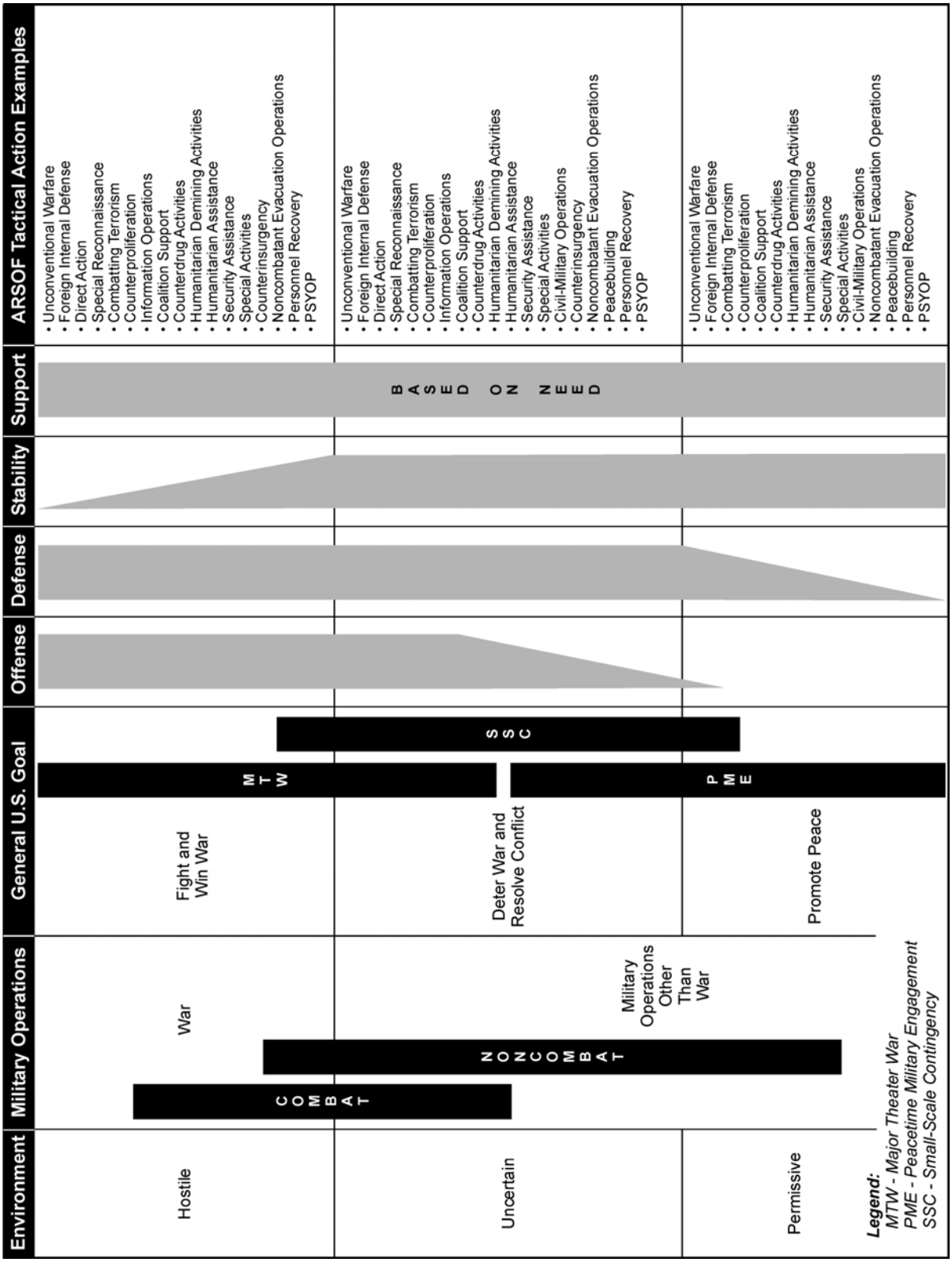


Figure 1-1. Range of Military Operations

- The *operational* level focuses on theater campaigns and major operations. Joint force commanders determine operational objectives that lead to the attainment of strategic-theater objectives. These objectives are attained through the design, organization, and conduct of campaigns and major operations that, in turn, guide tactical events. A geographic combatant commander, subordinate unified command commander, joint task force (JTF) commander, Service component commander, or functional component commander may employ ARSOF as part of a joint force to attain these operational objectives.
- The *tactical* level focuses on battles and engagements. Decisions at this level apply combat power to create advantages while in contact with or close to the enemy. ARSOF conduct tactical actions (offense, defense, stability, and support actions) designed to have significant effect in attaining operational objectives. PSYOP and CA tactical actions may directly attain tactical, operational, and strategic objectives at the same time.

1-3. The following paragraphs describe ARSOF applicability to the environment within the range of military operations. ARSOF are land oriented; their operations include a variety of offense, defense, stability, and support actions that help attain joint force dominance in war and MOOTW. In war, ARSOF normally conduct SO that support the theater campaign and major operations of subordinate forces. In MOOTW, ARSOF may conduct operations outside the continental United States (OCONUS) in a geographic combatant commander's area of responsibility (AOR). For example, an OCONUS operation could be in a foreign country supporting a U.S. ambassador or in a joint operations area in accordance with (IAW) a command relationship established by the designated JFC. In either situation, ARSOF offer viable military options, particularly when the situation calls for subtle, indirect, or low-visibility approaches. The small size, unique capabilities, and self-sufficiency (for short periods) of ARSOF provide the United States with feasible and appropriate military responses. These responses do not entail the degree of political liability or risk of escalation normally associated with employment of inherently larger and more visible conventional forces. Just as ARSOF may support other component (conventional) forces of a joint force, conventional forces also may support ARSOF missions. In any situation, the conduct of SO must support the JFC's goals, objectives, and concept of operation. Campaign and contingency planning address SO as part of these joint, multinational, and interagency efforts. ARSOF are most successful when integrated early into these types of activities.

WAR

1-4. War is large-scale, sustained combat between nations or organized groups within a nation. War involves regular and irregular forces in a series of connected battles and campaigns to achieve vital national, tribal, or ethnic objectives. War may be limited, with some self-imposed restraints on resources or objectives. It also may be general, with the total resources of a nation or nations employed and the survival of the nation at stake.

1-5. ARSOF can support a JFC in war through the conduct of a variety of offense, defense, stability, and support actions. These actions may either

directly accomplish the JFC's objectives or indirectly attain these objectives through the directed support to other subordinate forces of the JFC. In war, ARSOF are not normally the main effort, but rather supporting forces to the major air, land, and maritime combat forces.

1-6. SO missions may require unorthodox approaches, but these approaches do not negate the traditional principles of war. Rather, they place a different emphasis on their combination or relative importance. In some SO missions, surprise achieved through speed, stealth, audacity, deception, and new tactics or techniques can be far more effective and efficient than traditional conventional tactics that are based on massed firepower and tactical maneuvers. The following discussion of the principles of war highlights their application to ARSOF.

Objective

1-7. *Direct every military operation toward a clearly defined, decisive, and attainable objective.* ARSOF objectives are as much political, economic, and informational as they are military in nature. ARSOF planners must avoid adding a secondary objective by balancing risks versus gain. They must have a clear understanding of the capabilities and limitations of ARSOF. The addition of secondary objectives erodes the definition and decisiveness of the primary objective.

Offensive

1-8. *Seize, retain, and exploit the initiative.* ARSOF are inherently offensive in nature because they seek to strike or engage an adversary to compel, deter, or counter his actions. The strike or engagement conducted by ARSOF may take place alongside or by effect of a surrogate force. This force may be one that ARSOF has previously trained or is currently training. CA and PSYOP exploit the initiative by gaining the support of the civilians in the area of operations (AO).

Mass

1-9. *Mass the effects of overwhelming combat power at the decisive time and place.* ARSOF concentrate the effects of combat power at critical times and discriminate selected targets to achieve decisive results that accomplish the commander's objectives.

Economy of Force

1-10. *Employ all combat power available in the most effective way possible; allocate minimum essential combat power to secondary efforts.* ARSOF are used as an essential economy of force when military objectives are subordinate to political, economic, and informational objectives. Like PSYOP, CA and SF may preempt hostilities through stability operations, support operations, or humanitarian work. Such actions, in turn, may eliminate the need for escalation and the introduction of conventional forces.

Maneuver

1-11. *Place the enemy in a disadvantageous position through the flexible application of combat power.* ARSOF conduct maneuvers in the classical

sense on the strategic and operational battlefields. ARSOF possess a tremendous capability to gain a position of advantage for the geographic combatant commander, particularly when applying decisive combat power in an adversary's "rear area."

Unity of Command

1-12. *For every objective, seek unity of command and unity of effort.* Theater special operations command (SOC) commanders under the geographic combatant commanders can tailor the command and control (C2) architecture for ARSOF operations in one of two ways. The theater SOC commander can either place C2 under the direct control of the SOC or recommend subordinate joint force command relationships to ensure unity of effort of special operations forces (SOF). PSYOP and CA forces and staff are generally under the operational control (OPCON) of the theater commander, not the theater SOC. Therefore, integration, synchronization, and unity of effort for these forces are incumbent upon commanders and staffs at every level.

Security

1-13. *Never permit the enemy to acquire an unexpected advantage.* ARSOF can provide security to the JFC by denying an adversary the ability to use his "expected" advantages. They provide security through various intelligence collection methods, force protection (FP), and force applications.

Surprise

1-14. *Strike the enemy at a time and place or in a manner for which he is unprepared.* ARSOF can inhibit an adversary's decision making, deceive an adversary, or restrict an adversary's capability to react to the commander's operations or campaign.

Simplicity

1-15. *Prepare clear, uncomplicated plans and concise orders to ensure a thorough understanding.* ARSOF use unorthodox and sophisticated methods and equipment. The plans and procedures the force employs must be simple and direct to facilitate understanding, to withstand the stress of operational environments, and to allow for rapid adaptation to changing situations.

1-16. Regardless of the level of violence or scope of military involvement in MOOTW or war, nonmilitary instruments of power frequently support the military in its goal of defeating the enemy. Such defeat need not necessarily come from the annihilation of the enemy's military force. It may come from the destruction of the enemy's ability or will to continue. Selectively attacking a limited set of critical military, political, informational, and economic targets may achieve a cessation of hostilities and thereby avoid total or protracted war.

MILITARY OPERATIONS OTHER THAN WAR

1-17. MOOTW help shape the environment and respond to crises with the goal of deterring war, resolving conflict, and promoting peace. As described in JP 3-0, *Doctrine for Joint Operations*, MOOTW can consist of a peaceful

application of the military or involve the use or threat of military force. MOOTW may take place in permissive, uncertain, or hostile environments as defined in FM 3-0, *Operations*.

1-18. ARSOF can conduct tactical offensive, defensive, stability, and support actions in MOOTW. Examples of ARSOF tactical offensive actions in MOOTW are direct action (DA) and combatting terrorism (CBT). Examples of defensive actions are antiterrorism, foreign internal defense (FID), and certain types of PSYOP. FID is an example of a stability action. Counterdrug (CD) and humanitarian assistance (HA) are examples of support activities.

1-19. In many cases, the prime consideration in MOOTW involves providing information to influence the behavior and organize the activities of the local population. Selected ARSOF are particularly suited for MOOTW because of their functional expertise, region or country familiarity, and proficiency in target language and cultural skills.

1-20. Regular demonstrations of ARSOF readiness and capabilities in multinational exercises with host nation (HN) and allies worldwide contribute to deterrence. These demonstrations also provide a subtle, low-visibility means of extending U.S. influence. Likewise, ARSOF also contribute to the attainment of peacetime military objectives and may promote regional stability by advising, training, and assisting HNs and allies.

1-21. Complementing the principles of war are the principles of MOOTW. These principles consider the limited nature of MOOTW and the increased role of interagency and multinational activities.

Security

1-22. *Never permit hostile factions to acquire a military, political, or informational advantage.* ARSOF provide the JFC experts in numerous intelligence-gathering techniques, FP, CBT, and physical security measures. ARSOF personnel are trained to interact with U.S. and HN military and civilian personnel. Training provided ARSOF personnel gives them the ability to gain insights into the attitudes and beliefs of the culture and its willingness to use force against friendly forces.

Legitimacy

1-23. *Committed forces must sustain the legitimacy of the operation and the HN, where applicable.* A majority perception of the legality, morality, or righteousness of a set of actions is the basis for legitimacy. ARSOF's concern for human rights, demonstrated in educating local security forces and in the behavior of ARSOF themselves, can do much to enhance legitimacy on behalf of the local military.

Objective

1-24. *Direct every military operation toward a clearly defined, decisive, and attainable objective.* Selected ARSOF may be dominant in the MOOTW environment and may be decisive with support from the conventional forces. ARSOF (SF, CA, and PSYOP units) have theater-specific and regional orientation. Because of this orientation and their frequent deployments into their designated theater, these ARSOF units are familiar with their region's

people, culture, infrastructure, local conditions, language, and social mores. This experience can be of great value to the JFC in defining the desired end state. Similarly, during natural disasters, ARSOF assessment teams may be the first on the ground. They can relay to the JFC or the ambassador the magnitude of the problem and suggest actions to alleviate and stabilize the situation.

Perseverance

1-25. *Prepare for the measured, protracted application of military capability in support of strategic aims.* Some MOOTW may take years to achieve the desired results. The underlying causes of the crisis may be elusive, making it difficult to quickly achieve a decisive resolution. It is important to assess possible responses to a crisis in terms of the ways each option would impact on the long-term political objective. Selected ARSOF, with their regional orientation, are ideally suited to support a U.S. embassy's long-term development plan.

Unity of Effort

1-26. *Seek unity of effort in every operation.* A U.S. military chain of command normally will not have positive control over many of the agencies and multinational partners involved in MOOTW. In many cases, the U.S. military may be a supporting agency to other U.S. agencies. Key to success is the ability to understand one another's goals, resources, and needs. Specific relationships involving these agencies and multinational partners may be mission-specific, possibly not addressing command authority. The theater SOC will tailor the C2 to achieve unity of effort for the desired result. ARSOF personnel must use their interpersonal skills, training, and experience to persuade each agency or element to coordinate their efforts.

Restraint

1-27. *Prudently apply appropriate military capability.* Restraint requires the careful balancing of the need for security, the conduct of operations, and the political objective. A single, improperly handled incident could cause significant military and political consequences; therefore, judicious use of force is necessary. Clear, understandable, and appropriate commander's intent and rules of engagement (ROE) are essential—both to provide FP and to ensure appropriate restraint.

ARMY SPECIAL OPERATIONS FORCES

1-28. The unique capabilities of ARSOF are a function of the quality of their soldiers, their training and education, and the mission profiles they must execute. The competitive ARSOF selection process, coupled with technological training and education, produces an ARSOF soldier who is adaptable, mature, innovative, culturally aware, self-assured, and self-reliant. Thus, policy decision makers use ARSOF as a strategic and operational economy of force to expand the range of available options. Figure 1-2, page 1-8, shows the ARSOF organization.

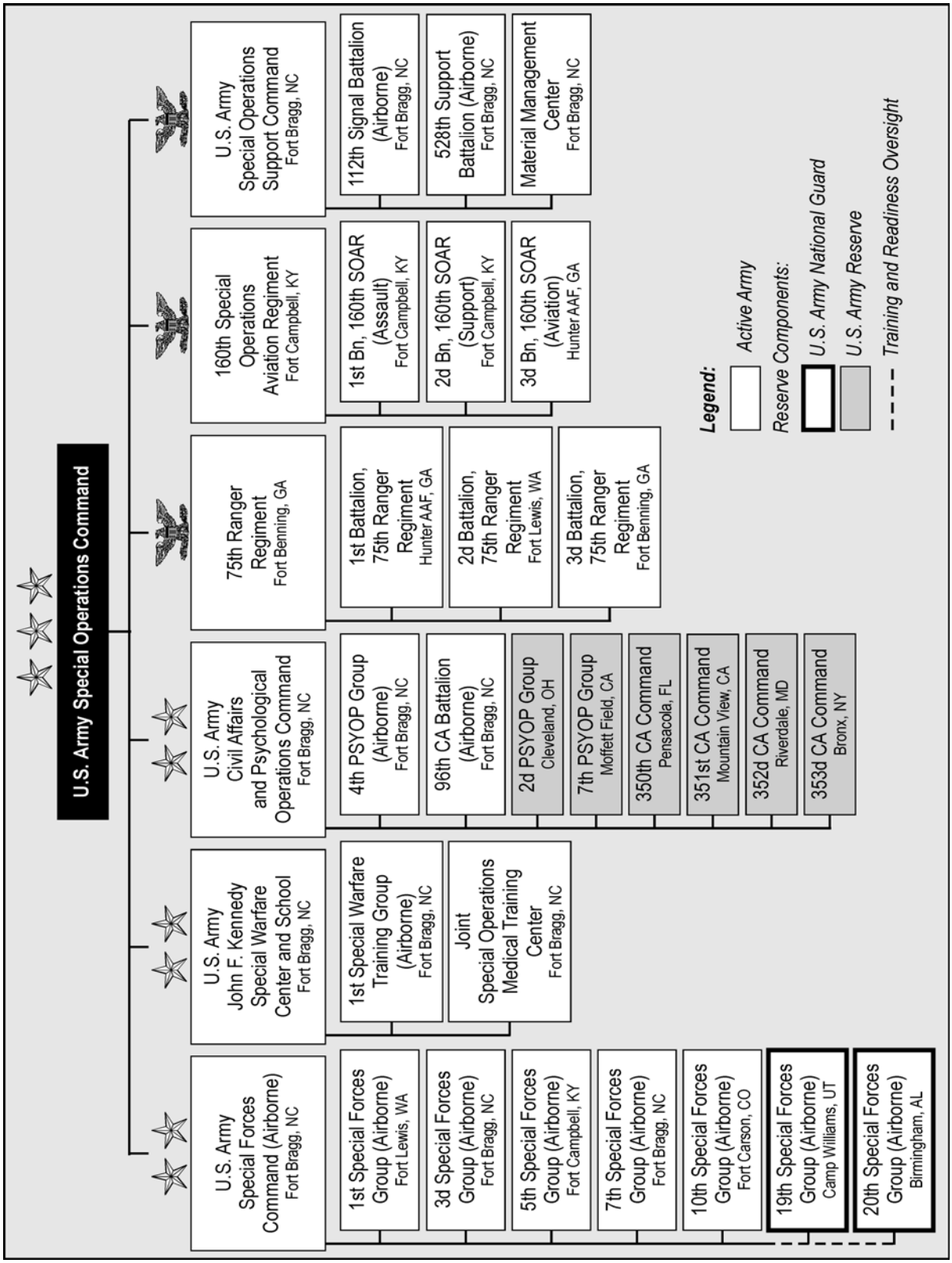


Figure 1-2. ARSOF Organization

1-29. ARSOF are specially organized, trained, and equipped military forces. They conduct SO to achieve military, political, economic, or informational objectives by generally unconventional means in hostile, denied, or politically sensitive areas. Decision makers may choose the ARSOF option because it provides the broadest range of capabilities that have direct applicability in an increasing number of environments. Political-military requirements often cast ARSOF into low-visibility environments that require oversight at the national level. ARSOF operations differ from conventional-force operations by their degree of acceptable physical and political risk, their modes of employment, and their operational techniques. ARSOF allow the geographic combatant commander or JFC to perform critical small-unit missions that directly strike or engage the aim or objective of his operational mission.

1-30. Early use of ARSOF in an operation may prevent or contain conflict and conserve national resources. When conflict is imminent, ARSOF may conduct a variety of prehostility missions. For example, ARSOF may conduct missions that signal determination, demonstrate support to allies, and begin the complicated processes of positioning forces for combat and preparing the operations area and/or battlespace.

1-31. During conflict, ARSOF may be most effective in conducting strategic and operational economy-of-force operations, generating military and diplomatic advantages disproportionate to the resources they represent. ARSOF can locate, seize, or destroy strategic and operational targets and obtain critical intelligence. They can analyze an enemy's defenses and diminish his morale. They can disorganize, disrupt, and demoralize his troops. They can also divert important resources.

1-32. ARSOF expand the options of the NCA and geographic combatant commanders, particularly in crises and contingencies (terrorism, insurgency, subversion, and sabotage) that fall between solely diplomatic initiatives and the overt use of large conventional forces. ARSOF elements' small size, rapid reaction, and self-sufficient nature provide military options that do not entail the risk of escalation normally associated with larger, more visible conventional forces. The use of ARSOF enables decision makers to prevent a conflict or to limit its scope. Therefore, decision makers can better control committed U.S. forces and resources. ARSOF may be the best choice for actions requiring a rapid response or a surgically precise, focused use of force.

1-33. ARSOF training is some of the most rigorous and technical in the world. It produces some of the most professional and expert soldiers in the world. ARSOF are mature forces who demonstrate superior performance in small groups or as part of an integrated U.S. response with other military forces as well as non-Department of Defense (DOD) and civilian agencies. Selected small, self-contained units can work swiftly and quietly without the noticeable presence of conventional forces. Even under the most austere conditions, these units are able to operate without the infrastructure often needed by a larger force. Thus, they can penetrate enemy territory by various means, sustain themselves in the denied area, and execute various missions.

1-34. Selected ARSOF need not use lethal force in a mission. Language skills, cross-cultural training, regional orientation, and understanding of the political context of their operational environments make them unparalleled

when operating in complex environments. Their skills enable them to work as effectively with civilian populations as with other military forces to influence situations favorably toward U.S. national interests. The ability of ARSOF to apply an indirect approach to a mission is one of their most important contributions to national military strategy.

ARMY SPECIAL OPERATIONS CHARACTERISTICS

1-35. To make sure missions selected for ARSOF are compatible with their capabilities, commanders must be familiar with the following SO characteristics:

- ARSOF personnel undergo careful selection processes or mission-specific training beyond basic military skills to achieve entry-level SO skills. These programs make unlikely any rapid replacement or generation of personnel with needed capabilities.
- Mature, experienced personnel compose ARSOF. Many maintain a high level of competency in more than one military specialty.
- Selected SO require a detailed knowledge of the cultural nuances and languages of a country or region where employed.
- ARSOF conduct specific tactical operations by using small units with unique talents that directly strike or engage strategic and operational aims or objectives.
- Planning for SO may begin at the unified, joint, or interagency levels for execution that requires extensive, rigorous rehearsals.
- SO are often low-visibility operations, or they may be combined with higher-visibility conventional operations. ARSOF can deploy at relatively low cost with a low profile that is less intrusive than that of larger conventional forces.
- Selected ARSOF units often conduct SO at great distance from operational bases. They employ sophisticated communications systems and means of insertion, support, and extraction to penetrate and return from hostile, denied, or politically sensitive areas.
- SO occur throughout the range of military operations (war and MOOTW).
- SO influence the will of foreign leadership to create conditions favorable to U.S. strategic aims and objectives.
- SO are often high-risk operations that have limited windows of execution and require first-time success.
- Employment of SO may require patient, long-term commitment and support to achieve U.S. national goals in an operational area.
- SO require theater and, frequently, national-level intelligence support.
- Most ARSOF are regionally oriented for employment. Cross-cultural communication skills are a routine part of their training.
- SO are inherently joint and sometimes multinational, requiring interagency and international coordination. The contribution of ARSOF

to national security is greatest when they are fully integrated into the JFC's plan at the earliest stages of planning.

- ARSOF can be task-organized quickly and deployed rapidly to provide tailored responses to many different situations.
- Selected ARSOF can gain access to hostile and denied areas.
- ARSOF units possess limited organic security and medical support.
- Selected ARSOF can live in austere, harsh environments without extensive support. For long-duration operations, ARSOF require support from theater Army.
- Selected ARSOF can survey and assess local situations and report these assessments rapidly.
- Selected ARSOF work closely with regional military and civilian authorities and populations.
- ARSOF are **not a substitute** for conventional forces but a necessary adjunct to existing conventional forces' capabilities. Depending upon requirements, ARSOF can operate independently or with conventional forces. ARSOF can assist and complement conventional forces so that they can achieve an objective that might not otherwise be attainable. The special skills and low-visibility capabilities inherent in ARSOF also provide an adaptable military response in situations or crises requiring tailored, precise execution and the focused use of force.

ARSOF TRUTHS

1-36. ARSOF truths (Figure 1-3) are timeless in nature. They address in some form each of the values prescribed by the Army.

Humans are more important than hardware. People—not equipment—make the critical difference. The right people, highly trained and working as a team, will accomplish the mission with the equipment available. Yet, the best equipment in the world cannot compensate for a lack of the right people.

Quality is better than quantity. A small number of people carefully selected, well-trained, and well-led are preferable to larger numbers of troops, some of whom may not be fully capable.

ARSOF cannot be mass-produced. It takes years to train operational units to the level of proficiency needed to accomplish difficult and specialized ARSOF missions. Integration of mature, competent individuals into fully capable units requires intense training in the ARSOF schools and the units. Hastening this process only degrades the ultimate capability.

Competent ARSOF cannot be created after emergencies arise. Creation of competent, fully mission-capable units takes time. Employment of fully capable ARSOF elements on short notice requires highly trained and constantly available ARSOF units in peacetime.

Figure 1-3. ARSOF Truths

SPECIAL OPERATIONS MISSION CRITERIA

1-37. SO mission criteria were developed to make sure the assets of SOF were committed only to the missions that supported the theater campaign,

were appropriate and feasible, and had an expected outcome that justified the risk. SOF commanders still apply the following criteria to assess proposed SOF missions.

1-38. *Is the mission appropriate for SOF?* The best use of ARSOF is against key strategic or operational targets that require unique skills and capabilities of ARSOF. If the targets are tactical, the use of ARSOF is not appropriate. Commanders should not assign ARSOF if the targets are not of strategic or operational importance. Commanders should not use ARSOF as a substitute for other forces.

1-39. *Does the mission support the geographic combatant commander's campaign plan?* If the mission does not support the JFC's campaign plan, more appropriate missions are probably available for ARSOF.

1-40. *Is the mission operationally feasible?* During course of action (COA) analysis, the ARSOF commander must realistically evaluate his force. Planners must understand that ARSOF are not structured for attrition or force-on-force warfare. They should not assign missions that are beyond SOF limitations and vulnerabilities.

1-41. *Are the required resources available to conduct the mission?* Some ARSOF missions may require support from conventional forces. Support involves aiding, protecting, complementing, and sustaining employed ARSOF. Support may include airlift, intelligence, communications, and logistics. Although a target may be vulnerable to ARSOF, lack of support may affect the chance for success or may invalidate the use of ARSOF.

1-42. *Does the expected outcome justify the risk?* Some operations that ARSOF can execute make only a marginal contribution to the JFC campaign plan and present great risk to personnel and materiel. Commanders should recognize the high value and limited resources of ARSOF. They must make sure the benefits of successful mission execution are measurable and in balance with the risks inherent with the mission. Risk assessment considers not only the potential loss of ARSOF units and equipment but also the risk of adverse effects on U.S. diplomatic and political interests should the mission fail.

ARMY SPECIAL OPERATIONS IMPERATIVES

1-43. The following paragraphs discuss the Army SO imperatives. Although the imperatives may not apply to all types of ARSOF, SOF commanders must include the applicable imperatives in their mission planning and execution.

UNDERSTAND THE OPERATIONAL ENVIRONMENT

1-44. ARSOF cannot dominate their environment without first gaining a clear understanding of the theater, including civilian influence, as well as enemy and friendly capabilities. Combat environmental research—political, economic, sociological, psychological, geographic, and military—is an essential prerequisite to accomplish before acting to influence the environment. ARSOF must know who the friendly and hostile decision makers are, what their objectives and strategies are, and how they interact.

The conditions of conflict can change. ARSOF must anticipate these changes in their environment and exploit fleeting opportunities.

RECOGNIZE POLITICAL IMPLICATIONS

1-45. Many SO advance critical political objectives. ARSOF must understand that their actions can have international consequences. Rules of engagement provide a framework that considers political implications. However, ROE cannot anticipate every situation. ARSOF must understand the intent of the ROE and act accordingly, despite any military disadvantage that may result. The advancement of the political objective may take precedence over the military disadvantages.

FACILITATE INTERAGENCY ACTIVITIES

1-46. ARSOF support and complement U.S. and multinational civilian programs driven by nonmilitary considerations. ARSOF can also operate in the ambiguous and complex political environments found in coalition operations or alliances formed to avert situations that would lead to human tragedy.

ENGAGE THE THREAT DISCRIMINATELY

1-47. ARSOF are a limited resource that cannot easily be replaced. ARSOF mission objectives require careful application of **when**, **where**, and **how**.

CONSIDER LONG-TERM EFFECTS

1-48. ARSOF must consider the political, economic, informational, and military effects when faced with dilemmas, since the solutions will have broad, far-reaching effects. ARSOF must accept legal and political constraints to avoid strategic failure while achieving tactical success. ARSOF must not jeopardize the success of national and theater long-term objectives by their desire for immediate or short-term effects. SO policies, plans, and operations must be consistent with the national and theater priorities and objectives they support. Inconsistency can lead to a loss of legitimacy and credibility at the national level.

ENSURE LEGITIMACY AND CREDIBILITY OF SPECIAL OPERATIONS

1-49. Significant legal and policy considerations apply to many SO activities. Legitimacy is the most crucial factor in developing and maintaining internal and international support. The United States cannot sustain its assistance to a foreign power without this legitimacy. The concept of legitimacy is broader than the strict legal definition contained in international law. The concept also includes the moral and political legitimacy of a government or resistance organization. The people of the nation and the international community determine SO legitimacy on the basis of collective perception of the credibility of its cause and methods. Without legitimacy and credibility, SO will not gain the support of foreign indigenous elements, the U.S. population, or the international community. ARSOF legal advisors must review all sensitive aspects of SO mission planning and execution.

ANTICIPATE AND CONTROL PSYCHOLOGICAL EFFECTS

1-50. All SO have significant psychological effects—some specifically produced and some based on perceptions. ARSOF must integrate PSYOP and public affairs (PA) into all their activities, anticipating and countering hostile propaganda and disinformation themes to allow for maximum control of the environment.

APPLY CAPABILITIES INDIRECTLY

1-51. The primary role of ARSOF in multinational operations is to advise, train, and assist indigenous military and paramilitary forces. The supported non-U.S. forces then serve as force multipliers in the pursuit of U.S. national security objectives with minimum U.S. visibility, risk, and cost. Long-term self-sufficiency of the foreign force must assume primary authority and accept responsibility for the success or failure of the mission. All U.S. efforts must reinforce and enhance the effectiveness, legitimacy, and credibility of the supported foreign government or group. (See Appendix A for further discussion of multinational operations.)

DEVELOP MULTIPLE OPTIONS

1-52. ARSOF must maintain their operational flexibility by developing a broad range of options. The key to operational flexibility includes—

- Developing contingency plans that anticipate problems during critical events.
- Using a deliberate and interactive planning and rehearsal process.
- Having the same people plan, rehearse, and execute the mission. These types of actions on the objective become a common point of departure, not inflexible blueprints.

Under these circumstances, the soldiers understand all the critical elements of the plan and alternate COAs, reasons for discarding alternate COAs, and unstated assumptions underlying unexpected difficulties.

ENSURE LONG-TERM SUSTAINMENT

1-53. Resourcing of ARSOF varies with each mission. ARSOF must demonstrate continuity of effort when dealing with political, economic, informational, and military programs. They must not begin programs that are beyond the economic, technological, or cultural capabilities of the HN to maintain without U.S. assistance. Such efforts will be counterproductive. SO policy, strategy, and programs must therefore be durable, consistent, and sustainable.

PROVIDE SUFFICIENT INTELLIGENCE

1-54. SO depend upon timely, relevant, accurate, and predictive intelligence. ARSOF must identify and prioritize their information requirements (IRs). Responses to ARSOF IRs must contain as much detail as time permits.

BALANCE SECURITY WITH SYNCHRONIZATION

1-55. Insufficient security may compromise a mission. Excessive security will usually cause the mission to fail because of inadequate coordination.

ARSOF MISSIONS

1-56. There are nine primary missions for ARSOF, as directed by Congress, the NCA, and the Joint Chiefs of Staff (JCS). These missions are described below.

UNCONVENTIONAL WARFARE

1-57. Unconventional warfare (UW) is a broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted by indigenous or surrogate forces that are organized, trained, equipped, supported, and directed in varying degrees by an external source. UW includes guerrilla warfare (GW) and other direct offensive, low-visibility, covert, or clandestine operations, and the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape (E&E). IEW support for UW normally requires IEW support characteristics associated with both direct and indirect missions given the parameters of this operation.

DIRECT ACTION

1-58. DA operations are short-duration strikes and small-scale offensive actions by SOF to seize, destroy, capture, recover, or inflict damage on designated enemy personnel or material. SOF conducting DA operations may—

- Conduct raid, ambush, or direct assault tactics.
- Conduct standoff attacks by fire from air, ground, or sea platforms.
- Provide terminal guidance for precision-guided munitions.
- Conduct independent sabotage.

1-59. DA operations are designed to achieve specific, well-defined, and often time-sensitive results of strategic and operational critical significance. DA operations may take place independently or as part of larger unconventional operations or campaigns. Although frequently considered close-combat-type operations, DA operations also include sniping and other standoff attacks by fire delivered or directed by SOF.

SPECIAL RECONNAISSANCE

1-60. Special reconnaissance (SR) consists of reconnaissance and surveillance actions conducted by SOF to obtain or verify, by visual observation or other collection methods, information on the capabilities, intentions, and activities of an actual or potential adversary. SR is also used to secure data on the meteorological, hydrographic, or geographic characteristics of a particular area. SR includes target acquisition, area assessment, and poststrike reconnaissance.

1-61. SR complements national and theater intelligence collection assets and systems by obtaining specific, well-defined, and time-sensitive information of strategic or operational significance. SR may complement or augment other

collection methods constrained by weather, terrain-masking, or hostile countermeasures. SR can also replace national or theater collection means that are rendered incapable or unavailable. SR is a human intelligence (HUMINT) function that places U.S. or U.S.-controlled "eyes on target" in hostile, denied, or (when authorized) politically sensitive territory.

FOREIGN INTERNAL DEFENSE

1-62. FID is the participation by civilian and military agencies of a government in any of the actions or programs taken by another government to free and protect its society from subversion, lawlessness, and insurgency. It is a joint and interagency activity of the U.S. Government (USG). To ARSOF, however, FID has a much broader meaning that encompasses a myriad of internal, external, and transnational threats. The primary mission in FID is to organize, train, advise, and assist HN military and paramilitary forces in their conduct of internal defense and development.

COMBATTING TERRORISM

1-63. CBT consists of actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. HN responsibilities, Department of Justice and Department of State (DOS) lead agency authority, legal and political restrictions, and appropriate DOD directives limit SOF involvement in CBT. Most CBT activities are classified. Further discussion of CBT is beyond the scope of this publication.

PSYCHOLOGICAL OPERATIONS

1-64. PSYOP are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. PSYOP are key components of information operations (IO) and support both SOF and conventional forces.

CIVIL AFFAIRS

1-65. CA are the designated Active Army and RC forces and units organized, trained, and equipped specifically to conduct CA activities and to support civil-military operations (CMO). CMO are the activities of a commander that establish, maintain, influence, or exploit relations between military forces, government and nongovernment civilian organizations and authorities, and the civilian population in friendly, neutral, or hostile AOs in order to facilitate military operations and consolidate and achieve U.S. national objectives. CMO may involve military forces performing those activities and functions normally the responsibility of the local government. These activities may occur before, during, or after other military operations. When directed, they may occur in the absence of military operations. CA forces augment CMO staffs of geographic theater Army component and maneuver commanders. CA activities are performed or supported by CA forces, and

embrace the relationship between military forces and civil authorities in areas where military forces are usually present and involve the application of CA functional specialty skills. All CA activities support CMO.

COUNTERPROLIFERATION OF WEAPONS OF MASS DESTRUCTION

1-66. Counterproliferation of weapons of mass destruction (CP-WMD) are activities of the DOD. These CP-WMD activities span the full range of U.S. efforts to combat proliferation, including diplomacy, arms control, export controls, and intelligence collection and analysis. Also, CP-WMD activities ensure U.S. forces and interests can be protected should they confront an adversary armed with weapons of mass destruction (WMD). Most CP-WMD activities are classified. Further discussion of CP-WMD is beyond the scope of this publication.

INFORMATION OPERATIONS

1-67. Over the next 20 years, developments in information technology will revolutionize how nations, organizations, and people interact. The rapid diffusion of information enabled by these technological advances challenges the relevance of traditional organizational sciences and management principles. The volume, accuracy, and speed of battlespace information available for commanders to make decisions will allow units and organizations to operate at levels most adversaries cannot match, while simultaneously protecting that capability.

1-68. IO are actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks, while defending one's own information, information-based processes, information systems, and computer-based networks. ARSOF actions provide support to strategic and theater IO. They include the exploitation, corruption, dominance, or destruction of an adversary's information system, while protecting the integrity of ARSOF systems from attacks.

1-69. IO integrates various elements, mutually supported by intelligence—to deny information to, influence, degrade, or destroy adversary capabilities—while protecting friendly capabilities against such actions. These elements include—

- Military deception.
- Counterdeception.
- Operations security (OPSEC).
- Physical security.
- Electronic warfare (EW).
- Information assurance.
- Physical destruction.
- PSYOP.
- Counterpropaganda.
- Counterintelligence (CI).

- Computer network attack.
- Computer network defense.

IO apply across the range of military operations, all levels of conflict, and can be offensive or defensive.

ARSOF COLLATERAL ACTIVITIES

1-70. Collateral activities are applications of ARSOF capabilities in missions other than those directed by Congress. The inherent capabilities of ARSOF mission profiles also make them suitable for employment in a range of collateral activities. These activities are other than primary missions for organizing, training, and equipping ARSOF.

COALITION SUPPORT

1-71. Coalition support improves the interaction of coalition partners and U.S. military forces, particularly in coalition warfare. Coalition support includes training coalition partners on tactics, techniques, and procedures (TTP); providing communications to integrate coalition partners into the coalition command and intelligence structure; and establishing liaison to coordinate for combat support (CS) and combat service support (CSS). ARSOF liaison officers (LNOs) or liaison elements (LEs) often give the JFC an accurate evaluation of the capabilities, location, and activities of coalition forces, thus facilitating JFC C2.

COMBAT SEARCH AND RESCUE

1-72. Combat search and rescue (CSAR) is a specific task performed by rescue forces to effect the recovery of distressed personnel during wartime or contingency operations. Each Service and the United States Special Operations Command (USSOCOM) are responsible for CSAR. The unique ability of ARSOF to penetrate air defense systems and to conduct joint air, ground, or sea operations deep within hostile or denied territory at night or in adverse weather makes these forces highly suited for this mission.

COUNTERDRUG ACTIVITIES

1-73. CD activities are active measures taken to detect, monitor, and counter the production, trafficking, and use of illegal drugs. Using their skills in cross-cultural communications, ARSOF train HN CD forces on critical skills required to conduct small-unit CD operations. ARSOF CD activities overseas support the geographic commander in chief's (CINC's) regional CD campaign plan or the U.S. ambassador's country-specific CD plans.

HUMANITARIAN DEMINING ACTIVITIES

1-74. Humanitarian demining (HD) activities are performed by ARSOF in support of a DOD program to help selected HNs establish their own demining organizations capable of conducting long-term and self-sustaining operations to reduce or eliminate the suffering and threats to the safety of its civilian populations caused by land mines and associated battlefield unexploded ordnance. SF teams train the HN cadre in techniques to locate, identify, and destroy land mines and unexploded ordnance. PSYOP teams assist HN

governments to develop and implement mine awareness programs to train local populations in identifying, avoiding, and reporting locations of land mines and unexploded ordnance until these threats are removed. CA teams train the HN demining headquarters in management and C2 of its subordinate elements. CA assets also provide liaison with the USG, United Nations (UN), and international and local nongovernmental organizations (NGOs) to coordinate support of the HN demining infrastructure.

HUMANITARIAN ASSISTANCE

1-75. HA consists of programs conducted to relieve or reduce the results of natural or man-made disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. HA provided by U.S. forces is limited in scope and duration. The assistance supplements or complements the efforts of the HN civil authorities or agencies that may have the primary responsibility for providing HA.

SECURITY ASSISTANCE

1-76. Security assistance (SA) consists of a group of programs or statutes by which the United States provides defense articles, military training, and other defense-related services by grant, loan, credit, or cash sales in furtherance of national policies and objectives. The primary ARSOF role in SA is to provide mobile training teams (MTTs). Public law prohibits personnel who provide SA services, including mobile training assistance, from performing combatant duties. SF, with CA and PSYOP attachments, are particularly effective in SA because they use the same regional orientation, communications, mobility, and other skills required for FID and UW missions. SA is a particularly valued activity because ARSOF train themselves in skills useful in stability operations and support operations while they train or otherwise assist foreign military forces.

SPECIAL ACTIVITIES

1-77. Special activities fall under Executive Order 12333, *United States Intelligence Activities*. They require a presidential finding and congressional oversight. ARSOF conduct them abroad in support of national foreign policy objectives, but in a manner that USG participation is neither apparent nor publicly acknowledged. Whether supporting or conducting a special activity, ARSOF may perform any of their primary missions, subject to the limitations imposed on special activities. Such activities are highly compartmentalized and centrally managed and controlled.

TARGETING AND MISSION PLANNING

1-78. Deliberate evaluation of an adversary's vulnerabilities and application of SOF capabilities at critical nodes are the foundation of SOF employment. The keystone of SOF mission planning is the operational element that will plan and execute the mission. The inherent qualities of SO planning encourage foresight. SOF select targets for exploitation with careful and deliberate consideration. Effective integration of SOF into a CINC's campaign is possible only through synchronized targeting and mission planning.

1-79. Targeting is the process of selecting targets and matching the appropriate response and method of engagement. It is the analysis of enemy situations relative to the commander's mission, objectives, and capabilities at his disposal. It identifies and nominates specific vulnerabilities that, if exploited, will accomplish the commander's purpose through delaying, disrupting, disabling, or destroying enemy forces or resources critical to the enemy. The JFC may establish a Joint Targeting Coordination Board (JTCB) to evaluate nominations to assess whether targets will achieve desired objectives.

1-80. The SO options available to the JFC include a myriad of lethal and nonlethal actions that can, when properly applied, optimize SOF capabilities. SOF targeting considerations include the political, military, economic, and psychological impact on the enemy force's capabilities and morale and its popular support base. Two distinctly different modes—direct and indirect—define the lethal and nonlethal force applied by ARSOF.

1-81. The targeting cycle portrays an analytical, systematic approach focusing on the targeting process that supports operational planning to achieve the objectives of the JFC. The interrelationship of the target development and mission planning phases dominates the six phases of the targeting cycle. All of these phases require proactive and synchronized intelligence support. Intelligence staff officers supporting SOF must anticipate mission needs and coordinate for the resources required to provide the most timely, relevant, accurate, and predictive intelligence possible.

PHASE 1–OBJECTIVES AND GUIDANCE

1-82. Objectives and guidance originate at the national level as broad concepts, such as the National Security Strategy and the National Military Strategy. The NCA communicate national security objectives through the Chairman of the Joint Chiefs of Staff (CJCS), who in turn prepares the biennial Joint Strategic Capabilities Plan (JSCP). The JSCP provides short-term (2 years) strategic guidance to the geographic CINCs and the Service chiefs. The JSCP assigns tasks, apportions major combat forces and strategic transportation for deliberate planning, and directs the geographic CINCs to develop plans supporting specific national security objectives. The geographic CINCs translate broad national and theater strategy into strategic and operational concepts through the development of theater campaign plans. The Joint Operation Planning and Execution System (JOPES) facilitates this planning process.

1-83. In all types of planning, the CINC (and subordinate JFCs) specifies the mission; spatially organizes the operational area into joint operations areas (JOAs), AOs, or joint special operations areas (JSOAs); organizes the forces (task organization and command relationships); and assigns missions and tasks to subordinates. The CINC provides a clear, concise intent (a broad purpose and required end state). Per JP 3-05, *Doctrine for Joint Special Operations,* he also provides a concept of how SOF will carry out the operations in the theater campaign. His concept for SOF may—

- Provide the concepts for SOF activities and sustainment that will transform national, alliance, and theater strategic guidance into military objectives.

- Describe the CINC's vision of SOF employment, including command relationships.
- Identify requirements for USSOCOM and Service components to prepare, provide, and sustain theater-assigned and -augmented SOF.
- Identify priority operational, weather, and information requirements that theater SOF must address.
- Define interagency coordination requirements.

1-84. The theater SOC's primary responsibility in theater planning is to integrate SO to complement or support the overall theater campaign plan. Subordinate joint SOF commands have similar responsibilities to their superior JFCs (for example, commander of joint special operations task forces [JSOTFs] to their JTF commanders). SO staff officers on JFC staffs are essential in ensuring integration of SOF into campaign and major operations plans.

PHASE 2–TARGET DEVELOPMENT

1-85. This part of the process is the systematic identification and evaluation of critical target nodes vulnerable to effective direct attack or indirect exploitation. Component commanders including the joint force special operations component commander (JFSOCC) nominate targets to the JFC. Supported commanders' nominations and priorities (for example, joint force land component commander [JFLCC] target nominations in the JFLCC AO) are given special emphasis in the JFC target development process. The JFC may establish a JTCB to evaluate nominations to assess whether targets will achieve desired objectives. The component commanders are left the details of targeting and execution. Typically, the JTCB reviews targeting information, develops targeting guidance and priorities, and prepares and refines joint targeting lists. The JFSOCC and the psychological operations task force (POTF) commanders are represented on the JTCB as separate functional component commanders.

PHASE 3–WEAPONEERING

1-86. Weaponeering is the process of determining the quantity of a specific type of lethal or nonlethal weapon required to achieve a specific level of damage to a given target. Analysts determine target vulnerability, weapon effect, munitions delivery accuracy, damage criteria, probability of kill, and weapon reliability. Normally, component representatives to the JTCB conduct this analysis.

PHASE 4–FORCE APPLICATION

1-87. Force application is the selection of forces for the mission. Either the JTCB or the JFC's staff recommend the appropriate forces. The goal is to select the available lethal or nonlethal forces that can best accomplish the commander's objectives within the specified period. The JFSOCC advises the JTCB or JFC's staff on the capabilities, limitations, and feasibility of supporting SOF. The joint psychological operations task force (JPOTF) advises the JFC on PSYOP capabilities. The JFC's CMO staff officer advises him on CMO and CA capabilities.

PHASE 5–MISSION PLANNING

1-88. The hallmark of SOF planning is decentralization down to the actual operational element that will execute the mission. With the assistance of the forward operational base (FOB) and Special Forces operational base (SFOB), operational elements conduct their detailed mission planning and coordination in isolation. The ARSOF elements tasked to perform a mission develop a concept of operation and produce an operations order (with contingencies) that they brief to a designated senior SOF commander for approval. ARSOF mission planning should—

- Always contribute substantially to the strategic or campaign plan being executed.
- Include complete orders or plans (insertion, resupply, fire and maneuver support, and extraction). They require thorough planning before committing the force. Planners must coordinate their SO mission planning with all applicable supporting and supported forces and agencies through the JFC. Detailed targeting and mission planning are vital to successful mission execution.
- Address the specific mission window of opportunity since SO targets normally are perishable either from a military or political viewpoint.

PHASE 6–COMBAT ASSESSMENT

1-89. In the final phase, the JFSOCC assesses the executed mission to determine if the employed SOF element accomplished the assigned mission. If the results do not meet the criteria established during the weaponeering phase, the JFC's staff or JTCB then determines what resources are required to reacquire the target and to achieve the desired effect. As stated in the above principles of SO mission planning, retasking a deployed ARSOF unit is frequently not a viable COA.

Chapter 2

ARSOF and the Intelligence and Electronic Warfare System

ARSOF operations are often conducted with a high degree of risk to obtain high-payoff returns while national-level interests are at stake. Success for ARSOF missions dictates that uncertainty associated with the threat and environment must be minimized through the application of intelligence operations and procedures.

INTRODUCTION

2-1. The ARSOF commander applies the IEW system throughout the range of operations. This principle is often stated as, "The commander drives intelligence." This chapter describes how the total IEW system works in concert with ARSOF to accomplish the mission. The IEW system supporting ARSOF includes organizations and assets from the national level down to the theater and tactical level, including the ARSOF soldier in the field (Figure 2-1, page 2-2).

2-2. History tells us that successful missions are dramatically influenced by the commander's ability to make the right decision at the right time. That ability is dynamically affected by good intelligence support. The IEW system must provide the commander needed information about the situation, the threat, the environment, and any external entity that could impact on the mission. The commander requires this IEW support whether engaged in one of the primary missions of ARSOF or a collateral activity. ARSOF intelligence staffs must understand the intelligence requirements of their higher headquarters (HQ) and subordinate commands and components, and identify organic intelligence capabilities and shortfalls. They must also access theater and national systems to alleviate shortfalls and ensure that timely, relevant, accurate, and predictive intelligence is provided to the commander and subordinate commands. This objective is achieved through the cooperative and comprehensive efforts of intelligence personnel of all disciplines during each phase of the intelligence cycle.

2-3. The missions assigned to ARSOF will directly support the operational and strategic requirements of the geographic CINC. These missions are integrated with vital elements of theater strategy and national objectives. ARSOF commanders use the IEW system to reduce uncertainty and to concentrate forces and combat systems where they will be most effective in accomplishing the mission. At the tactical level, the IEW mission is to support commanders with intelligence preparation of the battlespace, situation development, target development, support to targeting, and FP. At the strategic and operational levels, the IEW mission also includes indications and warning (I&W) and battle damage assessment (BDA).

Echelon	Producers	Organic Resources	Requests Support From
Theater	Intelligence Directorate (J2) Joint Intelligence Center (JIC) SOC J2 Theater Army G2	Human Intelligence Collectors (HICs) Technical Intelligence (TECHINT) Analysts Controlled Collection Counterintelligence (CI) Agents Signals Intelligence (SIGINT) Analysts High-Frequency (HF) Jamming Imagery Intelligence (IMINT) Collection and Analysis	HQ, U.S. Army HQ, U.S. Air Force HQ, U.S. Navy HQ, U.S. Marine Corps National-Level Agencies HN Allies United States Space Command (USSPACECOM) United States Transportation Command (USTRANSCOM)
USSOCOM	Special Operations Information Operations (SOIO) Staff Special Operations Command Joint Intelligence Center (SOCJIC)	Analysts National Agency Liaison Imagery Analysts	Theater JICs National-Level Agencies Echelons Above Corps Intelligence Center (EACIC)
United States Army Special Operations Command (USASOC)** U.S. Army Special Forces Command (USASFC)* U.S. Army Civil Affairs and Psychological Operations Command (USACAPOC)	Deputy Chief of Staff for Intelligence (DCSINT) G2 G2	Analysts (All) USASOC CI Agents ARSOF Technical Control and Analysis Element (TCAE) Imagery Technician HUMINT Technician	Theater SOC J2 USSOCOM**
Special Forces Group (SFG)	Group S2 Group Military Intelligence Detachment (MID) Battalion (Bn) S2	SR Teams CI Agents HICs Special Operations Team A (SOT-A) TCAE Imagery Analysts Soldiers	SOC JTF J2
Ranger Regiment (Rgt)	Rgt S2 Bn S2	CI Agents Ranger Reconnaissance Detachment (RRD) Soldiers Analysts Imagery Analysts	USASOC** SOC JTF
Special Operations Aviation Regiment (SOAR)	Rgt S2 Bn S2	Air Crews Soldiers Analysts CI Agents	USASOC** SOC JTF
CA	Bn S2	Soldiers Analysts	USASOC** SOC JTF
Psychological Operations Group (POG)	Testing and Evaluation Detachment (TED) Target Audience Analysis Detachment (TAAD) Group S2 Bn S2 PSYOP Development Center (PDC) Staff	HICs Soldiers PSYOP Specialists	USASOC** SOC JTF
		Legend: **Conflict or War **Peacetime*	

Figure 2-1. IEW Assets by Organizations and Echelon

ARSOF IEW CHARACTERISTICS

2-4. IEW support to ARSOF is based on the same principles as IEW support to conventional forces; all of the principles of force projection IEW operations apply. (See FM 34-1.) However, intelligence requirements unique to Army SO produce some distinct characteristics, as described below.

CRITICALITY OF IEW SUPPORT TO ARSOF

2-5. During the conduct of SO, especially during DA or IO, ARSOF may have only one opportunity to successfully execute a mission in denied areas. ARSOF commanders need extremely detailed and responsive IEW support because it is crucial in helping the commander make informed decisions during the military decision-making process (MDMP). Each intelligence discipline provides intelligence and combat information that commanders need to successfully complete their missions.

ARSOF IEW CAPABILITIES

2-6. Assets and products derived from the unique mission capabilities of ARSOF units, particularly in CI and HUMINT, are valuable tools for combatant commanders. The assets and products provide information or intelligence that may not be obtainable through other means. Additionally, ARSOF can provide SIGINT and EW assets to combatant commanders by passive and active means to target adversaries and to protect friendly C4I systems.

ARSOF IEW LIMITATIONS

2-7. ARSOF intelligence staffs above group or regiment level are limited in comparison with that of conventional formations. To overcome this limitation, ARSOF commanders and their staffs must understand how the total IEW system works and how to integrate IEW assets and products, along with the principles of synchronization and interoperability, to support their concept of the mission. The environments and types of operations will, of course, vary. The key to effective intelligence support is for ARSOF to fully use the entire IEW system. To do this, ARSOF commanders and intelligence personnel must work with the national agencies and theater intelligence centers to make the intelligence community aware of ARSOF requirements.

COMMUNICATIONS AND CONNECTIVITY

2-8. Rapid and unencumbered access to theater- and national-level intelligence agencies and their databases is of paramount importance. ARSOF S2s must be able to acquire data rapidly, process it, and pass it efficiently to operational users. Having this access is a critical, challenging component of successful intelligence operations. S2s must thoroughly understand the global command and control system (GCCS) and all of the communications assets and capabilities of their units. They must know how to “push and pull” data through existing communications architectures at fixed and remote sites.

ORGANIC INTELLIGENCE HOLDINGS

2-9. ARSOF operations, especially contingency missions, place special demand on ARSOF organic intelligence holdings. Short reaction times dictate that initial planning intelligence products be assembled quickly from garrison databases. The only way to achieve this level of responsiveness is to anticipate these requirements through the careful analysis and monitoring of theater and world events and to have the necessary intelligence holdings on hand for short-notice requirements. Intelligence holdings could include regional weather and light data, limited order of battle (OB) information, and geospatial information and services (GI&S) products.

DEMAND FOR HUMINT

2-10. Often accurate and relevant target-specific information critical for mission success can be obtained only through CI and HUMINT operations. HUMINT and CI information directly responds to priority intelligence requirements (PIR) and IRs and supports FP, PSYOP campaign plans, CA, IO, target development, and the other intelligence disciplines. HUMINT and CI capabilities include HN liaison, enemy prisoner of war (EPW) and line crosser screening/interrogation, screening operations, and counterintelligence force protection source operations (CFSO). These data could include plans of the internal layout of facilities, activities and intentions of security/threat forces, or potential areas for infiltration of assault forces. National-level technical collection means may be incapable of obtaining this specific level of data or lack the "loiter" time on the target needed to acquire needed information. ARSOF operators, who often prefer "talking with those who have been on the ground," frequently favor HUMINT-derived information. This bias is especially apparent when the human intelligence collectors (HICs) are actual operators. For example, when a Special Forces operational detachment A (SFODA) conducts an SR mission or an RRD team provides prestrike information to the commander of a Ranger task force. HUMINT information is important not only for DA missions; it can play a crucial role in every primary ARSOF mission, from UW to IO. Collateral activities also may rely heavily on HUMINT information often obtained through overt or open venues such as debriefings, interviews, and association with HN civilians.

EMPHASIS ON SURPRISE, DECEPTION, AND SECURITY

2-11. ARSOF missions are particularly sensitive to threat collection and targeting efforts. Counterintelligence, OPSEC, and deception must be applied to protect sensitive ARSOF missions across the range of military operations. Commanders at all levels should be well informed on the capability and effectiveness of threat intelligence and security services against ARSOF. The loss of security or the element of surprise is often an abort criterion for ARSOF missions. Where deception is used, the S2 must determine which threat sensors are available to collect the deception story, how much data to feed into the system to ensure the threat's intelligence agencies arrive at the desired conclusion, and how the threat decision maker will react to the deception effort. The clandestine or covert nature of some ARSOF activities also demand exhaustive postmission security measures to protect the

missions and the participants. ARSOF elements often must interface with high-level elements of DOD and other agencies to protect the mission and its clandestine or covert nature.

COMPARISON AND CONTRAST WITH CONVENTIONAL FORCES IEW SUPPORT

2-12. Most IEW requirements and procedures for ARSOF and conventional forces are the same. Yet, given the uniqueness of SO missions and roles, there are characteristics of IEW support that bear addressing. These are—

- *Level of detail.* The intricate planning and decentralized execution of SOF missions require intelligence support that is frequently more detailed or specific than that needed in conventional operations. ARSOF often require intelligence to avoid enemy forces, regardless of size or composition, as opposed to information that would allow conventional forces to directly engage the enemy.
- *Timeliness and accuracy of information.* Timely and accurate intelligence and unprocessed combat information can be a significant factor in operational success. Given the high risk factor or criticality of many ARSOF missions, uncertainty about the threat or environment reduces the chances for success more so than in the case of large-scale conventional operations. Equal with the need for accurate information is the need for timely information. Often the success of an ARSOF mission hinges upon having a key bit of knowledge at a specific time or event.
- *Operational element and analyst interface.* Given the sensitivity and critical need for very detailed information, especially in the context of DA operations, intelligence personnel often need to work directly with the forces that will execute a mission. Frequently both analysts and collectors will work hand in hand with operational planners and even with those executing the actual mission during planning, rehearsal, execution, and postoperational phases of a mission. Because ARSOF units often use forward staging bases, assigned intelligence personnel must be familiar with the conduct of split-based operations. This allows intelligence personnel to deploy forward intelligence "packages" and to maintain connectivity with the IEW system through communications with their higher HQ.

INTEGRATING IEW WITH OPERATIONS

2-13. The commander's role in IEW, before and throughout the mission, is central to the success or failure of IEW support to operations. The commander plays an essential role in keeping the intelligence effort focused.

INFORMATION REQUIREMENTS

2-14. The ARSOF commander directs the IEW process by establishing the commander's critical information requirements (CCIR). These requirements consist of the following:

- Commander's PIR.
- Essential elements of friendly information (EEFI)—information about friendly capabilities that must be protected from compromise.

- Friendly forces information requirements (FFIR)—information about the capabilities of his or adjacent units.

2-15. PIR are those critical pieces of intelligence that the commander must know about the adversary and the operational environment by a particular time to plan and execute a successful mission. The commander's PIR establish the what, why, when, where, and how of what he needs to know for his operations. The commander's PIR are critical in focusing and integrating the intelligence system. PIR are the basis for intelligence collection and production. ARSOF PIR are often as concerned with the status of HN governments and local populations as they are with the conventional military threats and the other characteristics of the AO. Some PIR may be strategically focused while others may focus on a tactical situation. The S2 recommends and the commander approves PIR. The S2 also may develop and approve IRs. These IRs reflect some of the intelligence requirements that are less critical to the commander's decisions, but still include information to support the operation. Once approved, PIR and IRs are integrated into the all-source intelligence collection plans that support situation and target development. The commander and S2 must—

- Identify, clearly articulate, and prioritize intelligence and targeting requirements.
- Understand the capabilities and limitations of the intelligence system.
- Know how to access, employ, and synchronize the support of the IEW system to its full potential.
- Provide for subordinates' information and resource requirements.

ARSOF S2

2-16. The ARSOF S2 is the ARSOF commander's link to the total IEW system. The commander relies on the S2 to provide him combat information and subsequently to produce intelligence with input from all available sources. The S2 must know the structure, capabilities, and missions of his unit. He must understand the full range of military operations and must be able to develop intelligence support for any missions assigned to his unit. He must know the composition of the IEW system, his place in that system, and how to use the system; otherwise, the S2 cannot answer the commander's PIR and IRs. The ARSOF S2 must be well versed in the intelligence requirements of ARSOF missions, and he must be familiar with the requirements of interagency and multinational coordination in the intelligence process. (Figure 2-2, page 2-7, depicts the SOF IEW requirements system.)

2-17. The S2 plans, supervises, and coordinates collection and analysis efforts to make sure the commander and staff elements get timely combat information and intelligence products. The S2 is responsible for maintaining the threat and environment portions of the current operating picture. Using the intelligence cycle and the intelligence preparation of the battlefield (IPB) process, the S2 develops and maintains the following:

- The command's intelligence database, which should include regional weather and light data.

- GI&S products.
- OB information.
- Biographical information.
- Current events files for the AOR.

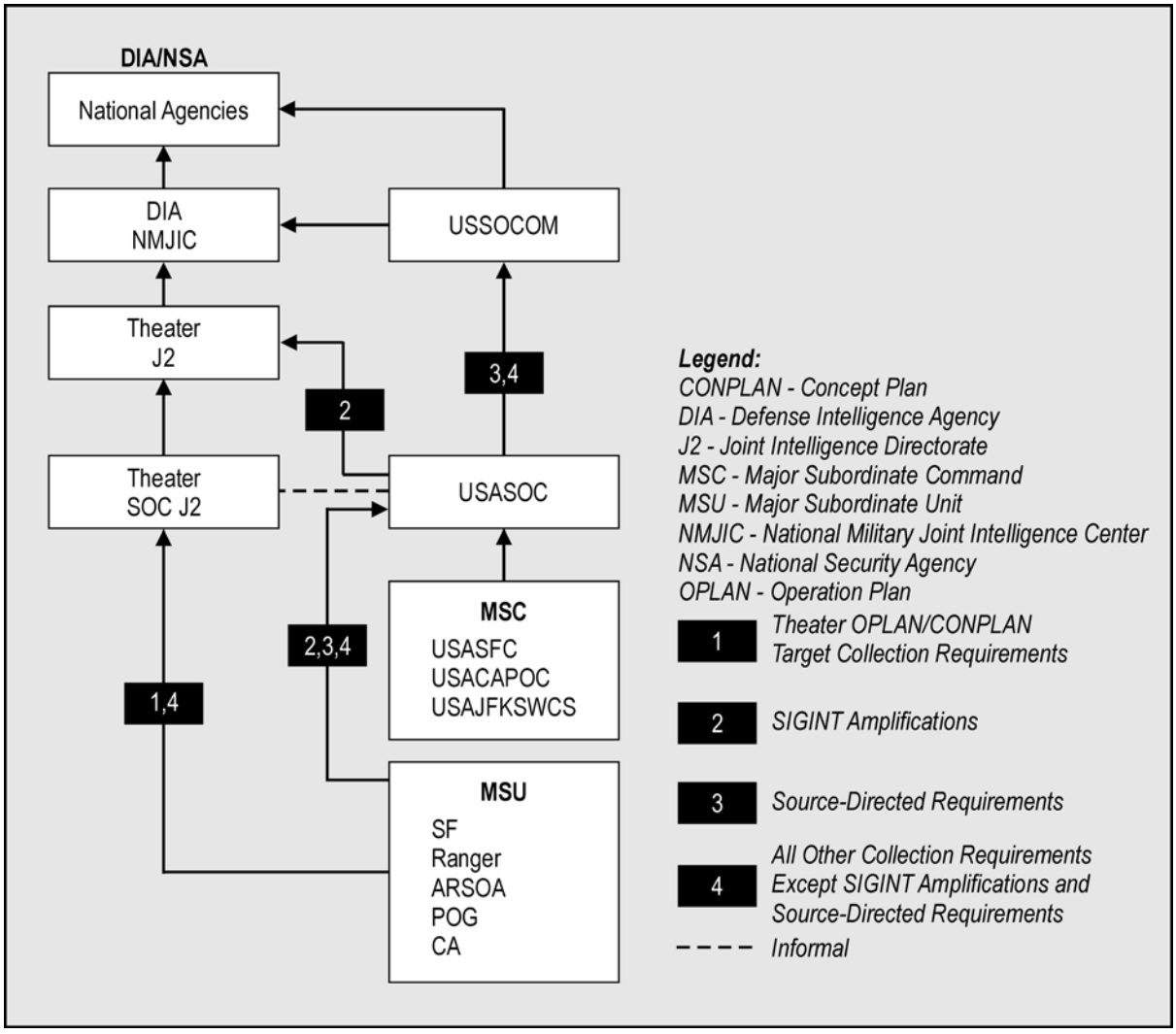


Figure 2-2. SOF IEW Requirements System

INTELLIGENCE IN THE MILITARY DECISION-MAKING PROCESS

2-18. The commander continually faces situations involving uncertainties, questionable or incomplete data, or several possible alternatives. As the primary decision maker, the commander, with the assistance of his staff, not only must decide what to do and how to do it, but he also must recognize if and when he must make a decision.

2-19. The MDMP is a tool that helps the commander and staff to develop estimates and a plan. It consists of seven steps:

- Step 1. Receipt of mission.
- Step 2. Mission analysis.
- Step 3. COA development.
- Step 4. COA analysis.
- Step 5. COA comparison.
- Step 6. COA approval.
- Step 7. Orders production.

2-20. The MDMP usually begins with either the receipt or the deduction of a mission by the commander. The operation order (OPORD) or tasking order (TASKORD) that a unit receives from its higher HQ lists tasks the higher HQ assigns to the unit.

2-21. During the MDMP, the IPB process intensifies. The ARSOF staff conducts the battlefield area evaluation (BAE), including clarifying the AO with the J3, G3, and/or S3 and determining the area of interest (AI). The S2 begins by pulling from available intelligence databases, both organic and via intelligence link (INTELINK). The S2 performs terrain and climate analysis, then contacts his supporting special operations weather team (SOWT) for target weather information. The S2 also analyzes the threat, determines its capabilities and vulnerabilities, prepares a situation template, and hypothesizes likely threat COAs. This basic process is applicable to any ARSOF primary mission or collateral activity.

2-22. The S2 is responsible for production of the intelligence estimate. This estimate consists of an analysis of the threat situation within the AI and the characteristics of the AO in terms of how they can affect the mission. The S2 uses the intelligence estimate to present conclusions and make recommendations, as appropriate. These might concern the following:

- The effect of the AO on friendly and enemy forces.
- The COAs open to the enemy and the order of their adoption.
- Enemy strengths, capabilities, and vulnerabilities that the force can exploit.
- The feasibility of various friendly COAs.

FM 34-3, *Intelligence Analysis*, provides detailed information on the intelligence estimate process.

2-23. The MDMP provides the most thorough mission analysis approach available in constrained time environments. The MDMP arrives at a solution to a problem (the "how" of conducting the mission) by analyzing in detail a number of friendly options against the full range of reasonable and available threat options. The resulting plan then serves as an optimum start point for later quick and effective adjustments as the unit begins its mission.

INTELLIGENCE CYCLE

2-24. Intelligence operations follow the intelligence cycle. The intelligence cycle focuses on the mission and the commander's concept of the operation. Intelligence operations have to be integrated into overall operations to achieve the commander's objectives.

2-25. The intelligence cycle follows a five-step process that focuses and directs intelligence operations. JP 2-01 defines the intelligence cycle as the process by which information is converted into intelligence and made available to users. The main goal of this cycle is to meet the commander's PIR and IRs and to keep intelligence current and relevant to upcoming operations.

2-26. The intelligence cycle conceptual model describes the process used to produce intelligence. There are no firm boundaries delineating where each phase of the cycle begins or ends. The intelligence cycle provides a process to understand and order the many activities involved in intelligence and is useful for understanding the interrelationships of the intelligence phases. The intelligence process may not continue through the entire cycle. For example, critical target data may be passed directly to the operator from a source, bypassing intermediates. Intelligence operations begin with a need for intelligence about the threat and environment of the AO and AI.

2-27. Each of the five steps is interwoven with tactical decision making and operational requirements. The S2 ensures that intelligence personnel actively participate in all aspects of mission planning and supervises each step. Figure 2-3, page 2-10, shows ARSOF unit intelligence cycle functional responsibilities. Note the redundancy of coverage inherent in the process. The five steps of the intelligence cycle are continuous; as a process model, they are conducted in sequence, but in reality, all are conducted concurrently. While available information is processed, additional information is collected, and the intelligence staff is planning and directing the collection effort to meet new demands.

2-28. Previously collected and processed information (intelligence) is disseminated as soon as it is available or needed. Often this process may be compressed to meet mission requirements. Products resulting from this process are used to support the ARSOF commander's changing PIR and IRs.

2-29. Intelligence planning begins concurrently with other staff planning. Detailed operational planning cannot be completed until an intelligence estimate is available. The S2 must be ready to provide an estimate for the existing operation and revise the current estimate to meet changing operational conditions.

2-30. As planning progresses and operational details are developed, the commander continues the decision-making process. As a result, intelligence plans are either substantiated or changed. The further an operation is projected into the future, the more likely it is that changes in the situation will alter intelligence plans. The commander's intent, concept of the operation, and the intelligence estimate are the basis for allocating resources. Intelligence planning and supervising must remain flexible.

UNIT	FUNCTION																				
	DIRECTION		COLLECTION					PROCESS		PRODUCTION							DISSEMINATION PROCEDURE(S)				
	DET RQMTS	TASK	GEN RQMTS	PRI RQMTS	VAL RQMTS	COL RQMTS	ASSET MGT	REC	EVAL	I&W	OB	THRT ASMT	CUR INTEL	EST	TGT INTEL	MDCI	DOWN-GRADE	SAN	FWD TO USER
SOC/JTF*	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
USASOC	X		X	X	X	X		X	X	X	X	X	X	X		X	X	X	X
USASFC	X		X	X	X			X	X									X	X
USACAPOC	X		X	X	X	X													
SOTSE	X		X	X	X	X			X		X	X	X	X	X		X		X
SF	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X
PSYOP	X	X	X	X	X	X	X	X	X		X	X	X	X	X		X		X
CA	X	X	X	X	X	X	X	X	X		X	X	X	X	X		X		X
ARSOA	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X
RANGER	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X
SO SIG BN	X		X										X						X
SO SPT BN	X		X										X						X

Legend:
** - When Deployed*
COL RQMTS - Collate Requirements
CUR INTEL - Current Intelligence
DET RQMTS - Determine Requirements
EST - Estimate
EVAL - Evaluate
FWD - Forward
GEN RQMTS - Generate Requirements
MDCI - Multidiscipline Counterintelligence
MGT - Management
PRI RQMTS - Prioritize Requirements
REC - Received
SAN - Sanitize
SIG - Signal
SOTSE - Special Operations Theater Support Element
SPT - Support
TGT INTEL - Target Intelligence
THRT ASMT - Threat Assessment
VAL RQMTS - Validate Requirements

Figure 2-3. Intelligence Cycle Functional Responsibilities

PLANNING AND DIRECTION

2-31. The commander, through the S2, directs the intelligence effort. The ARSOF S2 performs collection management planning before the operation begins and guides the effective employment of collection resources during the operation. Databases are developed and maintained through research and IPB. IPB, coupled with available databases, provides a foundation for situation and target development. This process provides a means for projecting battlefield events and activities in the operational area and for predicting COAs. By comparing these projections with actual events and activities as they occur, the S2 can provide the commander with timely, complete, and accurate intelligence.

2-32. Intelligence agencies from national level down constantly develop and maintain intelligence databases. The S2 accesses these databases to prepare initial intelligence estimates, analyze the AO, and identify probable enemy COAs. This analysis is based on mission requirements and the commander's PIR.

2-33. The S2, with thorough knowledge of all operational factors, develops collection requirements to support the commander's concept of the operation. The intelligence staff—

- Accesses databases.
- Tasks subordinate assets and submits collection requirements to higher echelons.
- Assesses capabilities.
- Directs, processes, and disseminates intelligence and combat information during and after deployment.
- Uses intelligence capabilities to forecast foreign intent, COAs, and vulnerabilities.
- Coordinates MDCI support before, during, and after the operation.

As these mission requirements change or as old requirements are met and new requirements are established, the S2 develops new PIR and IRs to answer them.

COLLECTION

2-34. Collection entails gathering information from all sources. PIR and IRs guide collection operations. The S2 focuses on named areas of interest (NAIs) that are points or areas where activity confirms or denies a particular threat COA or on target areas of interest (TAIs) that are engagement points or areas for ARSOF operations.

2-35. ARSOF TAIs could include key installations and critical facility nodes within a strategic target system. TAIs could also include nontraditional military targets such as the attitudes and beliefs of a given population group or even the psychological makeup of a particular foreign leader.

2-36. For ARSOF, the collection phase of the intelligence cycle begins as soon as mission area requirements are identified. The collection process uses all the means available within the IEW system—internal and external to the

ARSOF organizations. Collected information is reported to the collection manager of the S2 section or MI detachment. As incoming reports are received, they are matched with the collection requirements and forwarded to the all-source production section (ASPS) for processing.

PROCESSING

2-37. Processing is the phase of the intelligence cycle where information becomes intelligence. Collected data is transformed into a product that can readily be used in the analysis and production of intelligence. Processing results in a finished intelligence product that the ARSOF commander, staff, and operational elements use for planning and executing the mission. Processing consists of the three activities discussed below.

Recording

2-38. Recording refers to the integration of new information in the recording method being employed. The variations in recording and displaying information will affect how the information will be used. Recording can be done manually or by computer. It ranges from logging incoming message traffic to annotating digital microterrain products or posting information on an incident map or trap overlay.

Evaluation

2-39. Evaluation determines if the information is pertinent, reliable, and accurate. The analyst can rule out or confirm the validity of the information by applying his knowledge of threat doctrine, comparing reports from different disciplines, checking data files, and so forth. However, this process can require the reorientation of collection assets to confirm or deny the validity of a given report. This flexibility is especially critical for ARSOF units preparing to operate against targets in denied areas.

Analysis

2-40. Analysis determines the significance of the information on the basis of information and intelligence already known, and then draws conclusions about the probable meaning of the evaluated information. Analysis is a continuous process applied to all available data. However, it becomes critical during the threat integration function of the IPB process. I&W is another important task performed through analysis.

PRODUCTION

2-41. The production phase involves integrating, evaluating, analyzing, and interpreting confirmed information from single or multiple sources into a situation update or an assessment formatted as a document or briefing. Such finished intelligence addresses the specific intelligence concerns of the unit. Time constraints and operational considerations often tend to make the processing and production phases merge together.

DISSEMINATION

2-42. The final part of the intelligence cycle is dissemination. Intelligence and combat information are of little value if they are not delivered when and where they are needed. Failure to disseminate defeats a thorough and successful collection and processing effort. Since most intelligence and combat information is time-sensitive, intelligence products must be disseminated to the ARSOF commander and his planners and operators when they need it and in a form they can use. Dissemination is driven by ARSOF operational requirements. The fast-moving nature of ARSOF operations often dictates the need for transmitting information quickly. Combat information is reported through intelligence channels for processing and dissemination. Intelligence, combat information, and targeting data must be disseminated by using established procedures through a reliable, secure communications architecture, preferably in a near-real-time (NRT) fashion.

CHARACTERISTICS OF EFFECTIVE INTELLIGENCE

2-43. The effectiveness of intelligence is measured against certain standards. A failure to achieve any one of these standards may contribute to the failure of an ARSOF operation.

TIMELINESS

2-44. Intelligence must be provided early enough to support planning, influence decisions and execution of operations, and prevent surprise from enemy action. It must flow continuously to the customer before, during, and after an operation. The SOF S2 must work with the S6 to develop a robust intelligence communications architecture capable of overcoming challenges of distance and time to make information databases and products available to develop estimates, make decisions, and plan operations.

RELEVANCE

2-45. Intelligence must support the commander's concept of operation and the unit's mission. It must be tailored to the capabilities of the unit and intelligence priorities of the commander. Intelligence must be in a usable format that meets the specific needs of the requestor and explains its own significance. The intelligence section must anticipate these requirements based on the unit's capabilities. For example, when supporting a maritime operations team, tidal data should be available.

ACCURACY

2-46. Intelligence must give the commander a balanced, complete, and objective picture of the enemy and the operational environment. It should support and satisfy the priorities of the commander. To the extent possible, intelligence should correctly identify threat intentions, capabilities, limitations, and dispositions. It should be derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretation. Alternative or contradictory assessments should be presented, when necessary, to ensure balanced and bias-free intelligence.

PREDICTABILITY

2-47. Intelligence should tell the commander what the enemy is doing, can do, and his most likely course of action (MLCOA). Intelligence should anticipate the needs of the commander. Once an SO team deploys, the ability to push intelligence to the team may be very limited. Branches and sequels to the MLCOA should be discussed in as much detail as time permits.

INTELLIGENCE DISCIPLINES

2-48. Intelligence areas are divided into five general intelligence disciplines and two multidiscipline functions. The five general intelligence disciplines are—

- Open-source intelligence (OSINT).
- HUMINT.
- IMINT.
- SIGINT.
- Measurement and signature intelligence (MASINT).

The two multidiscipline functions are—

- CI.
- TECHINT.

2-49. By themselves, the disciplines and functions will rarely provide a comprehensive picture of the threat or situational awareness. Instead, each provides fragments of information that are synthesized through an analytical process to approach total situational awareness. If the sources of an intelligence product are from only one intelligence discipline, the final product is called a single-source intelligence product. The following are SOF-related examples of each intelligence discipline.

OPEN-SOURCE INTELLIGENCE

2-50. OSINT is information of potential intelligence value that is available to the public. Applying OSINT means leveraging expertise from outside the U.S. intelligence community. This creates an additional risk that must be weighed against developing the best possible visualization of the battlefield. OSINT processing analyzes and presents text, graphics, sound, and motion video in response to user requirements. For example, at the national level, the Foreign Broadcast Information Service (FBIS) provides translations of foreign broadcast and print media. As information technology becomes more readily available, ARSOF intelligence analysts must be able to exploit these sources, even at remote locations. OSINT may be the primary intelligence source for many ARSOF operations.

HUMAN INTELLIGENCE

2-51. HUMINT is derived from information collected and provided by human sources. HUMINT collection includes tactical reporting from combat units (patrols, SR, CI, and HICs) or by SOF operating in denied or politically sensitive areas. ARSOF units provide the IEW system with HUMINT through area assessments, SR, and postoperational debriefing of units. MI units support ARSOF with HUMINT through controlled collection (for

example, CFSO), interrogation, and tactical HUMINT operations. HUMINT is often the only source that can satisfy critical ARSOF intelligence requirements, whether from overt or controlled sources. Information collected by HUMINT collection is often unavailable by technical means. HUMINT is particularly important during stability operations and support operations when the detection of emerging threats cannot be satisfied by other means. However, early planning, placement, and synchronization of assets are critical factors in the success of HUMINT operations. HUMINT operations normally require long lead times to train and rehearse, gain access to a target area, and begin collection. Though it is not the easiest collection means to employ, HUMINT may often be the key to ARSOF mission success.

2-52. Typical CI and HUMINT collection operations include—

- HN liaison to determine foreign intelligence services (FIS) and terrorist threats.
- Overt elicitation of local nationals to monitor potential demonstrations, riots, and criminal activities.
- Interrogation of EPWs.
- Debriefing of SR and other friendly forces.
- Interpreter duties.
- Target language document exploitation (DOCEX).
- Open-source MDCI threat assessment.
- Area threat vulnerability assessment (TVA).
- CFSO.

IMAGERY INTELLIGENCE

2-53. IMINT is derived from the exploitation of products from visual photography, video, or infrared, electro-optical, and radar sensors. ARSOF units use IMINT for target analysis, infiltration and exfiltration, and general reconnaissance or area orientation. The results of the exploitation and the annotated images may be incorporated into an all-source product focusing on a given enemy target, target type, or activity.

SIGNALS INTELLIGENCE

2-54. SIGINT includes all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). The NSA exercises control over all SIGINT operations. SIGINT elements either assigned to or supporting Army SO may process COMINT. Depending on the level required for subsequent analysis and reporting, units in the operational area may forward collected information to higher-level assets or agencies for further processing. ELINT processing in support of SO may come from a number of sources, including assets attached to ARSOF, national ELINT assets, or combatant command intelligence production centers. ARSOF units use SIGINT products to prepare for and conduct infiltration and exfiltration, to locate actual or potential threat positions, and to determine or analyze possible enemy COAs.

MEASUREMENT AND SIGNATURE INTELLIGENCE

2-55. MASINT includes highly sophisticated application of technology and processing techniques to detect and identify specific foreign weapon systems on the basis of inadvertent signatures. This identification helps determine capabilities and intentions. One MASINT collection system currently organic to SF and Ranger units is the improved-remotely monitored battlefield sensor system (I-REMBASS), which can be employed to conduct FP operations.

COUNTERINTELLIGENCE

2-56. CI provides analysis of foreign intelligence threats to include espionage, sabotage, subversion, assassination, terrorism, and other threats. CI is a multidisciplined function that incorporates counter-HUMINT, counter-IMINT, and counter-SIGINT aspects to defeat or hinder threat intelligence collection and targeting. See FM 34-60, *Counterintelligence*, for more information on CI operations. The major CI functions are investigation, collection, operations, and analysis and production.

2-57. CI operations—

- Must include specific actions that support the protection of the force.
- Counter the foreign multidisciplined intelligence threat.
- Counter foreign sabotage, subversion, assassination, and terrorism.
- Can include conducting CFSO when approved by geographic CINC.

2-58. CI agents can support—

- Personnel security or information security (INFOSEC).
- Physical security.
- OPSEC.

2-59. MDCI analysis provides ARSOF commanders detailed assessments of foreign all-source intelligence and security threats near their operational bases and in their operational areas. These foreign threat assessments are critical to the unit's OPSEC and base defense programs to support the total FP effort. MDCI analysts also support ARSOF deception operations by determining foreign intelligence collection assets and how to thwart those collection efforts. MDCI analysts provide the S3 recommendations of friendly activities to support the deception. If these activities are used, the MDCI analysts will help evaluate their effectiveness.

TECHNICAL INTELLIGENCE

2-60. TECHINT is another multidisciplined function. It focuses on foreign technological developments and the performance and operational capabilities of foreign materiel that have or may eventually have a practical application for military use. ARSOF use TECHINT products to exploit foreign weapons and other targetable systems. Since ARSOF units often operate deep in hostile or denied territory, they are often first to discover, identify, and provide information on new or previously unidentified materiel.

ARSOF INTELLIGENCE TASKS

2-61. Like conventional MI, ARSOF IEW organizations accomplish their missions through six primary tasks that provide synchronized support for the commander's missions. These functions are further described in Figure 2-4 and the following paragraphs.

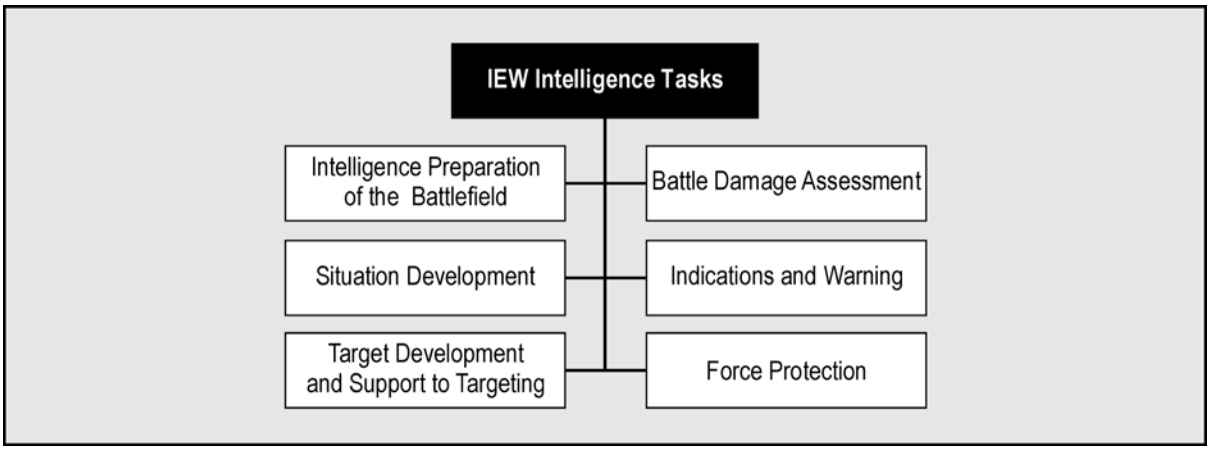


Figure 2-4. Intelligence Tasks

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

2-62. *Intelligence preparation of the battlespace* as defined in JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, is an analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process.

2-63. *Intelligence preparation of the battlefield (IPB)* as defined in FM 34-130, *Intelligence Preparation of the Battlefield*, is a systematic approach to analyzing the enemy, weather, and terrain in a specific geographic area. It integrates enemy doctrine with the weather and terrain as they relate to the mission and the specific battlefield environment. This is done to determine and evaluate enemy capabilities, vulnerabilities, and probable COAs.

2-64. SOF intelligence units continuously perform both of these tasks. The process for both tasks is the same. However, the resulting products and requests for information to support a team conducting a DA mission will be very different from the products and requests when supporting an SFOB conducting a FID mission. For detailed charts and an explanation of IPB, see FM 34-130.

2-65. IPB consists of four phases. Each of these phases produces the following particular products:

- *Define the battlefield environment.* This phase determines the boundaries of the AO and AI through coordination with the S3. At the completion of this phase, an accurate set of operations graphics has been produced.
- *Describe the battlefield's effects.* During this phase, intelligence personnel examine and determine the potential effects of terrain and weather in the target area on both friendly and enemy operations. The S2 section produces the modified combined obstacles overlay (MCOO) and other terrain products, as required. These may include a line of communications (LOC) overlay, a hydrology overlay, or an objective sketch. Weather analysis includes study of climatological, weather, and light data, and how each may affect both friendly and enemy operations. The S2 section, with support from the SOWT, produces a short brief on the climate in the target area, a light data chart for the time frame of the mission, and a weather forecast projected as far forward as possible, with expected effects on friendly and enemy capabilities. The S2 should also ensure that the possible effects of the weather on available light are discussed (for example, cloud cover obscuring moonlight).
- *Evaluate the threat/adversary*. Intelligence units use this evaluation process to generate doctrinal templates showing how threat units of the type known to be located in the target area would deploy for combat without the constraints of terrain and weather.
- *Determine threat/adversary COA.* In this phase, incoming information on threat units in the target area is integrated with the staff into the following different products:
  - A **situational template** incorporating the current situation, enemy doctrine, and OB, postulates how enemy units in the target area will react to the constraints of terrain and weather. A separate situational template should be produced for each possible enemy COA determined by the S2.
  - The **event template** depicts the phases of an enemy COA. It incorporates time-phased lines (TPLs) to portray direction and rates of movement and identifies NAIs for the commander.
  - The identification of enemy **high-value targets (HVTs)** are assets the commander requires for successful completion of his mission. The enemy must allocate resources to protect these assets that, in turn, feed into the targeting process and are used to generate the friendly high-payoff target (HPT) list.
  - As a result of war gaming, the planning staff produces the **decision support template (DST)** that identifies both friendly and enemy decision points and the commander's TAIs.

SITUATION DEVELOPMENT

2-66. Situation development is the process of continuously collecting and integrating intelligence and combat information to provide successive

estimates of the situation and projections of threat capabilities and intentions. These products let ARSOF commanders see and understand the operational environment in enough time and detail to employ their forces effectively. Situation development incorporates all five steps of the intelligence cycle.

TARGET DEVELOPMENT AND SUPPORT TO TARGETING

2-67. ARSOF conduct target development during peacetime, conflict, and war. ARSOF employ two distinct target development processes that overlap. These processes are the—

- Deliberate targeting process—a long-term process that occurs during peacetime.
- Adaptive targeting process—an accelerated process used during crisis or war.

2-68. The MI concept of targeting outlined in FM 34-series publications most closely parallels the SOF adaptive targeting process found in JP 3-05.5, *Joint Special Operations Targeting and Mission Planning Procedures*, and in FM 3-05 (FM 100-25). The target analysis technique used by SOF is criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER) as described in JP 3-05.5.

Deliberate Targeting Process

2-69. In the deliberate targeting process, ARSOF missions focus on facilities, installations, and system components that are critical to a threat's warfighting capabilities, infrastructure, or internal stability. This target selection program must examine all potential target systems to determine which are best suited to accomplish the geographic CINC's objectives. Since the deliberate targeting process occurs before hostilities, critical node selection is based on peacetime databases and analysis.

Adaptive Targeting Process

2-70. In the adaptive targeting process, target selection goals are not confined to destroying or damaging a fixed target. The major goals are to alter, affect, impede, or report threat activity. Threat targets that are identified and located by ARSOF in the JSOA become a potential set of targets.

2-71. However, while a conventional forces' targeteer can task units to pursue threat forces—much as a hunter stalks prey—the ARSOF targeteer must approach the deep-battle adaptive targeting process with the mindset of a trapper. The ARSOF S2 examines the JSOA and its adjoining areas to predict threat force movement patterns and activities. These analyses result in identifying NAIs that the ARSOF commander can nominate as future TAIs. These TAIs can then become assigned JSOAs for ARSOF missions.

2-72. The ARSOF S2 must know that the targeting process depends on the effective and timely use of the intelligence cycle. ARSOF target development is the result of complete and accurate situation development during peacetime, contingency planning, and battlefield analysis during conflict or

wartime. The IPB supports the target development process and provides the ARSOF commander with the intelligence needed to select valid target nodes for his operational element.

BATTLE DAMAGE ASSESSMENT

2-73. BDA, or combat assessment in some theaters, is an analytic method to determine the relative success of a mission against an enemy target. BDA is used to confirm or deny changes to enemy methods or patterns of activity that directly affect friendly operations. This makes BDA a predictive tool, as well as a measurement tool, for evaluating the degree of success of an operation, engagement, or battle. BDA gives the commander a continual assessment of enemy strength and the effect of friendly operations on the enemy. It is a means to measure progress, to determine if another strike is needed, and to determine how close the unit is to accomplishing targeting goals.

INDICATIONS AND WARNING

2-74. I&W is a critical subtask of the processing step of the intelligence cycle. This subtask is where the national strategic community monitors threat activity to determine if their political, military, economic, or diplomatic actions are a prelude to hostilities or other acts contrary to U.S. interests.

2-75. ARSOF are consumers and producers of I&W reporting. They use I&W reporting on world political-military developments to focus and refine their intelligence databases and to update and guide their contingency planning. Operational I&W intelligence becomes increasingly critical once an ARSOF element enters its final mission preparation and execution stages. Once deployed, ARSOF elements can provide unique, initial I&W reporting from denied areas and can confirm or deny I&W reporting from other sources.

FORCE PROTECTION

2-76. FP identifies the elements of the force most important to the threat and those elements most vulnerable to detection and attack through MDCI analysis. The purpose of FP is to deny the threat the opportunity to engage friendly forces, enabling ARSOF to achieve enhanced results during operations. FP includes the integrated application of physical security, CBT, OPSEC, and personal protective services.

Chapter 3

IEW Support to Special Forces Operations

This chapter describes the IEW support required for SF missions. It describes SF organization missions and the intelligence units that support SF. It provides specific information on organization, functions, and roles of each participating intelligence element. FM 3-05.20, *Special Forces Operations,* contains further information on SF organizations.

INTRODUCTION

3-1. The Special Forces group (airborne) (SFG[A]) is a unique combat arms organization. It can plan, conduct, and support SO in all operational environments and across the range of military operations. SF commanders integrate and synchronize their organic capabilities with those of other SOF and theater assets. Each SFG(A) is assigned an AOR, depending on OPLAN requirements, that provides the regional focus, which is a hallmark of ARSOF operations.

SF MISSIONS

3-2. SFG(A)s conduct UW, FID, DA, SR, CBT, counterproliferation (CP), and IO and collateral activities as required and within their capabilities. These wide-ranging missions require accurate, detailed, and timely intelligence that only a multidisciplined collection and analysis intelligence organization can obtain.

UNCONVENTIONAL WARFARE

3-3. UW is a broad spectrum of military and paramilitary operations against an established government or occupying power. UW operations normally are of long duration. Indigenous or surrogate forces organized, trained, equipped, supported, and directed in varying degrees by an external source predominantly conduct them.

3-4. UW includes GW and other direct offensive, low-visibility, covert, or clandestine operations. UW also includes the indirect activities of subversion, sabotage, intelligence collection, and E&E. UW normally involves inserting SF elements into areas controlled by hostile forces.

3-5. SF elements need detailed information and all-source intelligence on targets and target systems in the area, the situation within and between the insurgent groups, and virtually all other pertinent information that can be gathered. SF elements also may require the aid of indigenous assets prior to infiltration to help them survive and make initial contact with the insurgents.

3-6. To provide the best possible security for the UW forces, local intelligence nets must be organized and resourced. They must also be organized and resourced to meet the supported commander's intelligence requirements.

3-7. SF operational elements must receive multidisciplined intelligence tailored to their specific mission. This intelligence must be all-source, processed, and presented in a usable format for planning and operational employment of indigenous elements. National and theater intelligence means may be required to identify potential in-country sources.

3-8. Intelligence gathering during UW comes from various sources, including those developed within the AO. SF elements contact insurgents and guide them in operations that support U.S. national objectives. The intelligence requirements to support UW and effectively integrate indigenous elements include—

- Military and paramilitary organizations.
- Economics.
- Politics.
- Climate.
- Geography.
- Sociology.
- Ethnic composition.
- Religious factors.
- Personalities.

3-9. Because UW operations are wide-ranging and diverse in application, they need a wide range of support. This support includes everything from basic support to very sophisticated systems using automated data processing (ADP) and intelligence specialties. All-source intelligence is essential regardless of the mission.

FOREIGN INTERNAL DEFENSE

3-10. During FID missions, SF and other ARSOF support an HN government. These missions could include military, psychological, or civil-military operations. For FID missions, SF personnel must be thoroughly knowledgeable of the HN's demographics, psychology, religions, customs, and infrastructure. They should also know the sources of internal and external friction and agitation within the HN that could impact on the acceptability and success of the government. Successful FID missions require the use of the IPB process to develop the following intelligence products:

- The supported HN's detailed defense and security establishments' OB.
- Details on foreign intelligence organizations active within the HN.
- OB on insurgent groups with the potential to destabilize the HN's government.
- Available country studies about the HN, its people, and its infrastructure, including land use, LOCs, and population density studies.
- Key personalities.

DIRECT ACTION

3-11. SOF (primarily SF and Rangers) conduct DA missions to achieve various goals. The goals could include—

- Attacking the threat's key nodes and diminishing the threat's warfighting capability.
- Developing desired psychological effects through decisive and quick action in unexpected places.
- Preemptive strike.
- Physical destruction of HPTs.

3-12. A mission requires, at a minimum, detailed knowledge of the target sites, the infiltration and exfiltration routes, and OB of any threat security, quick reaction, or counterattack forces. Information about the target area is by necessity more detailed than that required for conventional targeting.

3-13. DA missions are often launched against targets deep within enemy-controlled territory, often far beyond the sensing capabilities of tactical collection systems. Each target requires construction of its own target intelligence package (TIP) as part of the mission planning folder containing detailed, target-specific data and in-depth area studies of the AI. (See Appendixes B and C for more information about the TIP. Appendix B discusses the TIP in the special operations mission planning folder [SOMPF]. Appendix C discusses the TIP formats.)

3-14. A complete picture of the situation is developed after a multidisciplined analysis of all categories of intelligence is completed and provided to the SF element. Each mission is an extensive effort requiring—

- Development and maintenance of a specific target database or TIP.
- Continuous monitoring of pertinent crises and other specific geographical areas to facilitate DA missions identified in existing OPLANs or concept plans (CONPLANs).
- Accessibility to and coordination with national-, strategic-, and operational-level collection systems before, during, and after the mission.
- Multidisciplined analysis of all information supporting the mission.

SPECIAL RECONNAISSANCE

3-15. ARSOF elements conduct SR missions to obtain information not available through other means. These operations generally have the same requirements for detailed intelligence information as DA missions. The objective of these missions, however, is to satisfy intelligence gaps or to confirm information of critical importance.

3-16. SR operations encompass a broad range of intelligence collection activities to include reconnaissance, surveillance, and target acquisition. The SR collection effort emphasizes alliance or U.S. unilateral intelligence requirements, not the requirements of an indigenous resistance organization. SR complements national and theater collection systems (such as high-altitude imagery or SIGINT) that are more vulnerable to weather, terrain,

masking, and hostile countermeasures. SR missions provide critical "ground truth," which is often not available through other means.

3-17. Typical SR missions include—

- Collection of strategic, political, economic, psychological, or military information through indirect means.
- Collection of critical military OB information (for example, nuclear, biological, and chemical [NBC] capabilities and intentions, commitment of second-echelon forces, and location of high-level HQ) in support of conventional forces' PIR.
- Collection of technical military information.
- Target acquisition and surveillance of hostile C2 systems, troop concentrations, deep-strike weapons, LOCs, WMD systems, and other military targets of strategic or operational significance.
- Location and surveillance of hostage, prisoner of war (PW), or political prisoner detention facilities.
- Poststrike reconnaissance for BDA.
- Meteorologic, geographic, or hydrographic reconnaissance to support specific air, land, or sea operations.

COMBATTING TERRORISM

3-18. CBT is the overarching term used to describe missions involving both offensive and defensive measures against terrorists. These missions include preemptive, concurrent, and punitive actions. This category of SF mission is not generic to all SF units. SF participation in CBT is limited to those specially organized, trained, and equipped SF units designated in theater CONPLANs. Most CBT operations are classified and their detailed procedures are beyond the scope of this publication.

3-19. Because terrorist organizations maintain a very low profile, it is extremely difficult to identify targets for CBT missions. For the committed SF unit to execute its mission with precision and limit collateral damage, the IEW system must support the mission by providing extremely accurate, detailed, and responsive intelligence.

3-20. Intelligence support to CBT must identify terrorist personalities, locations, organizational composition, and logistical support systems. It also must describe their weapons, equipment, training, and tactics, as well as pertinent information about any hostages. Close coordination between mission planners and various national and military intelligence agencies or law enforcement agencies is required to collate, analyze, and immediately provide the SF unit performing the CBT mission with the information it requires.

COUNTERPROLIFERATION

3-21. CP is a specialized mission assigned to designated SOF. CP-WMD missions of SF may include locating, identifying, and safeguarding WMD. Unless otherwise specified, all references to the performance of CP are OCONUS. SF is particularly well-suited to address these requirements because of its cultural orientation and linguistic capabilities. SF participation

in CP is through the conduct of SR, DA, and UW. Intelligence support to SF requires proactive and complete integration of the intelligence operations with the targeting cycle. Further discussion of CP is beyond the scope of this publication.

INFORMATION OPERATIONS

3-22. IO involves actions taken to affect adversary information and information systems, while defending one's own information and information systems to achieve information superiority in support of national military strategy. SF missions that support IO are UW, DA, SR, and FID. In addition to the requirements discussed with UW, DA, SR and FID, intelligence support to IO requires that intelligence assets and resources be allocated to determine the effectiveness of the IO. Internally to the SFOB and FOB, effective intelligence operations are required to support EW, OPSEC, and deception (the subordinate components of IO).

SF INTELLIGENCE ORGANIZATION

3-23. SF operations require leveraging organic IEW support with commensurate analysis, collection management, security, weather, and communications capabilities tailored to supported regional command requirements across the range of military operations.

3-24. The SFG possesses the most robust organic IEW structure of any ARSOF unit. The organization of SF intelligence assets is according to operational and analytical needs. There are IEW assets at the group, battalion, company, and SFODA levels. Each intelligence asset has its own missions, functions, and limitations.

3-25. The SF groups' intelligence staffs and MI detachments are the key components of the organic IEW team at the group or battalion level. The SF staff plans, organizes, directs, coordinates, and controls while the MI detachment commander executes the directives.

GROUP S2 SECTION

3-26. This section consists of an S2, assistant S2, and an intelligence warrant officer. Figure 3-1, page 3-6, depicts the SFG(A) S2 section.

Group S2

3-27. The group S2 is the MI major who is the primary staff officer responsible for all aspects of intelligence, CI, and security support in garrison and while deployed. He plans, coordinates, and directs all group-level intelligence collection, analysis, and production and approves all products prior to dissemination. He develops and recommends PIR and IRs for approval by the group commander, and maintains the group collection plan with the assistance of the group MID collection management and dissemination (CM&D) team. The S2 directs all group-level intelligence collection operations involving organic or attached assets operating out of the SFOB or Army special operations task force (ARSOTF).

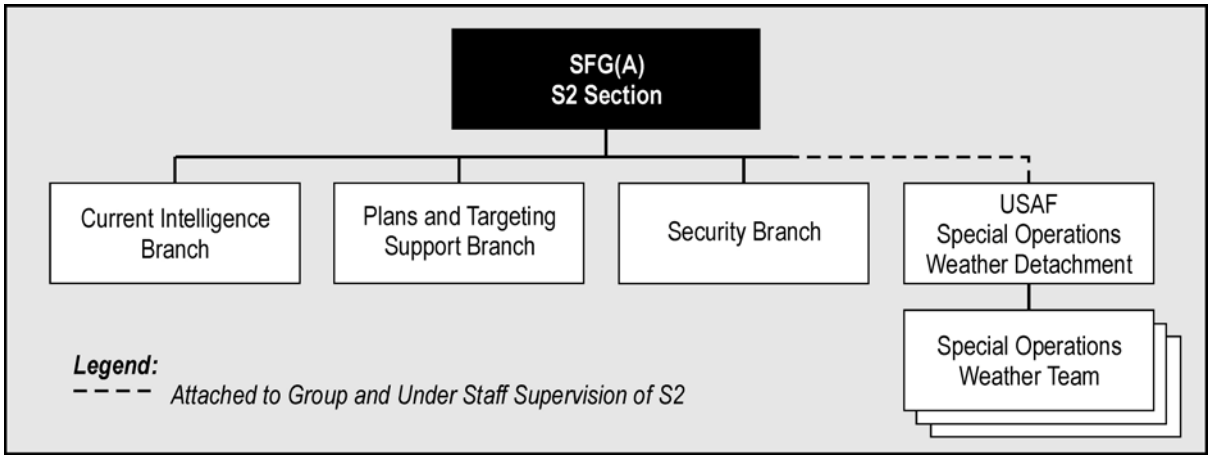


Figure 3-1. S2 Section, SFG(A)

3-28. The S2 identifies the need for collateral and sensitive compartmented information (SCI) intelligence communications support and intelligence ADP systems support. He works with the S6 in planning and coordinating SCI and ADP systems support. The S2 validates GI&S requirements and product requests. He conducts or coordinates for a wide variety of CI activities in support of group OPSEC and FP needs. When an SFOB is established, the S2 serves in the operations center (OPCEN) under the staff supervision of the OPCEN director. The S2 is responsible for the group's information security, information systems security for SCI systems, personnel security, and special security programs. He establishes and ensures that the group maintains an intelligence training program that trains MI and SF personnel. He coordinates with the group MID commander to establish a tactical sensitive compartmented information facility (T-SCIF). He coordinates tasking and OPCON of group MID assets with the requesting SF unit and the MID commander.

Group Assistant S2

3-29. The group assistant S2 is the MI captain who serves as the focal point for collection operations and current intelligence at group level. When the SFOB is established, he serves as chief of the S2 current intelligence branch, which is collocated with S3 operations in the OPCEN. His responsibilities include maintaining the current intelligence estimate and other current situation intelligence products and monitoring of the status of all deployed intelligence collection assets. He also develops taskings for the staff weather officer (SWO) and the United States Air Force (USAF) SOWT. The assistant S2 serves as the acting S2 or senior intelligence officer (SIO) in the absence of the S2.

Group Intelligence Warrant Officer

3-30. The group intelligence warrant officer is an SF warrant officer (180A) who is the assistant S2 for plans and targeting support at group level. When the SFOB is established, he serves as chief of the S2 plans and targeting support branch, which collocates with the S3 plans branch. He is responsible

for coordinating all aspects of intelligence support for future plans and targeting. For this reason, he must be completely familiar with all of the intelligence functions of the group MID. As the senior SF member of the S2 section, he works with and helps the group S2 and MID commander develop, focus, and coordinate intelligence training for personnel holding military occupational specialty (MOS) 18F or 180A.

GROUP MID

3-31. The group MID contains most of the group's single-source and all-source analysis capability. The MID is responsible for—

- Collection management.
- Single-source collection (SIGINT and CI/HUMINT).
- All-source fusion of single-source information.
- Analysis, production, and dissemination of finished intelligence products.
- Control and management of the attached SCI local area network (LAN) team.

The MID consists of four subordinate sections with functionally different responsibilities (Figure 3-2).

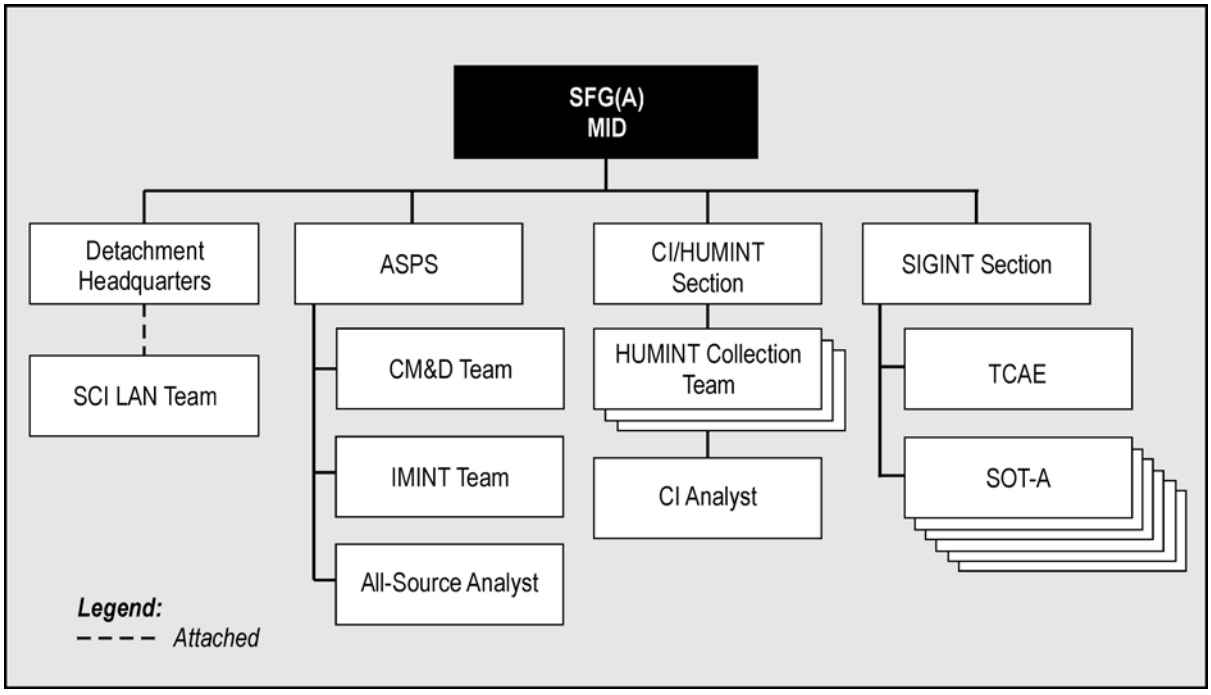


Figure 3-2. Special Forces Group MID

MID Commander

3-32. The MID commander has broad responsibilities, both directing the efforts of the analytic elements of the MID and mission support for the

intelligence collection activities of the SOT-As and CI/HUMINT teams deployed forward. The MID commander works directly with the S2, helping him develop the group's concept for intelligence operations. The MID commander is responsible for implementing the MID task organization, deploying collection assets and analytic augmentation to subordinate units as directed by the group commander. He is normally responsible for Uniform Code of Military Justice (UCMJ) and limited administrative actions for the MID, individual and collective training for MI specialties, and property accountability for equipment unique to the MID. However, the MID does not have the organic maintenance, supply, or administrative personnel to operate independently. The MID must rely on and coordinate closely with the group support company (GSC) for administrative and logistics support.

SCI LAN Team

3-33. The SCI LAN team is organic to the group signal detachment and operates in the T-SCIF. The team terminates SOT-A communications, and operates and maintains SCI communications and ADP systems linking the SFOB into the IEW system. They are responsible for maintaining SCI communications with higher and adjacent HQ and deployed FOBs.

All-Source Production Section

3-34. The ASPS is the hub of the MID and has broad intelligence support responsibilities. An all-source intelligence warrant officer (350B) directs the ASPS. The section has two subordinate elements with specific functions: the CM&D team and the IMINT team. It may be further subdivided into analysis teams focused on specific AORs in support of the subordinate battalions of the group.

3-35. The ASPS responds to all-source intelligence support taskings from the group S2. It provides in-depth all-source analysis, production, and collection management support to the group. It provides NRT I&W overwatch for deployed assets. The all-source analysts within the ASPS are responsible for developing the analysis of the AOR, IPB, target nomination development, and BDA. They prepare and continually update the current intelligence situation map (SITMAP). They maintain and use the unit intelligence reference files, databases, and intelligence ADP systems (see Chapter 8). They help the CM&D team develop the collection plan and identify new requirements to close any intelligence gaps. They prepare intelligence summaries and responses to requests for intelligence information (RIIs) and requests for information (RFIs) and provide intelligence briefings, as required. All the members of the ASPS contribute to the preparation of the intelligence estimate and its corresponding annexes. The all-source analysts are responsible for disseminating products to subordinate units in the required format. The ASPS coordinates production and enhances TIPs for subordinate FOBs, as required.

3-36. *CM&D Team*. The CM&D team of the ASPS receives, validates, and prioritizes all RIIs and RFIs from subordinate units and assigns them to the appropriate MID section. The section informs the ASPS chief upon PIR satisfaction and recommends new PIR, IRs, and specific information requirements (SIRs) for submission to the S2. It reports intelligence to higher

or lateral HQ, based on guidance from the S2, and coordinates dissemination of intelligence to subordinate and attached units.

3-37. A senior noncommissioned officer (NCO) leads the CM&D team. Because of limited personnel, the team may augment with other intelligence personnel from within the MID, as required. It develops and helps implement a dynamic collection plan that supports mission analysis and planning, targeting, I&W for deployed SFODs and SOT-As and FP requirements. Personnel from the single-source intelligence disciplines (SIGINT, CI/HUMINT, and IMINT) subordinate to the MID help the CM&D team with these tasks, as required. CM&D personnel work with the group S2 to develop the SFG(A)'s peacetime and contingency collection plans. As part of this effort, the team develops information objectives and collection emphasis. The team also works with the SIGINT and CI/HUMINT sections and the IMINT team to develop SIGINT amplifications, SIGINT end products review, and source-directed requirements (SDRs). The CM&D team also works with the S2 special security officer (SSO) to maintain the collateral-recurring document listing (CRDL), sensitive compartmented information-recurring document list (SCIRDL), and the statement of intelligence interest (SII).

3-38. *IMINT Team*. The IMINT team of the ASPS maintains and provides comprehensive historical and current imagery in hard and digitized form. The 96D imagery analysts of the team use their deployable light tables, secondary imagery dissemination system (SIDS), and imagery products from higher HQ to provide in-depth imagery analysis and production support to the group. This support includes detailed terrain and facility analysis, annotated prints and target graphics, current SIDS imagery of targets and key terrain, BDA, and highly accurate imagery-based object measurement support.

Signals Intelligence Section

3-39. The SIGINT section conducts single-source collection, collection management, and analysis. The section is led by a SIGINT warrant officer (352C) and consists of the TCAE and six signals intercept teams, known as SOT-As. The TCAE performs all SIGINT operational tasking authority (SOTA) functions on behalf of the group commander. The deployed TCAE or traffic analysis (TA) team exercises SOTA when it has been delegated.

3-40. *TCAE*. The TCAE accesses, updates, and maintains technical databases and appropriate SIGINT applications for specified countries within the SFG(A)'s AOR. The SIGINT analysts on this team operate the SIGINT-related programs accessed through the special operations forces intelligence vehicle (migration) (SOFIV-M). The TCAE provides critical, time-sensitive COMINT information to the all-source analysts (96B) within the ASPS to support situation development, intelligence summaries (INTSUMs), and intelligence briefings to the commander and staff. It is the TCAE's responsibility to provide technical reports to regional and theater SIGINT organizations. This effort occurs either during or after the deployment, depending upon time and communications path.

3-41. The TCAE—

- Determines specific SIGINT collection taskings from stated intelligence requirements received by the CM&D team.
- Monitors the effectiveness of collection efforts, redirecting coverage and providing technical feedback and support to the SOT-As and SIGINT personnel attached to SF battalion FOBs.
- Establishes, updates, and maintains the SFG(A)'s intercept tasking database.
- Ensures adherence to all legal aspects of SIGINT operations.
- Issues all appropriate SIGINT operational tasking authority reports.
- Establishes link to regional SIGINT operations center (RSOC) and national SIGINT elements in order to share single-source information between analysts.

3-42. The deployed TCAE team is an organic element of the SF group MID. The team is attached to the battalion from the group MID when directed by the group commander because signals intercept is required to support the operational mission. The group MID will task-organize the TA team from personnel and equipment organic to the group TCAE. The TA team will be accompanied by up to six SOT-As.

3-43. The SIGINT analysts of the TA team are responsible for FOB-level technical control of attached SOT-As, SIGINT analysis, and operational and technical reporting. They use and maintain threat electronic OB and technical support databases developed by the TCAE, or by other national- or theater-level SIGINT organizations. The TA team maintains the battalion SIGINT collection plan in coordination with the CM&D section. They translate general collection requirements assigned by the battalion CM&D section into specific SIGINT collection taskings for the SOT-As. Operational reporting consists of combat information that is purged of technical data and reported directly to the supported commander. Technical reporting is conducted through the TCAE communications architecture only.

3-44. *SOT-A*. The SOT-As are low-level SIGINT collection teams that intercept and report operational and technical information derived from tactical threat communications through prescribed communications paths. The mission of a SOT-A is to conduct SIGINT/EW in support of information operations (unilaterally or in conjunction with other SOF elements) to support existing and emerging SOF missions worldwide.

3-45. The primary roles of the SOT-A are FP (exploitation of threat communications and communications security [COMSEC]) and EW FID MTT. SOT-A collateral activities include signals research and target development (SRTD), electronic reconnaissance (ER), and support to personnel recovery (PR). The SOT-A is assigned roles dependent upon a thorough overall mission analysis and commander's approval. Up to six SOT-As may be attached to a subordinate battalion at the direction of the group commander. The SOT-As will be task-organized by the group MID according to mission requirements and predeployment analysis of the signals environment.

3-46. While engaged in an FP or early-warning role, a SOT-A—

- Can be employed in direct or general support to a SOF commander.
- Receives technical tasking from the accompanying TA team.
- Provides combat information (immediate threat, threat location, threat intent, threat capabilities and/or limitations, and so on) to the operational commander.
- Provides technical data to the TA team.

A SOT-A may also have collection missions in support of the S3 FP plan—for example, monitoring the supported unit's tactical communications for EEFI and signal security violations, and providing a COMSEC vulnerability assessment to the supported commander.

3-47. When conducting ER, the SOT-A can provide overall situational development information and locate and identify specific intelligence indicators to satisfy IRs (that is, target development, confirmation or denial of IPB information, and BDA). In this role, the SOT-A receives technical tasking from the TA team and reports technical data through the same element. A SOT-A conducts an SRTD at the request of either the theater or national elements, coordinated through the theater SOC. SRTDs are conducted to develop or verify current technical databases in potential theater hot spots, where national or theater assets do not routinely visit or have limited access.

3-48. A SOT-A using organic hand-held or manpack equipment can provide intercept and direction-finding of distress frequencies during PR missions. However, with the fielding of the combat survivor evader locator (CSEL) distress radio, this capability will be reduced. Any support to PR must be assigned with specific reporting instructions and should be assigned only after a thorough mission analysis.

3-49. If a SOT-A is to serve as an MTT as part of a FID mission conducted by an SF battalion or group, it must be approved by the NSA. The focus of any SIGINT training provided to HN SIGINT elements must be on low-level tactical SIGINT collection, radio direction-finding, and combat information recognition and reporting. Sharing advanced analytic functions and processes with third-party elements is not authorized.

3-50. SOT-As and TA teams can support all levels and types of SOF operations. SOT-As may deploy independently, operate together with other SOT-As, or may be attached to deploying SOF elements, into all three states of the environment.

CI/HUMINT Section

3-51. The CI/HUMINT section is responsible for a large number of tactical CI/HUMINT collection, analysis, production, and operational support activities. A counterintelligence warrant officer (351B) leads the CI/HUMINT section. The section consists of CI agents-analysts (97B) and HICs (97E) who operate in two-man teams. The CI agents and HUMINT collection teams may be attached to subordinate battalions. They are normally task-organized by language capability for this mission.

3-52. The section produces intelligence information reports (IIRs) and other formatted reports to disseminate the results of CI and HUMINT collection and liaison activities. The section uses locally collected intelligence and theater CI products to assess a wide variety of threats for the SFOB in the communications zone (COMMZ) or HN rear area. These threats include, but are not limited to, FIS; insurgents, terrorists, and criminals; dissident political factions; and anti-U.S. elements of the civilian population. The CI and HUMINT team also prepares and maintains the SFOB MDCI estimate, as well as comprehensive base defense, COMMZ, and HN rear area IPB products. These products permit the timely provision of I&W information and predictive intelligence on significant OPSEC and FP threats. The CI and HUMINT analysts develop the friendly force profiles and identify friendly vulnerabilities. When authorized, the CI/HUMINT analysts maintain a source management database.

3-53. In response to the situation and collection taskings from the CM&D team and the MID commander, the CI/HUMINT section plans, coordinates, and conducts CI liaison, EPW interrogation, DOCEX, overt collection, and refugee and evacuee debriefings. They also serve as the OPCEN staff focal point for FP operations. They process plans, coordinate source financial and administration support, and ensure regulatory intelligence oversight compliance. The team recommends EEFI and threat countermeasures and continually assesses the effectiveness of the base OPSEC countermeasures and base security plans. The CI and HUMINT team supports the OPSEC plan by providing Subversion and Espionage Directed Against U.S. Army (SAEDA) briefings and limited investigations. They also provide CI and security site surveys in support of SFOB relocations within the country and theater, as required.

BATTALION S2 SECTION

3-54. Figure 3-3 shows the organization of the SF battalion S2 section.

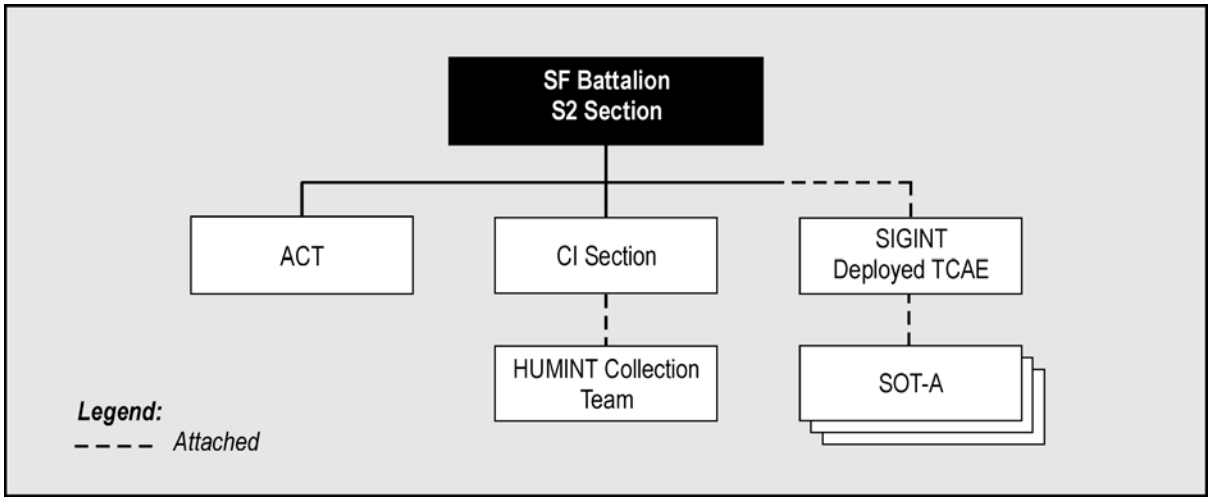


Figure 3-3. S2 Section, SF Battalion

Battalion S2

3-55. The battalion S2 is the primary staff officer responsible for all aspects of intelligence, CI, and security support in garrison and while deployed. He plans, coordinates, and directs all battalion-level intelligence collection, analysis, and production. The S2 also approves all products before dissemination. He develops and recommends PIR and IRs for approval by the battalion commander and maintains the battalion collection plan with the assistance of the analysis and control team (ACT). The S2 directs all intelligence collection operations involving battalion assets or attached assets from the group MID.

3-56. The S2 identifies the need for collateral and SCI intelligence communications support and intelligence ADP systems support. He works with the S6 in planning and coordinating SCI and ADP systems support. The battalion S2 validates battalion GI&S requirements and product requests. He provides recommendations to the group S4 for GI&S requisitions and requirements. The battalion S2 provides input to the group S2 for unit geographic area requirements for GI&S products and services to support OPLANs and CONPLANs. He conducts or coordinates for a wide variety of CI activities in support of battalion OPSEC and FP needs. When an FOB is established, the S2 serves in the OPCEN under the staff supervision of the OPCEN director. The S2 is responsible for battalion information security, personnel security, and special security programs. He exercises technical supervision over the battalion intelligence-training program to make sure it not only enhances MI career management fields (CMFs) but also includes the 18-series CMFs. When required, the S2 establishes a T-SCIF within the OPCEN.

Analysis and Control Team

3-57. The ACT is the hub of the S2 section and has broad intelligence support responsibilities. It consists of all-source intelligence analysts (96B) and IMINT analysts (96D). The ACT responds to all-source intelligence support taskings from the battalion S2. The 96B all-source intelligence analysts within the ACT monitor the unit collection plan and identify new requirements to close intelligence gaps. The ACT receives, validates, and prioritizes all RIIs and RFIs from subordinate units and assigns them to the appropriate team of the S2 section. The ACT informs the S2 of PIR satisfaction and recommends new PIR, IRs, and SIRs. It reports intelligence to higher or lateral HQ, based on guidance from the S2, and coordinates dissemination of intelligence to subordinate and attached units. They are responsible for IPB, situation and target development, and BDA. All members of the ACT contribute to the preparation of the S2's intelligence estimate. The ACT produces and updates TIPs for the SFODAs, Special Forces operational detachments B (SFODBs), and SOT-As. They maintain and use the unit intelligence reference files and databases and intelligence ADP systems (see Chapter 8). The ACT personnel translate all PIR from the group or the JFSOCC into SIRs for tasking to SFODAs, SFODBs, and SOT-As. The ACT personnel prepare INTSUMs, IIRs, and responses to RIIs, and present intelligence briefings, as required. The ACT provides all-source analysis and intelligence production support to the SF battalion. The 96B

all-source analysts within the ACT focus and refine the efforts of three single-source suborganizations—the IMINT team, the SIGINT deployed TCAE, and the CI/HUMINT team.

IMINT Analysts

3-58. Under the table(s) of organization and equipment (TOE), the battalion MID has only one 96D (IMINT analyst) assigned to it; however, he may be augmented with more IMINT analysts from the group MID, or assisted by one or more all-source analysts. The IMINT analyst maintains comprehensive historical and current mission area imagery files in hard copy and digitized form. He uses ADP systems on the SECRET Internet Protocol Router Network (SIPRNET) and the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) to provide imagery analysis support and production support to the FOB (see Chapter 8). This support includes detailed terrain and facility analysis, annotated prints and target graphics, current imagery of targets and key terrain, BDA, and highly accurate imagery-based object measurement support. He also develops reconnaissance requests for submission to higher HQ.

CI/HUMINT Team

3-59. The CI/HUMINT team consists of a counterintelligence agent (97B), augmented by an HIC (97E) from the group MID. The HIC is attached according to the target language of the battalion's current mission. The CI/HUMINT soldiers on this team are responsible for a large number of tactical CI/HUMINT analysis, production, collection, and operational support activities. This team produces IIRs and other formatted reports to disseminate the results of CI/HUMINT collection and liaison activities. The team uses locally collected intelligence and theater CI/HUMINT products to assess a wide variety of threats within the battalion AOR. These threats include, but are not limited to, FIS; insurgents, terrorists, and criminals; dissident political factions; and anti-U.S. elements of the civilian population.

3-60. The CI/HUMINT team prepares and maintains the battalion MDCI estimate and comprehensive base defense IPB products, and situational awareness in the COMMZ and HN rear area. These IPB products permit the timely reporting of I&W information and predictive analysis on significant OPSEC and FP threats. The CI/HUMINT specialists develop the profiles of the friendly force and identify friendly vulnerabilities.

3-61. In response to the situation and collection taskings from the S2, the CI/HUMINT team plans, coordinates, and conducts CI liaison, EPW interrogation, document exploitation, overt collection, and displaced civilian debriefings. The team also serves as the OPCEN focal point to support FP activities. It recommends EEFI and CI threat countermeasures, ensures compliance with intelligence oversight regulations, and continually assesses the effectiveness of the base OPSEC countermeasures and base security plans. The CI team supports the OPSEC plan by providing SAEDA briefings, TVAs, and conducting authorized investigations. It also provides CI and security site surveys in support of FOB relocation within the country or theater, as required.

DEPLOYED SF

3-62. The SFG(A) commander exercises C2 of deployed subordinate SF units through a network of operational bases—the SFOB, FOB, and advanced operational base (AOB). These operational bases all perform the functions of C2 for subordinate elements. They normally are located at securable and logistically supportable sites.

SFOB

3-63. The SFOB is a command, control, and support base established and operated by an SFG(A) from organic and attached resources and is responsible for SF operations within the JSOA. It may be designated as an ARSOTF and collocated with a JSOTF or a combined joint special operations task force (CJSOTF) HQ. It may provide a base structure upon which those organizations (which are often temporary) are built. It is responsible for all ARSOF operations within a given JSOA. The SFG(A) group S2 may be called upon to serve as the SIO for any of the above HQ. As the SIO of an ARSOTF, for example, the group S2 must address the intelligence requirements for all ARSOF elements and integrate their organic IEW support as a combined effort.

FOB

3-64. FOBs are command, control, and support bases established by the SF battalion. The primary mission of the FOB is to isolate, launch, and recover SFODAs and SOT-As.

AOB

3-65. The AOB is an SF C2 node built upon an SF company HQ that can control its organic or attached operational elements. The mission of the AOB is to conduct launch and recovery and radio relay for SFODAs and SOT-As. In some cases, the AOB (if properly augmented) can also isolate teams.

SOCCE

3-66. The SF company can also function as a special operations command and control element (SOCCE). As the primary link between a U.S. Army Corps, the FOB in the corps AO, and the JSOTF during an MTW, the SOCCE plays an integral part in the intelligence cycle. This function is enhanced by the special operations coordination element (SOCOORD) of the G3 (see FM 3-05 [FM 100-25]).

3-67. By receiving combat information from SFODAs (once the SFODAs are under tactical control [TACON] of the corps or operating in the corps AOR), the SOCCE can provide real-time combat information on second-echelon enemy dispositions in the vicinity of corps NAIs and TAIs. This assists corps intelligence analysts to paint a deep-battle picture for the corps that it cannot otherwise receive. Additionally, SFODAs supporting conventional corps-sized elements can provide a sensor-to-shooter link interdicting LOCs and HPTs before they pose a threat in the main battle area. For these two reasons, SFODAs are always included in the corps collection plan.

3-68. The SOCCE communications link with the FOB enables the seamless command of SFODAs operating in corps AORs. This relationship can assist in

the survival of the SFODA by deconflicting Army airspace command and control (A2C2) for infiltration and exfiltration routes and establishing no-fire areas (NFAs) and restricted fire areas (RFAs) preventing fratricide of the SFODA. Through the SOCCE/FOB link, the SOCOORD can also obtain JSOTF INTSUMs, which are very helpful to the corps in further developing a relative common picture for the deep battle.

SFOB or FOB Organization

3-69. Each SF group or battalion commander normally organizes the SFOB or FOB into an OPCEN, a support center (SPTCEN), and a signal center (SIGCEN). All three centers have their own organization and functions, but their activities are interdependent. Figure 3-4 shows this structure. FM 3-05.20, Chapter 6, discusses the OPCEN, SPTCEN, and SIGCEN organization and functions in detail. There is no set structure for an ARSOTF, yet the normal SFOB configuration readily lends itself to expanded C2 roles and functions.

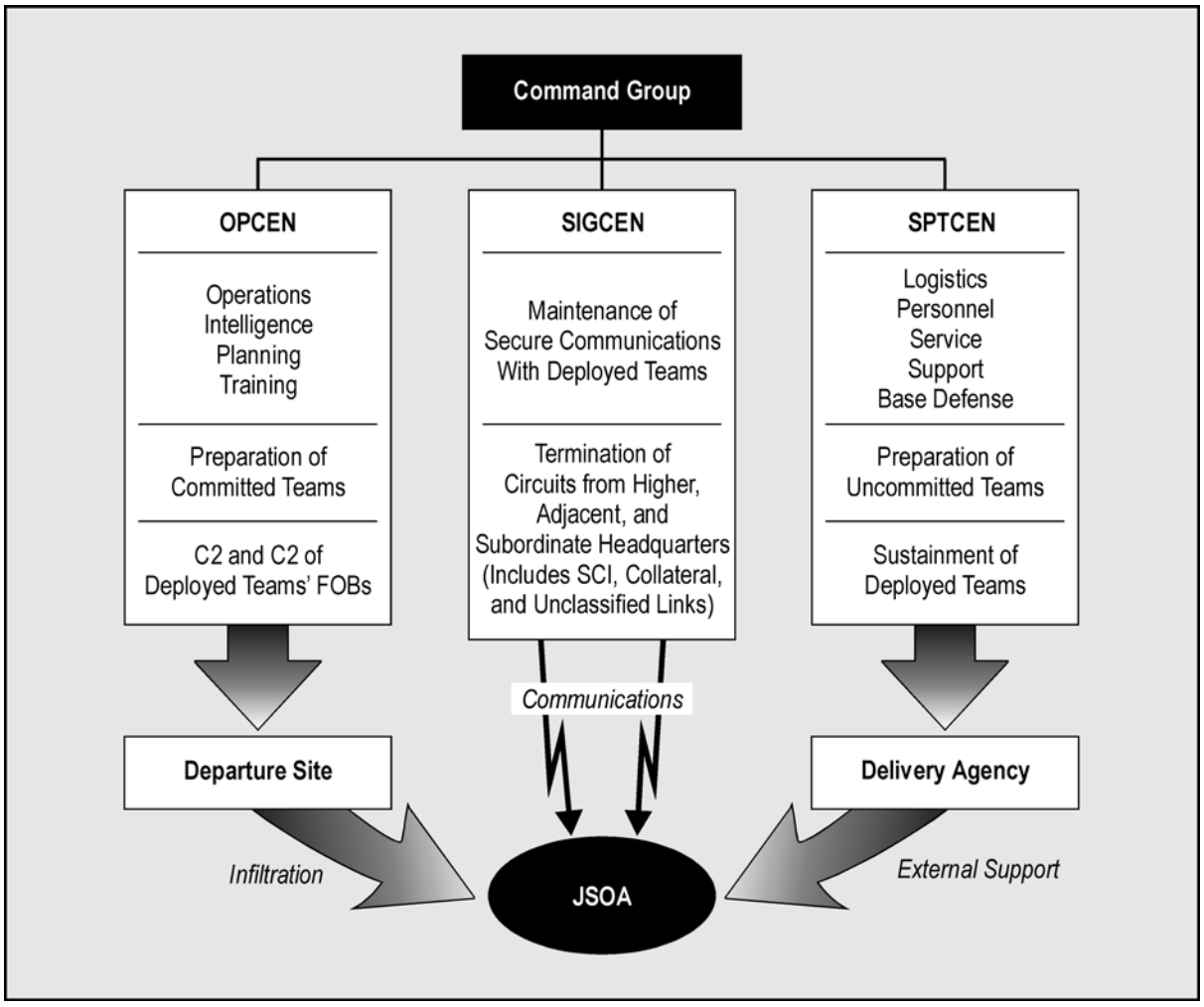


Figure 3-4. Example SFOB Organization

OPCEN Organization

3-70. IEW assets and activities normally are centralized within the OPCEN. The OPCEN is the functional activity that directs and controls SF operations in a designated AO and is under staff control of the S3. OPCENs are established at the SFOB and FOB echelons and provide similar functions and purposes.

3-71. The OPCEN, as shown in Figure 3-5, has staff supervision over a separate isolation facility (ISOFAC) with an SFODA LNO section, a HQ commandant, a MID, a liaison section, a consolidated plans section, and S2, S3, and S5 sections.

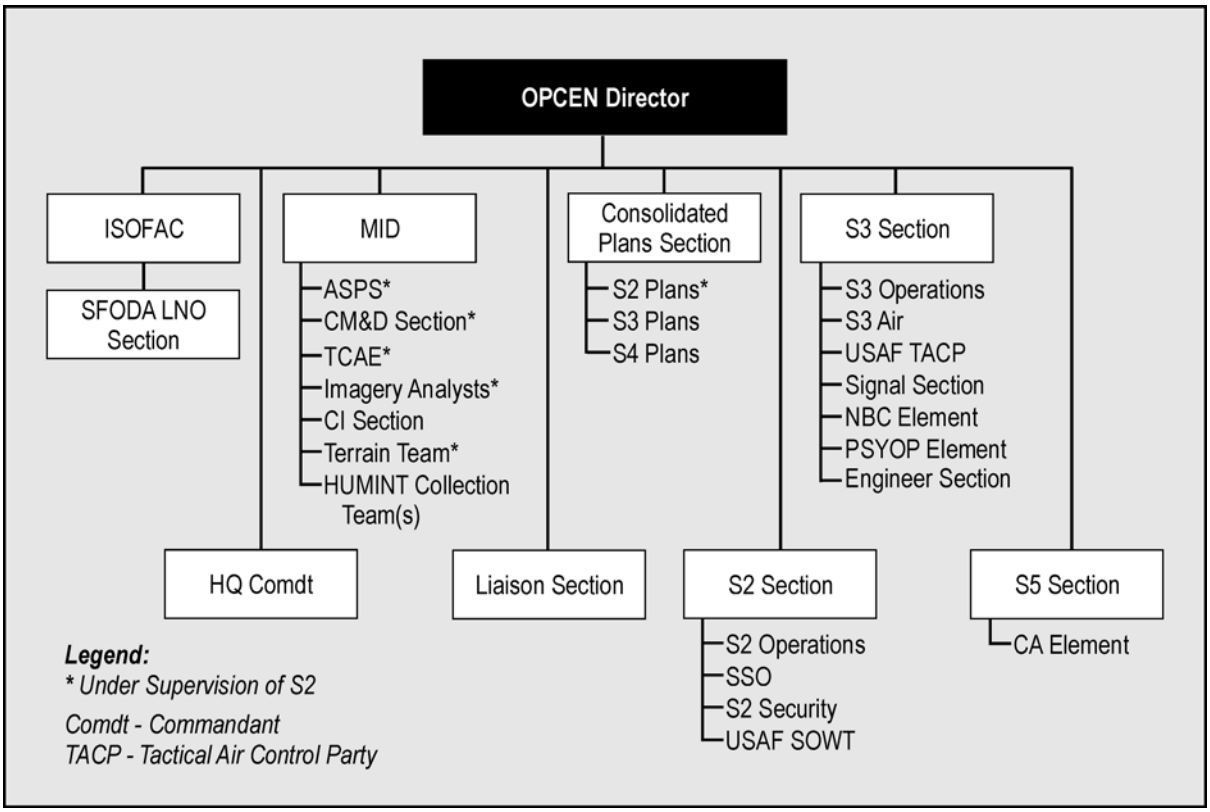


Figure 3-5. Example SF OPCEN Organization

3-72. Based on approved plans and guidance from the base commander, the OPCEN director (normally the S3) supervises all operational aspects of mission planning and execution. The OPCEN director synchronizes S2, S3, and S5 activities within the OPCEN. The OPCEN, which supervises an ISOFAC, must have sufficient ADP and communications to receive and produce products required by teams in isolation.

SF IEW ROLES AND FUNCTIONS

3-73. The following paragraphs represent an abbreviated list of the functions of the deployed S2 section and the MID in an SFOB OPCEN. Under the

leadership of the S2, the OPCEN intelligence section is the focal point for all-source intelligence production, collection management, and synchronization of the intelligence cycle. These are examples and should be interpreted as such. Each commander may task-organize his SFOB or FOB as required by mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC).

INTELLIGENCE SECTION (S2)

3-74. Under the staff supervision of the unit S2, the OPCEN intelligence section is the focal point for all-source intelligence production and collection management. This section consists of the S2 staff, elements of the group MID, and the SOWT. These personnel staff the ASPS, the CM&D team, imagery analysis team, and TCAE.

S2 Current Intelligence Branch

3-75. The S2 current intelligence branch directs and coordinates the daily operations of the S2 staff. It exercises staff supervision of the attached SOWT, the group MID, and all attached IEW elements.

S2 Plans and Targeting Support Branch

3-76. The consolidated plans section maintains OPLANs for the entire OPCEN. The S2 representative to the consolidated plans section coordinates and plans intelligence support for future and contingency SF operations. The S2 representative physically locates with the S3 or S5 plans branch or the consolidated plans section.

Security Branch

3-77. The S2 security branch develops unit personnel, information, ADP, and physical security programs and supervises their implementation. Under its staff supervision, the CI/HUMINT section of the MID provides CI support to the S3 OPSEC program and to deception planning.

USAF Special Operations Weather Team

3-78. The USAF SWO serves as a special staff officer to the group commander on all weather matters. The team should locate within the OPCEN to facilitate the exchange of information to other intelligence sections and the operational sections. The team provides—

- Current and forecast weather and light data.
- Information and analysis to support the determination of weather effects upon operations.
- Climatic analysis studies supporting all group missions.
- Forward area limited observing program (FALOP) and remote weather sensor training and mission support information to SFODAs in isolation.

3-79. When approved by the SFG(A) commander, the SOWT may attach team members to SFODAs, SFODBs, or SOT-As to gather critical weather observations from denied territory and regions for which there is an underdeveloped database.

MID ALL-SOURCE PRODUCTION SECTION

3-80. The ASPS performs IPB, develops target data, and consolidates information from all sources to meet the commander's mission needs. The ASPS—

- Processes, correlates, and integrates all-source intelligence in response to taskings from the CM&D section.
- Is the focal point for all situation and target development.
- Develops and maintains the unit's intelligence database, to include the intelligence journal, OB information, IPB products, targeting data, and the situation map.
- Monitors the CM&D collection plan and recommends revisions to close identified gaps.
- Receives and processes intelligence products and combat information from higher, lower, and adjacent commands.
- Prepares intelligence estimates, reports, summaries, and briefs, as required.

CM&D TEAM

3-81. The CM&D team of the ASPS formulates detailed collection requirements and tasks or requests the collection of required information. Normally collocated with the ASPS, the CM&D team—

- Performs intelligence collection management for the intelligence operations branch.
- Obtains the command's approved requirements from the S2, prioritizes them on the basis of SIO guidance, and translates them into the collection requirements.
- Prepares and continuously updates the unit collection plan and forwards the unit's IRs to the next higher command.
- Tasks organic and attached collection assets.
- Through the S3, requests intelligence collection mission tasking of organic teams or other subordinate non-MI assets.
- Disseminates combat information and intelligence within the command and to higher, lower, and adjacent HQ.

IMAGERY ANALYSIS TEAM

3-82. Imagery analysts extract information and develop intelligence mainly from imagery collected from commercial, national, and military imagery systems and sensors. Within SF units, imagery analysts are assigned to the group and battalion MIDs. A thorough knowledge of threat tactics and ground OB enables them to recognize, identify, locate, describe, and report information on objects, activities, and terrain from a variety of imagery products. Imagery analysts make associations between visible objects and configurations and analyze the results to determine strength, disposition, and enemy capabilities. They—

- Analyze imagery and report specific information on threat operations, activities, dispositions, logistics, communications, installations, and civilian activities and their possible effect on SF operations.

- Prepare and maintain imagery prints to supplement and update maps for SF operational planning.
- Extract information from imagery in direct support of unit mission area analysis.
- Support BDA.
- Prepare mosaics and target terrain models along with the terrain team to support operational planning.
- Accomplish imagery exploitation, reporting, and production for SFOB and FOB requirements from joint or theater imagery exploitation activities.
- Prepare and maintain an imagery database for the unit's specified mission areas.
- Provide technical assistance to the unit CM&D section, as required.

CI/HUMINT SECTION

3-83. The primary function of the CI/HUMINT section is to perform MDCI analysis to support the ASPS and the unit's FP, OPSEC, and deception programs. The section performs source administration functions supporting CFSO. The CI section—

- Supports the unit's personnel security and information security functions.
- Conducts liaison with other U.S. and HN security organizations located near the forward bases.
- Conducts MDCI analysis to support ASPS FP and situation and target development efforts.
- Develops detailed assessments of foreign intelligence and security threats near SFOBs and in SF AOs.
- Recommends appropriate OPSEC and FP measures to reduce friendly vulnerabilities.
- Evaluates, if possible, the effectiveness of OPSEC measures implemented to correct identified friendly vulnerabilities.
- Briefs deploying SF teams on the latest threat data.
- Provides SF teams with technical advice and assistance to prepare them to establish and operate during long-term UW missions.
- Supports IO by determining foreign vulnerabilities to deception.
- Provides the S3 with recommendations for deception measures and evaluates their effectiveness through MDCI analysis.
- Requests external support, when necessary, to evaluate foreign reactions to friendly deception operations.
- Uses current intelligence ADP (see Chapter 8) to exchange information with existing JTF, JSOTF, and ARSOTF databases.

3-84. The HUMINT analysis team—

- Is the fusion point for all HUMINT reporting and operational analysis.
- Determines gaps in reporting and coordinates with the collection manager to cross-cue other intelligence assets.

- Produces and disseminates HUMINT products and provides reporting feedback that supports the HUMINT teams.
- Uses analytical tools to develop long-term analysis and provides reporting feedback that supports the HUMINT teams.

HUMINT TEAMS

3-85. The teams may be attached to the subordinate battalions, a joint interrogation facility (JIF), or a designated EPW/detainee detention/holding area facility. HUMINT collection team activities include—

- Interrogating EPWs and civilian internees.
- Debriefing detainees, U.S. personnel, displaced persons, and other persons of intelligence interest.
- Exploiting foreign language open source/captured documents.
- Overt elicitation activities (liaison, escort, observer, translator, and treaty verification missions).
- Conducting CFSO IAW an approved umbrella concept.

TCAE

3-86. The group TCAE carries out SIGINT and EW management functions and provides technical control of SOT-As. Specific functions include—

- Producing the SIGINT collection plan.
- Providing centralized technical control and collection tasking authority over deployed SOT-As.
- Analyzing and correlating intercepted SIGINT traffic from the SOT-As with data from other sources and then passing these products to the ASPS and higher echelon TCAEs or SIGINT processing centers.
- Developing and maintaining the SIGINT technical database and the electronic order of battle database.
- Interfacing with theater and national intelligence systems to complete the integration of technical data generated by tactical units with the technical data produced by the NSA and pulling technical data required for SIGINT and EW operations.
- Providing technical support (such as SIGINT technical data) to SOT-As, as required.
- Performing all functions of the SIGINT collection management authority (CMA). The TCAE officer in charge (OIC) performs these functions, which are detailed in a separate CMA directive.

Note: Continental United States (CONUS)-based TCAEs interface directly with the Army TCAE during peacetime for all technical support requirements and readiness reporting required by United States Signals Intelligence Directive (USSID).

SOT-A

3-87. SOT-As detect, monitor, and exploit threat communications through communications transmission intercept and direction finding. SOT-As also

can deploy with SFODs to provide ER, FP, or MTT support. These functions may require SOT-As to—

- Deploy with an SFOD.
- Deploy independently and then infiltrate to join a deployed SFOD.
- Operate independently or with other SOT-As.

SOT-A Operations

3-88. The SOT-As can operate in all environments and across the range of military operations to support SO elements. Their small size and ability to task-organize in a variety of configurations enables them to contribute greatly to answering the SF commander's PIR and IRs.

Mission Profiles

3-89. When deployed with an SFOD, the SOT-A and the SFOD team should combine mission-planning tasks and CSS requirements whenever possible. A SOT-A can also support an SFOD team with limited interrogation, translation, interpretation, and communications support. The SOT-A team leader executes the tactical and technical aspects of the mission. In addition to providing EW to support the SFOD commander, the SOT-A transmits collected information to the TCAE for decryption, processing, analysis, threat recognition, and dissemination. The TCAE forwards this information to the next-higher SIGINT analysis node for further processing and then dissemination to the appropriate users.

Organization and Equipment

3-90. A basic SOT-A consists of four personnel. Each team can conduct both low-level voice intercept (LLVI), nonvoice (Morse) intercept, and limited direction finding. The primary EW system for SOT-A electronic warfare support (ES) operations is the AN/PRD-13 SOF SIGINT manpack system (SSMS), version 2 (see Chapter 8).

Capabilities and Limitations

3-91. SOT-A team members can operate in remote, denied areas much like SFODA members. In addition to their linguistic, international Morse code (IMC) and SIGINT skills, SOT-As are trained in tactical and fieldcraft techniques and are certified in the same basic skills as SFODAs. However, SOT-As are rarely certified in advanced SOF skills such as underwater operations (UWO) or military free-fall (MFF).

SOT-A Mission Tasking and the U.S. SIGINT System

3-92. The SFG(A) commander exercises tasking and technical control of SIGINT and EW operations through the group TCAE when SIGINT operational tasking authority has been delegated. The group TCAE translates each SOT-A mission tasking into a technical tasking. It forwards the tasking, IPB, or electronic preparation of the battlespace (EPB) products and technical data to support mission analysis to the SOT-A team leader. The team leader then executes the mission.

Terrain Team

3-93. The supporting terrain team collocates with and functions as an essential element of the OPCEN. The S2 tasks the team and controls its activities. The terrain team collects, compiles, and produces graphic and textual terrain data to support the SFG(A)'s needs. It also assists the ASPS in its IPB function by producing general and detailed terrain analysis, terrain studies, target models, overlays, and overprinted maps.

OTHER ORGANIC INTELLIGENCE ASSETS

3-94. In addition to the SF group and battalion S2 sections and the group MID, the SF company, SFODA, and group and battalion medical sections also participate in the intelligence collection effort.

SF COMPANY

3-95. The SF company technician is an SF warrant officer. He has staff responsibility for the unit's intelligence activities and training for the company and its operational detachments.

SFODA

3-96. At the SFODA level, the assistant operations and intelligence (O&I) NCO (MOS 18F) supervises intelligence training, collection, analysis, production, and dissemination activities for his team. The O&I NCO assists the operations sergeant by preparing area studies, briefbacks, OPLANs, and OPORDs. He helps conduct limited tactical questioning of EPWs. He briefs and debriefs patrols with or without the assistance of other detachment members.

MEDICAL SECTIONS

3-97. The group and battalion medical sections are excellent sources of information about the operational area, its associated health threats, and the medical personnel and facilities for these locations. The medical area studies developed by Army Medical Department (AMEDD) intelligence personnel are an additional source of information that is readily available over INTELINK.

NONORGANIC IEW SUPPORT TO SF

3-98. IEW support for SF consists of OSINT, HUMINT, IMINT, SIGINT, MASINT, CI, and TECHINT. Although organic IEW assets provide dedicated support to their respective operational bases, there is still a need for nonorganic support. In CONUS, this nonorganic support is normally requested through USASFC G2, the USASOC DCSINT, and the USSOCOM SOIO. OCONUS nonorganic support is requested through the SOC J2 and the theater J2.

IEW SUPPORT FROM HIGHER HEADQUARTERS

3-99. Intelligence requirements for SF operations can be very generic and satisfied mainly by OSINT sources or can be unique, highly sensitive, and can require compartmentalized handling. The Requirements Management

Division of USASOC coordinates with USSOCOM and theater intelligence organizations to provide the intelligence that cannot be provided by MSCs.

3-100. The SOC J2 is primarily concerned with in-theater IEW policy formulation, planning, and coordination. The SOC J2—

- Ensures sufficient intelligence support is available for each mission tasked by or through the SOC.
- Facilitates the theater IEW organizations' collection, production, and dissemination of intelligence to meet SOF requirements.
- Coordinates joint SO intelligence collection operations and the production and dissemination of TIPs to support SO targeting efforts.
- Tasks subordinate SOF units to collect and report information that supports SF IRs.
- Monitors RII status until the appropriate collection assets respond.
- Maintains adequate intelligence databases to support SOF requirements.

Chapter 4

IEW Support to Ranger Operations

This chapter discusses IEW support for Ranger units and Ranger operations. It briefly describes Ranger missions, organizations, and operational considerations. The chapter also describes Ranger IEW requirements and the IEW elements organic and external to Ranger units that provide this support.

INTRODUCTION

4-1. Rangers provide a responsive strike force for conducting DA missions normally as part of an integrated SOF contingent. Ranger operations rely on the elements of surprise, precise planning, and orchestrated execution to conduct special missions supporting vital U.S. interests. There is one active Ranger regiment with three Ranger battalions. Intelligence support for Ranger operations primarily focuses on providing target-specific information for objectives of strategic or national importance. At the battalion level, the intelligence structure parallels that of a light infantry battalion. The organic intelligence structure within the Ranger regimental headquarters is larger than that of an infantry brigade and is structured to provide linkage from higher echelons to the operational units.

RANGER MISSIONS

4-2. The Ranger regiment's mission is to plan and conduct SO against strategic or operational targets in support of national or theater objectives (FM 3-05 [FM 100-25], Chapter 3). The Ranger regiment and its subordinate battalions have a worldwide focus and are not regionally oriented, as are SF, CA, and PSYOP units. Ranger missions are diverse and carried out on any terrain and under any condition. Ranger operations have high-risk and high-payoff attributes. Therefore, accurate, detailed, and timely intelligence is critical for planning and executing Ranger missions. It is through active interface with the supporting IEW system that Rangers receive answers to specific target IRs since the Ranger regiment has limited organic intelligence assets.

4-3. The primary SO mission of Rangers is to plan and conduct DA by using special techniques and procedures. DA missions are short-duration strikes and other small-scale offensive actions to seize, destroy, or inflict damage on a specific target.

4-4. Ranger DA operations typically include—

- Raids against targets of strategic or operational value.
- Lodgment operations (such as airfield seizures).
- Noncombatant evacuation operations (NEO).

Ranger DA operations may support or be supported by other SO activities, or they may be conducted independently or with conventional military operations.

RANGER INTELLIGENCE ORGANIZATION

4-5. Intelligence assets organic to the Ranger regiment are organized according to operational and analytical needs. The Ranger regiment has organic assets it can use to perform intelligence functions and missions. Figure 4-1 shows the intelligence structure of the 75th Ranger Regiment HQ. The complete regimental intelligence structure consists of the regimental S2 section, the MID, which augments the S2 section, and the RRD. The regimental intelligence structure can be task-organized to support subordinate battalions by detaching personnel from the regimental HQ to the battalions. A flexible arrangement is necessary because of the types of missions the regiment performs. This organization—

- Conducts limited all-source intelligence collection, analysis, production, and dissemination to support situation and target development, IPB, CI, and IO activities.
- Identifies, validates, and coordinates unit requirements for GI&S and other intelligence products to support OPLANs and CONPLANs.
- Can function as an ARSOTF S2 or integrate Ranger intelligence operations as part of an ARSOTF or JSOTF intelligence structure.

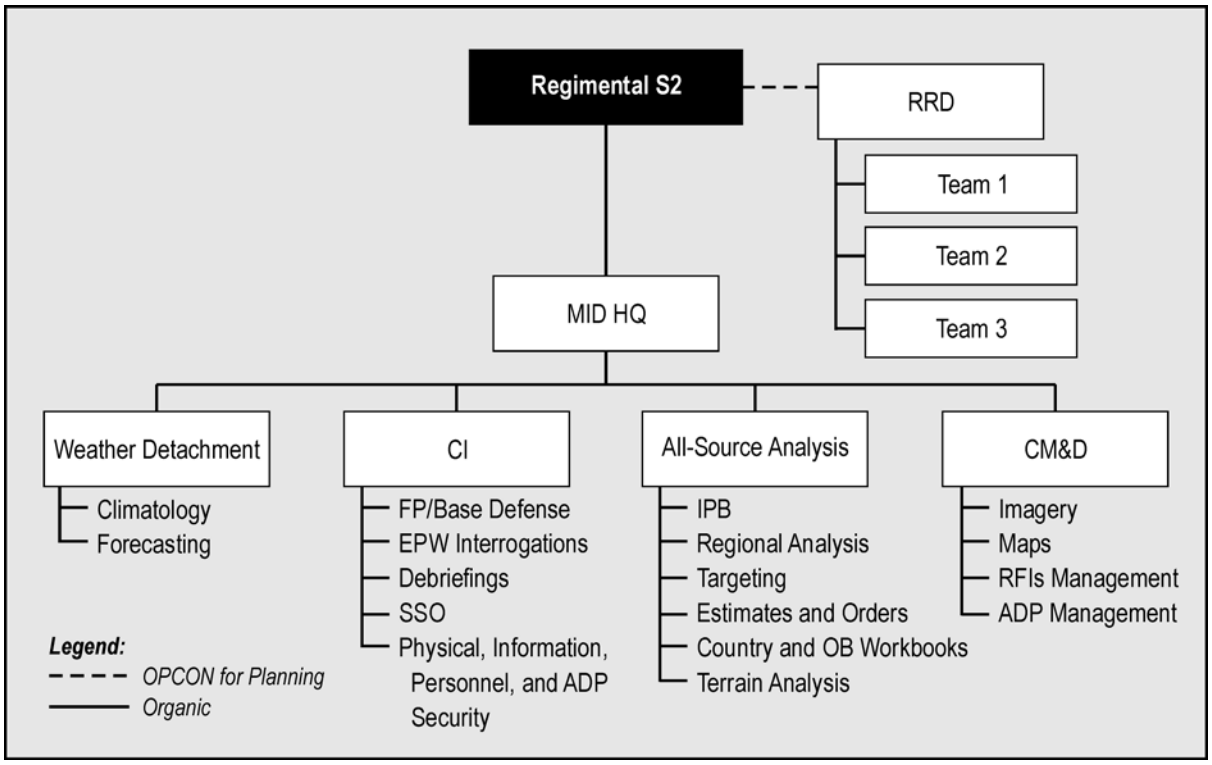


Figure 4-1. Ranger Regiment Intelligence Organization

REGIMENTAL S2 SECTION

4-6. As the primary intelligence advisor to the commander, the S2—

- Plans and directs the operations of the S2 section.
- Reports and forwards PIR and combat information to higher, lower, and adjacent echelons.
- Coordinates IO efforts (EW, OPSEC, and deception) with the JSOTF information operations officer.
- Provides staff supervision of the MID's activities supporting operational requirements.
- Coordinates closely with the fire support officer (FSO) to exchange battlefield information, integrate collection efforts with target acquisition requirements, and plan fire support coordination measures.
- Validates GI&S requirements and product requests.
- Identifies, confirms, and coordinates area requirements for GI&S products and services to support OPLANs and CONPLANs.

Whether the Ranger regiment operates as part of a JSOTF, an ARSOTF, or with a conventional force, the S2 needs significant support from other intelligence elements and agencies for comprehensive and timely intelligence support.

MILITARY INTELLIGENCE DETACHMENT

4-7. The MID performs collection management and production functions for the regiment. The MID—

- Performs all-source intelligence processing and analysis.
- Develops and is the primary architect of intelligence products constructed from regimental and outside sources.
- Maintains intelligence databases and/or TIPs on existing or emerging targets.
- Identifies existing intelligence gaps in the collection effort and information flow.
- Produces intelligence estimates and annexes supporting OPLANs, OPORDs, and fragmentary orders (FRAGOs).
- Coordinates with appropriate agencies to obtain detailed IPB of the target areas.
- Conducts detailed target development, including microterrain analysis; CARVER assessments; production of scale models of targets; and other related products, as directed.
- Responds to RIIs from elements.
- Briefs and debriefs the RRD teams.
- Provides intelligence briefings, reports, and other products, as required.

ANALYSIS SECTION

4-8. The analysis section maintains and updates target folders and threat OB files. It studies and processes information on specific theater target areas. The team also produces TIPs and estimates on threat COAs. Target intelligence, in this context, includes intelligence and information on the threat's organization, strength, and dispositions integrated with information derived from other sections organic to the MID and outside sources. This section produces intelligence products tailored for dissemination down to Ranger company level to facilitate operator tactical usability.

CM&D SECTION

4-9. The CM&D section synchronizes and monitors the S2's collection requirements with internal and external collection sources. It also performs RII management. It interprets IMINT products from a variety of sources (overhead, electro-optical, or ground) and integrates this imagery into TIPs or other products. It has specially trained imagery analysts with the technical expertise to accomplish these tasks in garrison or while deployed. External imagery support specialists and equipment can augment this section or it can be detached to support a Ranger battalion. The CM&D section ensures that the GI&S products from external sources are available.

CI SECTION

4-10. CI detects, evaluates, counteracts, or prevents foreign intelligence collection, subversion, sabotage, and terrorism. It determines security vulnerabilities and recommends countermeasures. CI operations support OPSEC, deception, and rear-area operations.

4-11. The regimental CI section primarily focuses on FP for deployed Ranger elements. It can also perform interrogation and debriefings of threat, nonbelligerent, and friendly personnel. It conducts CI liaison with U.S. and HN intelligence and law enforcement agencies as required. Members of the CI section use ADP equipment (see Chapter 8) to access databases, forward and receive CI information, and transmit tactical imagery. Elements of the CI section can deploy with any of the Ranger battalions or units with Rangers in their task organization, as required.

SPECIAL OPERATIONS WEATHER TEAM

4-12. The USAF SOWT serves as a special staff element to the commander on all weather matters. The team is able to access all available weather databases to provide current and forecast weather data and climatic analysis studies to support all missions. The team provides FALOP training to the RRD and provides mission-unique information during operations. The SOWT works closely with the analysis section to ensure data on weather and light are available for ascertaining weather effects on Ranger operations.

RANGER RECONNAISSANCE DETACHMENT

4-13. The RRD consists of three tactical teams and an HQ element. Its primary mission is to conduct tactical reconnaissance to support Ranger force DA missions. The RRD is under the OPCON of the S2 section for planning its

missions. The RRD teams give the regiment the capability to meet immediate on-the-ground tactical intelligence requirements. The RRD—

- Fulfills target area surveillance missions in an area before committing other Ranger elements to the operation.
- Engages hostile targets with direct fire, indirect fire, and demolitions.
- Conducts limited terminal guidance operations (TGO).
- Can conduct MFF, small-boat, and scout swimmer operations for infiltration and exfiltration of a target area.
- Conducts prestrike and poststrike surveillance on critical nodes for BDA requirements.
- Is specially trained to provide information on threat OB and target sites and to conduct route and limited NBC reconnaissance.
- Conducts pathfinder operations to reconnoiter, select, clear, and prepare landing zones (LZs) and drop zones (DZs).
- Can conduct autonomous tactical operations for up to 5 days in denied areas.

BATTALION S2 SECTION

4-14. The Ranger battalion S2 section consists of two officers—the S2 and assistant S2—and three enlisted soldiers. The section has a limited capability to collect and analyze information. Its mission is to support the battalion commander with basic intelligence database maintenance, collection management, analysis, and tactical intelligence production and dissemination for battalion operations. Regimental S2 elements or external assets, as required, augment the battalion S2 section. Additionally, the Ranger battalion S2—

- Tasks, through the S3, battalion elements to perform combat intelligence missions supporting battalion operations.
- Conducts intelligence training for battalion elements.
- Supports the planning, coordination, and execution of Ranger target rehearsals.
- Briefs and debriefs reconnaissance teams.
- Validates GI&S requirements and product requests.
- Coordinates with S4 for map requisitioning.
- Identifies, confirms, and coordinates priorities for input to regimental geographic area requirements for GI&S products and services.

OTHER ORGANIC SUPPORT

4-15. In addition to the support provided by the Ranger regiment, medical and fire support personnel provide other organic support. The regimental and battalion surgeons are a source of medical and NBC intelligence concerning possible deployment locations. They also provide valuable information on disease and health conditions in the AO. Fire support personnel are able to serve as a conduit for information collected by units providing supporting

fires. This may include detections by the counterbattery radar of an artillery unit or observations by pilots flying close air support (CAS) missions.

NONORGANIC IEW SUPPORT TO RANGER REGIMENT

4-16. Intelligence requirements for Ranger operations are specialized and sensitive. Nonorganic IEW support to the Ranger regiment is discussed in the following paragraphs.

IEW SUPPORT FROM HIGHER HEADQUARTERS

4-17. The USASOC DCSINT Requirements Management Division coordinates with USSOCOM SOIO, SOCJIC, and theater- and national-level intelligence agencies for the information and intelligence needs of the Ranger regiment.

4-18. When deployed, the JSOTF commander provides intelligence support to the Ranger regiment. The JSOTF J2 provides target-specific intelligence in the form of a TIP. The JSOTF J2 also provides MDCI and EW support to the Ranger force. The Ranger regiment normally places an intelligence LNO at the JSOTF or the appropriate intelligence production facility to ensure—

- The intelligence needs of the Ranger force are relayed to the appropriate intelligence-processing center.
- The resulting analysis is based on the specific needs of the Ranger force commander.

This LNO also coordinates with the corps or echelons above corps (EAC) targeting center when the Ranger force is OPCON to a conventional force. Close coordination between the regiment, the corps or EAC intelligence node, and the targeting center is essential to effectively employ Ranger forces.

CI/HUMINT SUPPORT

4-19. Although the Ranger regiment has its own organic CI section, it may sometimes require augmentation from CI personnel assigned to higher echelons or liaison with CI personnel assigned to adjacent units. Interrogation of EPWs is one of the primary HUMINT functions not organic to the Ranger battalion. However, the CI section of the Ranger regiment's MID can perform tactical questioning and limited interrogation with attached linguistic support.

SIGINT SUPPORT

4-20. SIGINT support to Ranger missions, including locating and countering threat C4I, is available (when directed by higher HQ) in the form of SOT-As or from the supported command's MI assets, if under OPCON of conventional forces. The type of support needed depends on the nature of the target and threat capabilities.

IMINT SUPPORT

4-21. The channels used to provide IMINT support depend on the agency and the requirement, the agency receiving the request, and command procedures. Corps and division assets provide tactical IMINT when the target area falls within the range of their organic systems, to include

unmanned aerial vehicles (UAVs). However, other Services and national assets normally provide IMINT supporting Ranger operations.

RANGER SUPPORT TO IEW SYSTEM

4-22. Like any other operational unit, Ranger forces can be excellent sources of combat information. Rangers are often the first to encounter the enemy and can confirm or deny friendly assessments of threat organization, equipment, capabilities, and morale. They can bring back captured threat equipment for evaluation and report on the effectiveness of friendly weapons on threat systems. Rangers can also provide real-time assessments of the target area civilian population's psychological and physical disposition for use in fine-tuning PSYOP and CA plans for follow-on forces. Ranger S2s must be proactive in debriefing Rangers to ensure this valuable information enters the IEW system.

Chapter 5

IEW Support to ARSOA

This chapter describes the IEW support required for ARSOA missions. It describes ARSOA organization and missions and the intelligence units that support ARSOA. Specific information on organization, functions, and roles of each participating intelligence asset is discussed. Further information on ARSOA is found in FM 3-05.60, *Army Special Operations Forces Aviation Operations*.

INTRODUCTION

5-1. ARSOA plans and conducts special air operations across the range of military operations. Specialized ARSOA aircraft and trained crews can penetrate hostile and sensitive airspace to conduct and support SO and theater-level operations. These assets operate with precise execution over extended ranges, under adverse weather conditions, and during times of limited visibility. ARSOA units are not regionally focused as in the case of SF, CA, and PSYOP units. Instead, ARSOA operates in all theaters under almost any environmental conditions.

5-2. Because of the high risks associated with ARSOA operations, their effectiveness depends largely on the ability of the S2 to gather, produce, and disseminate detailed operational intelligence to mission planners and operators in a timely manner.

5-3. The ARSOA consists of a regiment headquarters and headquarters company (HHC) and three battalions containing light attack, light assault, medium attack, airborne C2, medium lift, and heavy assault helicopters and maintenance assets. (See FM 3-05.60 for further details on the composition of the ARSOA.)

MISSIONS AND ORGANIZATION

5-4. The ARSOA employs state-of-the-art equipment to provide extremely accurate heliborne lift and attack capabilities in a wide range of mission profiles, to include:

- Force insertion and extraction.
- Aerial security.
- Armed attack.
- Casualty evacuation.
- Mine dispersal.
- C2 support.

5-5. Intelligence support for ARSOA operations must focus on surface-to-air-missile (SAM) and air defense artillery (ADA) threats during the infiltration and exfiltration phases of their missions. Additionally, ARSOA operations are heavily dependent on imagery products to aid in flight route and evasion and recovery (E&R) planning.

5-6. Per FM 3-05 (FM 100-25), the mission of ARSOA is to plan, conduct, and support special air operations by clandestinely penetrating hostile and denied airspace. ARSOA supports SOF conducting joint, combined, interagency, and liaison and coordination activities in regional crises and major conflicts. ARSOA organizes, equips, trains, validates, sustains, and employs assigned aviation units for the USSOCOM. Key mission-essential tasks for ARSOA are to—

- Infiltrate, resupply, and exfiltrate SOF and other designated personnel.
- Conduct DA or CAS by using organic attack helicopters providing aerial firepower or TGO for precision munitions, unilaterally or with other SOF.
- Conduct aerial SR (visual, photographic, and electronic) in support of SOF.
- Provide forward air control for CAS and indirect fires in support of SOF.
- Conduct assisted E&R when dedicated CSAR assets are not available in support of SO.

5-7. The most frequent ARSOA missions are infiltration, exfiltration, and providing aerial fire support platforms in support of other SOF. ARSOA units can provide general aviation support to SOF where use of conventional aviation assets is not appropriate, feasible, or available. These types of missions, however, detract from the primary mission of clandestine penetration into denied areas and decrease combat asset availability.

5-8. Accurate IEW support is vital to mission success and the survivability of ARSOA assets. Successful penetration and exfiltration dictate that ARSOA assets must avoid detection, unfavorable climatic conditions, and ADA threats.

ORGANIC INTELLIGENCE ASSETS

5-9. The only organic MI support in the ARSOA regiment and its subordinate battalions is their respective S2 staffs. ARSOA units have no other assigned IEW assets. Figure 5-1 shows the intelligence staff organization for the ARSOA.

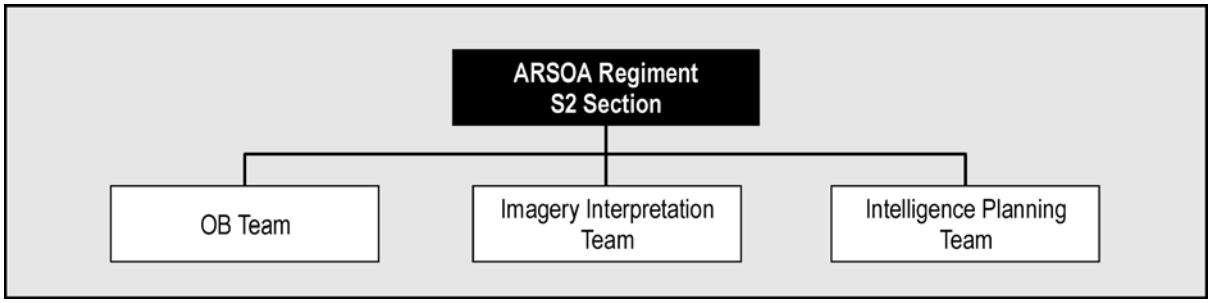


Figure 5-1. Intelligence Organization of the ARSOA

S2 RESPONSIBILITIES

5-10. The ARSOA S2 is the commander's staff representative for intelligence and CI measures. The S2—

- Recommends PIR to the commander and establishes IRs.
- Provides accurate air defense information to supported SOF units.
- Coordinates intelligence requirements with higher and supported echelons.
- Acquires sufficient imagery for ARSOA operations.
- Integrates intelligence support for E&R contingency planning.
- Provides an assessment of the foreign intelligence collection threat.
- Prepares and implements intelligence training programs.
- Exercises staff supervision of CI personnel.
- Helps the operations element identify EEFI and prepare vulnerability studies and countermeasures that units will use to support the force protection plan.
- Helps the S3 plan operations. The S2 and S3 should maintain common planning tools—ADP and map overlays.
- Coordinates weather information and analysis with the appropriate Army or Air Force weather element.
- Identifies, confirms, and coordinates priorities for unit GI&S products to support theater OPLANs and CONPLANs. Monitors and validates map requisitions.
- Validates GI&S requirements and product requests.

5-11. The ARSOA regiment S2 section has three teams: OB, imagery interpretation, and CINC intelligence planning. The ARSOA regimental S2 staff can augment battalion S2 sections, if required.

OB TEAM

5-12. This team develops and maintains threat OB databases. It studies, analyzes, integrates, and processes threat information on targets identified in theater planning documents or for contingency operations. It works closely with the other sections, ensuring the full integration and presentation of all requirements and products in a usable format for mission planning and execution. It also produces periodic intelligence assessments and briefings on potential threat areas where ARSOA could deploy.

IMAGERY INTERPRETATION TEAM

5-13. This team develops and maintains imagery data files (digital and hard copy) on identified or developing target areas. It uses ADP (see Chapter 8) and hard film-processing devices to meet imagery requirements for operational planning. ARSOA requires very detailed imagery for its missions, particularly around objective areas or constricted landing areas. The team

also prepares imagery mosaics that are a valuable tool for route selection and flight planning.

INTELLIGENCE PLANNING TEAM

5-14. This team coordinates with the theater intelligence support nodes that support the geographic combatant commanders to ensure that the regiment has each theater's most current intelligence products, estimates, and planning documents on hand. It ensures the identification and integration of ARSOA intelligence requirements into theater intelligence operations. It maintains specific architecture structural documents and plans for the integration of ARSOA into theater IEW architectures.

ARSOA INTELLIGENCE OPERATIONS

5-15. Intelligence support to ARSOA is often very specialized and sensitive. Yet it is similar to the support required for conventional aviation, differing mainly in its level of detail. ARSOA S2s and their supporting staffs use the same procedures and methods as any other intelligence support elements. IPB products for ARSOA mission planning focus on terrain, weather, and threat factors required for each phase of an operation (infiltration, objective area, exfiltration).

5-16. The AI for an ARSOA operation would incorporate the ranges of any threat sensors, ADA, or air attack assets that could target or disrupt movement to and from a given target area. Within the AO, ARSOA gives special emphasis to environmental conditions and all threat activities—both air and ground. Additionally, the locations and dispositions of potential refueling points, LZs, DZs, and airfields are considered for contingency plans.

TERRAIN CONSIDERATIONS

5-17. Detailed, in-depth terrain analysis for ARSOA operations is a critical step during the IPB process. ARSOA carefully studies flight routes to and from target areas since it normally operates during periods of limited visibility while flying at low levels. ARSOA often requires microterrain analysis in and around targeted areas since its assets may need to operate in very restricted terrain, to include heavily urbanized locales. Terrain products for ARSOA operations could include gridded target references, mensurated and annotated imagery (film and digital), and scaled-down rehearsal mock-ups and digital simulations. Some factors considered for ARSOA terrain analysis include, but are not limited to—

- Obstacles to flight along routes and target areas (terrain obstructions, utility wires, vegetation, structures, and so forth).
- Local terrain variances in altitude.
- Navigation reference points and checkpoints.
- Masked areas for observation and communication.
- Planned and contingency LZs.

WEATHER CONSIDERATIONS

5-18. Accurate, detailed, and specific weather and environmental data are crucial to ARSOA mission success. Severe local weather conditions can seriously degrade flight and target acquisition capabilities. Certain atmospheric conditions affect the propagation of aircraft noises, which impacts upon route selection. Some factors considered during weather analysis are—

- Lunar illumination and light angle of incidence.
- Expected temperature variations along flight routes.
- Atmospheric factors (visibility, barometric pressure, and wind conditions).
- Weather effects on time lines and schedules.

THREAT CONSIDERATIONS

5-19. In ARSOA operations, knowledge and avoidance or suppression of the foreign air defense threat is paramount. The staff of the ARSOA task force S2 must fully integrate into the local and theater area air defense command's warning network. It must closely coordinate with all available sources to avoid detection and minimize losses. To help ARSOA successfully penetrate denied airspace, the S2 must strive to identify, locate, and acquire every asset possible to exactly pinpoint enemy weapons systems (quantities and locations).

5-20. Threat locations and associated activities will normally have the greatest impact on the selection of flight routes and actions within the AO. ARSOA mission planners consider not only threats that can directly engage their aircraft, but also any sources that can acquire and report the movement and direction of ARSOA aircraft. Of particular concern to ARSOA operations are threat ADA and attack helicopter capabilities. Around target areas, ARSOA aircraft are especially vulnerable to threat small arms and man-portable missiles. Threat information supporting targeting by ARSOA assets is also required. This information could include the selection of vulnerable points for targets identified for destruction by attack helicopters or the disposition and expected actions of threat reaction forces during DA missions conducted with other SOF elements. Typical threat products used in ARSOA IPB are—

- Situation templates depicting known and likely enemy ADA sensor and weapons coverage and locations and reaction times of both ground forces and aircraft.
- Avenue-of-approach (AA) overlays identifying approaches and optimum engagement points for TGO or conventional attack operations.

EXTERNAL IEW SUPPORT

5-21. Since organic support is limited, ARSOA S2s must be adept at leveraging intelligence support from the IEW system using available systems support. ARSOA units normally operate in a support role as part of a larger SOF contingent (JSOTF, joint special operations air component [JSOAC],

ARSOTF). Consequently, ARSOF S2s should, whenever possible, integrate their intelligence operations with those of their supported units—especially when the supported unit has a more robust intelligence support structure.

5-22. The SOC J2, in coordination with theater resources, provides NRT intelligence throughout mission planning and execution for SO within his respective theater. The SOC J2 is the conduit for intelligence support for ARSOA in the theater. The ARSOA S2 must ensure that his section has the appropriate system support to integrate into the theater IEW architecture. The S2 must work closely with the S6 to coordinate this support.

5-23. The Requirements Management Division, USASOC, provides support for exercises and operations for ARSOA while in CONUS.

HUMINT SUPPORT

5-24. HUMINT is collected by using a variety of methods. HUMINT collectors—

- Interrogate EPWs and debrief or interview civilian internees, detainees, and refugees.
- Debrief returned captured U.S. personnel, escapees, and evaders.
- Exploit captured enemy documents (CEDs) and captured enemy material (CEM).
- Perform controlled collection.
- Conduct tactical and special reconnaissance.
- Conduct liaison with local military or paramilitary forces and the local population and obtain reports from friendly troops.

SIGINT SUPPORT

5-25. ARSOA aircraft can be equipped with onboard systems that can provide SIGINT support for missions. SIGINT-derived information is available through the supported unit's SIGINT channels.

5-26. Manpacked SIGINT support is available from SOT-As that are organic to SF groups. One use of SOT-As is to accompany ARSOA aircraft during missions providing early warning or indications of threat activities by intercepting voice and nonvoice communications. Properly equipped SOT-As can provide limited direction finding (DF) of threat and friendly emitters during flight. SOT-As can also support force protection operations at ARSOA forward area bases.

IMINT SUPPORT

5-27. IMINT is a significant source of critical operational data for ARSOA operations. IMINT comes from radar, photographic, infrared, and electro-optic sources. ARSOA uses detailed imagery to develop routes, to deconflict airspace, and to provide information for attacking targets.

5-28. ARSOA needs imagery for route planning and for operations in target areas. Target IMINT should cover the target during various conditions and angles to provide details and multiple perspectives of target terrain. The ARSOA imagery analyst must be able to accurately determine the

measurements of structures, spacing, and obstacles on or around target areas. Imagery mosaics are an extremely useful tool when conducting route planning. Additionally, ADP imagery display systems that display digital imagery perspectives can provide "pilot seat" perspectives for mission planning and rehearsals.

5-29. IMINT support is through either FRAGOs, intelligence annexes to the OPORD, standing operating procedures (SOPs), or RII. IMINT systems controlled by a higher HQ, other Services, or national agencies respond to approved RIIs through appropriate channels.

5-30. The channels used to provide IMINT support depend on the requesting unit and the requirement, the agency receiving the request, and command procedures. Theater, corps, and division assets can provide IMINT when the target area falls within the range of their organic systems. Other Services and national assets also can be tasked to provide dedicated IMINT support to ARSOA operations on the basis of availability and mission priorities.

ELECTRONIC WARFARE SUPPORT

5-31. Depending on the nature of the operation and threat capabilities, ARSOA may require direct EW support while conducting IO. The effects of fire for electronic attack (EA) are to disrupt, delay, divert, or deny the threat's C2 or the target acquisition capabilities of its weapons systems, while retaining friendly use of the electromagnetic spectrum. Active jamming can prevent enemy early warning radar from detecting airborne forces or, if detected, from determining their routes. Active jamming is especially critical if using ARSOA assets to conduct deep strikes against key targets as part of a joint attack operation.

5-32. EW also supports deception operations. During ARSOA missions, EW can mislead the threat by manipulating, distorting, or falsifying indicators, thus persuading the threat to react in a manner against his own interests. Also, false transmissions can support ARSOA deception plans or feints. EW planners can use selective jamming and imitative deception measures to disrupt foreign C2 nets, which reduce the enemy's ability to react to ARSOA presence.

5-33. Any EW operation requires close coordination so it does not disrupt friendly air-to-ground or ground-to-ground communications or reveal friendly force intentions.

CI SUPPORT

5-34. The ARSOA regiment has no organic CI support but CI is vital to ARSOA mission planning, preparation, and execution. CI supports force protection efforts by providing MDCI information and products, such as the MDCI appendix to the ARSOA regiment OPLANs and OPORDs. ARSOA S2s must request or coordinate for dedicated CI support, if required for operations. See FM 34-60 and FM 34-5, *(S) Human Intelligence and Related Counterintelligence Operations (U)*, for additional information on CI and HUMINT.

OTHER NONORGANIC SUPPORT

5-35. ARSOA requires other nonorganic support relating to weather and GI&S. Weather and GI&S support are discussed in the following paragraphs.

WEATHER SUPPORT

5-36. ARSOA is highly susceptible to the effects of weather, making it a critical aspect of mission planning. The SOWTs normally provide timely weather support to ARSOA. Direct weather support must include, but is not limited to—

- Forecasts of general weather conditions and specific meteorological data elements as described in the 24-hour forecast.
- Geophysical information and climatic studies and analyses.
- Weather advisories, warnings, and specialized weather briefings, to include flight weather briefings of routes and objective areas.
- Lunar and solar illumination data.

GI&S AND OTHER INTELLIGENCE PRODUCTS

5-37. The ARSOA regiment maintains an automatic distribution account with DIA to receive pertinent reports and studies. National assets can supply information for quick response missions and may even dedicate certain resources to support ARSOA. ARSOA units use their Department of Defense activity address code (DODAAC) to requisition standard National Imagery and Mapping Agency (NIMA) products directly from the Defense Logistics Agency (DLA) through the Army supply system. USASOC helps CONUS-based units obtain special GI&S products and services.

Chapter 6

IEW Support to PSYOP

This chapter discusses the mission and organization of PSYOP units, and the intelligence requirements of PSYOP. This chapter addresses the IEW support MI provides to PSYOP and the support PSYOP provides to the IEW system. See FM 3-05.30, *Psychological Operations*, for details on PSYOP.

INTRODUCTION

6-1. PSYOP units support conventional and SOF military operations worldwide by conducting strategic, operational, and tactical activities to influence opinions, emotions, attitudes, and behaviors of foreign audiences to create conditions favorable to U.S. or HN goals. PSYOP personnel receive cross-cultural and language training to obtain a regional orientation. Intelligence support for PSYOP focuses on the attitudes and inclinations of a given population group. Additionally, it needs to identify threat PSYOP activities and recommend countermeasures.

MISSIONS

6-2. Army PSYOP forces plan, conduct, and support PSYOP missions designed to support U.S. national policy. PSYOP include planned messages, products, and other actions in peace or war that are directed toward foreign enemy and neutral audiences. PSYOP support varied military, political, and diplomatic actions across the range of military operations. These missions can be strategic, operational, or tactical:

- Strategic PSYOP missions are conducted at the national or theater level to advance broad, long-term psychological objectives that support national psychological objectives.
- Operational PSYOP missions are conducted to achieve mid-term objectives that support theater campaigns and major operations.
- Tactical PSYOP missions are conducted to achieve immediate or short-term objectives that support tactical military operations.

Any of the above categories of PSYOP may support more than one level of the range of military operations.

6-3. PSYOP units, whether operating unilaterally or with conventional forces across the entire range of military operations, must always consider nonmilitary factors and objectives. PSYOP missions—

- Play a critical and integral role in achieving or addressing these nonmilitary objectives.
- Aid in accomplishing tactical, operational, and strategic military objectives.

- Contribute nonlethal leverage across the range of military operations and are key contributors to shaping the international security environment and reacting to events.
- Must be integrated with all operations to prevent contradictory or conflicting messages.

ORGANIZATION

6-4. Specifically organized and trained Army units conduct PSYOP missions. One Active Army and two RC PSYOP groups comprise the majority of PSYOP forces.

6-5. The Active Army psychological operations group (airborne) (POG[A]) has responsibility for:

- Planning and conduct of Army PSYOP activities authorized and implemented worldwide.
- Support of contingencies and open hostilities short of declared war. It also develops, coordinates, and controls peacetime PSYOP activities.
- Planning and execution of strategic and operational missions for all U.S. CINCs when war is declared.

The Active Army POG(A) consists of a group HHC, four regionally oriented PSYOP battalions, one tactical PSYOP battalion (TPB), one PSYOP dissemination battalion, and the Research and Analysis Division consisting of four regionally oriented strategic studies detachments (SSDs). (Figure 6-1).

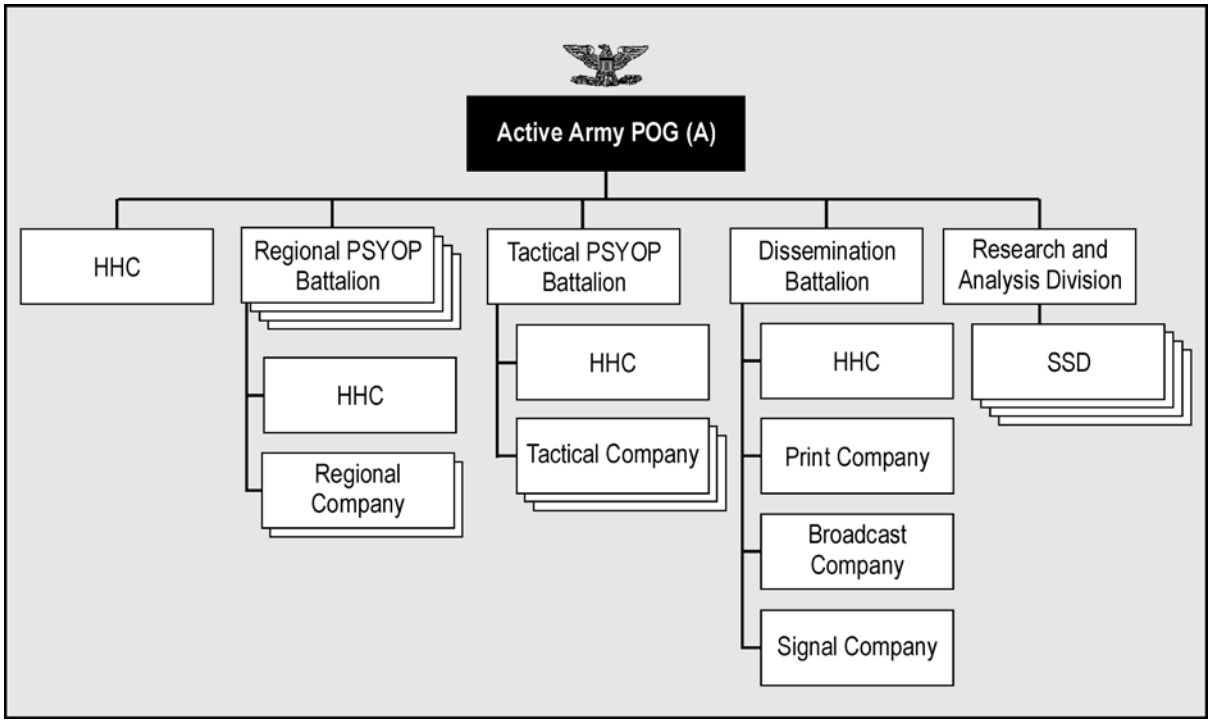


Figure 6-1. Active Army POG(A)

6-6. An element of the Active Army POG(A) normally is assigned as the JPOTF HQ of the unified command. This element may be designated as the senior PSYOP HQ over RC POGs or allied elements within the command.

6-7. Within the United States Army Reserve (USAR) are two POGs (Figure 6-2), consisting of tactical battalions, a dissemination battalion and, in one group, an enemy prisoner of war/civilian internee (EPW/CI) battalion. The JPOTF normally exercises OPCON of the elements of these units that are mobilized for contingency operations.

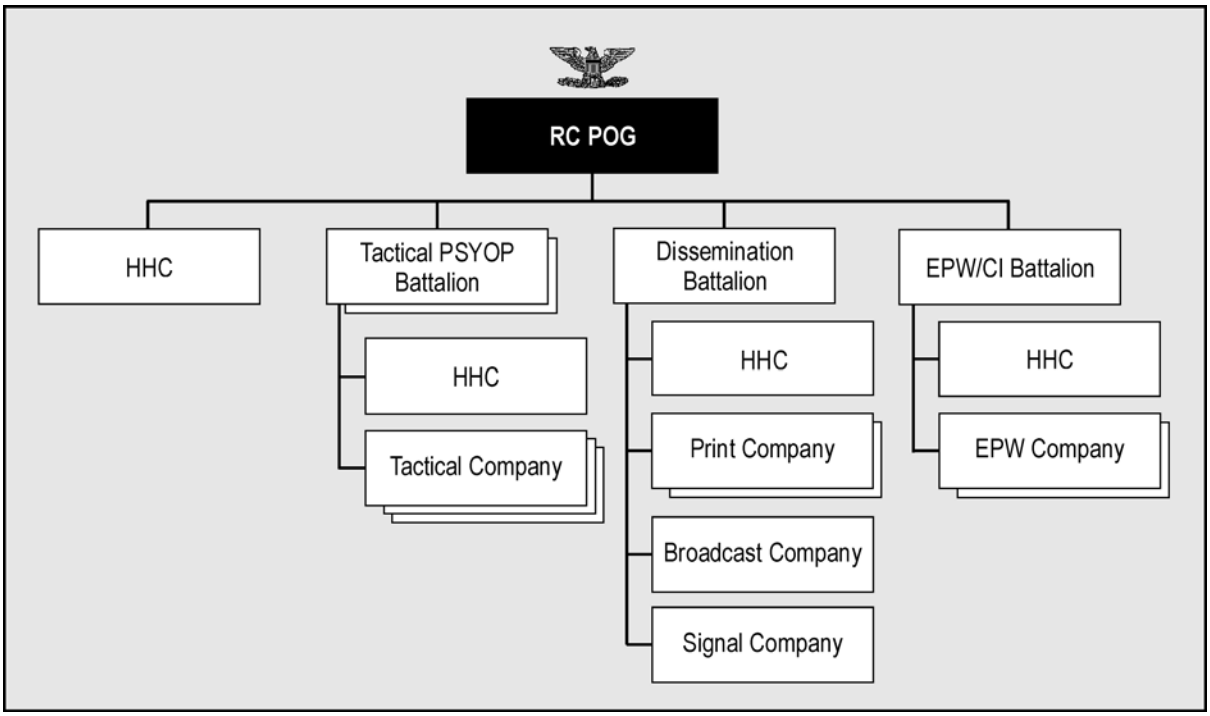


Figure 6-2. Example of a Reserve Component PSYOP Group

PSYOP INTELLIGENCE ORGANIZATION

RESEARCH AND ANALYSIS DIVISION

6-8. The deputy commanding officer for Research, Analysis, and Civilian Affairs (DCO/RACA) manages the Research and Analysis Division of the Active Army POG that supports all PSYOP groups and their subordinate elements. The DCO/RACA represents the commander in the intelligence production cycle, directs special projects and analyses to support contingencies and special actions, and supervises Army civilian PSYOP analysts assigned to the SSDs.

GROUP S2

6-9. The S2 staff organization of the POG facilitates the planning for collection and dissemination of intelligence required to conduct effective PSYOP. In PSYOP battalions, companies, and detachments that operate independently or support other forces, SIO is usually the S2 or the chief of

that unit's PDC. In these situations, the PDC chief establishes the same type relations with the supported unit's S2 as those normally established between a PSYOP S2 and the supported unit's S2.

BATTALION S2

6-10. The PSYOP battalion, whether a regional, tactical, or dissemination battalion, performs the same IEW roles and functions as the POG S2 section. The battalions are organized into a collection section and intelligence operations section.

6-11. PSYOP intelligence focuses on information about a particular target audience. This information includes the identity, location, conditions, vulnerabilities, susceptibilities, and effectiveness of a designated target audience or key personalities. Upon receipt of an impending PSYOP mission, the S2 accesses existing databases and available products to support the mission. He must query every available source including the theater SOC J2, the theater JIC, national, HN, and the supported units' resources. The S2 also refers to current versions of basic PSYOP studies (BPSs), special PSYOP studies (SPSs), and special PSYOP assessments (SPAs) pertaining to the target audience. These resources are processed and integrated as part of the PSYOP planning cycle.

6-12. The PSYOP S2—

- Accesses the IEW system to answer the commander's PIR and IRs.
- Ensures PSYOP intelligence elements can access the intelligence assets and products they need to support the commander.
- Ensures, as an intelligence producer, that the specialized products his intelligence elements produce go into the IEW system and are included in intelligence databases. He directs the intelligence effort to meet the commander's needs.
- Tasks organic and attached intelligence assets and forwards RIIs to higher HQ.
- Integrates PSYOP intelligence efforts with other units and agencies.
- Maintains current situation and environmental elements of the common operating picture.
- Identifies, confirms, and coordinates priorities for unit geographic area requirements for GI&S products and services to support OPLANs and CONPLANs.

OTHER ORGANIC SUPPORT

STRATEGIC STUDIES DETACHMENT

6-13. An SSD, organic to the Research and Analysis Division, supports each regional PSYOP battalion. The SSDs provide comprehensive analysis of PSYOP conditions, and potential target audiences within a given AOR. SSD civilian analysts, possessing advanced academic degrees and expert language skills, are responsible for the PSYOP portion of the Department of Defense Intelligence Production Program (DODIPP) by producing high quality SPSs and SPAs, and by writing the PSYOP appendix to the military capabilities

study (MCS). The analysts conduct thorough research and analysis of target countries, regions, groups, and issues to develop effective PSYOP. The detachments provide timely political, cultural, social, political-military, economic, and policy analyses to PSYOP commanders and their staff, as well as to other agencies. SSD analysts also assist in deliberate and contingency planning and deploy to support operations. The PSYOP studies and other SSD-generated analytical products are accessible through the PSYOP Automated System (POAS), which also provides the PSYOP community with access to various classified and unclassified databases. Commanders can access POAS through INTELINK and the SCI INTELINK systems.

TARGET AUDIENCE ANALYSIS DETACHMENT

6-14. The TAAD, an element of the regional PSYOP battalion, identifies target audiences and analyzes their attitudes, beliefs, vulnerabilities, and susceptibilities. TAAD and SSD personnel combine their efforts to monitor and analyze intelligence and prepare in-depth target audience analyses. The TAAD also analyzes opponent PSYOP to develop counterpropaganda programs.

TACTICAL PSYOP BATTALION

6-15. The TPB provides direct PSYOP support to corps-level units and below. TPBs develop, produce, and disseminate tactical products assigned by the POTF. Tactical PSYOP teams (TPTs) disseminate PSYOP products (loudspeaker messages, leaflets, and posters) in local areas, and conduct face-to-face communications with the target audiences. Because tactical PSYOP units have direct access to the local population and threat forces when disseminating products, they are able to collect information. TPTs provide the TPB and POTF with critical information on target audiences' attitudes and behaviors.

6-16. Some PSYOP units have radio monitoring elements. These elements—

- Overtly monitor threat and neutral commercial radio broadcasts.
- Are not capable of the direction finding, traffic analysis, and cryptologic operations as are IEW SIGINT collection and EW assets; however, they can be significant to the IEW collection effort.
- Record selected broadcasts and forward them to a PD for translation, transcription, and content analysis. These recordings can reveal a lot about the intended target audience of the broadcasts and the PSYOP intentions of the broadcaster.

EPW/CI BATTALION (RC)

6-17. A PSYOP EPW/CI battalion RC supports the PSYOP community. This battalion conducts tasks that support the overall PSYOP mission to include—

- Screening the EPW/CI camp population.
- Interviewing and surveying the camp population.
- Collecting PSYOP information.
- Disseminating reports of this information.
- Recording EPW surrender appeals.

6-18. During conflict, EPWs and civilian internees are continuous sources of current information of value for both PSYOP and intelligence operations.

TESTING AND EVALUATION DETACHMENT

6-19. Elements of the TED conduct surveys, interviews, and panels to collect PSYOP intelligence. These activities are different from tactical intelligence collection. They use techniques developed for market analysis, sociological research, and HUMINT techniques. The detachment's goal is to obtain information on attitudes, beliefs, behaviors, and social organizations.

6-20. Since the PSYOP producer must anticipate that its products will be subjected to analysis, there is a need for intelligence on the opposing PSYOP threat. This intelligence will come from a combination of OB, MDCI analysis, and PSYOP databases.

6-21. PSYOP can also provide intelligence of use to MDCI analysis and deception planning elements. This intelligence usually would concern sociological prejudices or predilections of a targeted force that could be manipulated or capitalized upon by the deception effort.

PSYOP ANALYSIS PROCESS

6-22. The PSYOP analysis process is a systematic and continuous process that PSYOP commanders and their staffs use to plan and conduct assigned missions. It is very similar to the intelligence cycle, as it is continuous and relies on intelligence data presented in a format not unlike the IPB process. The PSYOP analysis process builds on existing IPB but is oriented on populations as opposed to terrain or threat organizations. The process examines target audiences within and outside of the targeted PSYOP AO. The PSYOP analysis process correlates—

- Geographic analysis.
- Climate and weather analysis.
- Demographic evaluation and target audience analysis.
- Operational area evaluation.
- Database integration.

These factors are analyzed for expected target audience behavior and to identify means and requirements for desired behavior changes. FM 3-05.30, Chapter 10, provides a detailed description of this process.

NONORGANIC IEW SUPPORT TO PSYOP

6-23. PSYOP units plan, produce, and disseminate the products required to accomplish their missions. However, organic IEW support often is unable to provide enough support for mission success. Therefore, PSYOP S2s must leverage the support available in the IEW system to obtain the rest of the needed intelligence and information.

IEW SUPPORT FROM HIGHER ECHELONS

6-24. PSYOP missions often require IEW support from higher echelons. National- and theater-level IEW support is discussed in the following paragraphs.

National Support

6-25. The majority of PSYOP missions, particularly at the strategic and operational levels, require access to intelligence information and products produced at the national level. At the national level, the non-DOD agencies such as the Central Intelligence Agency (CIA) and DOS collect and produce valuable PSYOP-related intelligence. These agencies are engaged in every region of the world and are sanctioned to provide support for PSYOP intelligence purposes. Within DOD, the NMJIC, the National Ground Intelligence Center (NGIC), and NSA are excellent sources for intelligence reports and products. These agencies have extensive knowledge of potential target audiences. They also have available databases and collection frameworks in place with developed intelligence requirements and tasks that can support PSYOP efforts.

Theater Support

6-26. The primary concern of the SOC J2 is in-theater IEW policy formulation, planning, and coordination for deployed ARSOF, including PSYOP. The SOC J2—

- Ensures that sufficient intelligence support is available for each mission tasked by the SOC.
- Relies on the theater Service IEW organizations to collect, produce, and disseminate intelligence to meet PSYOP requirements.
- Tasks subordinate SOF units and coordinates with higher and adjacent units to collect and report information in support of PSYOP intelligence requirements.

6-27. Theater OPORDs, OPLANs, campaign plans, and supporting PSYOP and intelligence annexes contain specific PSYOP IRs. Most of these requirements are validated and incorporated into PSYOP and IEW collection plans. (See FMs 34-1, 34-2, and 34-40, *[S] Electronic Warfare Operations [U].*)

6-28. To meet some of these requirements, SIOs may need to reinforce or refocus available IEW assets. Often, the PSYOP or IEW SIO must enter the IEW system to access information or intelligence from other units, intelligence agencies, or sources at higher, lower, and adjacent echelons. Figure 6-3, page 6-8, shows examples of theater sources that support PSYOP.

TACTICAL SUPPORT

6-29. PSYOP intelligence personnel must coordinate with higher, adjacent, and supported units for access to their tactical HUMINT information. Swift exploitation of collected HUMINT information is critical. The S2s supporting tactical PSYOP must ensure there are enough conduits to support the exchange of perishable battlespace information to and from deployed PSYOP elements.

Units	Agencies	Other Sources That May Benefit PSYOP Intelligence
HN Military HN Paramilitary or Militia SF CA Military Police (MP) MI Units	HN Federal and Local Government HN Police HN Government Agencies (Economic and Commerce) State Department CIA DIA United States Information Agency (USIA) United States Agency for International Development (USAID)	EPWs Defectors Refugees Civilians (friendly and enemy) Documents Letters Published Material Poems Radio Television

Figure 6-3. Example of Organizations and Other Sources That Can Assist PSYOP Efforts

INTELLIGENCE DISCIPLINES SUPPORTING PSYOP

6-30. PSYOP analysts use HUMINT, SIGINT, IMINT, OSINT, TECHINT, and CI support to plan their missions. These intelligence disciplines are discussed in the following paragraphs.

HUMINT SUPPORT

6-31. IEW intelligence and information gathered from EPWs, defectors, line crossers, refugees, captured documents, and published materials often provide PSYOP intelligence elements with significant insights into the psychological situation in a specific area or within a target group. With consent and proper authority, these sources may be used to develop and test PSYOP products.

6-32. In addition to organic HICs, HUMINT support for PSYOP units is available from the supported theater's IEW assets. Otherwise, HICs are collocated at EPW collection points and holding facilities at echelons division and above. Interrogation information is then incorporated into the all-source product. When PSYOP units need information for mission planning that only HICs might provide, they must coordinate their requirements with the command that has HICs.

SIGINT SUPPORT

6-33. SIGINT assets support PSYOP by providing SIGINT and EW products extracted from locating, monitoring, and transcribing threat communications. EW assets support PSYOP by locating and jamming threat PSYOP transmitters. These assets provide information and intelligence that help reveal enemy activities or plans so that PSYOP can develop effective countermeasures.

IMINT SUPPORT

6-34. PSYOP units request IMINT support from the supported command. PSYOP analysts use IMINT in various ways. IMINT helps locate and

determine the capabilities and operational status of transmitters or printing plants. PSYOP analysts also use IMINT to locate mobile target groups.

6-35. By analyzing imagery of the location and architecture of key structures, PSYOP analysts can determine the ethnic or religious makeup of a town or village. Other uses for IMINT products include identifying and evaluating operational capabilities of transportation networks, factories, and other public structures or systems.

6-36. PSYOP analysts use IMINT to confirm or deny acts of rioting, acts of sabotage, demonstrations, and work slowdowns that are either the original PSYOP objective or an impact indicator of a PSYOP campaign or specific product.

OSINT SUPPORT

6-37. OSINT, through publications, academics, and mass media, can provide information on natural disasters, biographic information, culture, historical context, weather, and even BDA. Open-source data can also be purchased for geospatial and mapping data. Less obvious is the use of open-source materials such as graffiti and taggings to identify gang turf or to gauge public opinion.

TECHINT SUPPORT

6-38. PSYOP units can use TECHINT to focus their efforts on critical, highly technical threat units and installations. They can also identify alternative methods of PSYOP message dissemination through the analysis of the target population's information infrastructure.

6-39. The Captured Materiel Exploitation Center (CMEC) or a battlefield TECHINT team at corps produces TECHINT products. TECHINT is incorporated into all-source intelligence products. Specific requests for TECHINT support are coordinated through the SOC J2 to corps HQ or above.

CI SUPPORT

6-40. CI detects, evaluates, counteracts, or prevents foreign intelligence collection, subversion, sabotage, and terrorism. It determines security vulnerabilities and recommends countermeasures. CI operations support OPSEC, deception, and FP.

OTHER NONORGANIC SUPPORT

6-41. PSYOP planners must have access to the latest GI&S and weather information to plan and conduct their assigned missions. This support is readily available from the outside sources described below. Additionally, PSYOP planners must integrate their requirements with supported units to benefit from the collection of other intelligence, such as MASINT.

WEATHER

6-42. Weather and other environmental factors affect almost all PSYOP missions. Severe weather may degrade PSYOP dissemination efforts, as in the case of airborne leaflet drops. Sunspot activity can disrupt radio and

television broadcasts into a target area. Severe weather may also enhance PSYOP campaigns if it affects threat morale. Therefore, PSYOP units need accurate weather and environmental information. Required weather support includes—

- Forecasts of general weather conditions and specific elements of meteorological data, as described in the 24-hour forecast.
- Solar, geophysical information, and climatic studies and analysis.
- Weather advisories, warnings, and specialized weather products, as required.

6-43. The primary source for required weather intelligence support, to include specialized products, is the USAF 10th Combat Weather Squadron. This squadron is a component of the Air Force Special Operations Command (AFSOC) that provides special operations weather detachments (SOWDs) for attachment to ARSOF units.

GI&S AND OTHER INTELLIGENCE PRODUCTS

6-44. PSYOP units, using their DODAAC, may requisition standard NIMA products through the Army supply system directly from DLA. Intelligence products and services may also be requested from DIA. USASOC helps units obtain special GI&S products and services.

PSYOP SUPPORT TO IEW

6-45. PSYOP units also produce specialized intelligence products to support a variety of other combat and IEW missions and operations. PSYOP units develop these intelligence products by monitoring and assessing situations and evaluating their impact on specified target groups and national objectives. Finally, this information is combined with additional research on specific target groups.

6-46. The main focus of this production effort is on socioeconomic, political, and diplomatic factors. It also focuses on the military aspects of a region, situation, or group. These products include, but are not limited to—

- Strategic-level documents such as BPSs, SPSs, and SPAs.
- Operational- or tactical-level target analyses on specific target groups.
- PSYOP reports and estimates.

Although PSYOP units primarily use these products to conduct their operations, the products also contain information and intelligence that is useful to the ARSOF IEW community and other SOF. These products contain diverse information on social customs, enemy morale, and key nodes.

6-47. Through their specialized training and close contact with friendly and threat persons, PSYOP units can provide information of value to the PSYOP and intelligence efforts. PSYOP S2s and other intelligence personnel must ensure this information is placed in intelligence channels. PSYOP units can conduct PSYOP assessments of EPW/CI operations, coordinate the EPW/CI intelligence collection activities, or otherwise support the information flow from threat areas.

INFORMATION OPERATIONS

6-48. PSYOP are also an integral part of IO along with deception, EW, OPSEC, and physical destruction of C2 nodes. Providing "nonlethal firepower" in the C2 attack role, PSYOP facilitate the effectiveness of the other IO components by reinforcing desired adversary perceptions of a given situation. The main role of PSYOP in the C2 protect role is to help counter hostile propaganda efforts.

Chapter 7

IEW Support to Civil Affairs

This chapter discusses the mission, organization, and intelligence requirements of CA units and CMO. It addresses the IEW support MI provides to CA units, and the support CA operations provide to the IEW system. See FM 3-05.40, *Civil Affairs Operations* (currently published as FM 41-10), for further information.

INTRODUCTION

7-1. CA units help commanders fulfill their civil-military requirements to foreign governments and populations within an AOR. The vast majority of CA personnel are reservists who provide specialized civilian skills in such areas as civil administration, public safety, infrastructure, agriculture, and legal systems. CA unit intelligence requirements address the full spectrum of threat, cultural, social, political, economic, and environmental information within the area of present or potential operations. They focus on information that will support the successful execution and prevent the disruption of CMO activities. It is only through a coordinated effort that CA and MI assets can provide all the information necessary for the commander to accomplish the CA mission.

MISSIONS

7-2. There are six CA activities: foreign nation support, populace and resources control (PRC), HA, military civic actions, emergency services, and support to civil administration. CA activities are planned and conducted by CA forces due to the complexities and demands for specialized capabilities involved in working within areas normally the responsibility of indigenous civil governments or authorities.

7-3. CA units support the commander's missions by—

- Fulfilling responsibilities of the military under U.S. domestic and international laws relevant to civilian populations.
- Minimizing civilian interference with military operations and the impact of military operations on the civilian population.
- Coordinating military operations with civilian agencies of the USG, civilian agencies of other governments, and NGOs.
- Establishing and operating civil-military operations centers (CMOCs).
- Exercising military control of the civilian population in occupied or liberated areas until control can be returned to civilian or non-U.S. military authority.

- Providing advice and assistance in organization of auxiliaries and political actions.
- Providing assistance to meet the life-sustaining needs of the civilian population.
- Providing expertise in civil-sector functions normally the responsibility of civilian authorities. That expertise is applied to implement U.S. policy to advise or assist in rehabilitating or restoring civil-sector functions.
- Supplementing the intelligence effort by providing a conduit for information to flow from the population to the command.
- Acting as the staff focal point for cultural aspects that impact on military operations.
- Supplementing the intelligence effort by providing a conduit for information to flow from the population to the command.
- Acting as the staff focal point for cultural aspects that impact on military operations.

7-4. The CA contribution to an operation is embedded in the ability to rapidly analyze key civil aspects of the operational area, develop an implementing concept, and assess its impact through the operation. Because of the political-military nature and sensitivity of CMO and CA activities undertaken by U.S. commanders, whether in a unified or multinational context, their conduct will be governed by deliberate policy developed and promulgated by the NCA.

7-5. Successful CA activities, whether supporting SOF or conventional forces, depend on the support of the population. Most U.S. military operations occur in a low-threat environment with the objective of winning popular support. CA units must therefore help other SOF mobilize this support, keeping in mind the impact of their activities on civilians. CA forces, as part of SOF, must remain politically attuned, regionally oriented, and linguistically capable of supporting SO.

ORGANIZATION

7-6. The theater SOC integrates CA into joint SO activities. Task-organized CA elements may be attached to the theater SOC for a specific period to provide dedicated support. The vast majority of the Army CA force is in the RC. This force consists of four CA commands that support four geographic combatant commanders. These organizations provide CA support to the geographic CINCs, as necessary, with organic brigades and battalions. Unlike conventional forces, CA units are area-oriented and must concentrate on a specific theater and its associated languages, cultures, and environments.

7-7. CA units should be tailored before employment, taking into consideration METT-TC. Figure 7-1, page 7-3, reflects the typical support relationships of the different levels of CA units and elements.

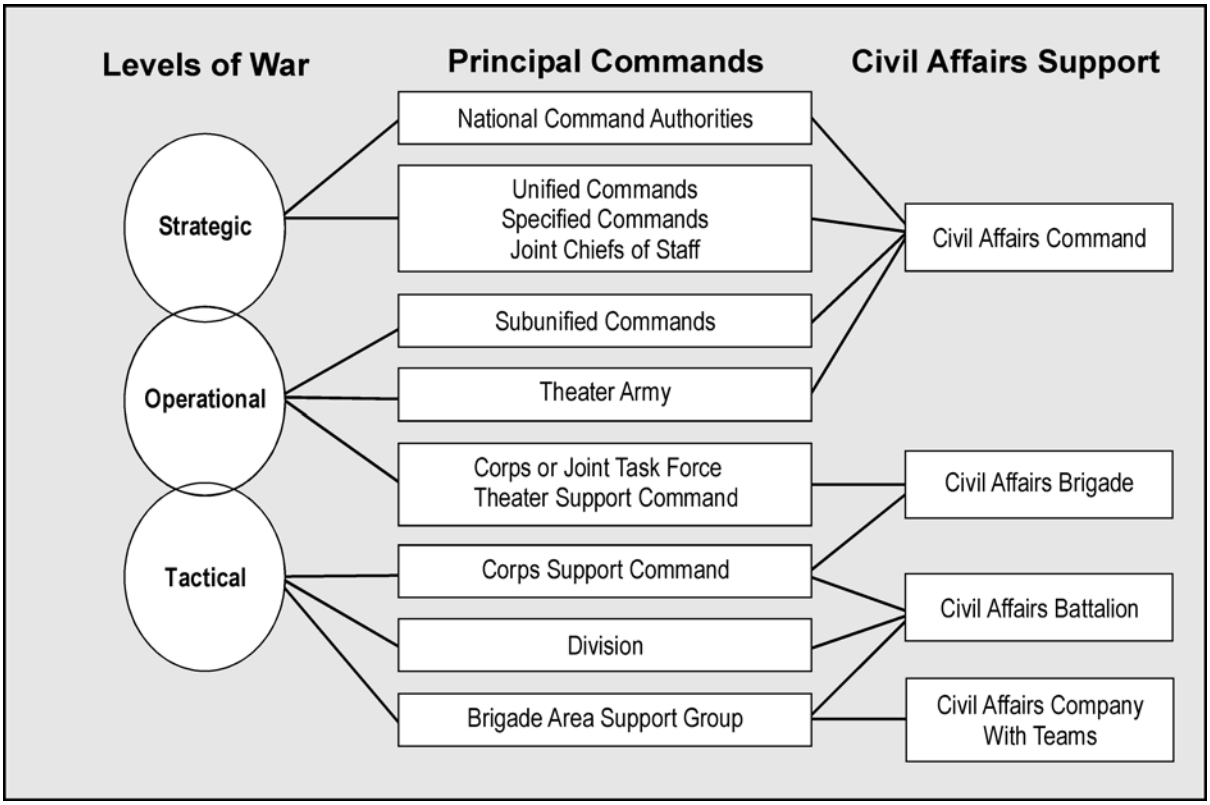


Figure 7-1. Typical Levels of CA Support

CA COMMAND (RC)

7-8. The CA command's mission is to plan, manage, and conduct CMO operations that support the field commander. The CA command may also provide staff support to component services and joint theater staff as required. Figure 7-2, page 7-4, presents the organization of the CA command.

7-9. The CA command provides predeployment C2 of geographically oriented CA brigades and battalions. The CA command trains, equips, and prepares its subordinate units for mobilization and deployment during war and peacetime operations. When deployed, CA units are attached to the supported command. The CA command can influence the CA unity of effort and plans through technical advice to CA units attached in the theater. All CA command elements not attached to subordinate commands remain under the C2 of the CA command.

7-10. The CA command employs its organic CA plans, programs, and policy team (CAP3T) to provide a CMO staff element for the unified command, subunified command, component service HQ, and functional command. CA command assets or separate support teams may augment CMO staffs. All 16 CA functional specialties are contained in the command's government, economics and/or commerce, public facilities, and special functions teams.

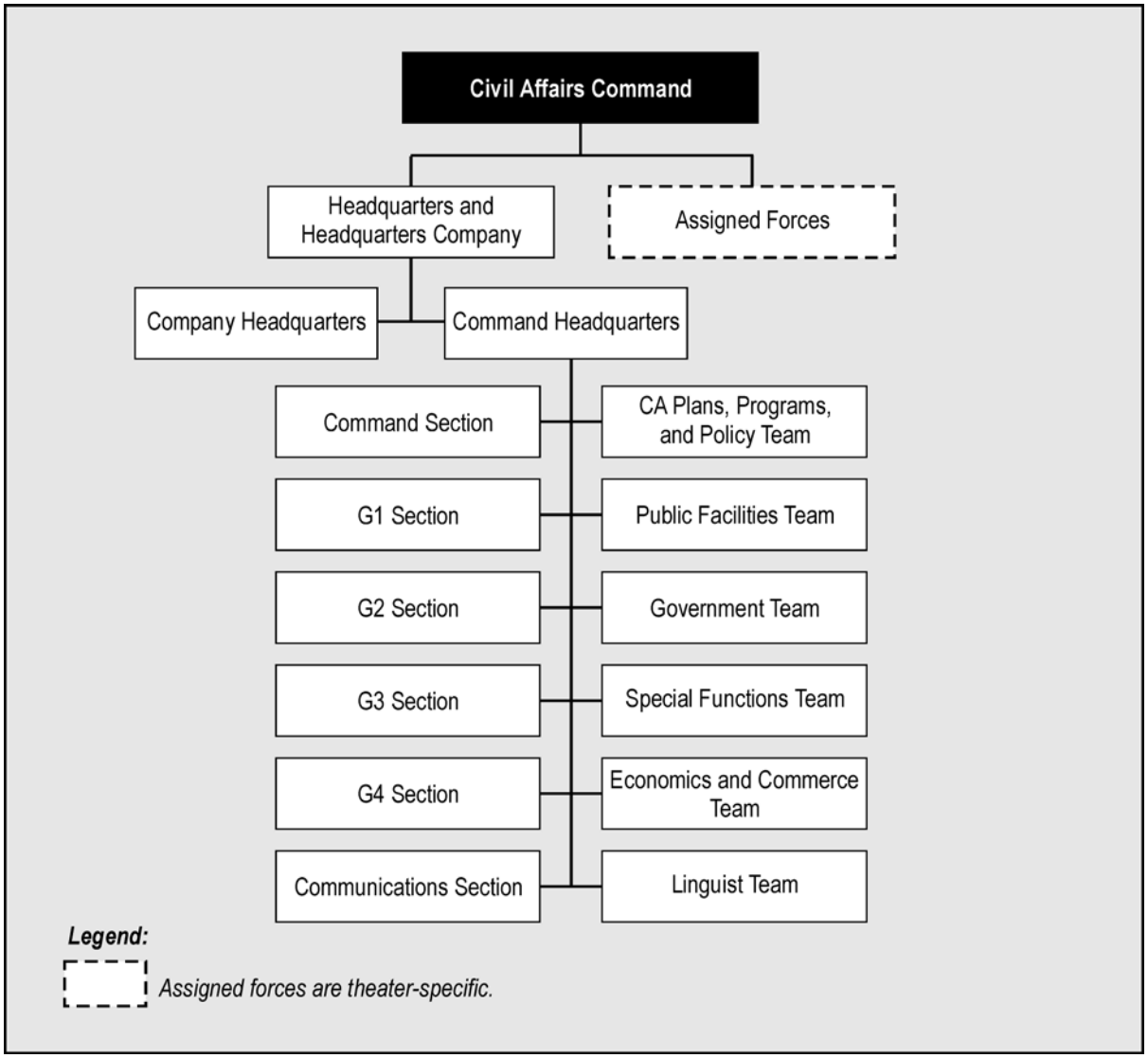


Figure 7-2. CA Command Structure

CA BRIGADE (RC)

7-11. The CA brigade supports the corps and JTF levels. The CA brigade accomplishes its mission through attachment. It provides predeployment C2 of geographically oriented CA battalions and subordinate elements. The supported unit chain of command provides C2 of attached CA units through normal operational channels. All CA brigade elements not attached to subordinate commands remain under the C2 of the CA brigade.

7-12. When a CA brigade is designated the senior CA unit in a theater, it is aligned to the theater Army and assumes the duties of a CA command. A support team (CAP3T) is added to the brigade's organization when it is the senior CA unit in the theater. Like the CA command, the CA brigade has functional teams that contain all functional specialties. The CA brigade can

influence unity of effort and plans through technical advice to CA units attached in the theater. Figure 7-3 presents the CA brigade (RC) structure.

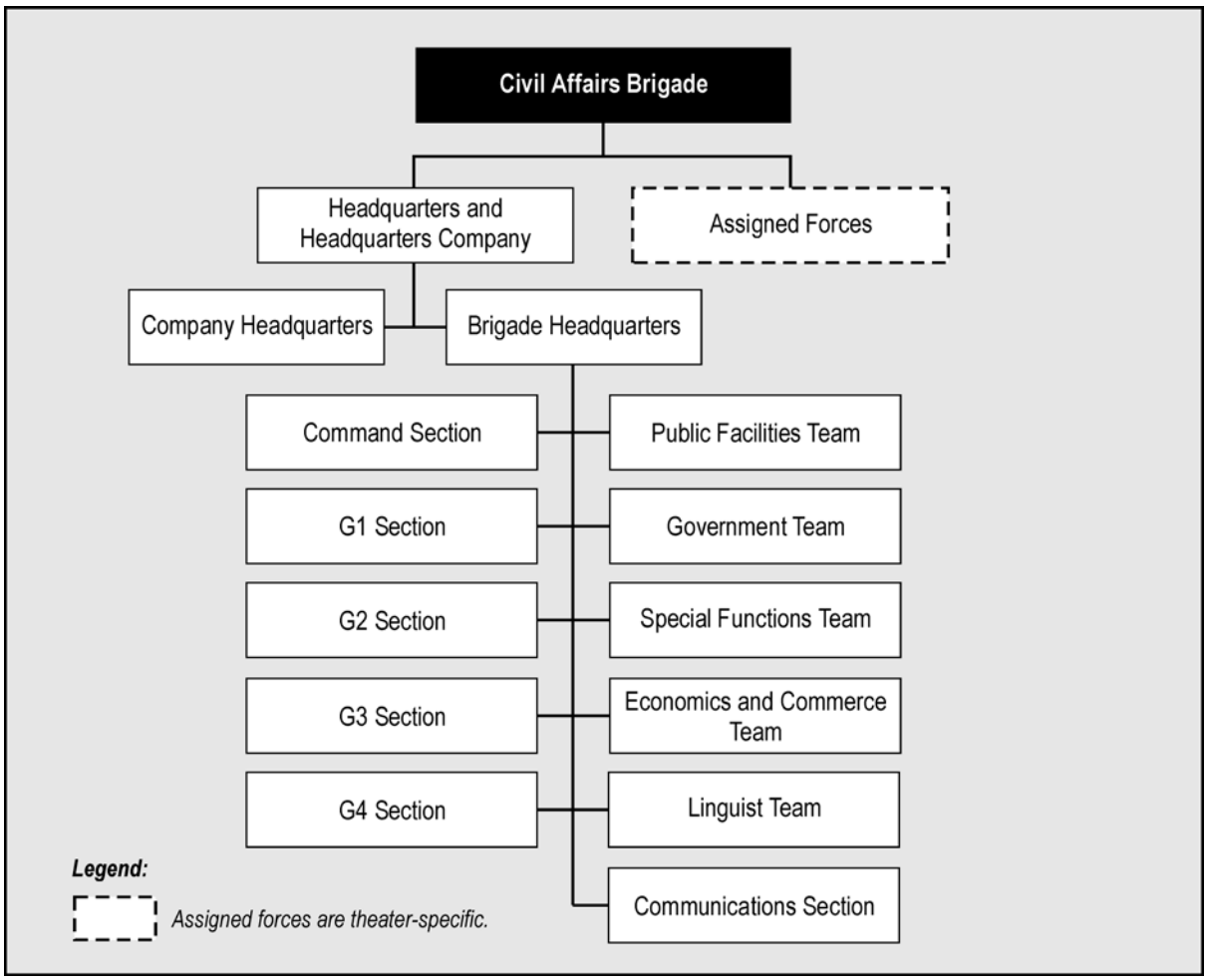


Figure 7-3. CA Brigade (RC) Structure

CA BATTALION (RC AND ACTIVE ARMY)

7-13. CA battalions can be assigned to the theater army, SF group HQ or ARSOTF, HQ CA command, HQ CA brigade (when designated senior CA unit), JTF, or JSOTF, as required. They—

- Function as a C2 element in multiple theaters for CA units assigned or attached to U.S. joint service or functional component and combined commands for contingency and crisis.
- Can deploy rapidly into any theater to provide CA support to U.S. joint service or functional component and combined commanders.
- Plan and conduct CA operations in support of SOF in FID and UW environments and in support of conventional forces.

- Help U.S. military SOF that are coordinated as a part of a U.S. security assistance program.
- Facilitate the relationships between the military forces, civil authorities, and people of the nations in which the military forces are located to execute CA-type activities.
- Plan, train, and teach foreign nation military forces to execute CA-type activities supporting military civic action, PRC, civil defense, community relations, and other programs, as required.
- Conduct CA activities in direct support (DS) of other SOF units during the conduct of their missions.
- Train, advise, and help other agencies about the cultural environment and ways to conduct and support military civic action projects where operations occur or are anticipated.
- Identify and help acquire available local resources, facilities, and support to enhance the ability of the commander to accomplish the mission.
- Provide in-country support and assistance to the U.S. country team and other USG agencies, as required or directed (for example, the USAID or USIA).
- Provide advice on the administration of refugee camps.
- Support SOF in UW operations; for example, advise and assist indigenous resistance forces, when directed, in developing political infrastructures to extend influence and legitimacy in contested areas.
- Provide technical advice and assistance to minimize local population interference with U.S. military operations and conduct NEO to minimize adverse effects on mission accomplishment.
- Provide humanitarian and civic assistance under U.S. and foreign national laws or under international agreements, in coordination with the staff judge advocate, to allow the commander to fulfill legal and moral obligations to the local population.
- Supplement the intelligence cycle and psychological and information operations activities at the operational and tactical levels.
- Provide a regionally oriented language capability.

CA BATTALION (GS)

7-14. The CA battalion (general support [GS]), found only in the Active Army, plans and conducts CA activities in support of other military operations. The Active Army battalion consists of an HHC and five regionally oriented companies that are aligned with each geographic combatant commander. It is composed of CA generalists and provides immediate operational access to CA assets for employment. It is the only CA unit available for immediate deployment. The unit is prepared to perform CA generalist tasks at all levels—strategic, operational, and tactical—until RC CA units can be mobilized and deployed to the theater. Figure 7-4, page 7-7, shows the structure of the CA battalion (GS). Figure 7-5, page 7-7, shows the structure of the USAR CA battalion.

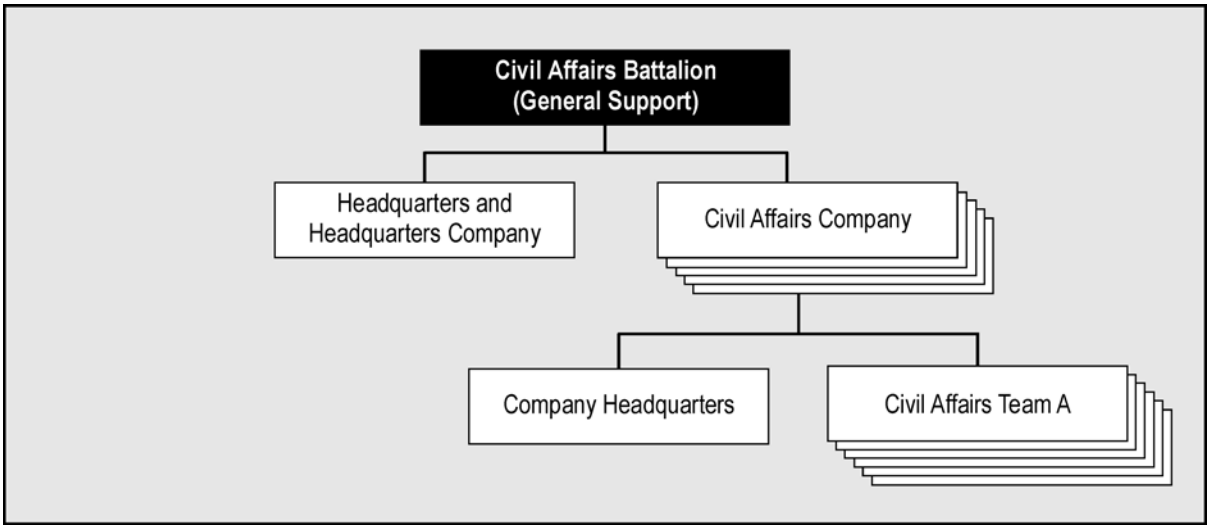


Figure 7-4. CA Battalion (GS) Structure

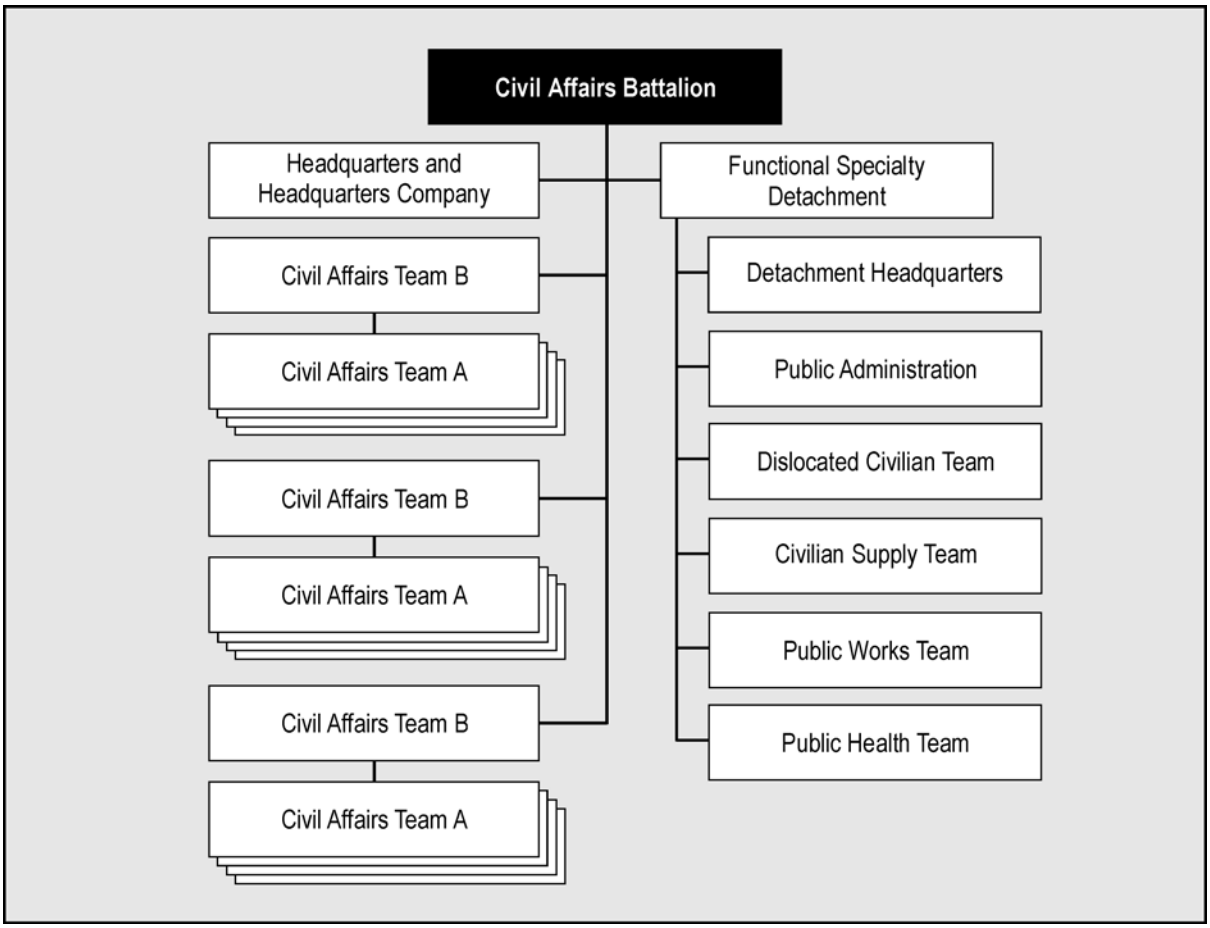


Figure 7-5. USAR CA Battalion Structure

THE CMO STAFF SECTION (S5 OR G5)

7-15. The CMO staff section (S5 or G5) provides the daily planning and execution of CMO for ARSOF at the battalion, group, and ARSOTF levels. The senior CMO officer normally is located in the main command post. The CMO staff is augmented by CA personnel as required to ensure adequate manning of the CMOC and the CMO cells (main command post and rear command post).

INTELLIGENCE REQUIREMENTS

7-16. The CA commander relies on his S2 to provide intelligence and pertinent information. Accurate, complete, and timely CA intelligence enables the commander and staff to estimate, in advance, what effect CMO may have on the mission or COAs of the supported unit or HQ. Ongoing intelligence support concerning popular attitudes toward civic action projects allows the commander to fine-tune projects to better meet area needs. The scope and nature of the CMO mission determine the type of intelligence support required by the CA unit. Examples of CA intelligence requirements include, but are not limited to, intelligence or information about the—

- Topography, hydrography, climate, weather, and terrain (including land formation, drainage, vegetation, and soils).
- Communications, transportation, utilities, power, and natural resources.
- Economic system and state of development, including the following:
  - Principal industrial, scientific, and technical capabilities.
  - Commercial processes.
  - Banking structure.
  - Monetary system.
  - Price and commodity controls.
  - Extent and nature of agricultural production.
- State of technological advancement.
- Labor potential, including availability by type and skill, practices, and organizations.
- Demographics of the civilian population, population census, location, ethnic composition, dietary habits, and health factors.
- Foodstuffs, tobacco products, or alcoholic beverages peculiar to the area.
- Social institutions and attitude of the population, including ideological, religious, and cultural aspects.
- Sociological factors, including key personnel (administrators, legal, and business) and the real power structure in the area.
- Educational philosophy, standards, and facilities; important cultural activities; and repositories.
- Political system, governmental structure, personalities, laws, and political heritage.
- Structure, orientation, capabilities, and reliability of indigenous public safety and law enforcement organizations.

- Documentary items, including passports, visas, vehicle operator licenses, and birth and marriage records.
- Effects of war damage.
- Resistance movements.
- Organization and operation of hostile forces in the area and the extent and degree of voluntary local support.
- Hostile civilian activities, including espionage, sabotage, and other factors of subversion and disaffection.
- Other existing conditions or factors relating to all CA functional specialties.

7-17. This intelligence support helps the commander and staff determine the—

- Conditions existing within an operational area.
- Techniques and the degree of control to use on the local population.
- Identities and backgrounds of key personalities, groups, or regions.
- Required resources available from U.S. forces or HN sources.
- Measures required to reestablish or develop viable political, economic, and sociological conditions.

7-18. Intelligence on potential threat activities is critical for the commander's FP efforts. These activities include possible terrorism, sabotage, and propaganda directed against planned or ongoing civic action projects. Such timely intelligence can allow for planning and implementing effective countermeasures.

CA INTELLIGENCE ORGANIZATION

7-19. The CA unit intelligence officer (S2 or G2) and his relatively small staff are the only MI assets organic to the CA unit. The CA commander directs the intelligence process through his S2 or G2 and the CMOC.

7-20. When deployed, the S2 or G2—

- Supervises organic and attached intelligence assets.
- Integrates CA intelligence efforts with other units' and agencies' efforts and products.
- Establishes liaison with HN military and government agencies, as required.
- Coordinates with the chief of the security assistance organization and the area coordination center in each operational area to meet the commander's intelligence needs.
- Assesses enemy CA and PSYOP capabilities, potential COAs, and their effect.
- Integrates with other CA and supported unit staffs.
- Produces and disseminates CA intelligence products and CA CMO estimates.

7-21. Organic intelligence assets within CA units are relatively limited. Therefore, a key component of successful CA and/or CMO intelligence support is the ability of CA unit intelligence personnel to integrate themselves into the theater intelligence architecture through the S2 or G2s of their higher HQ and supported units.

7-22. In garrison, the S2 or G2 ensures that intelligence products, such as area studies, are available for each country and area where CA and/or CMO operations might be conducted. The S2 or G2 develops and maintains an information database for his unit's geopolitical focus. This includes historical and geographical information, current periodic intelligence reports and partially developed products for contingency or crisis planning. Potential CA and/or CMO missions that support theater OPLANs and CONPLANs receive highest priority during the development process.

CMO PREPARATION OF THE BATTLESPACE

7-23. The S2 or G2 uses a slightly modified version of the standard IPB process as a methodology to support his efforts. This process is known as the CMO preparation of the battlespace (CMOPB). The CMOPB is a total staff effort that integrates, analyzes, and evaluates friendly force capabilities, which include allied and/or coalition forces, government agencies, and NGOs available against potential CMO activities or projects. The preferred results of the CMOPB are graphical products that portray information related to the CA functional specialties. These products are then used to analyze and compare CA and/or CMO COAs in each of these broad categories. Graphic products could include overlays or ADP outputs to reveal issues or items important to CA units. Some of these overlays include—

- Demographics: Shows dominant racial, religious, cultural, or political population densities. The S2 or G2 uses these overlays to create templates of prevailing attitudes and loyalties in nonhomogeneous populations.
- Infrastructure: Depicts public utilities by showing the location and capability or capacity of all public utility nodes (such as power stations and substations, pumping stations, telephone company switches, and waste handling facilities). These overlays, when used with maneuver overlays, can project the impact combat operations will have on the local population's ability to maintain basic living conditions.
- Medical support: Illustrates available health services support showing the location of private and public health service facilities (such as hospitals; pharmacies; and doctors, dentists, and veterinary offices). These overlays should reveal details such as capacity, age, capabilities, and equipment about each facility.
- Protected or restricted targets: Pinpoints locations of hospitals, national monuments, religious shrines or houses of worship, and other places protected by the Laws of War and the Geneva Convention.
- Displaced civilians: Shows population displacement. These overlays include—

- Projected overlays showing the routes the displaced population most likely will use given a set of projected conditions (for example, disruption of the food supply or physical destruction of an urban area).
- Current situation overlays showing routes currently in use by the displaced population, including the refugee camps that have developed or are beginning to develop.

NONORGANIC IEW SUPPORT TO CA

7-24. Since CA units have limited organic intelligence assets, nonorganic intelligence support is required. Nonorganic support enables the S2 or G2 to develop accurate, complete, and timely intelligence to help the commander estimate the influence of CA factors on the mission or potential COAs.

IEW SUPPORT FROM THEATER HIGHER HEADQUARTERS

7-25. As is the case of all other ARSOF in-theater intelligence activities, the CA unit S2 or G2 coordinates with the SOC J2 or the S2, G2, or J2 of his supported unit for access to all-source intelligence and IEW support. The theater JIC is the primary source for all-source intelligence support to all in-theater ARSOF. With guidance from the CA unit commander, the S2 or G2 prioritizes, validates, and consolidates all standing and routine RIIs that are being submitted to the JIC.

7-26. Under the staff supervision of the theater J2, the JIC—

- Responds to CA- and/or CMO-sponsored RIIs by integrating them into the theater requirements list.
- Monitors RII status until the appropriate collection assets respond.
- Maintains an intelligence database to support ARSOF requirements.

7-27. OPORDs, OPLANs, campaign plans, and supporting CA and intelligence annexes contain specific CA and/or CMO intelligence requirements. Necessary requirements are validated, prioritized, and incorporated into overall collection efforts. (See FMs 34-1 and 34-2.)

IEW SUPPORT FROM SUPPORTED UNITS

7-28. Single-source IEW support from the following disciplines also can be provided by most supported units, from the ARSOTF to theater level:

- SIGINT assets, which include the SOT-As assigned to SF units and assets with longer-range capabilities assigned to conventional MI units, can be accessed through the S2, G2, or J2 of their parent unit. CA units use SIGINT to pinpoint telecommunications and mass media facilities in target areas and to help assess the effectiveness of CMO by monitoring hostile forces in the area.
- IMINT products, ranging from photos taken by a reconnaissance patrol to those taken by national assets, can be requested and obtained through S2, G2, or J2 channels. CA units can use IMINT to locate and determine the operational status of key civil infrastructure in denied areas. The IMINT used by CA units can include identifying and

evaluating the operational capabilities of transportation networks, factories, and other public structures and systems.

- TECHINT assets normally are assigned only at theater level and higher, but their products can be requested through S2, G2, or J2 channels and the theater JIC. CA units use TECHINT to identify key technical characteristics and specifications of threat construction equipment, industrial facilities, and utilities (for example, electric and gas) in target areas.
- OSINT assets, through publications, academics, and mass media, can provide information on natural disasters, biographic information, culture, historical context, weather, and even BDA. Open-source data can also be purchased for geospatial and mapping data. Less obvious is the use of open-source materials such as graffiti and taggings to identify gang turf or to gauge public opinion.
- HUMINT assets, such as HICs, are available from the units normally assigned to an ARSOTF, and from the MI battalions and brigades assigned to conventional units from division to theater level. CA units use HUMINT to help determine the extent of war damage in threat-controlled areas. HUMINT can also help to locate key technical personnel who can be of use in repairing or operating key infrastructure once friendly forces arrive.
- CI agents and analysts are available from units assigned to the ARSOTF or JTF. CI soldiers are trained to detect, evaluate, counteract, and prevent foreign intelligence collection, subversion, sabotage, and terrorism. CI support is essential to the security and FP efforts of CMO.

OTHER NONORGANIC SUPPORT

7-29. CA requires nonorganic support relating to weather and GI&S. The following paragraphs discuss weather and GI&S support.

WEATHER SUPPORT

7-30. Weather support for CMO can be obtained through the JSOTF J2, who has access to the USAF SOWTs assigned to Army SF. Regardless of the primary mission, CA units must have advanced knowledge of seasonal and nonseasonal weather patterns. Direct weather support should include, but not be limited to—

- Weather advisories and warnings.
- Long-range weather forecasts.
- Precipitation patterns.
- Wind patterns.
- Tidal data.

7-31. Natural disasters are often the impetus behind CMO missions such as in the case of Hurricane Andrew, which severely damaged portions of South Florida. Other natural disasters such as earthquakes, tornadoes, and floods often require the deployment of U.S. forces to assist in disaster relief efforts

within the United States and on foreign soil. Severe weather during combat and noncombat missions may require the diversion of resources to relief operations.

GI&S AND OTHER INTELLIGENCE PRODUCTS

7-32. CA units, using their DODAAC, may requisition standard NIMA products through the Army supply system directly from DLA, the appropriate installation map depot, or the supporting OCONUS Army map depot. USASOC helps units obtain special GI&S products and services.

CA SUPPORT TO IEW SYSTEM

7-33. Although CA personnel are in an ideal position to collect a variety of information that may be of intelligence value, it is not their primary mission. Their job is to establish a close working relationship with the local population in day-to-day operations. CA information collection activities encompass the complete spectrum of cultural, social, political, and economic issues within the present or potential AO. A coordinated effort of CA and MI allows CA activities with their wide range of activities and contacts to provide the commander information for mission accomplishment.

7-34. Thus, this places CA personnel in a favorable position to—

- Passively collect information of intelligence value.
- Assist intelligence personnel in civilian-related activities.
- Identify local civilians with special skills or backgrounds that may aid the intelligence community.

7-35. Although valuable to the overall intelligence process, the role of soldiers engaged in CA and/or CMO activities must be passive. CA units collect and report information; however, CA personnel are not and must avoid appearing to be intelligence agents. Title 10 of the U.S. Code prohibits intelligence collection by military personnel unless authorized by competent legal authority.

Chapter 8

ARSOF IEW Support Systems and Architecture

The ARSOF S2 relies on the support of national and theater intelligence organizations to provide the ARSOF unit commander timely, relevant, and accurate intelligence. The ARSOF S2 is rarely capable of satisfying all the commander's requirements using only intelligence resources organic to ARSOF and its components, or even the theater-level intelligence resources. The S2 depends upon national, joint, and even coalition intelligence organizations for comprehensive intelligence support.

INTRODUCTION

8-1. An understanding of the structure of the entire intelligence community and how it interrelates, from the national to the tactical level, is critical for successful ARSOF intelligence operations. JP 2-01 and JP 2-02 describe these relationships in detail. The following is an overview of the hierarchy of IEW organizations, available support systems, and the procedures used to obtain support from those supporting agencies.

CONNECTIVITY, ARCHITECTURE, AND SYSTEMS

8-2. ARSOF IEW consists of a wide range of intelligence and communications sytems. The following paragraphs discuss IEW systems and how they are interconnected.

CONNECTIVITY

8-3. Joint interoperability, streamlined flow of information, and pull-down of intelligence tailored to the needs of ARSOF are key to successful intelligence systems support. The C4I for the Warrior program is a joint-level, broadly connected system intended to provide total battlespace information to commanders and establish a global C4I capability for the warfighter to "plug in" anytime, anywhere, for any mission (JP 2-01). Figure 8-1, page 8-2, illustrates this C4I connectivity for deployed forces.

SYSTEMS AND AUTOMATION

8-4. A wide range of national, theater, and component intelligence and communication systems are available to CONUS and OCONUS ARSOF. The continuing evolution of the primary Department of Defense Intelligence Information System (DODIIS), including the Joint Worldwide Intelligence Communications System (JWICS) and workstations compliant with the Joint Deployable Intelligence Support System (JDISS), enables the design and implementation of a robust and flexible capability. Figure 8-2, page 8-2, portrays the DODIIS intelligence architecture.

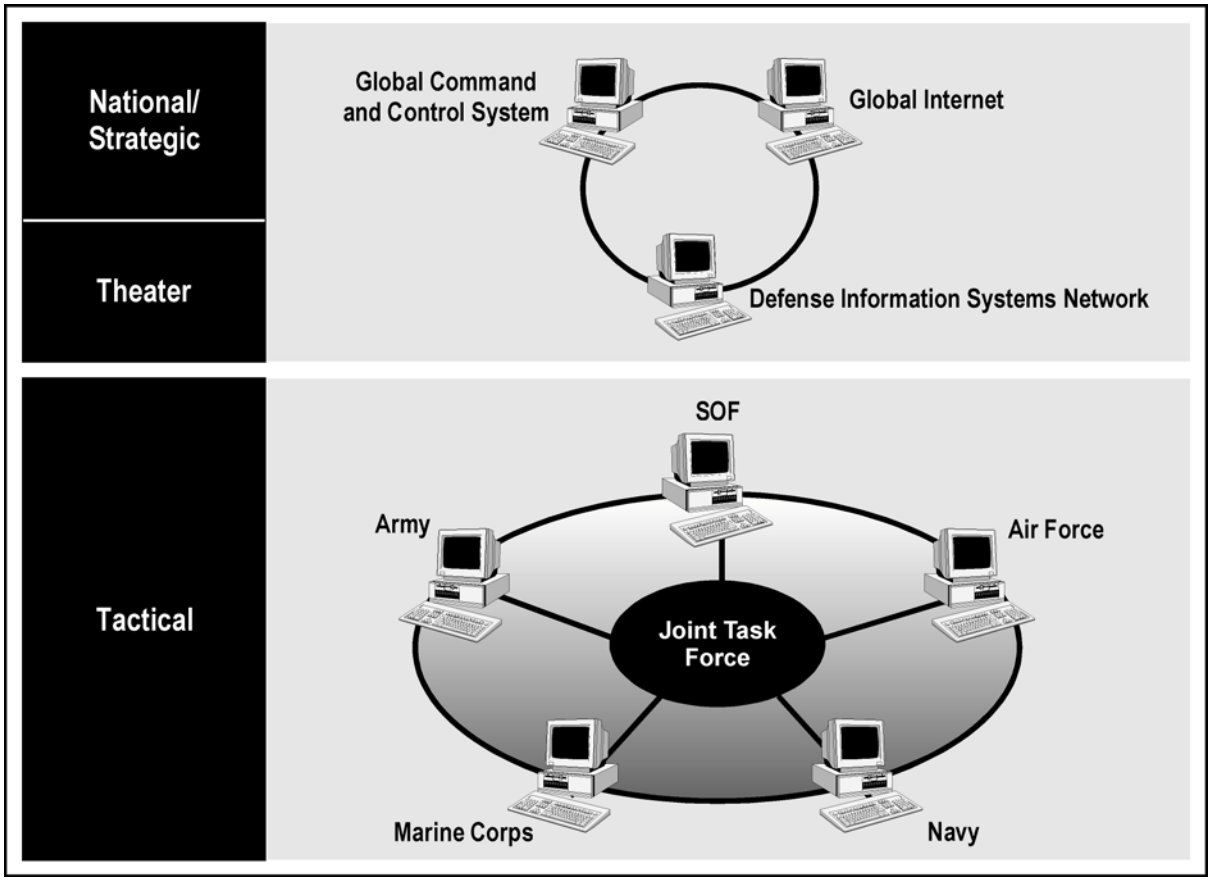


Figure 8-1. C4I for the Warrior Concept

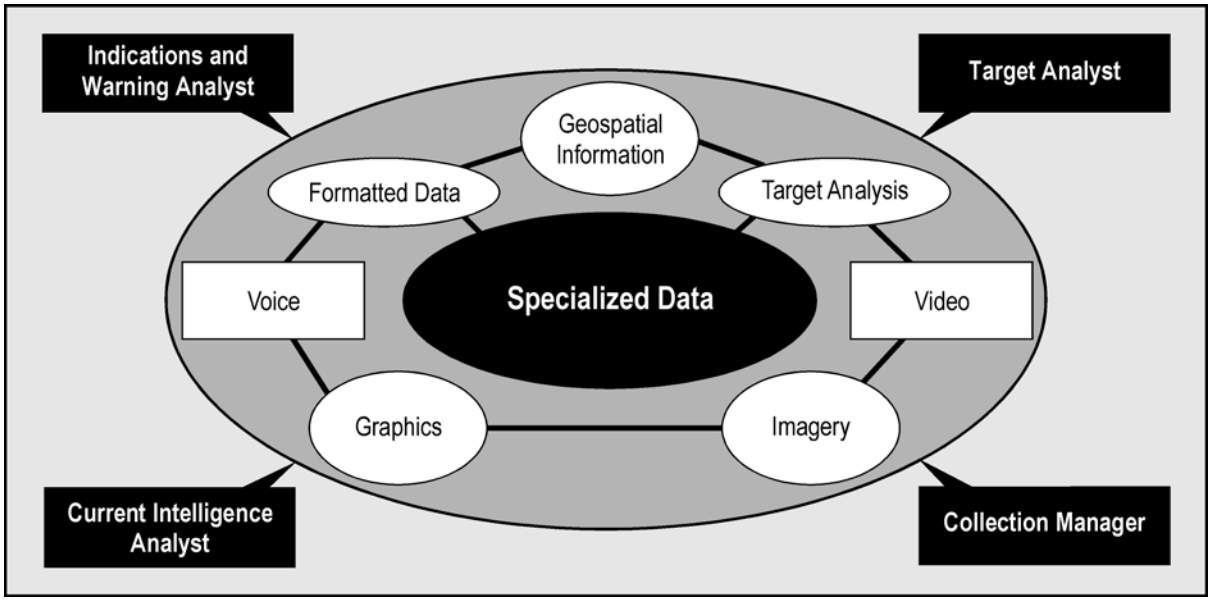


Figure 8-2. DODIIS Intelligence Architecture

8-5. The DODIIS intelligence architecture does not, however, ensure that intelligence and communications systems can be deployed without much planning and coordination for theater-deployed ARSOF. Supporting communications paths will probably have to be procured or extended to link the ARSOF C4I node with the Defense Information Systems Network (DISN). The ARSOF S2 must understand current systems well enough to tailor an architecture integrating intelligence sensors, processors, dissemination systems, databases, and ADP and communications systems. Figure 8-3 depicts the joint intelligence architecture structure.

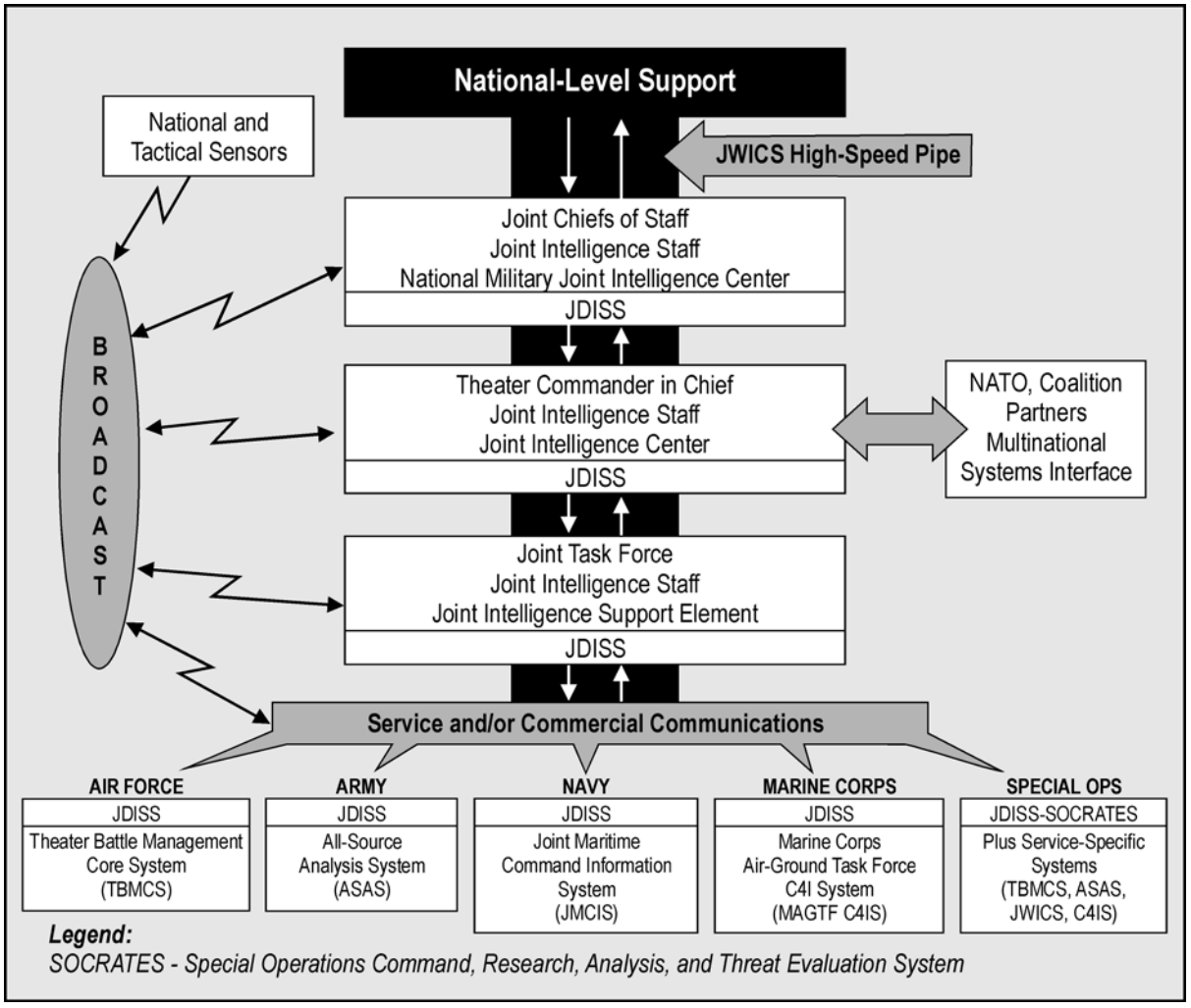


Figure 8-3. Joint Intelligence Architecture

AUTOMATED DATA PROCESSING

8-6. ADP systems provide the basic framework for the timely movement and transfer of intelligence in each phase of the intelligence cycle to commanders and other key decision makers. Communications and ADP technology are undergoing continuous evolution, affecting intelligence architecture, systems,

and applications. The Defense Communications System and theater communications systems link intelligence agencies with their supporting, supported, and adjacent commands. For example, USASOC interfaces with USSOCOM and national or DOD production centers via these ADP systems.

CHARACTERISTICS OF ADP SUPPORT

8-7. ADP systems support all IEW tasks. Depending upon system configuration, national- and theater-level ADP systems can provide—

- NRT intelligence to users, as requested.
- Data supporting the deliberate planning process, contingency planning, and training requirements.
- Global access to secondary imagery.
- Analyst-to-analyst communications.
- Graphics or fused intelligence plotting.
- Remote database access.
- Automated mission planning or rehearsal.
- Automated intelligence message handling.
- Electronic mail (E-mail).
- Automated collection and requirements management.

ARSOF IEW SYSTEMS

8-8. Existing systems that are available for ARSOF IEW support include—

- *JWICS*. This system is the SCI portion of the DISN. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. The purpose of JWICS is to provide for interoperable, seamless, and responsive intelligence communications connectivity for the MI community to support operations. This effort has included the development of JWICS in three modes—fixed, containerized, and mobile—with the capability of supporting a joint force joint intelligence support element (JISE) or national intelligence support team in a building and/or field site. Each group and deployed battalion requires a means to access JWICS.
- *JDISS-SOCRATES*. The JDISS-SOCRATES program is an umbrella intelligence systems support architecture, which integrates existing intelligence data handling system (IDHS) elements and hosts databases with information of specific interest to SOF into a LAN-based, multifunctional intelligence support system. The JDISS-SOCRATES LAN/wide area network (WAN) provides single-terminal access to all JDISS hosts. The LAN/WAN is extended via the SOF command, control, communications, and intelligence (C3I) telecommunications system, SCAMPI, and JWICS, providing both in-garrison and deployed connectivity. Core capabilities resident on a typical JDISS-SOCRATES workstation include intelligence data and message processing, requirements management, image and map handling, database access, library services, and E-mail/analyst chat.

Additionally, units with imagery analysts are fielded the Enhanced Imagery Workstation (EIW) under the SOCRATES program. The EIW provides a unit a significant imagery exploitation and geographic information system production capability. The system is fielded down to the battalion level.

- *Deployable JDISS.* Deployable JDISS is a modular workstation that provides deployed SOF personnel with the functionality of an in-garrison JDISS-SOCRATES workstation. Workstations may be configured as stand-alone systems or as integrated units operating on a remote LAN. With communications connectivity, the system is capable of sending and receiving high-resolution digital imagery, map products, and data. The deployable JDISS consists of a network termination (NT) JDISS configured laptop. The system is being fielded two per battalion/group.
- *Man-Transportable SOCRATES-Meteorological and Oceanographic System (MTS-METOC).* MTS-METOC is a briefcase-sized (and eventually notebook-sized) highly mobile, modular analysis system that gives deployed personnel at the battalion and FOB level the capability to download satellite weather data through organic communications to provide weather support. Each workstation, printer, and external compact disc–read-only memory (CD-ROM) unit is mounted in a ruggedized transit case with neither system weighing more than 30 pounds.
- *SOFIV-M.* The SOFIV-M is a SOCRATES intelligence processing system that provides SOF with automated intelligence product generation and dissemination capabilities. SOFIV-M is mission-tailorable and -scalable for use by a variety of SOF units. SOFIV-M is a web browser-based system that uses Netscape to connect to the JWICS or the SIPRNET INTELINK "home pages." The SFOB uses SOFIV-M to receive, process, and manipulate unfinished NRT intelligence information as well as information resident in a variety of national and theater intelligence databases. The SOFIV-M uses the latest JDISS software for analyst operations and is configured to accept theater-unique software applications. The deployed SOFIV-M can interface with fixed or mobile communications equipment to send and receive data, and record communications. This capability allows SOFIV-M operators to search national, theater, and service intelligence sites for intelligence data in support of mission requirements. It also allows users to receive unfinished NRT information and process/manipulate it into usable intelligence in a field environment. It is designed to rapidly disseminate critical intelligence between SOF elements, conventional forces, intelligence facilities, and national intelligence agencies. The system is fielded to the group level.
- *Briefcase Multimission Advanced Tactical Terminal (BMATT).* BMATT is a briefcase-sized (and eventually notebook-sized) highly mobile, intelligence receiver. The BMATT provides NRT interface with global and theater intelligence threat warning broadcasts without greatly increasing space and weight requirements. The system is fielded down to the battalion level.

- *I-REMBASS*. I-REMBASS is a lightweight, tactical monitoring system consisting of magnetic, seismic-acoustic, and infrared sensors, monitors and code programmers, and data repeaters. The system is used for surveillance, detection, target classification, and target direction of movement. I-REMBASS can be used as a means to enhance FP measures. Repeater units can be used to extend signal range beyond the line of sight.
- *AN/PRD-13 SOF SIGINT Manpack System (SSMS)*. The SSMS is a manpacked SIGINT system designed to meet current and developing threat capabilities. It can also be used to enhance FP measures through monitoring of threat communications and DF. The system is man-transportable and airborne-capable.
- *EIW*. The EIW is an imagery analyst workstation with dual screens for stereo capability. It is tailored with applications and peripheral hardware to meet USSOCOM imagery receipt, exploitation, production, and dissemination requirements. It is on the SOCRATES (USSOCOM network), which allows the SOCJIC to file transfer protocol (FTP) raw or exploited imagery products directly to users. EIWs are fielded to each Active Army SFG, Ranger regiment, and SOAR. All ARSOF units have the following imagery requirements and the EIW provides these capabilities:
  - Access to imagery and equipment able to receive and disseminate imagery products.
  - Manipulate imagery and have the capability to generate hard and soft copy products.
  - The capability to store and archive imagery products.

  Included with the EIW is a large format plotter and a color printer. EIW software includes Earth Resources Data Analysis System (ERDAS), image exploitation support system (IESS) interface, electronic light table (ELT) 4000, Imagery Product Library (IPL)/Demand-Driven Direct Digital Dissemination (5D) browser, and requirements management system (RMS).
- *ASAS-RWS/AN TYQ-93(V)2 All-Source Analysis System*. The ASAS-RWS supports the S2 with improved Army Battle Command System (ABCS) interoperability on a defense information infrastructure (DII) common operating environment (COE). The infrastructure provides client-server data exchanges, stand-alone, and networked operations. Specific functionality includes situation development, targeting support, IPB, surveillance and reconnaissance support, IMINT, CI/HUMINT, BDA, and collateral level SIGINT. It supports collaborative planning, static and dynamic overlays, dissemination criteria, freehand draw, and ABCS common look-and-feel graphic user interface. ASAS-RWS allows graphical, including imagery, selected message exchanges, and database population necessary to support the full threat spectrum in different environments. The system is fielded to the SFG, SOAR, and Ranger regiment levels.
- *ASAS-LIGHT/AN TYQ-93(V)3 All-Source Analysis System*. The ASAS-L provides a lightweight, tactical intelligence system capable of

interfacing with ASAS-RWS and other ABCS networked systems using a variety of radio and network protocols. ASAS-L incorporates many of the same features as ASAS-RWS in a notebook personal computer (PC). It can accomplish the direct exchange of map graphics and overlays with ASAS-RWS. It uses the Joint Mapping Tool Kit as a mapping package, supports standard ASAS all-source correlated database (ASCDB) and custom, user-defined, database capability. It provides the intelligence analyst with some IPB capabilities such as manual templating, modified combined obstacle overlay development, and overlay capabilities for COA development. It provides viewing and limited imagery annotation capability with both commercial-off-the-shelf (COTS) and Government-off-the-shelf (GOTS) software tools and standard suite of office automation applications. The system is fielded to ARSOF battalions.

- *ASAS-Single Source, AN/TYQ-52(V) All-Source Analysis System*. The ASAS-SS is a component of ASAS Block I and provides SIGINT analysts tools capable of sophisticated analytic processing and reporting. The ASAS-SS receives SCI-level SIGINT information and processes it into multidiscipline intelligence products. In support of this, the ASAS-SS is capable of automatically receiving and processing messages from national to tactical collectors and passing relevant data into local databases. The ASAS-SS provides a comprehensive set of ELINT, COMINT, and intelligence correlation analysis tools, as well as national database browsers. It supports the generation of messages using DD-173, DOI-103, and JANAP-128 formats. The system is fielded to the SFGs.
- *AN/USQ-161(V)1(c) Joint Tactical Terminal-Briefcase (JTT[B])*. The JTT(B) will allow Army SOF to receive the Intelligence Broadcast System (IBS), a series of secure broadcast intelligence downlinks, to support operations against likely targets, as well as to quickly develop and tailor new databases to unexpected threats. The systems deliver critical time-sensitive battlefield targeting information to tactical commanders and intelligence nodes at all echelons, in NRT at collateral level. It will support the intelligence analyst in the areas of I&W, situation assessment, target analysis, mission planning and rehearsal, imagery analysis, and electronic support measures. Additionally, it will provide extensive capability to manipulate data received via the IBS and to overlay these products with database information. It will also provide word processing, message text generation, and local network services.
- *AN/PYQ-3(V)2 Counterintelligence/Human Intelligence Automated Tool Set (CHATS)*. The CHATS is a team leader device that interfaces with ASAS-RWS, CI/Interrogations Operations workstation, and the Individual Tactical Reporting Tool (ITRT) agents/collector device. It provides automation capability to collect, manage, receive, store, and export text, electronic data, and digital imagery information; and prepare, process, and disseminate standard messages. The system is fielded to the SF battalion, PSYOP battalion, SOAR, and Ranger regiment levels.

- *Joint Threat Warning System (JTWS).* The JTWS is a USSOCOM-developed system that migrates legacy SIGINT capabilities used by various USSOCOM components into an evolutionary acquisition strategy. JTWS will provide timely products to the warfighter, pacing rapid technology advancements. It provides a plug-and-play software architecture across maritime, air, and ground applications, which allows tailorable and scalable approach for each mission from simple radar warning receiver (RWR)-type functions in the Body Worn variant to a fully capable suite of COMINT and ELINT systems in the Team Transportable (TT) System (full interoperability). Variants include the Body-Worn System (BWS), TT, Man Packable, Maritime, and Air.
- *All-Source Analysis System AN/PYQ-8 Individual Tactical Reporting Tool (ITRT).* ITRT is a hand-held device designed for the individual CI agent or HIC. The ITRT provides a notepad and recording capability, report masks, limited mapping capability, local database, ability to receive, process, store and disseminate digital imagery, message masks, and a communications interface with CHATS. The system is fielded to the SF battalion, PSYOP battalion, SOAR, and Ranger regiment levels.
- *All-Source Analysis System: Counterintelligence and Interrogation Operations Workstation (CI&I OPS WS).* CI&I OPS WS provides S2X/G2X at all levels with CI/HUMINT automation support for CI and interrogation planning and management operations. Automated support includes CI/interrogation planning tools; communications interfaces for national-level databases; reporting tools; analysis tools; and asset, source, and mission management tools. The system is fielded to the SFGs.
- *Digital Topographic Support System-Deployable: AN/TYQ-77 DTSS-D.* The DTSS accepts topographic and multispectral imagery data from the NIMA's standard digital databases and from commercial sources. DTSS functional capabilities include the creation of intervisibility, mobility, environmental, 3-dimensional terrain visualization, and special-purpose products; and the creation, augmentation, modification, and management of topographic data. The DTSS will provide updated map background and terrain intelligence information to the ABCS workstations, and accept terrain intelligence and data updates from these systems. The DTSS-D uses COTS technology in printers, scanners, and computer workstations, combined with image processing and geographic information system software. The DTSS-D provides the capability to generate and print image maps from commercial and national imagery.
- *Integrated Meteorological System-Light: AN/PMQ-40 IMETS-L.* The IMETS is the Army's tactical weather communication, intelligence, and information system providing digital weather support to enable SOWTs to support tactical units. The IMETS-L is interoperable with other ABCS systems. During mission execution, IMETS-L helps SOWTs to advise supported units to evaluate what they can see, shoot, and communicate better with than threat systems in all weather. To produce digital weather information, IMETS-L combines advanced

observations from weather satellites (WXSATs), upper air information, surface weather observing networks, and numerical models to build a gridded meteorological database (GMDB) in the AO. IMETS-L enhances the tactical commander's situation awareness by providing visualization of weather. This system is fielded to the SF battalion, SOAR, and Ranger regiment levels.

ARSOF DATABASES

8-9. The following are some of the current intelligence systems and databases accessible via the JDISS-SOCRATES:

- *INTELINK.* INTELINK (Figure 8-4) is a principal electronic means for intelligence product dissemination. INTELINK builds on ongoing architectural initiatives at the TOP SECRET and/or SCI and SECRET and UNCLASSIFIED classification levels. INTELINK provides a comprehensive set of tools to query, access, and retrieve information. INTELINK permits collaboration among analysts and users and will simplify access to a variety of services. The ARSOF S2 should assess the availability of INTELINK access among assigned and en route forces.

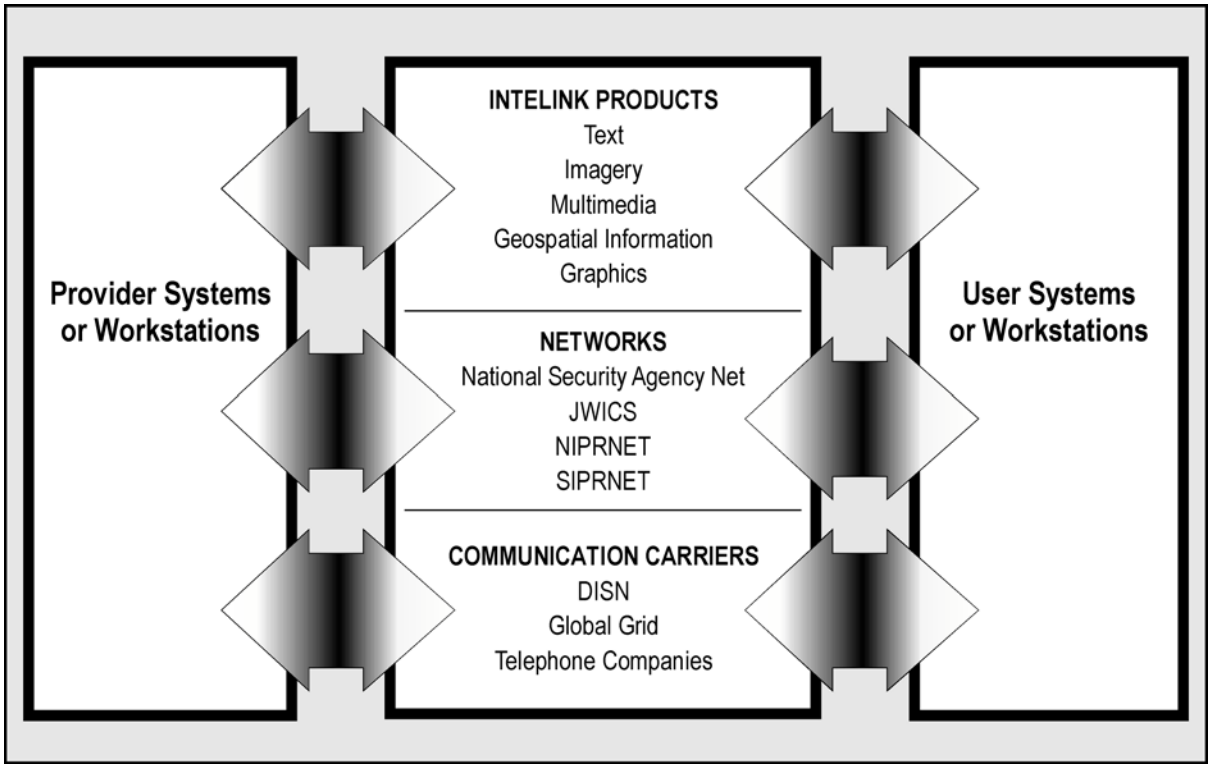


Figure 8-4. INTELINK

- *Special Operations Debrief and Retrieval System (SODARS).* The SODARS program was developed to automate and store after-action reports and debriefing reports from SOF elements that conducted

OCONUS missions. This information is used for future planning and in preparing SOF personnel for OCONUS deployments. The overall SODARS program is managed by the J2, USSOCOM.

- *Migration Defense Intelligence Threat Data System (MDITDS).* The MDITDS is the DODIIS community's automated information system (AIS) reengineering and development program for threat analysis production. MDITDS is responsible for migrating explicitly defined, mission-specific functions. The MDITDS consists of a message-processing pipeline with an interface to Automatic Digital Network (AUTODIN) message traffic and press feeds (e.g., Associated Press [AP], Reuters, and FBIS). A web-based user interface to a collection of databases provides analytical tools and threat assessment capabilities to the user.
- *Modernized Integrated Database (MIDB).* The MIDB has been designated by the DOD as the migration system for the production and analysis of the general military intelligence database. This program replaced the Military Intelligence Integrated Data System/Integrated Database (MIIDS/IDB) and integrates data and applications from other existing intelligence databases into a common baseline. The MIDB program objective is to provide a controlled set of common data elements and applications that will permit rapid, accurate exchange and analysis of intelligence information at production centers, joint commands, Service components, and tactical units.
- *POAS.* POAS provides an automated capability to support state-of-the-art planning, implementation, and evaluation of U.S. PSYOP. This system provides support at the tactical, operational, and strategic levels during war and MOOTW. It provides support for up to 2,000 local and remote users (150 simultaneously) and data links between the user, the rear command center, and theater- and national-level approval authorities. Capabilities also include database management, word processing, message traffic reception, and archiving. POAS is SECRET with multilevel security interconnectivity at the SCI level.
- *IPL.* The IPL is a NIMA-sponsored effort to develop the standard United States Imagery and Geospatial Services (USIGS) product archive system. The IPL provides a library of imagery products accessible to imagery customers worldwide. IPL provides an automated capability to receive imagery from multiple sources, maintain a database of imagery and imagery products to imagery clients, and transfer imagery products using specified formats and compression ratios. IPL is the designated NIMA migration system for the storage and standard dissemination of imagery products, and replaces the 5D.

ARSOTF IEW ARCHITECTURE AND SUPPORT CHANNELS

8-10. There is no "cookie cutter" solution for establishing supporting intelligence architecture for a deployed ARSOTF. Each mission or deployment will create a unique set of circumstances for the S2 and S6 to overcome based upon available technology and systems. The goal is to "plug in" to the theater supporting systems architecture at the lowest level

possible. Commanders at all levels must clearly articulate in operational documents where the priority for limited C4I resources should reside. The following are some basic considerations for establishing C4I architecture priorities:

- Collocate the best support systems at the operational launch base (intermediate staging base, FOB). Clustering imagery and analysis systems in a remote centralized HQ that does not launch operational forces will have little benefit for operational elements unless they can obtain the same level of products. The soldiers who will execute the mission obviously need the best imagery and information.
- Combine intelligence resources of different units. Intelligence staffs and support agencies are by nature modular and can be combined or tailored to create a synergy of resources and personnel talent. For example, the intelligence staffs of an ARSOTF and SFOB should consider pooling personnel and equipment under the supervision of the ARSOTF S2.
- S2 at all levels must develop and maintain a current intelligence communications architecture status report. This report reflects all available theater and national systems and the conduit by which their information is received.

8-11. For illustration, Figure 8-5, page 8-12, depicts a notional ARSOTF architecture. Deployed or in-theater ARSOF units follow the request flow process depicted in Figure 8-6, page 8-13. Due to the time sensitivity of many requirements, responses to RFIs can be pushed directly from a collector or agency to the request originator.

MACOM IEW SUPPORT

8-12. USASOC is the major Army command (MACOM) for SO. USASOC is USSOCOM's Army component and consists of Active Army and RC units.

U.S. ARMY SPECIAL OPERATIONS COMMAND

8-13. USASOC provides trained and ready SF, Ranger, ARSOA, PSYOP, and CA forces to geographic combatant commanders and American ambassadors. USASOC develops unique SO doctrine, tactics, techniques, and materiel support.

USASOC OFFICE OF THE DEPUTY CHIEF OF STAFF, INTELLIGENCE (ODCSINT)

8-14. The ODCSINT advises and assists the commanding general (CG) and his staff on all intelligence and security matters. It provides deliberate and crisis-action intelligence support to all CONUS-based ARSOF, including collection, requirements management, analysis, production, and dissemination. It also provides intelligence and security support to assigned units preparing to conduct SO, PSYOP, or CA missions or exercises. Figure 8-7, page 8-13, shows the ODCSINT organization, and its functions are further described below.

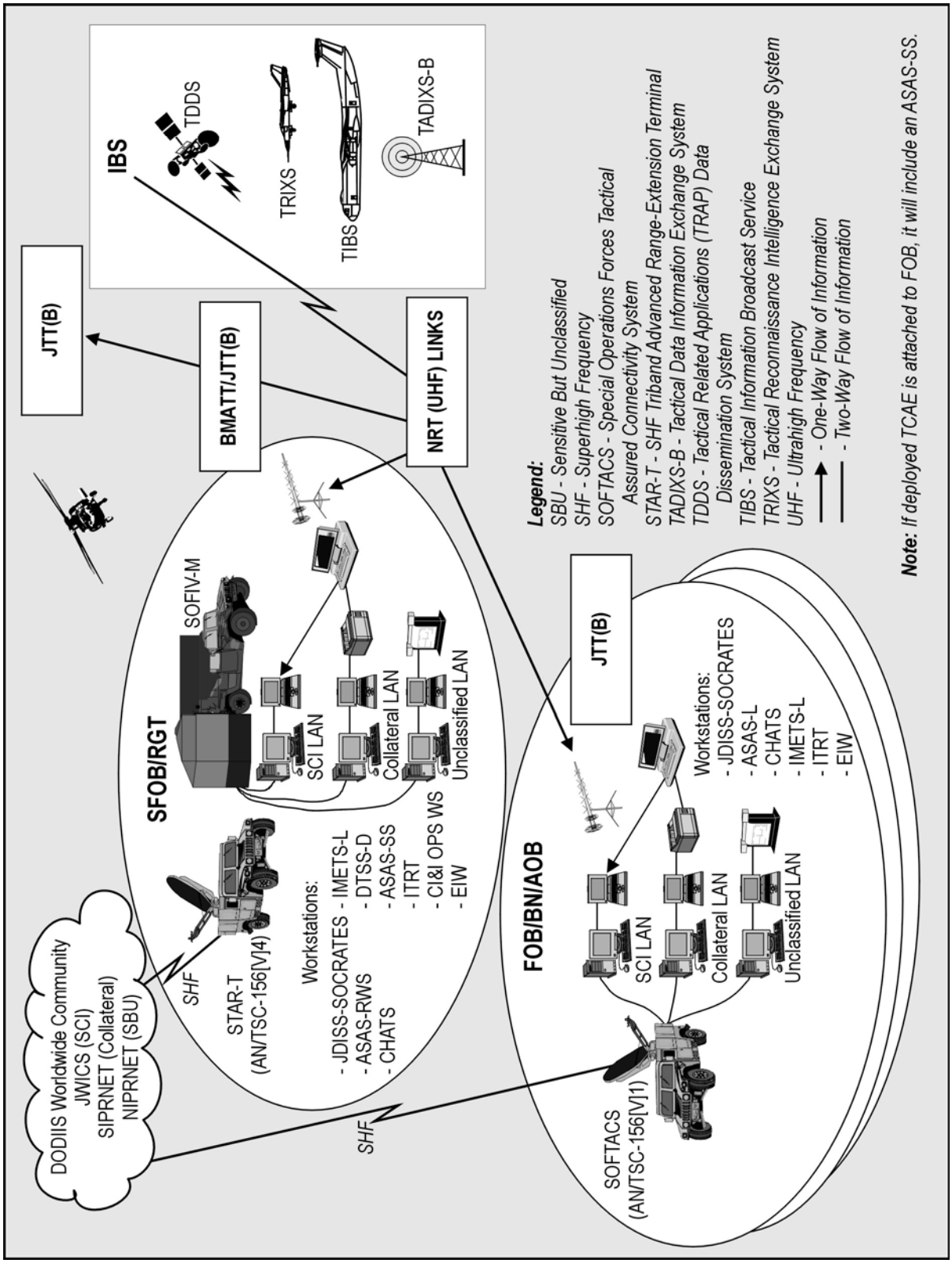


Figure 8-5. Notional ARSOTF Architecture

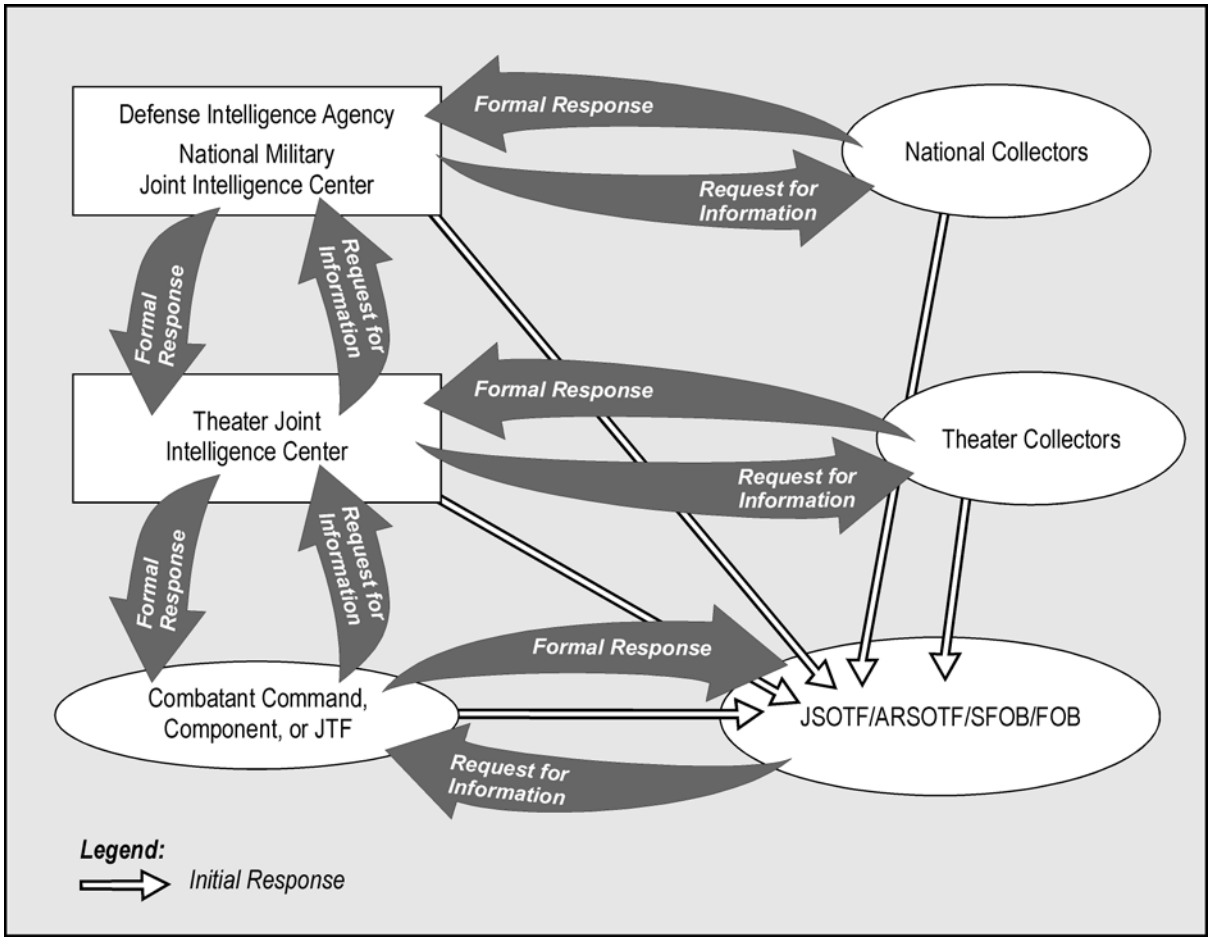


Figure 8-6. Theater Request Flow

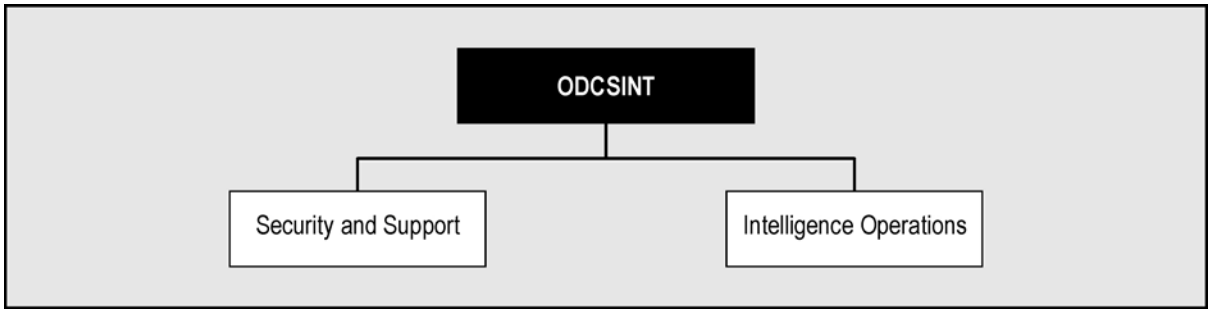


Figure 8-7. USASOC ODCSINT Organization

8-15. The major functions of the ODCSINT are as follows:

- Direct intelligence, counterintelligence, security, GI&S, and weather activities supporting Active Army and RC ARSOF.
- Advise the USASOC commander on intelligence training matters, to include current policy, doctrine, and concepts.

- Develop and promulgate policy and guidance for evaluating and monitoring the readiness status of the Active Army and RC intelligence units and personnel and managing the command intelligence readiness training (REDTRAIN) program.
- Ensure, in coordination with USSOCOM, the continuity and compatibility of theater CINC and component SOF intelligence subarchitectures and supporting USASOC subarchitectures and policies.
- Develop and implement policy and programs to safeguard defense information, including information processed by automation resources within the command.
- Manage SIGINT mission activities for Active Army and RC ARSOF. Provide oversight for the planning and usage of SIGINT and/or IEW equipment of ARSOF National Guard units.
- Interface with USSOCOM, Headquarters, Department of the Army (HQDA), USAJFKSWCS, and U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) to identify, refine, and resolve MI doctrine, training, equipment, and personnel requirements within ARSOF.
- Direct the Security Education and Awareness Program for USASOC IAW USSOCOM and HQDA regulations and directives.
- Establish, facilitate, and maintain planning, programming, and policy guidance for long-range intelligence plans, objectives, and architectures.
- Develop and implement policy and exercise oversight for all intelligence automation systems within USASOC and its MSCs and MSUs.
- Develop, implement, and manage the USASOC intelligence oversight program.
- Develop and maintain the intelligence functional area supporting architecture that must be linked to the core, essential, and supporting tasks of the USASOC mission architecture for resource justification.
- Be a member of the Sensitive Activities Oversight Council.
- Provide interface with the Office of the Deputy Chief of Staff for Operations (ODCSOPS).
- Serve as MACOM TCAE; provide dedicated technical support to ARSOF SIGINT and EW elements.

INTELLIGENCE OPERATIONS DIVISION

8-16. The intelligence operations division—

- Serves as point of contact (POC) for all facets of deliberate (real-world and/or exercise) and crisis-action intelligence support to CONUS-based ARSOF, including collection, requirements management, analysis, production, and dissemination.
- Conducts continuous and direct liaison with senior intelligence counterparts at USSOCOM, NSA, DIA, CIA, DOD, Department of Army (DA), geographic combatant commanders, and other government

and nongovernment agencies to monitor global intelligence management policy and procedures.

- Provides intelligence, threat, and CI support to ARSOF.
- Identifies the ARSOF substantive IRs for incorporation into the national IR collection apparatus.
- Manages the ARSOF DIA Joint Dissemination System account; validates and processes ARSOF requirements for DIA accounts and SIIs.
- Coordinates and manages the ARSOF special access programs.
- Develops and coordinates intelligence requirements guidance and policy.
- Registers, validates, and processes all CONUS SIGINT, IMINT, HUMINT, OSINT, MASINT, all-source, and CI requirements from subordinate units, and monitors and deconflicts MSC and MSU OCONUS theater-related IRs.
- Reviews and validates ARSOF input to the SODARS.
- Provides intelligence threat support for the command force development functions—concept and doctrine developments, combat developments, and training.
- Provides threat briefings for security assistance team training, orientation course, and USAJFKSWCS training courses, as required.
- Maintains an intelligence reference library (hard copy) supporting ARSOF.
- Reviews and validates ARSOF intelligence concepts of operation.
- Manages the ARSOF SIGINT program and functions as the ARSOF TCAE.
- Supports the ARSOF threat evaluation at the U.S. Army Training and Doctrine Command's (TRADOC's) combat training centers, as required or requested.
- Administers the USASOC intelligence badges and credentials account.
- Develops policy and implements directives for CI support to the MACOM.
- Directs the intelligence property book program; administers the USASOC intelligence property book account; and conducts inspections to ensure that subordinate units have the necessary equipment.
- Reviews, updates, and/or validates all threat scenarios, basic threat country data, threat OB, and threat TTPs taught or used in USAJFKSWCS institutional training and simulation activities, as requested.
- Participates as the threat subject matter expert and controller for all USAJFKSWCS simulation training activities supporting the ARSOF Battle Lab, as required.

- Prepares SOF intelligence input to DOD and HQDA plans, studies, and products; coordinates with USSOCOM, HQDA, and TRADOC proponents.
- Provides input to the Deputy Chief of Staff for Force Development and Integration (DCSFDI) on the intelligence aspects of force integration, requirements, and resource management.
- Ensures compliance with the Foreign Military Intelligence Collection Activities Program.
- Manages and implements the ARSOF Cryptologic Training Evaluation Program.
- Coordinates for SIGINT-related technical courses through national and Service schools for all ARSOF personnel.
- Conducts foreign travel briefings for USASOC personnel traveling to high- or potential-threat areas.
- Manages the MACOM SAEDA program and provides SAEDA briefings to the MACOM staff, as required.
- Manages the ARSOF IMINT requirements.
- Advises the ARSOF S2s on cryptologic operational issues.
- Serves as the USASOC manager for GI&S requirements; researches and maintains data on all NIMA terrain-related products; identifies GI&S products applicable to ARSOF; and provides GI&S-related support to the MSCs and MSUs.
- Develops and publishes USASOC GI&S policy and guidance; reviews and validates MSC and MSU GI&S requirements (including NIMA accounts); and reviews, validates, and coordinates for the production of multispectral imagery (MSI) and GI&S products for the command.
- Manages and coordinates environmental services (meteorological, oceanographic, and atmospheric sciences) and related activities for the command. The division also interfaces with USSOCOM; HQDA; HQ, USAF; AFSOC; theater SOCs; and other DOD agencies on environmental matters.
- Provides policy and guidance to ARSOF on the conduct of CFSO.
- Monitors personnel management and assignment of all Active Army MI soldiers and officers.
- Develops, implements, and monitors the USASOC Intelligence Oversight Program; reviews unit reports and submits periodic reports to HQDA.
- Conducts liaison with intelligence units/agencies, Criminal Investigation Division (CID), and other local and national-level agencies on CI-related matters, as required.
- Administers and manages USASOC IPLs in support of ARSOF CONUS and exercise imagery production requirements.
- Reviews and validates/endorses USASOC MSC/MSU GI&S requirements, including NIMA accounts; reviews, validates, and

coordinates for the production of MSI and GI&S products for the command.

- Serves as the manager for the USASOC REDTRAIN Program; establishes funding priorities and guidance; validates MSC/MSU intelligence training requirements; recommends REDTRAIN-designated fund allocations to MSCs; and justifies resources in the program objective management (POM) process and monitors execution during the budget year.
- Serves as the manager for the USASOC Total Army Language Program (TALP); establishes funding priorities and guidance; validates MSC/MSU language requirements; and justifies resources in the POM process and monitors execution during the budget year.
- Serves as the Command Language Program Manager (CLPM) for ARSOF MI linguists.
- Serves as the DCSINT focal point for all intelligence training requirements and issues; coordinates with HQDA, USSOCOM, USAIC&FH, TRADOC, and other Army agencies on intelligence training issues relevant to ARSOF.
- Identifies intelligence training shortfalls throughout the command and initiates corrective action; ensures the establishment of intelligence training programs at subordinate units; provides assistance and oversight for intelligence training programs, including MI language training; and validates and processes all requirements for DOD intelligence schools and courses.
- Serves as MACOM intelligence point of contact for Status of Resources and Training System (SORTS), Unit Status Report (USR), and Joint Monthly Readiness Review (JMRR) requirements.
- Provides current and estimative intelligence and threat support to USASOC and MSC commanders and staff.
- Coordinates intelligence threat issues with the Deputy Chief of Staff for Operations and Plans (DCSOPS) FP personnel and USAJFKSWCS training companies.
- Develops and reviews threat/vulnerabilities for risk management and recommends countermeasures.
- Serves as the functional proponent and user representative for all ARSOF intelligence battlefield operating system (IBOS) requirements, in coordination with DCSFDI; coordinates with DOD, HQDA, and USAIC&FH on IEW systems.
- Manages the USASOC Tactical Exploitation of National Capabilities Program (TENCAP) and the USSOCOM National System Support Programs; provides input to the POM process and monitors execution during the budget year.
- Serves as the DCSINT focal point for intelligence doctrinal, force structure, Force XXI, and other future MI operational and organizational requirements.

- Serves as the DCSINT focal point for intelligence aspects of experiments and proofs of concept demonstrations (i.e., JCS special projects, advanced concepts technology demonstrations [ACTDs], and Army warfighter experiments [AWEs]).
- Directs and manages the USASOC portions of the SOCRATES program and USASOC-procured intelligence systems; serves as the configuration control manager for USASOC systems, Remote Terminal Security Officer (RTSO), and DODIIS Access Security Officer (DASO); and coordinates equipment replacements, upgrades, maintenance, and sustainment funding support.
- Validates and processes requirements for new or enhanced capabilities to satisfy ARSOF MI mission requirements; provides system administration and customer support for JDISS-SOCRATES and ASAS systems.
- Manages and executes SOCRATES sustainment funds in support of USASOC and its components' intelligence operations.
- Reviews and proposes changes to long-term requirements in the National SIGINT Requirements List (NSRL).
- Manages SOF-directed access to national and theater technical SIGINT databases.
- Coordinates and manages the command TVA program and coordinates with local and national-level agencies on TVA matters, as required.

Note: Figure 8-8 displays the CONUS-related RFI process.

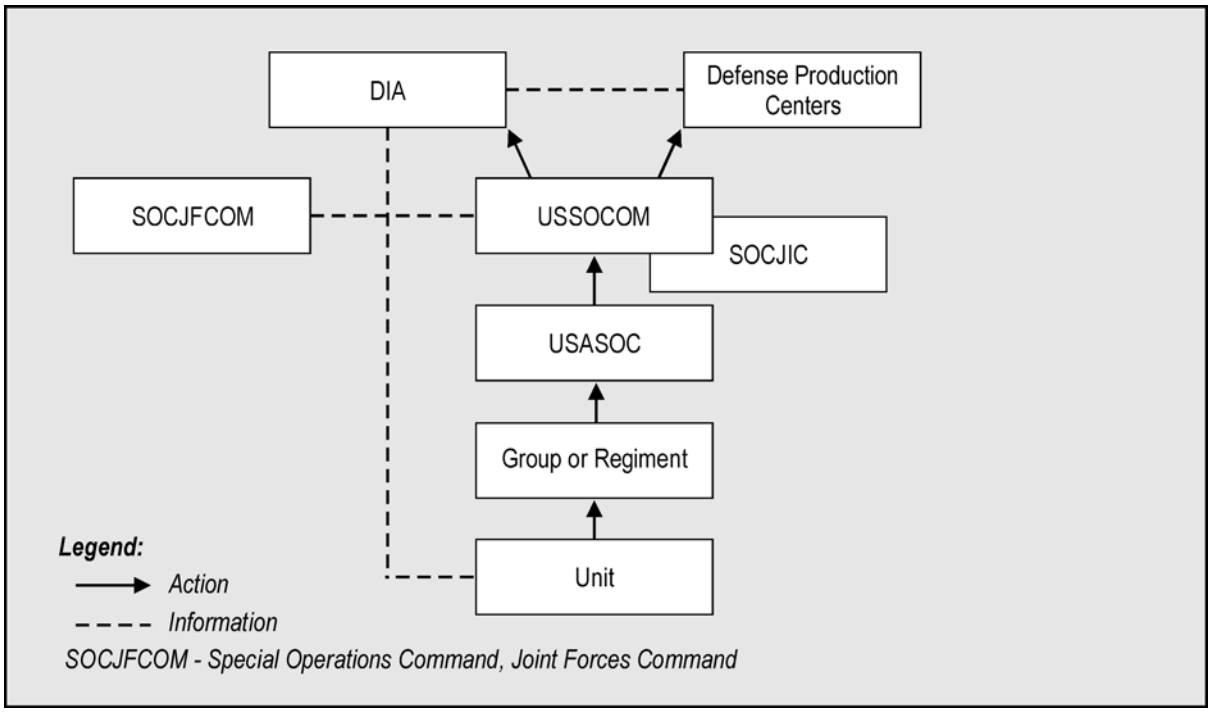


Figure 8-8. CONUS-Related RFI Process

SECURITY AND SUPPORT DIVISION

8-17. The security and support division is comprised of a security guard force for the HQ building, information security, personnel security, SSO, dedicated sensitive activities personnel and support office. The following are the major functions of the division:

- Serves as the DCSINT Information Management Officer and is responsible for coordination with the Deputy Chief of Staff for Information Management (DCSIM) on all nonintelligence information systems for the DCSINT.
- Directs information, systems, personnel, and technology transfer and/or disclosure of information to foreign nationals.
- Develops information security policy, and directs the program to safeguard classified information within USASOC.
- Establishes and manages the command information systems security (ISS) program, to include defining the ISS personnel structure, the GCCS, and the DODIIS computer security (COMPUSEC) program.
- Coordinates with Central Clearance Facility, Defense Investigative Services Center, DA, and Office of Personnel Management for USASOC security clearance issues.
- Directs the compromising emanations control program (terminal electromagnetic pulse escape safeguard technique [TEMPEST]); develops policies and procedures, reviews reports, and coordinates emanations security inspections for the program.
- Directs the technology transfer and disclosure of information to foreign nationals and contractors program to protect against unauthorized disclosure of classified and unclassified sensitive information to foreign nationals.
- Directs the CI aspects of the COMSEC monitoring program for the MACOM, and develops procedures to protect sensitive government transmissions.
- Directs the Department of Energy (DOE) Access and Certification Program; provides policy and procedures; and certifies U.S. DOE requests for visits, access, briefings, and debriefings.
- Establishes and oversees an ISS training program, directs the security education program, and manages and executes the USASOC Security Managers Course.
- Conducts security advice and assistance visits to subordinate commands and units.
- Conducts security inspections at subordinate units to ensure compliance with USASOC and HQDA policies and directives.
- Provides policy and procedures for the command COMSEC program; implements and monitors the DA Cryptographic Access Program (DACAP); and approves procedures for safeguarding, transporting, and controlling COMSEC and controlled cryptographic items (CCI).

- Develops, executes, and defends the INFOSEC resource program requirements for the HQDA planning, programming, and budget execution process.
- Evaluates new, modified, and reconfigured construction plans of sensitive facilities to ensure TEMPEST compliance IAW current policy.
- Establishes and manages the command ISS monitoring program.
- Establishes and implements policy relating to information system virus reporting procedures.
- Maintains liaison with Director of Information Systems Command, Control, Communications, and Computers (DISC4); Defense Information Systems Agency (DISA); HQDA; Land Information Warfare Activity (LIWA); Army Computer Emergency Response Team (ACERT); supporting Regional Computer Emergency Response Team (RCERT); supporting theater network operations centers (TNOCs); CID; and U.S. Army Intelligence and Security Command (INSCOM) elements.
- Directs INFOSEC monitoring program for MACOM and develops procedures to protect sensitive government transmissions.
- Manages the guard force for the HQ building, USASOC, and prepares and implements HQ security policy.
- Serves as the focal point for the establishment of Special Security Offices to support missions of subordinate units.
- Administers the SCI security management system for RC units under USASOC in coordination with the National Guard Bureau and Office of the Chief of Army Reserve.
- Manages the command and subordinate unit SCI billet structures; serves as the approval authority for the establishment of new SCI billet series and additions/deletions of billets to established series.
- Provides USASOC coordination with central clearance facility on SCI security clearance issues.
- Evaluates new, modified, and reconfigured construction plans for sensitive compartmented information facilities (SCIFs) for subordinate units to ensure TEMPEST and physical security compliance, and to recommend realistic and economical alternatives IAW current DOD policy.
- Controls the procurement and issue of SCI courier authorizations; approves/denies all requests from subordinate units for hand-carrying of SCI material on commercial aircraft worldwide.
- Reviews/approves the deployment of T-SCIFs.
- Provides USASOC coordination with HQDA, DIA, and other DOD agencies on SCI policy issues; develops and implements SCI security policies and procedures for the command.
- Establishes and manages the USASOC Industrial Security Oversight Program.

- Provides DCSINT input to the USSOCOM strategic planning process, USASOC mission area analysis (MAA), the CINC integrated priority list, the Commander's Narrative, the Army Plan (TAP), and Army POM.
- Reviews requests/requirements for and coordinates technical surveillance countermeasures (TSCM) services for subordinate unit SCIFs.
- Provides SCI support to DOD and other government organizations when requested by the Director of Central Intelligence (DCI), DIA, or DCSINT.
- Establishes and administers the MACOM SCI security management program and ensures administration of the program within respective MSCs and MSUs is IAW applicable regulations and guidance.
- Provides and coordinates for training in SCI security policy and procedures for USASOC personnel assigned to execute SCI security functions.
- Provides the following through Sensitive Activities Office personnel:
  - Implementation and execution of multidiscipline security management responsibilities required by security policies and programs specific for sensitive activities.
  - Security oversight of USASOC sensitive activities unit security programs via day-to-day liaison, advice and assistance visits, and security inspections.
  - Oversight of the Special Mission Badge and Credential Program IAW AR 525-17, *(S) Special Mission Badges and Credentials (U)*.
  - Focal Point Control Officer for the Army Compartmented Element (ACE) and Sensitive Activities staff offices.
  - Management and administration of the established Special Security Office support for HQ, USASOC and its MSCs.

DEPARTMENT OF THE ARMY IEW SUPPORT

8-18. The DCSINT, INSCOM, and NGIC provide IEW support to the Army. These agencies are discussed in more detail in the following paragraphs.

DEPUTY CHIEF OF STAFF FOR INTELLIGENCE

8-19. The DCSINT is responsible to the Chief of Staff, Army, for long-range planning and policy guidance on all matters relating to Army intelligence, security, and CI activities. The DCSINT manages the Army portion of the national foreign intelligence programs, Army departmental-level general MI and scientific and technical (S&T) intelligence production missions, intelligence readiness training, the Army Language Program, and the Army Foreign Materiel Program. The DCSINT exercises staff supervision over the INSCOM, and has operational control over its departmental production resources.

INTELLIGENCE AND SECURITY COMMAND

8-20. INSCOM, headquartered at Fort Belvoir, Virginia, is responsible for Army EAC IEW operations. With subordinate commands located worldwide, INSCOM is a major participant in national intelligence activities and support to theater IEW operations. Its subordinate commands consist of three broad categories of organizations that provide cryptologic, general military, and theater intelligence support to strategic- and operational-level commanders in the areas of tactical intelligence and related activities. INSCOM acts as a bridge between the national intelligence community and the theater Army commander at the operational level.

NATIONAL GROUND INTELLIGENCE CENTER

8-21. The NGIC, located in Charlottesville, Virginia, is subordinate to INSCOM and under the operational control of the Army's DCSINT. The NGIC has responsibility for the military ground component while supporting Service, national, and departmental agencies. The NGIC—

- Provides all-source scientific, technical, and general MI on foreign ground forces supporting Army Title 10 requirements.
- Provides IMINT and secondary imagery dissemination to support training, exercises, and contingency planning.
- Executes the Army's foreign materiel acquisition requirements and exploitation program.
- Provides current and future ground capabilities threat assessments to support operational forces, the combat and materiel development community, contingency planners, force planners, war game personnel, and doctrine development organizations.
- Provides detailed analysis and production of systems' capabilities and parametric data for all foreign ground and ground-related systems. (Examples of these systems are helicopters, air defense guns, infantry and armor, antiarmor, fire support, engineer mines, EW, reconnaissance, chemical warfare, directed energy weapons, and C4I systems.)
- Produces assessments of ground systems trends.
- Has a shared production and database maintenance responsibility for selected countries.
- Provides reinforcing support to other intelligence centers, as required.

JOINT AND THEATER-LEVEL IEW SUPPORT

8-22. USSOCOM provides joint IEW support. USSOCOM is the unified combatant command (COCOM) for special operations.

UNITED STATES SPECIAL OPERATIONS COMMAND

8-23. The Secretary of Defense assigns all CONUS-based SOF to the Commander in Chief, United States Special Operations Command (USCINCSOC). Figure 8-9, page 8-23, shows the command relationships between USCINCSOC and the SOF units of each of the services. (See Figure 1-2, page 1-8, for the structure of the U.S. Army Special Operations Command.)

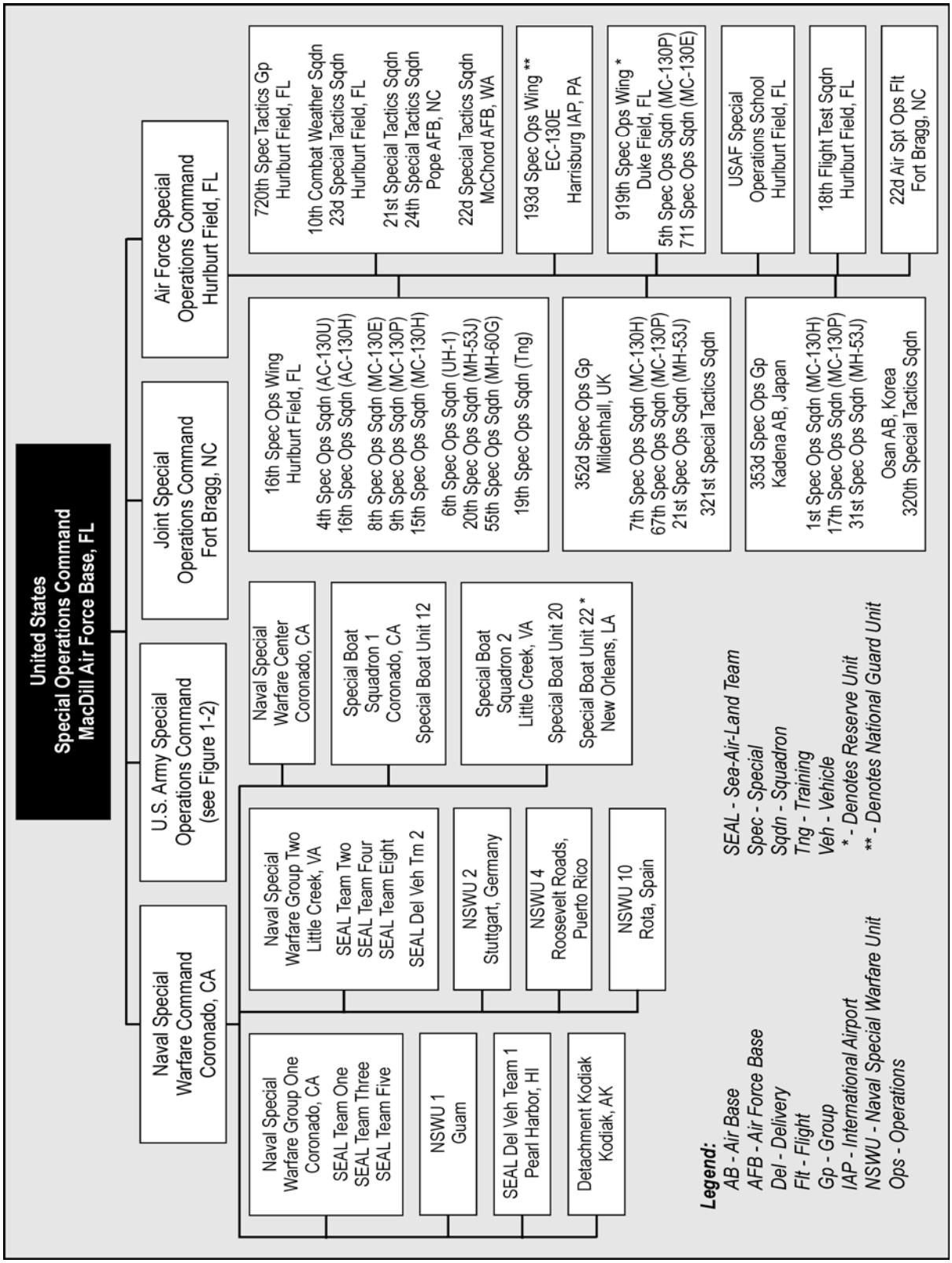


Figure 8-9. USSOCOM Structure

8-24. The CINC exercises COCOM of assigned forces through a combination of Service and joint component commanders. The USCINCSOC exercises COCOM over those forces through Service component commanders, functional component commanders, or its subordinate unified command. USCINCSOC, as a supporting commander, provides SOF to the commanders of other combatant commands for operational employment.

8-25. USSOCOM and the theaters it supports have command arrangement agreements that authorize direct liaison authority (DIRLAUTH) between SOF operational elements and the supported theater's SOC. These direct channels support ARSOF intelligence tasking and reporting requirements. Therefore, DIRLAUTH arrangements are extended to the ARSOF MSUs and the organizations that will exercise OPCON over them in contingencies and wartime.

Special Operations Intelligence and Information Operations Directorate, USSOCOM

8-26. The SOIO establishes the policy, guidance, and overall direction of SOF intelligence operations. Figure 8-10 depicts the SOIO organization. The SOIO—

- Develops intelligence plans, policies, and requirements.
- Plans and conducts intelligence participation in exercises and real-world situations (manning JSOTF).
- Recommends the use of intelligence in developing SOF doctrine, techniques, and procedures.
- Establishes and maintains liaison with DOD agencies, the Services, and other U.S. commands.
- Guides the proper use of the General Defense Intelligence Plan (GDIP) and intelligence funds.
- Establishes intelligence crisis-action teams.

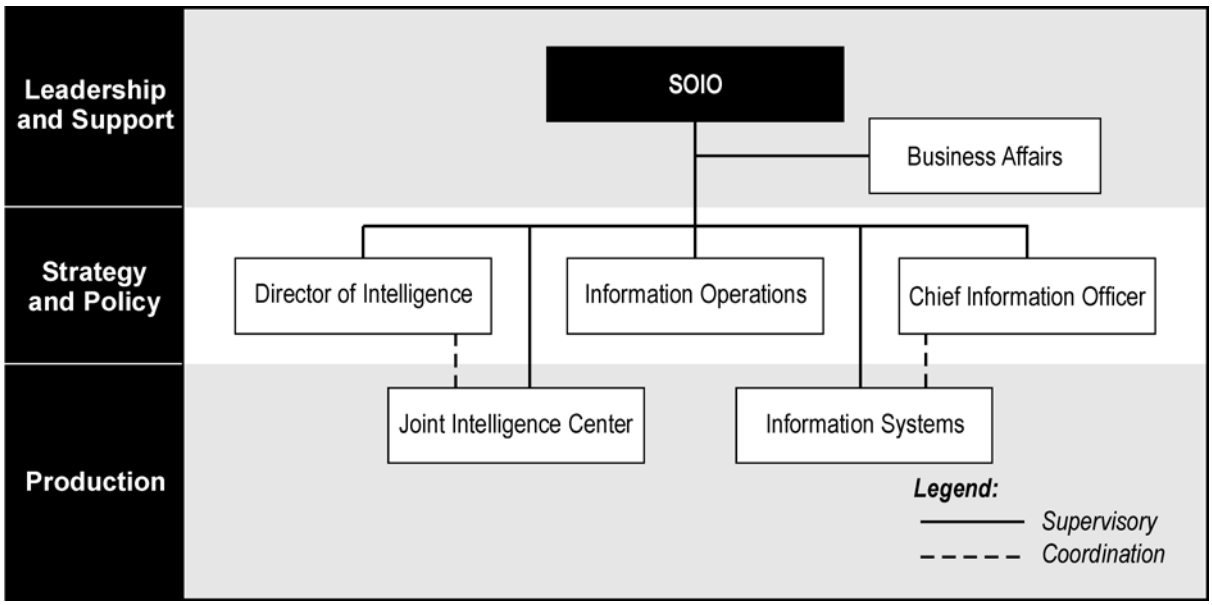


Figure 8-10. Directorate of Special Operations Information Operations

USSOCOM Joint Intelligence Center

8-27. The SOCJIC produces a variety of scheduled and ad hoc intelligence support. It also reinforces theater JIC production efforts on SOF-related issues (Figure 8-11).

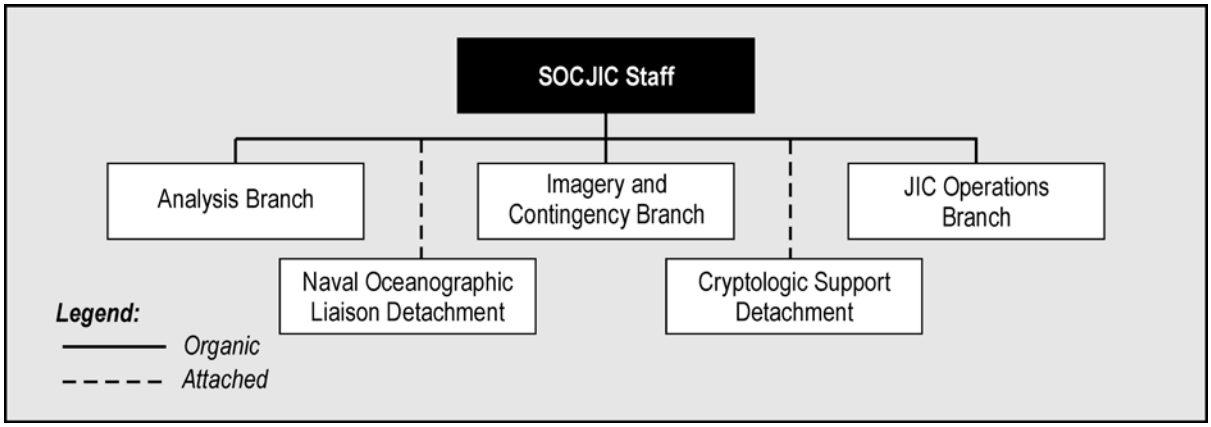


Figure 8-11. SOCJIC Organizational Structure

8-28. As a GDIP production center, the SOCJIC is a contributor to the DODIPP. The SOCJIC provides complementary SOF-unique intelligence support to all theater SOCs upon request of the theater JIC. Specifically, its mission is to provide timely analysis, production, and dissemination of all-source, fused intelligence relating to special operations to—

- Theater CINCs.
- Theater SOCs and supported commands.
- USSOCOM component commands and subordinate units.

In supporting this mission, the SOCJIC develops and disseminates specific written, visual, and multimedia products. These products support current, general military, and operational intelligence, including threat analysis and assessment. The SOCJIC electronically disseminates standardized and recurring products via the JDISS-SOCRATES. The SOCJIC provides backup to the theater CINC's intelligence resources to satisfy SOF production requests. It responds to SOF tasking requirements that the theater validated but which are beyond the capabilities of the theater JIC. It disseminates all intelligence products in the most expeditious manner, with JDISS-SOCRATES the preferred medium. The SOCJIC augments JSOTFs, using its analysts, equipment operators, and systems division support personnel. Because of limited personnel resources, requests for exercise and real-world support are considered on a case-by-case basis.

8-29. USSOCOM provides intelligence support to theater SOCs from its SOCJIC and from deployable SOF intelligence support packages. USSOCOM deploys tailored packages of personnel, systems, and equipment to theater CINCs for direct support to theater SOF. These tailored packages achieve

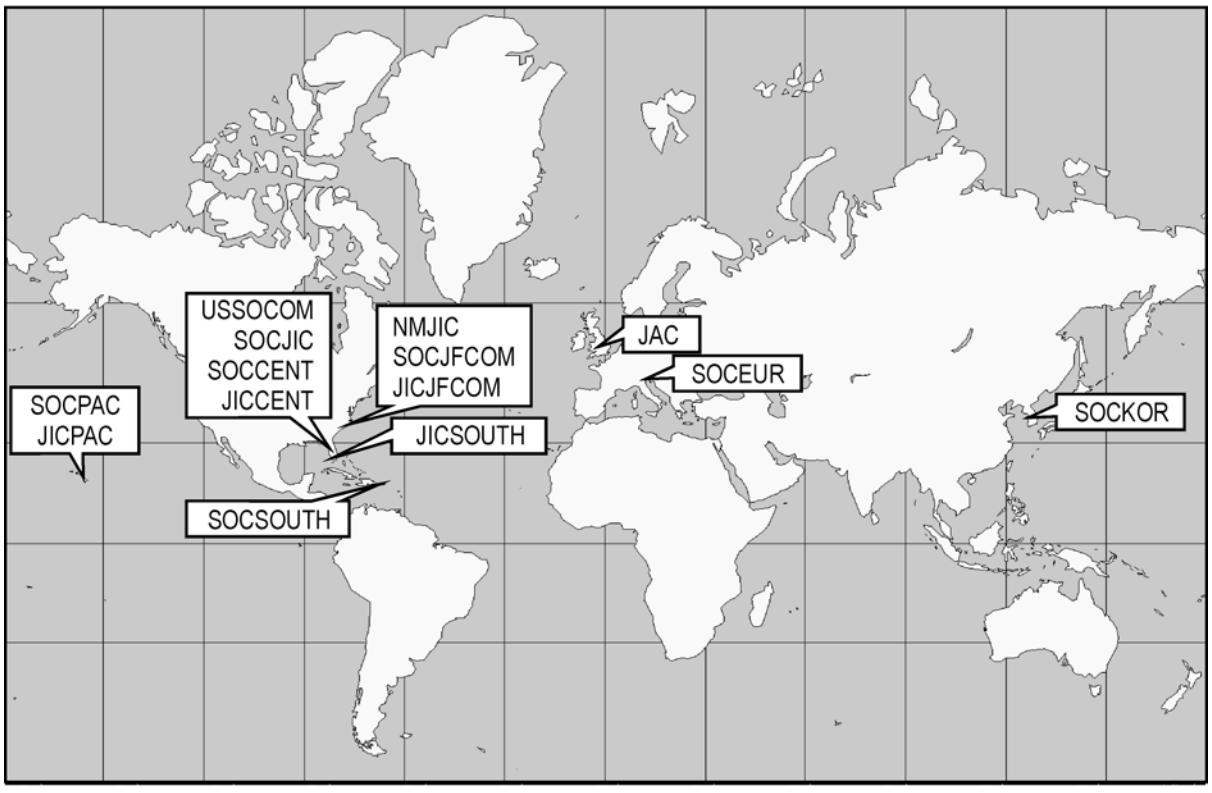
connectivity with the theater JIC for access to general MI databases focused on the AO, plus other operational needs.

ARSOF IN THEATER

8-30. ARSOF permanently based in-theater are under COCOM of the geographic combatant commander. The geographic combatant commander normally exercises operational command of all assigned and attached SOF through the theater SOC. There are five theater SOCs and one SOC supporting a subunified command:

- Special Operations Command, Joint Forces Command (SOCJFCOM).
- Special Operations Command Central (SOCCENT).
- Special Operations Command Europe (SOCEUR).
- Special Operations Command South (SOCSOUTH).
- Special Operations Command Pacific (SOCPAC).
- Special Operations Command Korea (SOCKOR)—a subunified command of United States Pacific Command (USPACOM).

8-31. For deployed or permanently based OCONUS ARSOF units, the respective JIC provides theater intelligence support through the SOC J2. The JIC ultimately provides intelligence support for military operations within its designated COCOM AOR. Figure 8-12 identifies each of the theater JICs along with its supported CINC. The exception, by name only, is the joint analysis center (JAC) located at Royal Air Force Molesworth, United Kingdom, which provides intelligence support for United States European Command



(USEUCOM).

Figure 8-12. Theater JICs and SOCs

8-32. If the JIC is unable to meet the combatant commander's requirements, it forwards requests to the NMJIC, the SOCJIC, or to subordinate command levels. A subordinate J2, such as the SOC J2, may receive augmentation from the JIC in the form of a JISE. The JISE can support OB analysis, analysis of C4I, targeting support, and collection management and provide 24-hour watch. Figure 8-13 is an example of a typical joint intelligence staff organization.

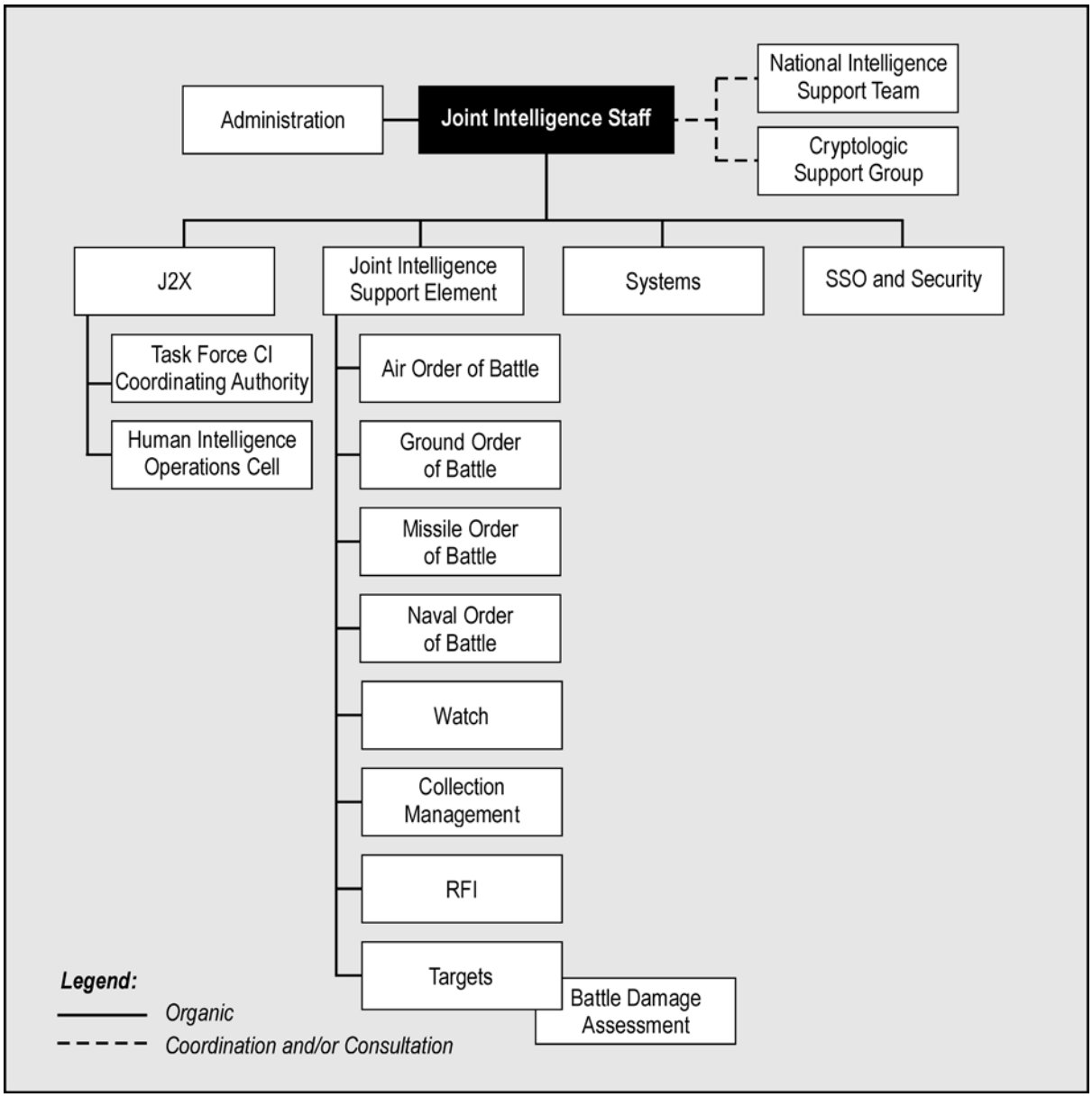


Figure 8-13. Joint Intelligence Staff Organization

SOC J2

8-33. The theater SOC J2s are relatively lightly manned although they are in subunified command structures. Consequently, without major augmentation of personnel, automation, and communications connectivity, the SOC J2s cannot provide support for deployment or employment of significant ARSOF units. They are augmented rapidly in crises, as demonstrated by SOCJFCOM during Operation RESTORE DEMOCRACY in Haiti. During peacetime or conflict, the SOCs rely heavily on the theater intelligence support system that is designed primarily to support conventional force requirements. Consequently, the SOC J2 is the theater SOF intelligence facilitator and tasker. The role of the SOC J2 includes, but is not limited to—

- Ensuring there is enough intelligence support requested for each mission tasked by the SO commander.
- Coordinating with theater J2 or C2 to collect, produce, and disseminate intelligence to meet SOF mission requirements.
- Forwarding collection and production asset requests to J2 or C2 levels to satisfy SOF intelligence requirements.
- Coordinating joint and combined SO intelligence collection operations and the production and dissemination of TIPs to support SO missions.
- Coordinating with the SOC J6 to ensure the availability of SCI voice and data communications between SOC headquarters, SOC components, and joint commands.
- Maintaining direct liaison with operational and strategic-level intelligence agencies.
- Developing IEW policies, plans, and programs for joint SOF intelligence within the respective theater.
- Maintaining GI&S products for immediate contingency use by the SOC headquarters.

Figure 8-14, page 8-29, illustrates how theater tasking and information exchanges occur between the CINCs' components and national support agencies.

NATIONAL-LEVEL IEW SUPPORT

8-34. The 13 DOD and non-DOD agencies that make up the National Intelligence Community (NIC) are shown in Figure 8-15, page 8-29. The DCI, who serves as a statutory advisor to the National Security Council (NSC), leads the NIC.

CENTRAL INTELLIGENCE AGENCY

8-35. The CIA's primary areas of expertise are in HUMINT collection, imagery, all-source analysis, and the production of political and economic intelligence.

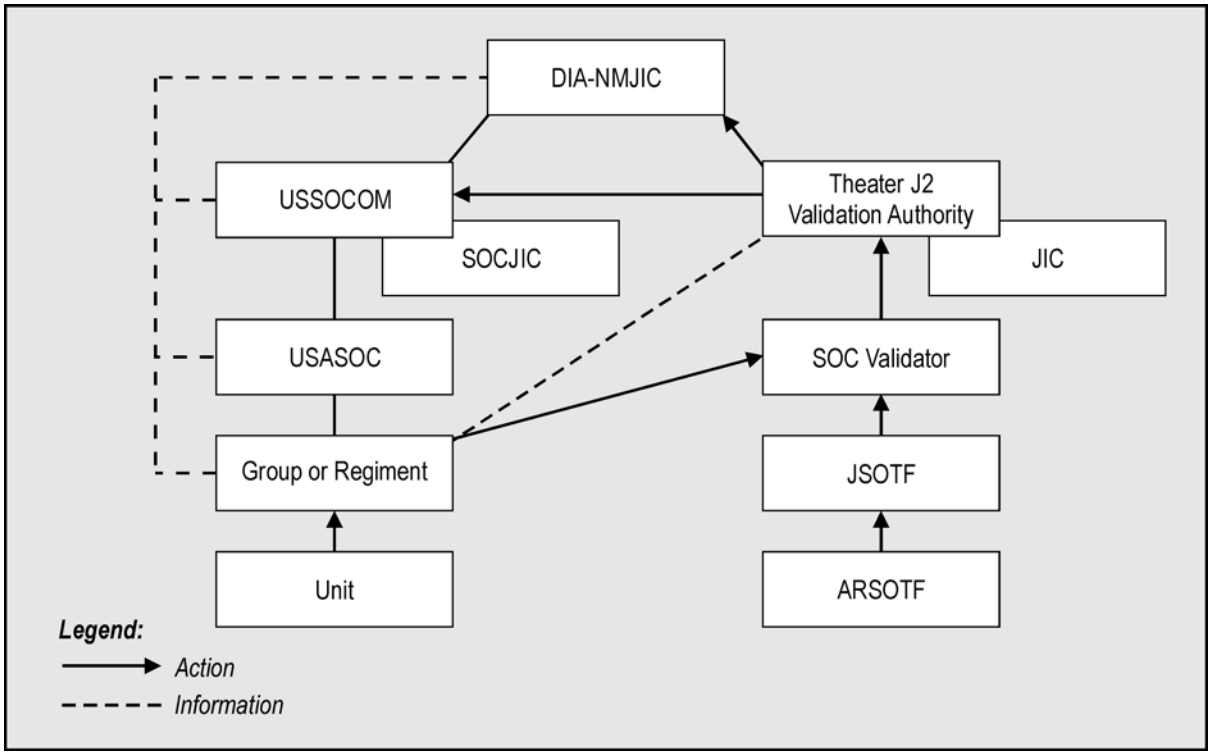


Figure 8-14. Theater-Related RFI Process

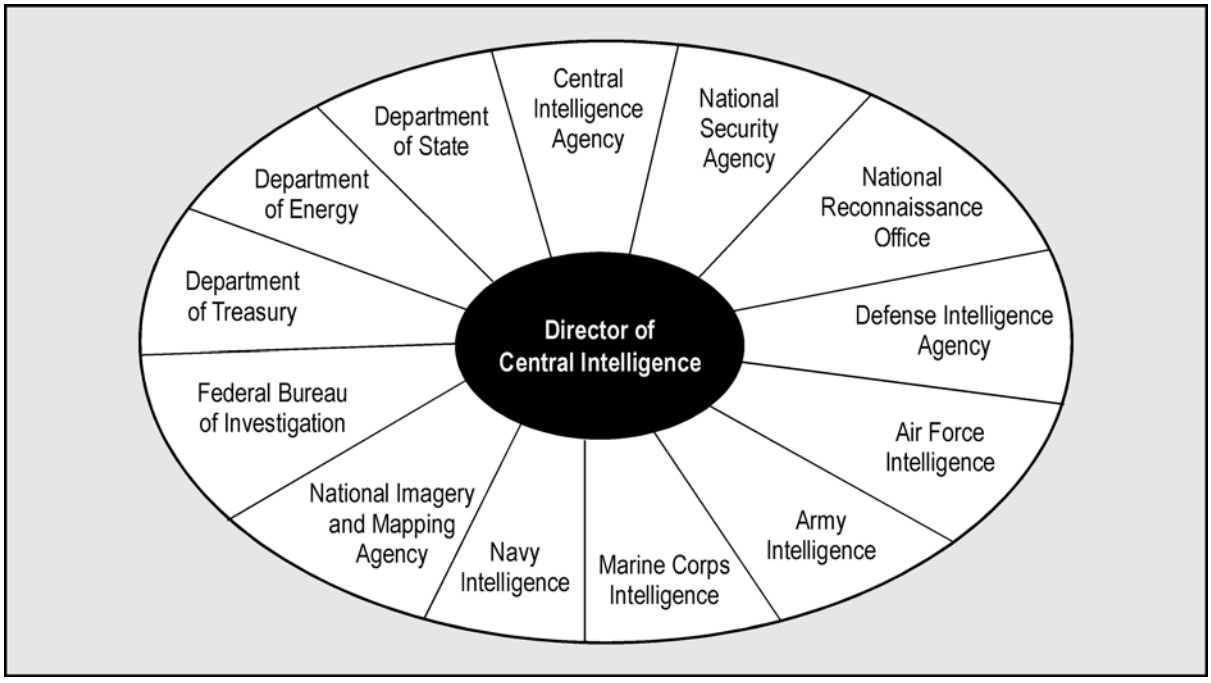


Figure 8-15. Intelligence Community Membership

DIRECTOR OF CENTRAL INTELLIGENCE

8-36. The DCI is the top policymaker for the intelligence community. As such, the DCI develops policies for and provides guidance on future intelligence needs and capabilities. The DCI serves as the principal intelligence advisor to the NCA and can serve as the Director of the CIA. In most administrations, the DCI is also the Director of the CIA; however, this is not always the case. He is also the head of the entire U.S. intelligence community and is a statutory advisor to the NSC.

OFFICE OF MILITARY AFFAIRS

8-37. The Office of Military Affairs (OMA) falls under the Associate Director of Central Intelligence for Military Support, a military officer of flag rank. CIA and military personnel staff the OMA. As the agency's single POC for military support, the OMA negotiates, coordinates, manages, and monitors all aspects of agency support for military operations. This support is a continuous process that can be enhanced or modified to respond to a crisis or a developing operation. Interaction between the OMA and the DCI representatives to the Office of the Secretary of Defense, the Joint Staff, and the combatant commands facilitates the provision of national-level intelligence supporting joint operations, contingency and operational planning, and exercises. It is through the OMA that CIA support for SOF and conventional forces intelligence support is facilitated.

DOD COMPONENTS

8-38. Several different intelligence agencies are components of the DOD. These agencies are discussed below.

The JCS Joint Staff Directorate for Intelligence, J2

8-39. The JCS Joint Staff Directorate for Intelligence, J2 is a unique organization in that it is a major component of DIA, a combat support agency, and a fully integrated element of the Joint Staff. Joint Staff J2 is composed of six deputy directorates. The following three make up the core of the NMJIC:

- Deputy Director for Crisis Management (J2M).
- Deputy Director for Crisis Operations (J2O).
- Deputy Director for Targeting Support (J2T).

The other three deputy directorates are as follows:

- Deputy Director for Administration (J2A).
- Deputy Director for Joint Staff Support (J2J).
- Deputy Director for Assessment, Doctrine, Requirements, and Capabilities (J2P).

8-40. Joint Staff J2 provides all-source intelligence to the CJCS, the Office of the Secretary of Defense (OSD), the Joint Staff, and the combatant commands. As such, the Joint Staff J2 draws deeply on DIA's broad range of capabilities to accomplish its mission and functions.

National Military Joint Intelligence Center

8-41. To accomplish assigned crisis intelligence functions, the Joint Staff J2 operates the NMJIC, which is collocated in the Pentagon with the National Military Command Center (NMCC). The NMJIC is comprised of the elements of the Joint Staff J2-DIA, as noted above, and elements from the NSA, NIMA, and the CIA. The NMJIC is the focal point for intelligence activities supporting joint operations. Joint force intelligence requirements are forwarded through combatant command JICs to the NMJIC, where appropriate national assets are tasked to meet the needs of geographic combatant commanders.

Defense Intelligence Agency

8-42. DIA was formed to unify the overall intelligence efforts of the three military departments. DIA plans and directs, collects, processes, exploits, disseminates, and evaluates and integrates military intelligence for DOD. DIA's support to policymakers focuses on developing national-level intelligence assessments, presenting perspectives for defense policy, and providing I&W of a potential crisis. DIA organizes, directs, and manages DOD intelligence sources to maximize the effectiveness of DOD intelligence programs. DIA is the primary producer of military intelligence. It coordinates intelligence functions with the three military departments. DIA satisfies intelligence requirements for DOD components. It provides imagery support for DOD components and manages the IDHSs. DIA is organized into six directorates and the Joint Military Intelligence College (Figure 8-16).

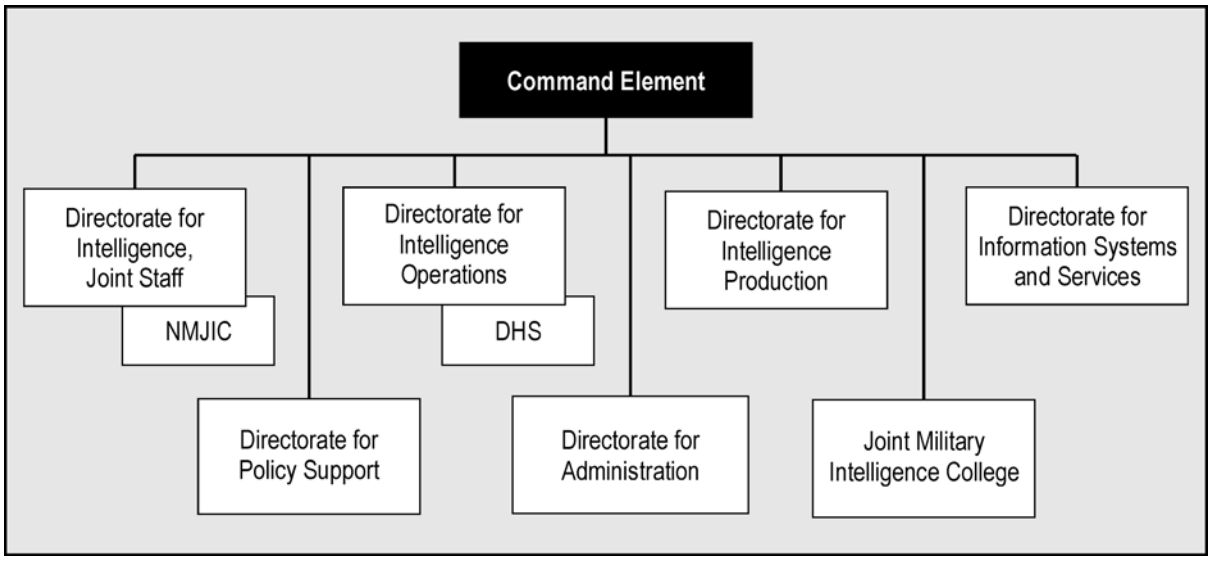


Figure 8-16. DIA Organization

Defense HUMINT Service

8-43. Under the DIA Directorate of Intelligence Operations, Defense HUMINT Service (DHS) conducts nontactical HUMINT activities. DHS

deploys forward HUMINT support elements to each combatant command to provide a conduit for coordination for DHS, to ensure that the theater Directorate of Intelligence (J2) is apprised of DHS activities, and to help the command obtain HUMINT support.

National Security Agency

8-44. The NSA is a DOD combat support agency that manages the U.S. Cryptologic System and the United States Signals Intelligence System. The Director, NSA (DIRNSA), is responsible to the Secretary of Defense (SECDEF) to ensure U.S. cryptologic planning is coherent and provides effective use of cryptologic resources. The DIRNSA also functions as the SIGINT and information systems security advisor to the SECDEF, CJCS, and geographic combatant commanders.

National Imagery and Mapping Agency

8-45. NIMA is a DOD combat support agency responsible for the consolidation of geospatial information and services. NIMA uses mission-specific data sets to produce specific GI&S products in digital, hard copy, and textual form.

Appendix A

Multinational and Interagency Intelligence

When the United States has common political or strategic objectives with allied and friendly nations, some situations may require that their military capabilities act in concert as a single and seamless force or as one operable system against an adversary. Military operations with coalition partners may take place under bilateral, multinational, or UN auspices. There may be situations where intelligence should be shared with NGOs outside usual political-military channels, requiring policy and dissemination criteria and authority for each instance.

DOCTRINE FOR MULTINATIONAL OPERATIONS

A-1. There is no single intelligence doctrine for multinational operations. Each coalition or alliance must develop its own unique TTP. There are, however, principles and concepts that provide an initial position for developing the objectives and nature of multinational doctrines.

MULTINATIONAL INTELLIGENCE ARCHITECTURE

A-2. The intelligence architecture discussed in Chapter 8 provides a framework to build the multinational intelligence architecture. Figure A-1, page A-2, provides an example of a multinational architecture that supports coalition forces and features JDISS as the core capability for disseminating released or approved-for-release U.S. intelligence information. The multinational architecture portrayed in Figure A-1 was established to provide support to U.S. and UN forces in Somalia as members of the United Nations Operations in Somalia II (UNOSOM II) effort. As the figure shows, two levels of information (intelligence) were established: Level 1 (shown to, but not retained by, coalition or UN) and Level 2 (intelligence properly cleared for release to coalition or UN). Level 1 intelligence remains within U.S.-only channels, while Level 2 flows to the UNOSOM II information center in Mogadishu either from the UN or via the U.S. Intelligence Support Element in Somalia.

JOINT AND MULTINATIONAL DOCTRINE RELATIONSHIP

A-3. There are close analogies between joint and multinational doctrines that stem from similar needs—to present an adversary a seamless force and for unity of effort of multiple force elements. Many of the principles, issues, and answers to joint operations will be the same or similar in multinational operations. For multinational doctrines, a need exists to understand differences in cultural and national perspectives to adapt doctrines or forge new ones.

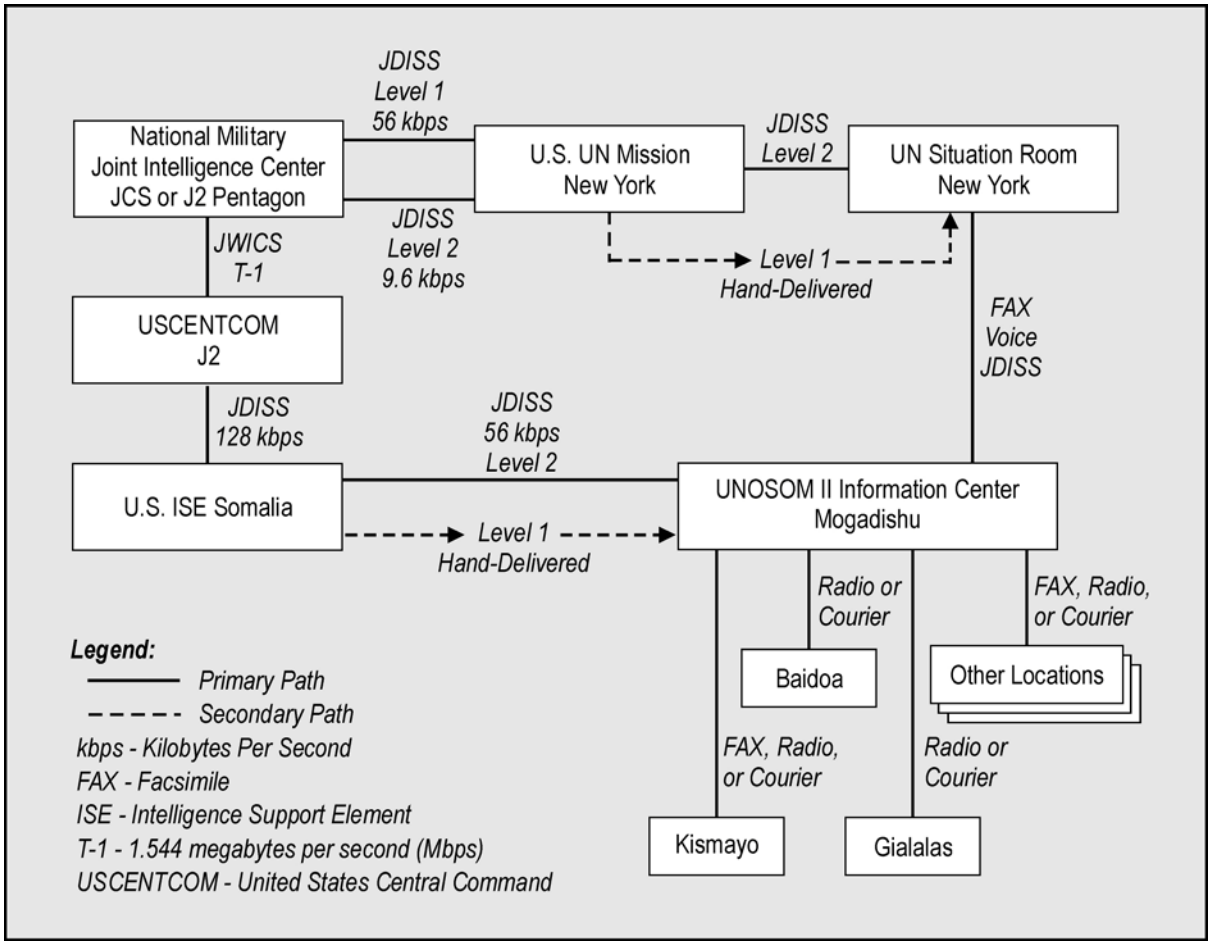


Figure A-1. Multinational Intelligence Architecture

MULTINATIONAL INTELLIGENCE PRINCIPLES

A-4. The principles in Figure A-2 are considerations for building intelligence doctrine for multinational operations. These considerations are in addition to the appropriate principles found in joint intelligence doctrine.

- Adjust National Differences Among Nations
- Employ Unity of Effort Against Common Threat
- Determine and Plan Requirements for Intelligence Special Arrangements
- Coordinate Intelligence-Sharing
- Provide for Complementary Intelligence Operations
- Operate Multinational Intelligence Center
- Conduct Intelligence Liaison Exchange Activities

Figure A-2. Intelligence for Multinational Operations

ADJUST NATIONAL DIFFERENCES AMONG NATIONS

A-5. A key to effective multinational intelligence is a readiness, beginning with the highest levels of command, to make required adjustments to national concepts for intelligence support and make the multinational action effective. Areas that need to be addressed include designating a single director of intelligence, adjusting those intelligence support differences that may affect the integrated employment of intelligence resources, and sharing intelligence and information. With these things done, successful intelligence support rests in the vision, leadership, skill, and judgment of the multinational command and staff groups.

EMPLOY UNITY OF EFFORT AGAINST COMMON THREAT

A-6. Intelligence officers of each nation need to view the threat from multinational and national perspectives. When the alliance or coalition faces a common adversary, a threat to one element of an alliance or coalition by the common adversary should be considered a threat to all alliance or coalition elements.

DETERMINE AND PLAN REQUIREMENTS FOR INTELLIGENCE SPECIAL ARRANGEMENTS

A-7. The multinational command and national forces' intelligence requirements, production, and use should be agreed on, planned, and exercised well in advance of operations. For anticipated situations and operations, a prime objective should be attaining compatibility of intelligence doctrine and concepts, intelligence systems, intelligence-related communications, language and terms, and intelligence services and products.

A-8. Solutions to problems should be developed and tried before their need in actual operations so that doctrines and procedures do not become a trial-and-error methodology during combat. The concepts and exercise programs of the NATO and the United States-Republic of Korea Combined Forces Command provide illustrations of multinational doctrine development and testing.

A-9. Special arrangements unique to coalitions and alliances should be considered for developing, communicating, and using intelligence where there are differences in nations' cultures, languages and terminology, organizations and structures, operating and intelligence concepts, methodologies, and equipment.

COORDINATE INTELLIGENCE-SHARING

A-10. The nations should share all relevant and pertinent intelligence about the situation and adversary to attain the best-possible common understanding of threatened interests, to determine relevant and attainable objectives, and to achieve unified efforts against the adversary. The nations should conceive and exercise the methodology for exchanging intelligence well before operations begin. They must, when necessary, monitor and adapt the exchange during operations to meet better-understood or changing circumstances. The ARSOF commander should have personnel knowledgeable in foreign disclosure policy and procedures, and should obtain necessary foreign disclosure authorization from the JFSOCC as soon as

possible. Assignment of personnel familiar with foreign disclosure regulations to the joint or multinational task force will facilitate the efficient flow of intelligence.

A-11. Sharing intelligence sources and methods, including cooperative intelligence collection and production, may help attain the common objectives of the alliance members or coalition partners. However, when intelligence sources and methods cannot be shared among allied or coalition nations, the intelligence should be provided after it is sanitized by effectively separating the information from the sources and methods used to obtain it. This sanitizing process must also be exercised in peacetime for both known and probable allies. Intelligence production agencies should consider use of tear lines to separate that intelligence and information within a given report that may be immediately disclosed to alliance members or coalition partners.

PROVIDE FOR COMPLEMENTARY INTELLIGENCE OPERATIONS

A-12. Intelligence efforts of the nations should be complementary. Because each nation will have intelligence system strengths and limitations or unique and valuable capabilities, the sum of intelligence resources and capabilities of the nations should be available for application to the whole of the intelligence problem. HN CI capabilities, if available, can contribute significantly to FP.

OPERATE MULTINATIONAL INTELLIGENCE CENTER

A-13. When there is a multinational command, a multinational intelligence center should be established. Creating the center provides a facility for the commander, the director of intelligence, and staffs to develop multinational intelligence requirements statements and acquire and fuse the nations' intelligence contributions. The multinational intelligence center should include a representative from all nations participating in the multinational operation.

CONDUCT INTELLIGENCE LIAISON EXCHANGE ACTIVITIES

A-14. During multinational operations, inherent problems exist due to differences in culture, languages, terms, doctrines, methodologies, and operational intelligence requirements. A robust intelligence liaison among commands, and among supporting and supported organizations minimizes these problems.

INTERAGENCY INTELLIGENCE

A-15. Interagency coordination forges the vital link between the military, economic, political, diplomatic, and informational entities of the USG. Despite philosophical and operational differences, efforts must be coordinated between USG agencies, partner nations, NGOs, regional and international organizations, and the agencies of the HN during foreign and domestic operations. (See Figure A-3, page A-5, for a model of the coordination between military and nonmilitary organizations in domestic operations.)

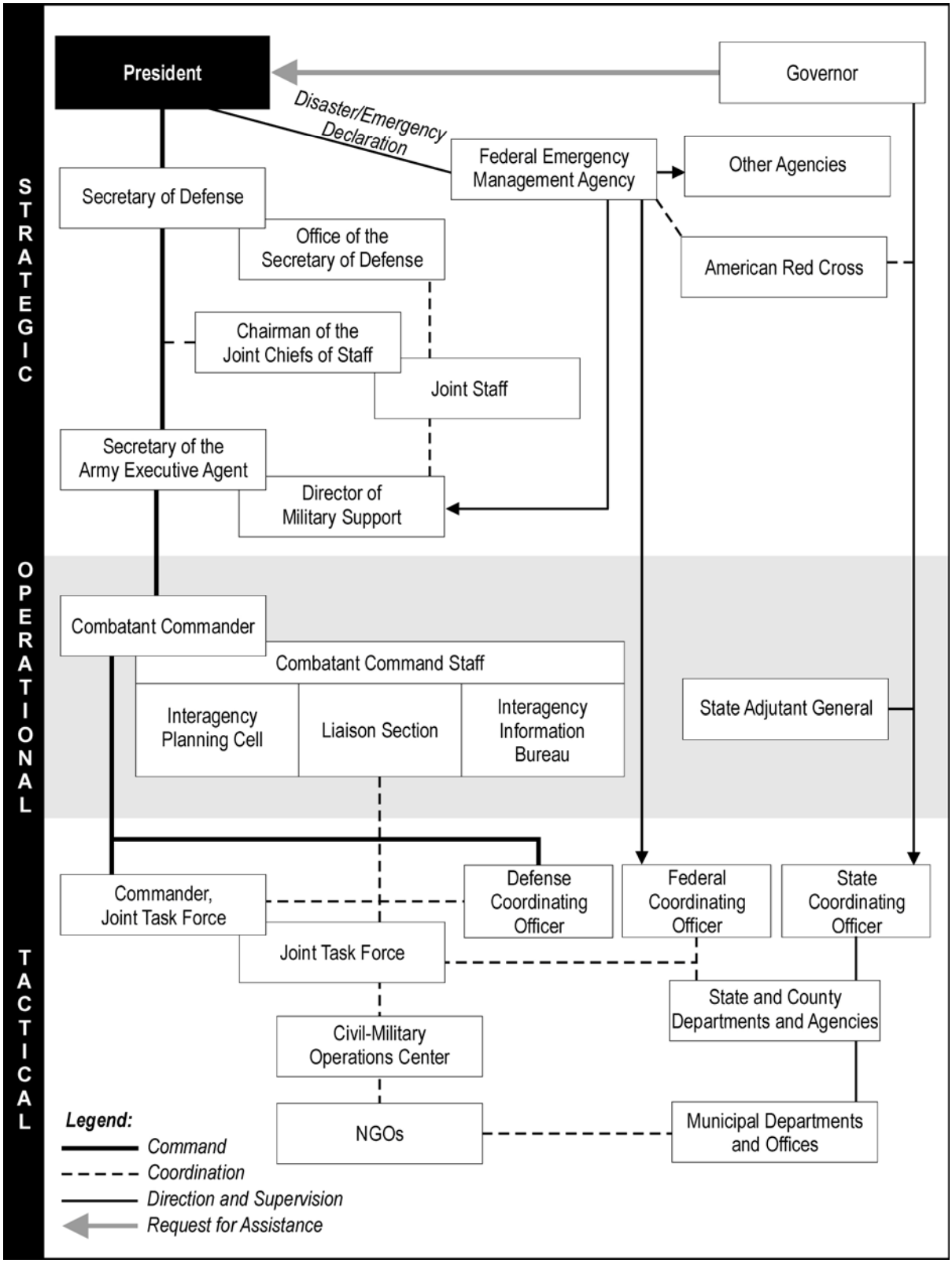


Figure A-3. Military and Nonmilitary Coordination Model—Domestic Operations

A-16. The combatant command's staff should coordinate for the deployment of a National Intelligence Support Team (NIST) to help ensure JTF connectivity with the theater JIC and national intelligence agencies. The interagency support provided by a NIST allows access to agency-unique information and analysis. It affords a link to national-level databases and information that can provide information beyond the organic resources of the JTF. NIST members are available to the JTF and combatant command HQ before deployment for team-building activities and predeployment briefings. Participating agencies retain control of their members deployed with the NIST, but the NIST operates under the staff supervision of the JTF J2.

A-17. The JIC is the primary intelligence organization providing support to joint operations in theater. It produces and provides the intelligence required to support the joint force commander and staff, components, task forces, and elements. It also coordinates support from other intelligence organizations.

A-18. The JISE is the primary intelligence apparatus of the commander, joint task force (CJTF). It is established along with the JTF itself. The JISE may constitute a new entity, or it may be little more than the combatant command's JIC, or elements thereof, moving forward.

A-19. Essential elements of information and intelligence must also be shared between and among all command elements supporting the JTF and combatant command (to include USTRANSCOM elements providing strategic lift).

A-20. JTF intelligence operations require redundant communications capabilities to properly support various complex requirements. Joint intelligence planners for JTF operations will normally prepare a detailed intelligence architecture that will support all components during the course of each unique operation. Standard JTF intelligence operations require JWICS capability to provide the JTF commander secure video teleconferencing and data capability. JWICS also provides a secure data path for the JDISS that provides secure intelligence data processing and image processing. Each Service also will use its own joint-compatible Service-unique intelligence systems to support its specific requirements.

A-21. The JTF and combatant command staffs should make every attempt to exploit open-source information in preparing and executing interagency operations.

A-22. The JISE will face unique challenges in providing adequate and appropriate support to the JTF. The JISE will have to meld traditional sources of classified military information with unclassified information from open sources and local HUMINT. The sensitivities of nonmilitary partners in interagency activities to the concept of military intelligence will complicate the melding process.

A-23. Consideration must be given to control of sensitive or classified military information in forums such as the CMOC that include representatives of other USG agencies, NGOs, and regional and international organizations. Procedures for the control and disclosure of classified information practiced by the DOD normally do not exist within other agencies. This omission may result in the inadvertent or intentional passage

of sensitive information to individuals not cleared for access to such information.

A-24. The geographic combatant commander has the authority and responsibility to control the disclosure and release of classified military information within the JOA IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5221.01A, *Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations*. In the absence of sufficient guidance, command J2s should share only information that is mission essential, affects lower-level operations, and is perishable. When required, the appropriate operational echelon should receive authority to downgrade a classification or to sanitize information. Any U.S. classified information released to a non-U.S. force or organization requires proper markings to indicate that it is releasable.

A-25. Most organizations can only provide a minimal level of security protection to classified information given them by the United States. Therefore, it is likely that they will disclose the information they receive to unauthorized individuals.

A-26. JTF operations may require significant FP support based on the uniqueness of the operational area into which the forces deploy. An operational force protection package may need to be deployed in advance echelon forces to quickly develop the on-the-ground situation for the JTF commander. FP teams can consist of CI personnel, HICs, interpreters, and other specially trained personnel, as required. FP teams will normally have mobile communications and may use the CHATS system to communicate critical data to the JTF. (See Figure A-4, page A-8, for a model of coordination between military and nonmilitary organizations in foreign operations. Figure A-5, page A-9, provides a comparison of agency organization.)

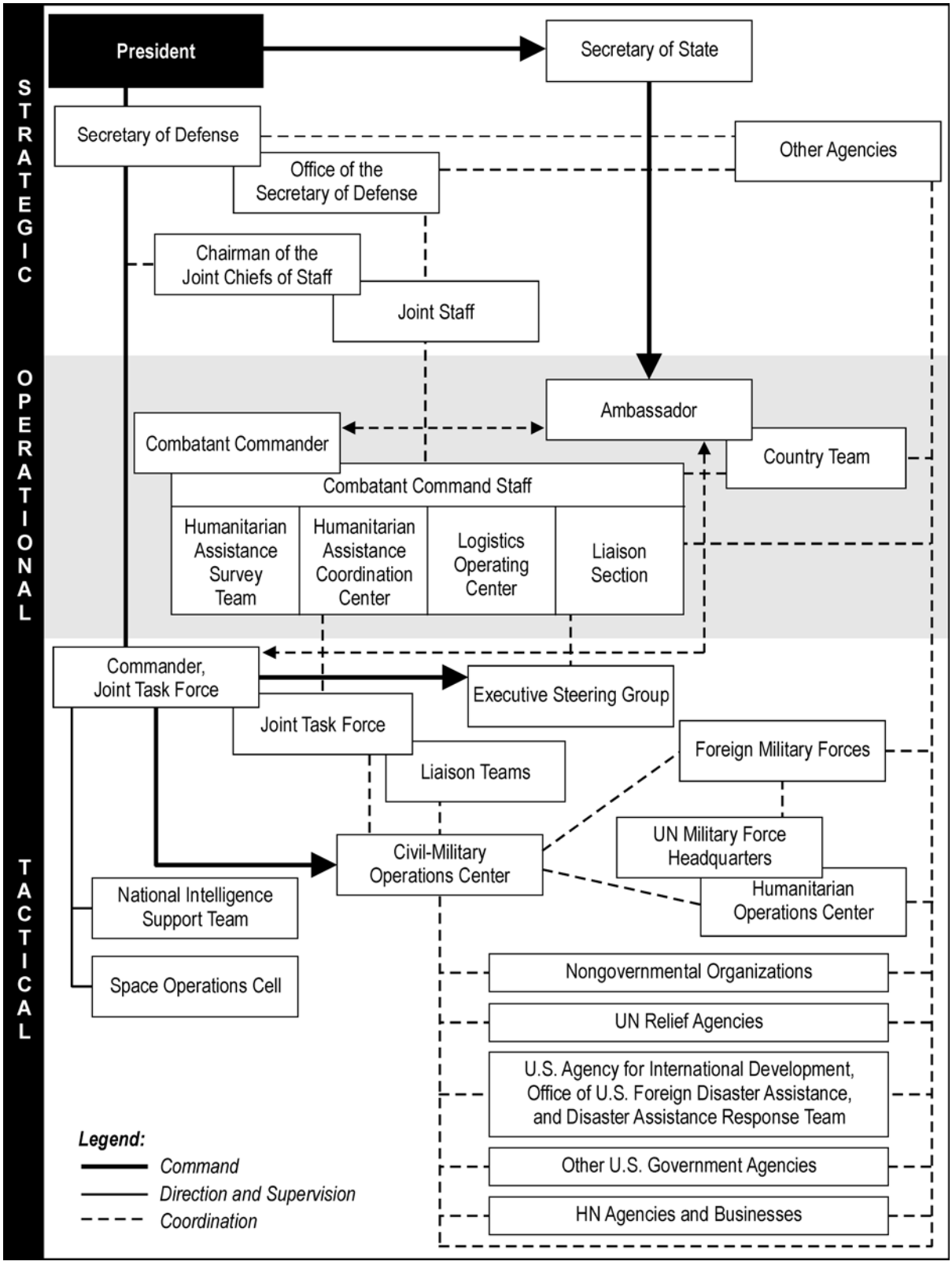


Figure A-4. Military and Nonmilitary Coordination Model—Foreign Operations

	Executive Departments and Agencies	Armed Forces of the United States	State and Local Government	REGIONAL AND INTERNATIONAL		NGOs
				NATO	UN	
Strategic	• Department Secretaries • Agency Directors • USAID • Federal Emergency Management Agency (FEMA)	• Secretary of Defense • Chairman, Joint Chiefs of Staff • Geographic Combatant Commander (5)	• Governor • State Adjutant General	• NATO Headquarters • Supreme Allied Commander, Europe (SACEUR)	• UN Headquarters • Functional Headquarters (e.g., UN High Commissioner for Refugees)	• National Headquarters • President/Chief Executive Officer
Operational	• Ambassador/Embassy Staff (1) • Liaisons (2) • Federal Coordinating Officer (FCO) (3) • USAID Office of Foreign Disaster Assistance (OFDA)	• CJTF (6) • Defense Coordinating Officer (DCO) (3)	• State Coordinating Officer (SCO) (3) • Office of Emergency Management (OEM) • Department/Agency	• Major Subordinate Commands (e.g., Allied Forces Southern Europe)	• Special Representative to the Secretary General (7) **Note:** UN Command Korea, when activated, is the only UN organization at the operational level.	• Regional Offices • Field Offices
Tactical	• Ambassador/Embassy Staff • Consul/Consulate Staff • OFDA Disaster Assistance Response Team (DART) (4)	• JTF Service Components	• National Guard Unit Commanders • County Commissioner • City Mayor/Manager • County/City Services (e.g., Police, Emergency Medical Services)	• Principal Subordinate Commands (e.g., Allied Land Forces Southern Europe) • Commander, Combined Joint Task Force • Task Element/Unit	• Special Representative to the Secretary General • Military Force Commander • Teams • Observers	• Field Office in Program Country • Relief Workers

1. The ambassador and embassy staff (which includes the country team) function at both the operational and tactical levels by supporting joint operation planning conducted by a geographic combatant commander or CJTF.
2. Liaisons at the operational level may include the foreign policy advisor (FPA) or political advisor (POLAD) assigned to the geographic combatant commander by the Department of State, the CIA liaison officer, or any specifically assigned person. Other USG agencies do not have a similar counterpart to the geographic combatant commander.
3. The FCO, DCO, and SCO and their staffs are the primary coordinators for domestic support operations.
4. USAID's OFDA provides its rapidly deployable DART in response to international disasters. A DART provides specialists, trained in a variety of disaster relief skills, to assist U.S. embassies and USAID missions with the management of USG response to disasters.
5. The geographic combatant commander, within the context of unified action, may function at both the strategic and operational levels in synchronizing the application of all instruments of national power in time, space, and purpose with the actions of other military forces, USG agencies, NGOs, regional and international organizations, and corporations toward theater strategic objectives.
6. The Commander, Joint Task Force, coordinates the actions of other military forces, USG agencies, NGOs, regional and international organizations, and corporations toward theater operational objectives.
7. The Special Representative to the UN Secretary General may function at both the operational and tactical levels.

Figure A-5. Comparison of Agency Organizational Structures

Appendix B

Special Operations Mission Planning Folder Format

Upon receipt of the plan of execution (POE) and mission support plans, the JFSOC target panel assembles a SOMPF for the target and forwards it to the JFSOC for review and approval. The SOMPF consists of five parts (JP 3-05.5) as shown below.

PART 1: MISSION TASKING PACKAGE

B-1. Upon receipt of the CINC or JFC tasking, the JFSOCC forwards the mission tasking package (MTP) to the ARSOF Mission Planning Agent (MPA). The MTP includes all transmittal documents, target identification data, CINC and/or JFC mission guidance, a record of changes, and a record of distribution in the format shown in Figure B-1, pages B-1 and B-2.

(Classification)

Section I: Tasking and Transmittal Documents

A. ( ) JFSOCC Tasking: *The external directive that tasks the JFSOCC to plan and execute the mission.*

B. ( ) SOF MPA Letter of Transmittal: *The internal JFSOCC directive that tasks the MPA to develop a POE (Part 3 of the SOMPF).*

C. ( ) COORDINATING INSTRUCTIONS: *These instructions normally delegate coordinating authority to the MPA and direct liaison to all concerned parties.*

Section II: Target Identification Data

A. ( ) NAME: *Target, target system, or objective area.*

B. ( ) BASIC ENCYCLOPEDIA (BE) NUMBER: *Target identification number in automated database.*

C. ( ) MISSION NUMBER: *Internal JFSOCC target identification number, if applicable.*

D. ( ) FUNCTIONAL CLASSIFICATION CODE: *As described in DIAM 65-3-1-1, (C) Standard Coding System Functional Classification Handbook (U), and the target data inventory (TDI) handbooks found on the MIDB.*

E. ( ) COUNTRY: *Name.*

F. ( ) JSOA COORDINATES: *Universal transverse mercator* (*UTM).*

G. ( ) GEOGRAPHIC COORDINATES: *Latitude and longitude.*

(Classification)

Figure B-1. Sample Format for Part 1 (MTP) of SOMPF

(Classification)

H. ( ) GENERAL DESCRIPTION AND TARGET SIGNIFICANCE: *Self-explanatory.*

Section III: JFC Mission Guidance

A. ( ) MISSION STATEMENT: *What the JFC wants accomplished and when, where, and why he wants it accomplished.*

B. ( ) SPECIFIC OBJECTIVES: *Specific tasks that must be accomplished.*

C. ( ) COMMANDER'S GUIDANCE (AIR/NAVAL/GROUND OPTIONS): *Desired results, specific COAs the commander wants the MPA to consider, and mission constraints and restraints.*

D. ( ) COMMAND AND SIGNAL: *Command relationships during mission planning and execution and required signal links and reports.*

Section IV: Record of Changes

Record of changes posted to the MTP during its existence.

Section V: Record of Distribution

Record of organization to which MTP has been distributed.

(Classification)

Figure B-1. Sample Format for Part 1 (MTP) of SOMPF (Continued)

PART 2: FEASIBILITY ASSESSMENT

B-2. The feasibility assessment (FA) addresses the validity of the SOF mission, the capability of the MPA (unilaterally or as part of a joint or combined operation) to accomplish the mission within an acceptable degree of risk, and the psychological reaction of friendly, enemy, and neutral nations. (See Chapter 1, page 1-11, Special Operations Mission Criteria.) The format aids the FA process. The MPA reserves detailed planning and the selection of a preferred COA for the development of a POE should the FA indicate the mission is feasible. The MPA must immediately identify all information shortfalls that would preclude development of an FA. As a minimum, the MPA needs imagery, an area study, maps, and OB information to produce an FA. The process outlined in Figure B-2, pages B-3 through B-5, may be compressed during a crisis.

PART 3: TARGET INTELLIGENCE PACKAGE

B-3. The appropriate theater Service intelligence production agency (IPA) is tasked through the Service component commander to prepare the TIP and provide the intelligence required to support the prioritized SOMPF production schedule. Upon receipt of the FA, and upon determination to task for a POE, the JFSOCC passes the additional intelligence requirements listed in Section VII of the FA to the appropriate IPA with its tasking for TIP production. See Appendix C for TIP formats for SR or DA and FID or UW missions.

(Classification)

Copy ____ of ____ Copies
____ SFG(A), 1st SF
Location
Date

Feasibility Assessment of Mission # _____ ( )

Section I: Mission ( )

A. ( ) TARGET IDENTIFICATION DATA. (*Use data from MTP*.)

B. ( ) MISSION STATEMENT AND COMMANDER'S GUIDANCE. *Restate the assigned mission and its purpose. List any intermediate tasks, specified or implied, that MPA considers necessary to accomplish the mission. Multiple missions must be stated in priority*.

Section II: Commander's Assessment ( )

A. ( ) FEASIBILITY AS A TARGET. *The MPA commander provides his assessment of the mission, to include specific answers to the following questions:*

1. ( ) Is the mission appropriate for SOF?

2. ( ) Does the mission support the geographic combatant commander's campaign plan?

3. ( ) Is the mission operationally feasible?

B. ( ) PROBABILITY OF MISSION SUCCESS.

1. ( ) Are the required resources available to conduct the mission?

2. ( ) Does the expected outcome justify the risk?

C. ( ) RECOMMENDATION. *Should the JFSOCC recommend or direct execution of this mission? If not, why not? With what degree of risk can this mission be accomplished?*

Section III: Assumptions ( )

( ) *Include any assumptions required as a basis for initiating planning. An assumption, while not fact, must have a basis in fact. Assumptions must be valid and essential to a solution to the problem.*

Section IV: Factors Affecting Courses of Action ( )

This section is the foundation of the assessment. Discuss in each paragraph those conditions that impact on the capability of the MPA to effectively accomplish the mission. Be concise but complete. Determine those facts of the situation that will influence friendly and hostile actions. This section is not meant to be the same as Part III (TIP) of the SOMPF and should reflect only those facts that are salient to the situation. Analyze each fact and deduce the probable effect on other facts and on hostile and friendly actions. Include the following, as appropriate (some categories may not be applicable or foreseeable during peacetime planning):

A. ( ) CHARACTERISTICS OF THE JSOA. Include analyses of the effects of pertinent characteristics of the JSOA.

1. ( ) Weather. *Analyze the effects of weather and light data on mission feasibility.*

(Classification)

Figure B-2. Sample Format for Part 2 (FA) of SOMPF

(Classification)

2. ( ) Terrain. *Analyze effects of terrain on hostile and friendly operations. Identify key terrain features and AAs.*

3. ( ) Other pertinent factors. *Identify political, economic, sociological, psychological, and other factors such as hydrography, environment, communications, science, technology, materiel, transportation, and manpower. Analyze their effects on friendly and hostile operations.*

B. ( ) HOSTILE SITUATION.

1. ( ) Composition. *Identify name, organization, and major equipment of hostile forces, including police, paramilitary, and internal security forces.*

2. ( ) Dispositions. *Identify locations of hostile forces, including fire support systems. Note differences between normal, alert, and deployed dispositions.*

3. ( ) Strength. *State in the following terms:*

a. ( ) Committed forces. *State number and size of hostile units committed against friendly forces.*

b. ( ) Location of reinforcements and estimated reaction times.

c. ( ) NBC capabilities.

4. ( ) Significant hostile activity. *Summarize recent and current activities of hostile forces that may affect mission accomplishment. Consider such items as hostile employment of new or unconventional weapons, tactics, techniques, materiel, or troops.*

5. ( ) Peculiarities and weaknesses. *Indicate hostile peculiarities and weaknesses that will favorably influence the mission.*

6. ( ) Vulnerability to deception. *Indicate vulnerability of hostile forces to tactical and strategic deception (to include PSYOP).*

7. ( ) Hostile capabilities. *Identify and analyze COAs that hostile forces can physically perform and that could influence mission accomplishment. Include exploitable hostile vulnerabilities.*

C. ( ) FRIENDLY SITUATION. *Identify and analyze the same considerations as those included in paragraph B above. State recent and present significant activities, peculiarities, and weaknesses and include such items as morale, training, personnel, and logistics. The information is usually in abbreviated form because it may be a repetition of what is generally known. Friendly dispositions are significant, however, and must be described in enough detail to determine how they influence the choice of a COA.*

Section V: Courses of Action ( )

A. ( ) IDENTIFICATION OF COAs. *The MTP may direct consideration of several COAs. Develop additional COAs, as required. Outline each COA in enough detail to make one COA distinguishable from other COAs during analysis and comparison.*

B. ( ) ANALYSIS OF COAs. *Analyze each postulated COA to determine its advantages and disadvantages in terms of risk versus probability of success. During the analysis, add details, make revisions, and fully develop each COA.*

(Classification)

Figure B-2. Sample Format for Part 2 (FA) of SOMPF (Continued)

(Classification)

C. ( ) COMPARISON OF COAs. *Compare each friendly COA against a set of significant factors to determine likely outcomes. Significant factors may include METT-TC, the principles of war, and the SO imperatives.*

D. ( ) RECOMMENDED COA. *State which COA offers the greatest probability of success. Bear in mind the completed TIP may confirm the COA chosen or indicate an alternate COA as a more desirable option.*

Section VI: Intelligence Requirements ( )

( ) *List in priority the essential intelligence (beyond that provided in the MTP) required to develop a POE.*

Section VII: Special Requirements ( )

A. ( ) PERSONNEL. *State how many personnel are needed to perform the mission. List any requirements for special skills.*

B. ( ) LOGISTICS. *List nonorganic materiel and services that are essential to mission success.*

C. ( ) OTHER. *List any other special requirements.*

Section VIII: Indigenous Support ( )

( ) *Indicate indigenous support that would increase probability of success.*

(Classification)

Figure B-2. Sample Format for Part 2 (FA) of SOMPF (Continued)

PART 4: PLAN OF EXECUTION

B-4. SOF MPAs develop a POE for each target assigned by using the format in Figure B-3, pages B-5 and B-6. POEs cannot be fully developed until the MPA receives the TIP and mission support plans (MSPs). This fact dictates concurrent planning and continuous coordination among all concerned. See JP 3-05.5 for a more detailed format.

(Classification)

Section I: Commander's Estimate of the Situation.

This section updates the FA to select a feasible COA to accomplish the mission.

Section II: Special Operations Unit Plan.

This section includes a full mission profile expanding the COA option selected in the commander's estimate. It addresses tactical aspects such as method and location of infiltration, movement to the

(Classification)

Figure B-3. Sample Format for Part 4 (POE) of SOMPF

(Classification)

objective area, actions in the objective area, and movement to and method of exfiltration. To preserve OPSEC, this section will be issued separately from the SOMPF and with a limited distribution.

Section III: Supporting Plans.

This section contains appropriate supporting plans and annexes prepared by supporting agencies.

Section IV: Limiting Factors.

This section is completed by the MPA and outlines limiting factors that surfaced during development of sections I and II of the POE. Correspondence or message traffic related to the adjustment or improvement of the limiting factors are enclosed in this section with annotated updates to provide a current capability status reference for planners.

(Classification)

Figure B-3. Sample Format for Part 4 (POE) of SOMPF (Continued)

PART 5: MISSION SUPPORT PLANS

B-5. The MSPs include fixed- and rotary-wing aircraft, surface ships, and submarines. Figure B-4, pages B-6 through B-10, depicts a sample format for Part 5 of the SOMPF.

(Classification)

Section I: Mission

A. ( ) Target identification data. *(Use data from MTP.)*

B. ( ) Mission statement. (*Use data from MTP.)*

Section II: Mission Summary

A. ( ) Mission tasking. (*Use data from MTP.)*

B. ( ) Objective area. (*Use data from MTP.)*

C. ( ) General concept. (*Use data from MTP.)*

D. ( ) Summary of limiting factors. *(Use data from FA.)*

E. ( ) Probability of mission success. (*Use data from FA.)*

Section III: Assumptions

( ) *Include any assumptions required as a basis for initiating planning. An assumption, while not fact, must have a basis in fact. Assumptions must be valid and essential to a solution to the problem.*

(Classification)

Figure B-4. Sample Format for Part 5 (MSP) of SOMPF

(Classification)

Section IV: Threat Assessment

A. ( ) Composition. *Identify name, organization, and major equipment of hostile forces, including police, paramilitary, and internal security forces.*

B. ( ) Dispositions. *Identify locations of hostile forces, including fire support systems. Note differences between normal, alert, and deployed dispositions.*

C. ( ) Strength. *State in the following terms:*

1. ( ) Committed forces. *State number and size of hostile units committed against friendly forces.*

2. ( ) Location of reinforcements and estimated reaction times.

3. ( ) NBC capabilities.

D. ( ) Significant hostile activity. *Summarize recent and current activities of hostile forces that may affect mission accomplishment. Consider such items as hostile employment of new or unconventional weapons, tactics, techniques, materiel, or troops.*

E. ( ) Peculiarities and weaknesses. *Indicate hostile peculiarities and weaknesses that will favorably influence the mission.*

F. ( ) Vulnerability to deception. *Indicate vulnerability of hostile forces to tactical and strategic deception (to include PSYOP).*

G. ( ) Hostile capabilities. *Identify and analyze COAs that hostile forces can physically perform and that could influence mission accomplishment. Include exploitable hostile vulnerabilities.*

Section V: Navigation and Overall Mission Portrayal

Note: *This represents the entire infiltration and exfiltration route from launch to recovery on a suitable scale chart annotating all information deemed necessary by the planning cell for portrayal of the mission. This should include, but is not limited to, the following:*

A. ( ) Launch base(s).

B. ( ) Intermediate staging base(s).

C. ( ) LZ(s), DZ(s), recovery zone(s) (RZ[s]), seaward launch point(s) (SLP[s]), beach landing site(s) (BLS[s]), and seaward recovery point(s) (SRP[s]).

D. ( ) Recovery base(s).

E. ( ) Abort and/or emergency divert base(s).

F. ( ) Air refueling track(s) and forward arming and refueling points (FARPs).

G. ( ) Routes.

1. ( ) Ingress.

2. ( ) Egress.

3. ( ) Orbiting and holding.

(Classification)

Figure B-4. Sample Format for Part 5 (MSP) of SOMPF (Continued)

(Classification)

4. ( ) Safe passage procedures.

5. ( ) Strip charts, navigation logs, global positioning satellite receivers, and other aids (as required).

Section VI: Supporting Plans

A. ( ) Overall schedule of events.

B. ( ) Prelaunch requirements.

1. ( ) Updates to OBs.

2. ( ) Essential elements of information (EEI).

3. ( ) Problem areas and key factors.

C. ( ) Insertion and extraction platform(s) factors and logistic considerations.

D. ( ) Command, control, and communications.

1. ( ) Security preparations.

2. ( ) Departure procedures (overt or deception procedures).

3. ( ) Communications equipment requirements.

a. ( ) Insertion and extraction platform(s).

b. ( ) SOC.

4. ( ) Specialized operational procedures and techniques.

5. ( ) Radio silence areas.

6. ( ) Point of no return (PONR).

7. ( ) Joint communications-electronics operating instructions for air mission.

8. ( ) Deception.

E. ( ) Emergency procedures.

1. ( ) Engine-out capability.

2. ( ) Weather.

3. ( ) Incorrect or obsolete intelligence.

4. ( ) Insertion and extraction platform(s) abort procedures.

a. ( ) Late departure procedures.

b. ( ) Maintenance problems.

c. ( ) Battle damage.

(Classification)

Figure B-4. Sample Format for Part 5 (MSP) of SOMPF (Continued)

(Classification)

d. ( ) Platform destruction.

e. ( ) Bump plan.

5. ( ) Drop or other fuel-related malfunctions.

6. ( ) Lost communications procedures.

7. ( ) Mission-abort procedures.

F. ( ) Evasion plan of action.

1. ( ) Crew/embarked personnel responsibilities.

2. ( ) Immediate actions upon sinking, ditching, or bailout.

3. ( ) Evasion movement.

4. ( ) SAFE area intelligence description (SAID).

5. ( ) Selected area for evasion (SAFE).

6. ( ) Evasion team communications.

7. ( ) Search and rescue (SAR) contact procedures.

Section VII: Limiting Factors

A. ( ) Intelligence/intelligence gaps/periodic intelligence updates.

B. ( ) Weather.

C. ( ) Equipment.

D. ( ) Munitions.

E. ( ) Tactics.

F. ( ) Logistics (including combat service support and hazardous material).

G. ( ) Personnel.

H. ( ) Training.

I. ( ) Supporting forces.

J. ( ) ROE and legal issues.

K. ( ) CI environment.

Section VIII: Special Operations Aviation, Surface Ship, and Submarine Requirements from AFSOC, ARSOF, or Navy Special Operations Forces (NAVSOF) to Conduct Initial Assessment(s)

A. ( ) Target coordinates.

(Classification)

Figure B-4. Sample Format for Part 5 (MSP) of SOMPF (Continued)

(Classification)

B. ( ) Maximum and/or minimum distances the DZs, LZs, RZs, SLPs, BLSs, and SRPs can be from the target.

C. ( ) Time frame in OPLAN or CONPLAN scenario, (e.g., D-day, D-XX, or D+XX).

D. ( ) Desired launch and recovery base(s).

E. ( ) Type of delivery or recovery required (e.g., airdrop, airland, fast rope, SEAL delivery vehicle [SDV], combat rubber raiding craft [CRRC]) and platform preferred.

F. ( ) Number of personnel to be transferred and approximate weight per person.

G. ( ) Approximate size and weight of additional equipment.

H. ( ) Type and quantity of hazardous material (e.g., gasoline, lithium batteries, etc.).

I. ( ) Assumptions made during supported unit's FA and POE.

J. ( ) Desired time over target.

K. ( ) Resupply and/or extraction requirements.

Note: *Some of the information may not be readily available. Information in hand will normally suffice to conduct the POE. However, all efforts should be made to obtain the above information and to incorporate it into the POE.*

(Classification)

Figure B-4. Sample Format for Part 5 (MSP) of SOMPF (Continued)

Appendix C

Special Operations Forces Target Intelligence Package

This appendix contains sample formats for the TIP. (The TIP is also a part of the SOMPF [Appendix B].) For detailed requirements of each paragraph, see JP 3-05.5.

DA AND SR MISSIONS

C-1. The sample format for DA and SR missions is shown in Figure C-1, pages C-1 and C-2.

(Classification)

Section 1: Target Identification and Description

A. Target identification data.

B. Description and significance.

C. Detailed target description.

D. Target vulnerability assessment.

Section 2: Natural Environment

A. Geographic data (including terrain and hazards to movement).

B. Meteorological data (climatological overview and tables and illumination data).

C. Hydrographic data (coastal, waterways, lakes, luminescence, etc.).

Section 3: Threat

A. Ground forces.

B. Paramilitary and indigenous forces (including intelligence and security and police services).

C. Naval forces (including Coast Guard and maritime border guard).

D. Air forces.

E. Air defense forces (including radars, passive detectors, and C4I).

F. Electronic OB.

G. Space-based assets.

H. CI environment (efforts of indigenous forces to collect against SOF elements).

I. Other.

(Classification)

Figure C-1. Sample TIP Format for DA and SR Missions

(Classification)

Section 4: Demographics and Cultural Features

A. Area population characteristics.

B. Languages, dialects, and ethnic composition.

C. Social conditions.

D. Religious factors.

E. Political characteristics.

F. Economic conditions.

G. Miscellaneous (for example, currency, holidays, dress, and customs).

Section 5: Lines of Communication and Information Systems

A. Airfields.

B. Railways.

C. Roadways.

D. Waterways.

E. Ports.

F. Petroleum, oils, and lubricants (POL).

G. Power grid.

H. Public information media and telecommunications (print, radio, television, telephone, etc.).

Section 6: Infiltration and Exfiltration (potential DZs, LZs, RZs, SLPs, BLSs, SRPs)

A. Potential zones.

B. Choke points between insertion point(s) and objective.

Section 7: Survival, Evasion, Resistance, Escape, Recovery (SERER) Data (See JP 3-50.3, *Joint Doctrine for Evasion and Recovery.*)

A. SAFE data.

B. SAID data.

C. Survival data.

Section 8: Unique Intelligence (mission-specific requirements not covered above)

Section 9: Intelligence Shortfalls

Appendix A: Bibliography

Appendix B: Glossary

Appendix C: Imagery

Appendix D: Maps and Charts

Appendix E: SCI (if applicable)

(Classification)

Figure C-1. Sample TIP Format for DA and SR Missions (Continued)

FID AND UW MISSIONS

C-2. The sample format for FID and UW missions is shown in Figure C-2, pages C-3 and C-4.

(Classification)

Section 1: Objective Area (OA) Identification and Description

A. OA identification data.

B. Description and significance.

Section 2: Natural Environment

A. Geographic data (including terrain and hazards to movement).

B. Meteorological data (climatological overview, tables, and illumination data).

C. Hydrographic data (coastal, waterways, lakes, etc.).

D. Water sources (color-coded overlay).

E. Flora and fauna (plants and animals of tactical importance).

Section 3: Threat

A. Objective country (enemy OB).

B. Opposition and resistance forces.

C. CI environment (efforts of indigenous forces to collect against SOF elements).

Section 4: Demographics and Cultural, Political, and Social Features (EEI must be answered for the objective country and opposition and resistance forces.)

A. Area population characteristics (include resistance potential).

B. Languages, dialects, and ethnic composition.

C. Social conditions.

D. Religious factors.

E. Political characteristics.

F. Available labor force.

G. Customs (social, religious, cultural), weapons, mores, etc.

H. Medical capabilities.

I. Health and sanitation conditions.

J. Economic conditions.

K. Currency, holidays, and dress.

Section 5: Lines of Communication and Information Systems

A. Airfields.

B. Railways.

C. Roadways.

(Classification)

Figure C-2. Sample TIP Format for FID and UW Missions

(Classification)

D. Waterways.
E. Ports.
F. POL.
G. Power grid.
H. Public information media and telecommunications (print, radio, television, telephone, etc.).
I. Exploitable civilian transportation.
J. Primary mode(s) of transportation.
K. U.S.-provided materials and services.
L. Stockpiles.
M. War-sustaining industries.
N. War-sustaining resupply.
O. Movement control centers.

Section 6: Infiltration and Exfiltration (potential DZs, LZs, RZs, SLPs, BLSs, SRPs)

A. Potential zones.
B. Choke points between insertion point(s) and objective.

Section 7: FID and Military Assistance (EEI must be answered for the objective country and opposition and resistance forces.)

A. Military assistance provided.
B. Foreign personnel (noncombatants).
C. Foreign military material.
D. Deployments of foreign personnel and equipment.
E. Foreign contractors' services and construction.
F. U.S. support.

Section 8: SERER Data (See JP 3-50.3.)

A. SAFE data.
B. SAID data.
C. Survival data.

Section 9: Unique Intelligence (mission-specific requirements not covered above)

Section 10: Intelligence Shortfalls

Appendix A: Bibliography

Appendix B: Glossary

Appendix C: Imagery

Appendix D: Maps and Charts

Appendix E: SCI (if applicable)

(Classification)

Figure C-2. Sample TIP Format for FID and UW Missions (Continued)

Glossary

5D	Demand-Driven Direct Digital Dissemination
A2C2	Army airspace command and control
AA	avenue of approach
AAF	Army airfield
AB	air base
ABCS	Army Battle Command System
ACE	Army compartmented element
ACERT	Army Computer Emergency Response Team
ACT	analysis and control team
ACTD	advanced concepts technology demonstration
ADA	air defense artillery
administrative control	Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. (JP 1-02)
ADP	automated data processing
adversary	Anyone who contends with, opposes, or acts against one's interest. An adversary is not necessarily an enemy.
AFB	Air Force Base
AFSOC	Air Force Special Operations Command
AI	area of interest
AIS	automated information system
AK	Alaska
AL	Alabama
AMEDD	Army Medical Department
antiterrorism	Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. (JP 1-02)
AO	area of operation
AOB	advanced operational base

AOR area of responsibility—1. The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. 2. In naval usage, a predefined area of enemy terrain for which supporting ships are responsible for covering by fire on known targets or targets of opportunity and by observation. (JP 1-02)

AP Associated Press

area assessment The commander's prescribed collection of specific information that commences upon employment and is a continuous operation. It confirms, corrects, refutes, or adds to previous intelligence acquired from area studies and other sources prior to employment. (JP 1-02)

ARSOA Army special operations aviation

ARSOF Army special operations forces—Those active and reserve component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. (JP 1-02)

ARSOTF Army special operations task force—A temporary or semipermanent grouping of ARSOF units under one commander and formed to carry out a specific operation or a continuing mission.

ASAS All-Source Analysis System

ASAS-L All-Source Analysis System-Light

ASAS-RWS All-Source Analysis System Remote Workstation

ASAS-SS All-Source Analysis System-Single Source

ASCDB all-source correlated database

ASPS all-source production section

asset (intelligence) Any resource—person, group, relationship, instrument, installation, or supply—at the disposition of an intelligence organization for use in an operational or support role. Often used with a qualifying term such as agent asset or propaganda asset. (JP 1-02)

assign 1. To place units or personnel in an organization where such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel. 2. To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. (JP 1-02)

attach 1. The placement of units or personnel in an organization where such placement is relatively temporary. 2. The detailing of individuals to specific functions where such functions are secondary or relatively temporary, e.g., attached for quarters and rations; attached for flying duty. (JP 1-02)

AUTODIN Automatic Digital Network

auxiliary In unconventional warfare, that element of the resistance force established to provide the organized civilian support of the resistance movement. (AR 310-25)

AWE Army warfighter experiment

BAE battlefield area evaluation

BDA battle damage assessment

BE basic encyclopedia

BLS beach landing site

BMATT briefcase multimission advanced tactical terminal

bn battalion

BPS basic PSYOP study

BWS body-worn system

C2 command and control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP 1-02)

C3I command, control, communications, and intelligence

C4I command, control, communications, computers, and intelligence

C4IS command, control, communications, computers, and intelligence system

CA Civil Affairs; California

campaign A series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space. (JP 1-02)

campaign plan A plan for a series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space. (JP 1-02)

CAP3T CA plans, programs, and policy team

capability The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention.) (JP 1-02)

CARVER criticality, accessibility, recuperability, vulnerability, effect, and recognizability (memory aid)

CAS close air support

CBT combatting terrorism

CCI	controlled cryptographic items
CCIR	commander's critical information requirements
CD	counterdrug
CD-ROM	compact disc–read-only memory
CED	captured enemy document
cell	Small group of individuals who work together for clandestine or subversive purposes. (JP 1-02)
CEM	captured enemy material
CFSO	counterintelligence force protection source operations
CG	commanding general
chain of command	The succession of commanding officers from a superior to a subordinate through which command is exercised. Also called command channel.
CHATS	counterintelligence/HUMINT automated tool set
CI	civilian internee; counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)
CIA	Central Intelligence Agency
CID	Criminal Investigation Division
CI&I OPS WS	Counterintelligence and Interrogation Operations Workstation
CINC	commander in chief
civil assistance	Military necessity may require a commander to provide life-sustaining services, maintain order, or control distribution of goods and services within his assigned operational area. Civil assistance differs from other forms of civil administration because it is based on the commander's decision. All other forms of civil administration require NCA approval. (FM 41-10)
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJSOTF	combined joint special operations task force
CJTF	commander, joint task force
CLPM	Command Language Program Manager
CM&D	collection management and dissemination
CMA	collection management authority
CMEC	Captured Materiel Exploitation Center

CMF career management field

CMO civil-military operations

CMOC civil-military operations center

CMOPB CMO preparation of the battlespace

CO Colorado

COA course of action

coalition An ad hoc arrangement between two or more nations for common action. (JP 1-02)

COCOM combatant command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

COE common operating environment

col collate

collateral activities The inherent capabilities of all military forces may periodically be applied to accomplish missions other than those for which the forces are principally organized, trained, and equipped. Collateral activities in which special operations forces, by virtue of inherent capabilities, may be tasked to participate include humanitarian assistance, security assistance, search and rescue, counterdrug, antiterrorism and other security activities, and special activities. (JP 3-05)

collateral damage Unintended and undesirable civilian personnel injuries or material damage adjacent to a target produced by the effects of demolition weapons.

combat information Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (JP 1-02)

combatant command (command authority) Nontransferable command authority established by Title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be

exercised through the commanders of subordinate organizations. Normally, this authority is exercised through the subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). (JP 1-02)

combined Between two or more forces or agencies of two or more allies. (JP 1-02)

comdt commandant

COMINT communications intelligence

comm communications

command 1. The authority that a commander in the Armed Forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. 2. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action. 3. A unit or units, an organization, or an area under the command of one individual. (JP 1-02)

COMMZ communications zone

compromise The known or suspected exposure of clandestine personnel, installations, or other assets, or of classified information or material, to an unauthorized person. (JP 1-02)

COMPUSEC computer security

COMSEC communications security

conditions Those external elements that affect a target audience but over which they have little or no control. Conditions may be man-made or environmental in nature. (FM 3-05.30)

CONPLAN concept plan

contingency An emergency involving military forces caused by natural disasters, terrorists, subversives, or by required military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response, and special procedures to ensure the safety and readiness of personnel, installations, and equipment. (JP 1-02)

CONUS continental United States

conventional forces Those forces capable of conducting operations using nonnuclear weapons. (JP 1-02)

COTS commercial-off-the-shelf

counterinsurgency Those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency. (JP 1-02*)*

country team The senior, in-country, United States coordinating and supervising body, headed by the Chief of the United States diplomatic mission, and composed of the senior member of each represented United States department or agency, as desired by the Chief of the U.S. diplomatic mission. (JP 1-02)

CP counterproliferation

CP-WMD counterproliferation of weapons of mass destruction

CRDL collateral-recurring document listing

crisis An incident or situation involving a threat to the United States, its territories, citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, political, or military importance that commitment of U.S. military forces and resources is contemplated to achieve national objectives. (JP 1-02)

critical information Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02)

CRRC combat rubber raiding craft

CS combat support

CSAR combat search and rescue—A specific task performed by rescue forces to effect the recovery of distressed personnel during war or military operations other than war. (JP 1-02)

CSEL combat survivor evader locator (radio)

CSS combat service support

cur current

DA direct action; Department of Army

DACAP Department of Army Cryptographic Access Program

DART Disaster Assistance Response Team

DASO DODIIS Access Security Officer

data Representation of facts, concepts, or instruction in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (JP 1-02)

DCI Director of Central Intelligence

DCO Defense Coordinating Officer

DCO/RACA deputy commanding officer for Research, Analysis, and Civilian Affairs

DCSFDI Deputy Chief of Staff for Force Development and Integration

DCSIM Deputy Chief of Staff for Information Management

DCSINT Deputy Chief of Staff for Intelligence

DCSOPS Deputy Chief of Staff for Operations and Plans

D-day unnamed day on which operations commence or are scheduled to commence (JP 1-02)

deception Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (JP 1-02)

del delivery

denied area An area under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities. (JP 1-02)

det determine

DF direction finding

DHS Defense HUMINT Service

DIA Defense Intelligence Agency

DIAM Defense Intelligence Agency Manual

DII defense information infrastructure

direct liaison authorized That authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command. Direct liaison authorized is more applicable to planning than operations and always carries with it the requirement of keeping the commander granting direct liaison authorized informed. Direct liaison authorized is a coordination relationship, not an authority through which command may be exercised. (JP 1-02)

DIRLAUTH direct liaison authority

DIRNSA Director, National Security Agency

DISA Defense Information Systems Agency

DISC4 Director of Information Systems Command, Control, Communications, and Computers

DISN Defense Information Systems Network

diversion The act of drawing the attention and forces of an enemy from the point of the principal operation; an attack, alarm, or feint that diverts attention. (JP 1-02)

DLA Defense Logistics Agency

DOCEX	document exploitation
DOD	Department of Defense
DODAAC	Department of Defense activity address code
DODIIS	Department of Defense Intelligence Information System
DODIPP	Department of Defense Intelligence Production Program
DOE	Department of Energy
DOS	Department of State
DS	direct support—1. A mission requiring a force to support another specific force and authorizing it to answer to the supported force's request for assistance. 2. In NATO, the support provided by a unit or formation but required to give priority to the support required by that unit or formation. (FM 101-5-1)
DST	decision support template
DTSS	Digital Topographic Support System
DTSS-D	Digital Topographic Support System-Deployable
DZ	drop zone
E&E	evasion and escape
E&R	evasion and recovery
EA	electronic attack
EAC	echelons above corps
EACIC	echelons above corps intelligence center
EEFI	essential elements of friendly information
EEI	essential elements of information
EIW	Enhanced Imagery Workstation
ELINT	electronic intelligence
ELT	electronic light table
E-mail	electronic mail
EPB	electronic preparation of the battlespace
EPW	enemy prisoner of war
EPW/CI	enemy prisoner of war/civilian internee
ER	electronic reconnaissance
ERDAS	Earth Resources Data Analysis System
ES	electronic warfare support
est	estimate
eval	evaluate

EW electronic warfare—Any military action involving the use of electromagnetic and directed energy to control, determine, exploit the electromagnetic spectrum, or to attack the enemy. (JP 1-02)

executive order Order issued by the President by virtue of the authority vested in him by the Constitution or by an act of Congress. It has the force of law. (AR 310-25)

exfiltration The removal of personnel or units from areas under enemy control. (JP 1-02)

FA feasibility assessment

FALOP forward area limited observing program

FARP forward arming and refueling point

fax facsimile

FBIS Foreign Broadcast Information Service

FCO federal coordinating officer

FEMA Federal Emergency Management Agency

FFIR friendly forces information requirements

FID foreign internal defense—Participation by civilian and military agencies of a government in any of the action programs taken by another government to free and protect its society from subversion, lawlessness, and insurgency. (JP 1-02)

FIS foreign intelligence services

FISINT foreign instrumentation signals intelligence

FL Florida

flt flight

FM field manual

FOB forward operational base—In special operations, a base usually located in friendly territory or afloat that is established to extend command and control or communications or to provide support for training and tactical operations. Facilities may be established for temporary or longer duration operations and may include an airfield or an unimproved airstrip, an anchorage, or a pier. The forward operational base may be the location of special operations component headquarters or a smaller unit controlled or supported by a main operational base. (JP 1-02)

force multiplier A capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment. (JP 1-02)

foreign nation support The identification, coordination, and acquisition of foreign nation resources, such as supplies, material, and labor, to support U.S. military forces and operations. (JP 3-57)

FP force protection—Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combatting terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (JP 1-02)

FPA foreign policy advisor

FRAGO fragmentary order

FSO fire support officer

FTP file transfer protocol

functional component command A command normally, but not necessarily, composed of forces of two or more Military Departments which may be established across the range of military operations to perform particular operational missions that may be of short duration or may extend over a period of time. (JP 1-02)

fwd forward

G1 Assistant Chief of Staff, G1 (Personnel)

G2 Assistant Chief of Staff, G2 (Intelligence)

G2X G2 CI/HUMINT staff element

G3 Assistant Chief of Staff, G3 (Operations and Plans)

G4 Assistant Chief of Staff, G4 (Logistics)

G5 Assistant Chief of Staff, G5 (Civil Affairs)

GA Georgia

GCCS global command and control system

GDIP General Defense Intelligence Plan

gen generate

GI&S geospatial information and services

GMDB gridded meteorological database

GOTS Government-off-the-shelf

GS general support—Support given to the supported force as a whole and not to any particular subdivision thereof. (FM 101-5-1)

GSC group support company

GW guerrilla warfare

HA humanitarian assistance

hazard Any actual or potential condition that can cause injury, illness, or death of personnel, damage to or loss of equipment, property or mission degradation. (FM 101-5)

HD humanitarian demining

HF high frequency

HHC headquarters and headquarters company

HI Hawaii

HIC human intelligence collector

HN host nation—nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory. (JP 1-02)

HPT high-payoff target

HQ headquarters

HQDA Headquarters, Department of the Army

HUMINT human intelligence—A category of intelligence derived from information collected and provided by human sources. (JP 1-02)

HVT high-value target

I&W indications and warning

IAP international airport

IAW in accordance with

IBOS intelligence battlefield operating system

IBS Intelligence Broadcast System

IDHS intelligence data handling system

IESS image exploitation support system

IEW intelligence and electronic warfare

IIR intelligence information report

IMC international Morse code

IMETS Integrated Meteorological System

IMETS-L Integrated Meteorological System-Light

IMINT imagery intelligence

indicator In intelligence usage, an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action.

infiltration The movement through or into an area or territory occupied by either friendly or enemy troops or organizations. The movement is made either by small groups or by individuals at extended or irregular intervals. When used in connection with the enemy, it infers that contact is avoided. (JP 1-02)

information Facts, data, or instructions in any medium or form. (JP 1-02)

INFOSEC information security

INSCOM	United States Army Intelligence and Security Command
insurgency	1. An organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict. (JP 1-02) 2. A condition resulting from a revolt or insurrection against a constituted government which falls short of civil war. (FM 41-10)
intel	intelligence
INTELINK	intelligence link
intelligence requirements	Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (JP 1-02)
internal defense and development	The full range of measures taken by a nation to promote its growth and to protect itself from subversion, lawlessness, and insurgency. It focuses on building viable institutions (political, economic, social, and military) that respond to the needs of society. (JP 1-02)
INTSUM	intelligence summary
IO	information operations
IPA	intelligence production agency
IPB	intelligence preparation of the battlefield
IPL	Imagery Product Library
IR	information requirement
I-REMBASS	improved-remotely monitored battlefield sensor system
ISA	International Standardization Agreement
ISE	intelligence support element
ISOFAC	isolation facility
ISS	information systems security
ITRT	Individual Tactical Reporting Tool
IW	information warfare
J2	Intelligence Directorate
J2A	Deputy Director for Administration
J2J	Deputy Director for Joint Staff Support
J2M	Deputy Director for Crisis Management
J2O	Deputy Director for Crisis Operations
J2P	Deputy Director for Assessment, Doctrine Requirements, and Capabilities
J2T	Deputy Director for Targeting Support
J2X	Deputy Director for CI/HUMINT

J3 Operations Directorate

J6 Command, Control, Communications, and Computer Systems Directorate

JAC joint analysis center

JCS Joint Chiefs of Staff

JDISS Joint Deployable Intelligence Support System

JFC joint force commander

JFLCC joint force land component commander

JFSOCC joint forces special operations component commander

JIC joint intelligence center

JICCENT Joint Intelligence Center, United States Central Command

JICJFCOM Joint Intelligence Center, United States Joint Forces Command

JICPAC Joint Intelligence Center, United States Pacific Command

JICSOUTH Joint Intelligence Center, United States Southern Command

JIF joint interrogation facility

JISE joint intelligence support element

JMCIS Joint Maritime Command Information System

JMRR Joint Monthly Readiness Review

JOA joint operations area

joint Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (JP 1-02)

joint force A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (JP 1-02)

joint operations A general term to describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces. (JP 1-02)

JOPES Joint Operation Planning and Execution System

JP joint publication

JPOTF joint psychological operations task force

JSCP Joint Strategic Capabilities Plan

JSOA joint special operations area

JSOAC joint special operations air component

JSOTF joint special operations task force

JTCB Joint Targeting Coordination Board

JTF joint task force—A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. (JP 1-02)

JTT(B) Joint Tactical Terminal-Briefcase

JTWS Joint Threat Warning System

JWICS Joint Worldwide Intelligence Communications System

kbps kilobytes per second

KY Kentucky

LA Louisiana

LAN local area network

LE liaison element

LIWA Land Information Warfare Activity

LLVI low-level voice intercept

LNO liaison officer

LOC line of communication

LZ landing zone

MAA mission area analysis

MACOM major Army command

MAGTF C4IS Marine Corps Air-Ground Task Force C4I System

MASINT measurement and signature intelligence

Mbps megabytes per second

MCOO modified combined obstacles overlay

MCS military capabilities study

MD Maryland

MDCI multidiscipline counterintelligence

MDITDS Migration Defense Intelligence Threat Data System

MDMP military decision-making process

media Transmitters of information and psychological products.

METOC meteorological and oceanographic

METT-TC mission, enemy, terrain and weather, troops and support available, time available, and civil considerations

MFF military free-fall

mgt management

MI military intelligence

MID military intelligence detachment

MIDB modernized integrated database

MIIDS/IDB Military Intelligence Integrated Data System/Integrated Database

military civic action The use of preponderantly indigenous military forces on projects useful to the local population at all levels in such fields as education, training, public works, agriculture, transportation, communications, health, sanitation, and others contributing to economic and social development, which would also serve to improve the standing of the military forces with the population. (U.S. forces may at times advise or engage in military civic action in overseas areas.) (JP 1-02)

MLCOA most likely course of action

MOOTW military operations other than war—Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and occur before, during, and after war. (JP 1-02)

MOS military occupational specialty

MP military police

MPA mission planning agent

MSC major subordinate command

MSI multispectral imagery

MSP mission support plan

MSU major subordinate unit

MTP mission tasking package

MTS man-transportable SOCRATES

MTT mobile training team—A team consisting of one or more U.S. military or civilian personnel sent on temporary duty, often to a foreign nation, to give instruction. The mission of the team is to train indigenous personnel to operate, maintain, and employ weapons and support systems, or to develop a self-training capability in a particular skill. The National Command Authorities may direct a team to train either military or civilian indigenous personnel, depending upon host nation requests. (JP 1-02)

MTW major theater war

multinational operations A collective term to describe military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance. (JP 1-02)

NAI	named area of interest
NATO	North Atlantic Treaty Organization
NAVSOF	Navy special operations forces
NBC	nuclear, biological, and chemical
NC	North Carolina
NCA	National Command Authorities—The President and the Secretary of Defense or their duly deputized alternates or successors. (JP 1-02)
NCO	noncommissioned officer
NEO	noncombatant evacuation operations
NFA	no-fire area
NGIC	National Ground Intelligence Center
NGO	nongovernmental organization
NIC	National Intelligence Community
NIMA	National Imagery and Mapping Agency
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Intelligence Support Team
NMCC	National Military Command Center
NMJIC	National Military Joint Intelligence Center
NRT	near-real-time
NSA	National Security Agency
NSC	National Security Council
NSRL	National SIGINT Requirements List
NSWU	naval special warfare unit
NT	network termination
NY	New York
O&I	operations and intelligence
OA	objective area
OB	order of battle
OCONUS	outside the continental United States
ODCSINT	Office of the Deputy Chief of Staff for Intelligence
ODCSOPS	Office of the Deputy Chief of Staff for Operations
OEM	office of emergency management
OFDA	Office of Foreign Disaster Assistance
OH	Ohio

OIC officer in charge

OMA Office of Military Affairs

OPCEN operations center

OPCON operational control—Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally, this authority is exercised through subordinate joint force commanders and Service or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. (JP 1-02)

operational continuum The general states of peace, conflict, and war within which various types of military operations are conducted.

operational environment A composite of the conditions, circumstances, and influences which affect the employment of military forces and bear on the decisions of the unit commander. Some examples are: a. permissive environment—operational environment in which host country military and law enforcement agencies have control and the intent and capability to assist operations that a unit intends to conduct. b. uncertain environment—operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have totally effective control of the territory and population in the intended area of operations. c. hostile environment—operational environment in which hostile forces have control and the intent and capability to effectively oppose or react to the operations a unit intends to conduct. (JP 1-02)

OPLAN operation plan

OPORD operation order

ops operations

OPSEC operations security—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that

	can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
PA	public affairs; Pennsylvania
paramilitary forces	Forces or groups which are distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission. (JP 1-02)
PC	personal computer
PDC	PSYOP development center
peacekeeping	Military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease-fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement. (JP 1-02)
PIR	priority intelligence requirements
PME	peacetime military engagement
POAS	PSYOP automated system
POC	point of contact
POE	plan of execution
POG	psychological operations group
POG(A)	psychological operations group (airborne)
POL	petroleum, oils, and lubricants
POLAD	political advisor
POM	program objective management
PONR	point of no return—A point along an aircraft track beyond which its endurance will not permit return to its own or some other associated base on its own fuel supply. (JP 1-02)
POTF	psychological operations task force
power	The ability or capacity to perform effectively or target audience effectiveness. (FM 33-1)
PR	personnel recovery
PRC	populace and resources control
pri	prioritize

product Any visual, audio, or audiovisual item generated and disseminated in support of a PSYOP program.

propaganda Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. See also black propaganda; grey propaganda; white propaganda. (JP 1-02)

PSYOP Psychological Operations—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign government, organizations, groups, and individuals. The purpose of Psychological Operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 1-02)

PW prisoner of war

RC Reserve Component

RCERT Regional Computer Emergency Response Team

rec received

REDTRAIN readiness training

refugee A civilian who, by reason of real or imagined danger, has left home to seek safety elsewhere. (JP 1-02)

resistance movement An organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability. (JP 1-02)

RFA restricted fire area

RFI request for information

rgt regiment

RII request for intelligence information—RIIs are usually generated by a subordinate command, but may be sent laterally or down as taskings, to obtain intelligence or information collection support for needs that exceed organic capabilities. Requests received that exceed organic requirements are always consolidated and forwarded to the next higher echelon as RII. When prepared, the RII must indicate the degree of urgency and the type of request being made. When received, the requests are assigned priorities depending on the criticality and the timeline specified by the requester.

risk Chance of hazard or bad consequences; the probability of exposure to chance of injury or loss from a hazard; risk level is expressed in terms of hazard probability and severity. (FM 101-5)

risk assessment Identification and assessment of hazards (first two steps of risk management process); an identified hazard is assessed to determine the risk (both the probability of occurrence and

resulting severity) of a hazardous incident due to the presence of the hazard.

RMS requirements management system

ROE rules of engagement

rqmts requirements

RRD Ranger reconnaissance detachment

RSOC regional SIGINT operations center

RTSO remote terminal security officer

RWR radar warning receiver

RZ recovery zone

S2 intelligence officer

S2X S2 CI/HUMINT staff element

S3 operations and training officer

S4 logistics officer

S5 civil-military operations officer

S6 signal officer

S&T scientific and technical

SA security assistance—Group of programs authorized by the Foreign Assistance Act of 1961, as amended, and the Arms Export Control Act of 1976, as amended, or other related statutes by which the United States provides defense articles, military training, and other defense-related services, by grant, loan, credit, or cash sales in furtherance of national policies and objectives. (JP 1-02)

SACEUR supreme allied commander, Europe

SAEDA Subversion and Espionage Directed Against U.S. Army

SAFE selected area for evasion

SAID SAFE area intelligence description

SAM surface-to-air missile

san sanitize

SAR search and rescue

SBU sensitive but unclassified

SCAMPI (Is not an acronym)

SCI sensitive compartmented information

SCIF sensitive compartmented information facility

SCIRDL sensitive compartmented information-recurring document listing

SCO	state coordinating officer
SDR	source-directed requirement
SDV	SEAL delivery vehicle
SEAL	sea-air-land team
SECDEF	Secretary of Defense
security assistance organization	All Department of Defense elements located in a foreign country with assigned responsibilities for carrying out security assistance management functions. It includes military assistance advisory groups, military missions and groups, offices of defense and military cooperation, liaison groups, and defense attaché personnel designated to perform security assistance functions. (JP 1-02)
SERER	survival, evasion, resistance, escape, recovery
service component command	A command consisting of the Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under the command, including the support forces that have been assigned to a combatant command, or further assigned to a subordinate unified command or joint task force. (JP 1-02)
SF	Special Forces
SFG	Special Forces group
SFG(A)	Special Forces group (airborne)
SFOB	Special Forces operational base
SFODA	Special Forces operational detachment A
SFODB	Special Forces operational detachment B
SHF	superhigh frequency
SIDS	Secondary Imagery Dissemination System
sig	signal
SIGCEN	signal center
SIGINT	signals intelligence
SII	statement of intelligence interest
SIO	senior intelligence officer
SIPRNET	SECRET Internet Protocol Router Network
SIR	specific information requirement
SITMAP	situation map
SLP	seaward launch point
SO	special operations
SOAR	special operations aviation regiment

SOC special operations command

SOCCE special operations command and control element

SOCCENT Special Operations Component, United States Central Command

SOCEUR Special Operations Component, United States European Command

SOCJFCOM Special Operations Command, Joint Forces Command

SOCJIC Special Operations Command Joint Intelligence Center

SOCKOR Special Operations Command, Korea

SOCOORD special operations coordination element

SOCPAC Special Operations Component, United States Pacific Command

SOCRATES Special Operations Command, Research, Analysis, and Threat Evaluation System

SOCSOUTH Special Operations Component, United States Southern Command

SODARS special operations debrief and retrieval system

SOF special operations forces

SOFIV-M special operations forces intelligence vehicle (migration)

SOFTACS Special Operations Forces Tactical Assured Connectivity System

SOIO special operations information operations

SOMPF special operations mission planning folder

SOP standing operating procedure

SORTS Status of Resources and Training System

SOT-A special operations team A—A four-soldier team with specialized equipment designed to provide threat warning and/or situational awareness information to a supported commander through SIGINT/EW operations. These teams can operate independently or as augmentation to another SOF element.

SOTA SIGINT operational tasking authority—The authority delegated by Director, NSA, to the tactical commander to provide direct tasking on organic SIGINT/EW assets for SOF.

SOTSE special operations theater support element

SOWD special operations weather detachment

SOWT special operations weather team—A task-organized team of Air Force personnel organized, trained, and equipped to collect critical weather observations from data-sparse areas. These teams are trained to operate independently in permissive or semipermissive environments, or as augmentation to special operations elements in nonpermissive environments in direct support of special operations. (JP 1-02)

SPA special PSYOP assessment

spec special

SPS special PSYOP study

spt support

SPTCEN support center

sqdn squadron

SR special reconnaissance

SRP seaward recovery point

SRTD signals research and target development

SSC small-scale contingency

SSD strategic studies detachment

SSMS SOF SIGINT manpack system

SSO special security officer

STAR-T SHF triband advanced range-extension terminal

subversion Action designed to undermine the military, economic, psychological, or political strength or morale of a regime. (JP 1-02)

supported commander The commander having primary responsibility for all aspects of a task assigned by the Joint Strategic Capabilities Plan or other joint operation planning authority. In the context of joint operation planning, this term refers to the commander who prepares operation plans or operation orders in response to requirements of the Chairman of the Joint Chiefs of Staff. (JP 1-02)

supporting commander A commander who provides augmentation forces or other support to a supported commander or who develops a supporting plan. Includes the designated combatant commands and Defense agencies as appropriate. (JP 1-02)

SWO staff weather officer

T-1 1.544 megabytes per second

TA traffic analysis

TAAD target audience analysis detachment

TACON tactical control—Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and, usually, local direction and control of movements or maneuvers necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. (JP 1-02)

TACP	tactical air control party
TADIXS-B	tactical data information exchange system-B
TAI	target area of interest
TALP	Total Army Language Program
TAP	The Army Plan
target	A geographical area, complex, or installation planned for capture or destruction by military forces. (JP 1-02)
target audience	An individual or group selected for influence or attack by means of Psychological Operations. (JP 1-02)
TASKORD	tasking order
TBMCS	Theater Battle Management Core System
TCAE	technical control and analysis element
TDDS	tactical related applications (TRAP) data dissemination system
TDI	target data inventory
TECHINT	technical intelligence
technical control	The executive authority to regulate and supervise technical activities by providing specialized or professional guidance and direction.
TED	testing and evaluation detachment
TEMPEST	terminal electromagnetic pulse escape safeguard technique
TENCAP	Tactical Exploitation of National Capabilities Program
terrorism	The calculated use of unlawful violence or threat of unlawful violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (JP 1-02)
TGO	terminal guidance operations
tgt	target
theme	A subject, topic, or line of persuasion used to achieve a psychological objective.
threat	The ability of an enemy to limit, neutralize, or destroy the effectiveness of a current or projected mission organization or item of equipment. (TRADOC Reg 381-1)
thrt asmt	threat assessment
TIBS	tactical information broadcast service
TIP	target intelligence package
tng	training
TNOC	theater network operations center

TOE	table(s) of organization and equipment
TPB	tactical psychological operations battalion
TPL	time-phased line
TPT	tactical psychological operations team
TRADOC	United States Army Training and Doctrine Command
traffic analysis team	Task-organized element with necessary resources, attached to deploying commanders to exercise SIGINT collection management, analysis, and reporting functions.
TRIXS	tactical reconnaissance intelligence exchange system
T-SCIF	tactical SCIF
TSCM	technical surveillance countermeasures
TT	team transportable
TTP	tactics, techniques, and procedures
TVA	threat vulnerability assessment
UAV	unmanned aerial vehicle
UCMJ	Uniform Code of Military Justice
UHF	ultrahigh frequency
UK	United Kingdom
UN	United Nations
unified command	A command with a broad continuing mission under a single commander and composed of significant assigned components or two or more Military Departments, and which is established and so designated by the President, through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Also called unified combatant command. (JP 1-02)
unified command plan	The document, approved by the President, which sets forth basic guidance to all unified combatant commanders; establishes their missions, responsibilities, and force structure; delineates the general geographical area of responsibility for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders. (JP 1-02)
UNOSOM II	United Nations Operations in Somalia II
U.S.	United States
USACAPOC	United States Army Civil Affairs and Psychological Operations Command
USAF	United States Air Force
USAIC&FH	United States Army Intelligence Center and Fort Huachuca
USAID	United States Agency for International Development

USAJFKSWCS	United States Army John F. Kennedy Special Warfare Center and School
USAR	United States Army Reserve
USASFC	United States Army Special Forces Command
USASOC	United States Army Special Operations Command
USCENTCOM	United States Central Command
USCINCSOC	Commander in Chief, United States Special Operations Command
USEUCOM	United States European Command
USG	United States Government
USIA	United States Information Agency
USIGS	United States Imagery and Geospatial Services
USJFCOM	United States Joint Forces Command
USPACOM	United States Pacific Command
USR	unit status report
USSID	United States Signals Intelligence Directive
USSOCOM	United States Special Operations Command
USSPACECOM	United States Space Command
USTRANSCOM	United States Transportation Command
UT	Utah
UTM	universal transverse mercator
UW	unconventional warfare
UWO	underwater operations
VA	Virginia
val	validate
veh	vehicle
WA	Washington
WAN	wide area network
WMD	weapons of mass destruction
WXSAT	weather satellite

Bibliography

AR 525-17. *(S) Special Mission Badges and Credentials (U).* 30 August 1991.

AR 530-1. *Operations Security (OPSEC).* 3 March 1995.

CJCSI 5221.01A. *Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations*. 6 April 1999.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*. 1 February 1974.

DIAM 65-3-1. *(C) Standard Coding System Functional Classification Handbook (U)*. 1 February 1985.

Executive Order 12333, *United States Intelligence Activities.* 4 December 1981.

FM 3-0. *Operations.* 14 June 2001.

FM 3-05.20. *Special Forces Operations*. 26 June 2001.

FM 3-05.30. *Psychological Operations.* 19 June 2000.

FM 3-05.60. *Army Special Operations Forces Aviation Operations.* 16 October 2000.

FM 7-85. *Ranger Unit Operations*. 9 June 1987.

FM 34-1. *Intelligence and Electronic Warfare Operations*. 27 September 1994.

FM 34-2. *Collection Management and Synchronization Planning*. 8 March 1994.

FM 34-3. *Intelligence Analysis*. 15 March 1990.

FM 34-5. *(S) Human Intelligence and Related Counterintelligence Operations (U)*. 29 July 1994.

FM 34-8. *Combat Commander's Handbook on Intelligence*. 28 September 1992.

FM 34-40. *(S) Electronic Warfare Operations (U)*. 9 October 1987.

FM 34-52. *Intelligence Interrogation*. 28 September 1992.

FM 34-54. *Technical lntelligence*. 30 January 1998.

FM 34-60. *Counterintelligence.* 3 October 1995.

FM 34-81/AFM 105-4. *Weather Support for Army Tactical Operations*. 31 August 1989.

FM 34-130. *Intelligence Preparation of the Battlefield*. 8 July 1994.

FM 41-10. *Civil Affairs Operations.* 14 February 2000.

FM 100-20. *Military Operations In Low Intensity Conflict*. 5 December 1990.

FM 100-25. *Doctrine for Army Special Operations Forces*. 1 August 1999.

FM 101-5. *Staff Organization and Operations*. 31 May 1997.

FM 101-5-1/MCRP 5-2A. *Operational Terms and Graphics*. 30 September 1997.

JP 1. *Joint Warfare for the U.S. Armed Forces*. 10 January 1995.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 1 September 2000.

JP 2-0. *Doctrine for Intelligence Support to Joint Operations*. 9 March 2000.

JP 2-01. *Joint Intelligence Support to Military Operations*. 20 November 1996.

JP 2-02. *National Intelligence Support to Joint Operations*. 28 September 1998.

JP 2-03. *Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations*. 31 March 1999.

JP 3-0. *Doctrine for Joint Operations*. 1 February 1995.

JP 3-05. *Doctrine for Joint Special Operations*. 17 April 1998.

JP 3-05.3. *Joint Special Operations Operational Procedures*. 25 August 1993.

JP 3-05.5. *Joint Special Operations Targeting and Mission Planning Procedures*. 10 August 1993.

JP 3-50.3. *Joint Doctrine for Evasion and Recovery*. 6 September 1996.

JP 5-03.1. *Joint Operation Planning and Execution System, Volume 1 (Planning Policies and Procedures)*. 4 August 1993.

Roach, James S., Jr. *Joint Special Operations Targeting: An Alternate Scheme.* U.S. Army War College, Carlisle Barracks, PA 17013-5050. March 1989.

TC 34-55. *Imagery Intelligence*. 3 October 1988.

The following publication is automatically distributed to USASOC personnel.

USASOC Reg 381-1. *(S) Special Operations Debriefing and Retrieval System (SODARS) (U)*. 29 Nov 1999.

For a copy of the following publication, write to HQ, USSOCOM, 7701 Tampa Point Boulevard, ATTN: SOOP-JD, MacDill Air Force Base, FL 33621-5323.

USSOCOM Pub 1. *Special Operations in Peace and War*. 25 January 1996.

The following publication is automatically provided to users of SODARS.

USSOCOM SODARS Reference Guide. 9 April 1998.

Index

A

advanced operational base (AOB), 3-15
Air Force Special Operations Command (AFSOC), 6-10, 8-16, B-9
all-source production section (ASPS), 2-12, 3-8, 3-9, 3-19 through 3-21, 3-23
analysis and control team (ACT), 3-13, 3-14
area assessment, 1-15, 2-14
area of operations (AO), 1-4, 1-20, 2-8, 2-18, 5-4, 7-13, 8-9, 8-25
area of responsibility (AOR), 1-3, 2-7, 3-1, 3-8, 3-9, 3-15, 6-4
Army special operations aviation (ARSOA), v, 5-1 through 5-8, 8-11
Army special operations task force (ARSOTF), 3-5, 3-15, 3-16, 4-2, 5-5, 7-12, 8-10 through 8-12

B

battle damage assessment (BDA), 2-1, 2-20, 3-4, 3-8, 3-9, 3-11, 3-13, 3-14, 3-20, 4-5

C

Chairman, Joint Chiefs of Staff (CJCS), 1-20, 8-30, 8-32
Civil Affairs (CA), v, 1-3 through 1-6, 1-16, 1-17, 1-19, 7-1 through 7-13, 8-11
civil-military operations (CMO), 1-16, 1-17, 1-21, 7-1, 7-3, 7-8, 7-10 through 7-13
collateral activities, 1-18, 1-19, 2-4, 3-1, 3-10
collection management and dissemination (CM&D), 3-5, 3-8 through 3-10, 3-18 through 3-20, 4-4
combat search and rescue (CSAR), 1-18, 5-2
combatting terrorism (CBT), 1-6, 1-16, 2-20, 3-1, 3-4
commander in chief (CINC), 1-18 through 1-20, 2-1, 2-16, 2-19, 6-2, 7-2, 8-14, 8-21, 8-24 through 8-26, B-1
Commander in Chief, United States Special Operations Command (USCINCSOC), 8-22 through 8-24
commander's critical information requirements (CCIR), 2-5
communications security (COMSEC), 3-10, 3-11, 8-19
communications zone (COMMZ), 3-12, 3-14
concept plan (CONPLAN), 3-3, 3-4, 3-13, 4-2, 4-3
counterintelligence (CI), 2-3, 2-4, 2-14 through 2-16, 3-11, 3-12, 3-14, 3-20, 4-4, 4-6, 5-7, 6-8, 6-9, 7-12, 8-8, 8-15
country team, 1-1, 7-6
course of action (COA), 1-12, 2-8, 2-11, 2-18, 7-9, 7-11, 8-7, B-4, B-5
criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER), 2-19, 4-3

D

deception, 1-4, 1-17, 2-4, 2-16, 3-5, 3-20, 4-3, 4-4, 5-7, 6-6, 6-9, 6-11, B-8
Department of State (DOS), 1-16, 6-7
direct action (DA), 1-6, 1-15, 2-4, 2-5, 3-1, 3-3, 3-5, 4-1, 5-2, 5-5, C-1, C-2

E

electronic warfare (EW), 1-17, 2-3, 3-5, 3-10, 3-21, 3-22, 4-3, 4-6, 6-8, 6-11, 8-14, 8-22
enemy prisoner of war (EPW), 2-4, 3-12, 3-21, 4-6, 5-6, 6-3, 6-5, 6-8, 6-11
essential elements of friendly information (EEFI), 2-5, 3-11, 3-12, 3-14, 5-3
evasion and recovery (E&R), 5-2, 5-3

F

feasibility assessment (FA), B-2 through B-6
force protection (FP), 1-5, 1-7, 2-1, 2-16, 2-20, 3-9 through 3-14, 3-20, 4-4, 7-9, 8-6, A-7
foreign intelligence services (FIS), 2-15, 3-12, 3-14
foreign internal defense (FID), 1-6, 1-16, 3-1, 3-2, 3-5, 3-10, 3-11, 7-5, C-3, C-4
forward operational base (FOB), 1-22, 3-13 through 3-18, 8-5, 8-11

G

global command and control system (GCCS), 2-3, 8-2, 8-19
group support company (GSC), 3-8

H

headquarters and headquarters company (HHC), 5-1, 6-2, 6-3, 7-6
host nation (HN), 1-6, 1-16, 1-18, 1-19, 2-4, 2-6, 2-15, 3-2, 3-12, 7-9

human intelligence (HUMINT), 1-16, 2-4, 2-14, 2-15, 3-11, 3-12, 3-14, 3-20, 3-21, 3-23, 4-6, 5-6, 5-7, 6-7, 6-8, 7-12, 8-28, 8-31, 8-32

I

imagery intelligence (IMINT), 2-2, 2-14, 2-15, 3-9, 3-13, 3-14, 3-23, 4-6, 5-6, 5-7, 6-8, 6-9, 7-11, 7-12, 8-6, 8-16, 8-22
indications and warning (I&W), 2-1, 2-20, 3-8, 3-9, 3-12, 3-14, 8-7, 8-31
information operations (IO), 1-16 through 1-18, 3-1, 3-5, 6-11
information requirement (IR), 1-14, 2-6, 2-9, 2-11, 3-5, 3-8, 3-11, 6-4, 6-7, 8-15
intelligence
  cycle, 2-1, 2-6, 2-9 through 2-13, 2-19, 2-20, 3-18, 8-3
  disciplines, 2-14 through 2-16, 6-8, 6-9
intelligence information report (IIR), 3-12 through 3-14
intelligence preparation of the battlefield (IPB), 2-6, 2-8, 2-11, 2-17, 2-18, 2-20, 3-2, 3-14, 4-2, 5-4, 5-5, 6-6, 7-10, 8-6, 8-7
isolation facility (ISOFAC), 3-17

J

Joint Chiefs of Staff (JCS), 1-15, 8-3, 8-18, 8-30
joint force commander (JFC), 1-1, 1-3 through 1-7, 1-11, 1-12, 1-18, 1-20 through 1-22, B-1, B-2
joint force special operations component commander (JFSOCC), 1-21, 1-22, 3-13, A-3, B-1, B-3
joint intelligence center (JIC), 2-2, 7-11, 8-25 through 8-27, 8-31, A-6
joint special operations air component (JSOAC), 5-5
joint special operations area (JSOA), 1-20, 2-19, 3-15, B-3
joint special operations task force (JSOTF), 1-21, 3-15, 4-2, 4-3, 4-6, 5-5, 7-5, 7-12, 8-24
Joint Targeting Coordination Board (JTCB), 1-20, 1-21, 1-22
joint task force (JTF), 1-3, 1-21, A-6, A-7
Joint Worldwide Intelligence Communications System (JWICS), 8-1, 8-4, 8-5, A-6

M

meteorological and oceanographic (METOC), 8-5
military intelligence detachment (MID), 3-6 through 3-10, 3-14, 3-17 through 3-19, 4-2 through 4-4, 4-6
military operations other than war (MOOTW), v, 1-3, 1-5 through 1-7, 1-10, 8-10
mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC), 3-18, 7-2
mission planning agent (MPA), B-1 through B-5
missions:
  ARSOA, 5-1, 5-2
  ARSOF, 1-15 through 1-17
  CA, 7-1, 7-2
  PSYOP, 6-1, 6-2
  Ranger, 4-1, 4-2
  SF, 3-1 through 3-5
mobile training team (MTT), 1-19, 3-10, 3-11, 3-22
multidiscipline counterintelligence (MDCI), 2-10, 2-11, 2-16, 2-20, 3-20, 4-6, 5-7, 6-6

N

named area of interest (NAI), 2-11, 2-18, 2-19
National Command Authorities (NCA), 1-1, 1-9, 1-15, 1-20, 7-2, 8-30
nongovernmental organization (NGO), 1-19, A-1, A-4, A-8, A-9
North Atlantic Treaty Organization (NATO), 8-3, A-9
nuclear, biological, and chemical (NBC), 3-4, 4-5, B-4, B-7

O

offense, 1-3
operations center (OPCEN), 3-6, 3-13, 3-14, 3-16 through 3-18
operations security (OPSEC), 1-17, 2-16, 3-12, 3-14, 3-20, 4-4, 6-9, 6-11

P

personnel recovery (PR), 3-10, 3-11
plan of execution (POE), B-1, B-2, B-5, B-6
priority intelligence requirements (PIR), 2-4, 2-6, 2-9, 2-11, 3-8, 3-13
psychological operations (PSYOP), v, 1-16, 1-18, 1-19, 6-1 through 6-11, 8-10

R

Ranger, v, 3-3, 4-1 through 4-7, 8-6 through 8-9
request for information (RFI), 3-8, 8-11, 8-18, 8-29
request for intelligence information (RII), 3-8, 3-13, 4-4, 5-7, 7-11
rules of engagement (ROE), 1-7, 1-13

S

secondary imagery dissemination system (SIDS), 3-9
senior intelligence officer (SIO), 3-6, 3-15, 6-3, 6-7
sensitive compartmented information (SCI), 3-6, 3-8, 3-13, 8-7, 8-9, 8-10, 8-20, 8-21, 8-28
sensitive compartmented information facility (SCIF), 3-6, 3-8, 3-13
sensitive compartmented information-recurring document listing (SCIRDL), 3-9
SIGINT operational tasking authority (SOTA), 3-9
signal center (SIGCEN), 3-16
signals intelligence (SIGINT), 2-3, 2-14, 2-15, 3-7, 3-9 through 3-11, 3-21, 3-22, 4-6, 5-6, 6-5, 6-8, 7-11, 8-6 through 8-8, 8-14 through 8-16, 8-18, 8-32
situation map (SITMAP), 3-8
source-directed requirement (SDR), 3-9
Special Forces (SF), 1-4, 1-18, 1-19, 3-1 through 3-24
Special Forces Group (Airborne) (SFG[A]), 3-1, 3-6, 3-7, 3-9, 3-10, 3-15, 3-22
Special Forces operational base (SFOB), 1-22, 2-17, 3-6, 3-8, 3-12, 3-15 through 3-18, 3-20, 8-5
Special Forces operational detachment A (SFODA), 2-4, 3-13, 3-15 through 3-18, 3-22, 3-23
Special Forces operational detachment B (SFODB), 3-13, 3-18
special operations command (SOC), 1-5, 1-21, 2-2, 2-7, 3-24, 5-5, 6-4, 6-7, 6-9, 7-2, 7-11, 8-26 through 8-28
special operations command and control element (SOCCE), 3-15, 3-16
Special Operations Command, Research, Analysis, and Threat Evaluation System (SOCRATES), 8-4 through 8-6, 8-18, 8-25
special operations coordination element (SOCOORD), 3-15, 3-16
special operations forces (SOF), 1-5, 1-12, 1-15, 1-19 through 1-22, 2-7, 2-14, 2-17, 2-19, 3-3, 3-4, 3-10, 3-11, 3-24, 5-2, 5-5, 8-5, 8-22, 8-24, 8-25, 8-28
special operations mission planning folder (SOMPF), 3-3, B-1 through B-10
special operations team A (SOT-A), 2-2, 3-8 through 3-11, 3-13, 3-21, 3-22, 4-6, 5-6, 7-11
special operations weather team (SOWT), 2-8, 2-18, 3-6, 3-18, 4-4, 5-8, 7-12, 8-8
special reconnaissance (SR), 1-15, 1-16, 2-14, 2-15, 3-1, 3-3 through 3-5, 5-2, C-1, C-2
specific information requirement (SIR), 3-8, 3-13
stability operations, 1-4, 1-19, 2-15
staff weather officer (SWO), 3-6, 3-18
standing operating procedure (SOP), 5-7
statement of intelligence interest (SII), 3-9, 8-15
Subversion and Espionage Directed Against the Army (SAEDA), 3-12, 3-14, 8-16
support center (SPTCEN), 3-16
support operations, 1-4, 1-19, 2-15

T

Tactical Air Control Party (TACP), 3-17
target intelligence package (TIP), 3-3, 3-8, 3-13, 3-24, 4-4, B-5, C-1 through C-4
targeting, 1-19 through 1-22, 2-19, 2-20, 3-6, 3-7, 3-18, 3-19, 3-24, 8-6, 8-27
tasking order (TASKORD), 2-8
traffic analysis team (SIGINT) (TA team), 3-9 through 3-11

U

unconventional warfare (UW), 1-15, 1-19, 3-1 through 3-2, 3-5, 3-20, 7-5, 7-6, C-3, C-4
United States Army John F. Kennedy Special Warfare Center and School (USAJFKSWCS), vi, 1-8, 2-7, 8-14, 8-15, 8-17
United States Army Special Operations Command (USASOC), 1-8, 2-2, 2-7, 2-10, 3-23, 3-24, 4-6, 5-6, 5-8, 6-10, 7-13, 8-4, 8-11, 8-13 through 8-21
United States Special Operations Command (USSOCOM), 1-18, 1-21, 2-2, 2-7, 3-23, 3-24, 4-6, 5-2, 8-6, 8-8, 8-10, 8-11, 8-14, 8-16, 8-17, 8-21 through 8-25

W

weapons of mass destruction (WMD), 1-17, 3-4

FM 3-05.102
31 AUGUST 2001

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
0124107

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number 114874, requirements for FM 3-05.102.

PIN: 079253-000