ATTP 3-90.15 (FM 3-90.15)

Site Exploitation Operations

JULY 2010

Headquarters, Department of the Army

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

Army Tactics, Techniques, and Procedures
No. 3-90.15

Headquarters
Department of the Army
Washington, DC, 8 July 2010

Site Exploitation Operations

Contents

***This publication supersedes FM 3-90.15, 25 April 2007.**

Figures

Tables

Preface

This Army tactics, techniques, and procedures provides doctrinal guidance and considerations for Army forces conducting site exploitation operations. It replaces FM 3-90.15, *Sensitive Site Operations*, 25 April 2007. Site exploitation doctrine now includes all sites that have the potential to yield valuable information, whether or not they are designated as sensitive. Site exploitation is an enduring and integral mission in support of full spectrum operations.

This manual rescinds *sensitive site exploitation* as a doctrinal term. The former definition of *sensitive site exploitation* appeared in the 2007 edition of FM 3-90.15. That definition, which had originated as an Army term, also appeared in JP 1-02 but will be removed. This manual redefines *site exploitation*, which appeared in the 2007 edition of FM 3-90.15. The new definition of site exploitation will appear in the next revision of FM 1-02.

When joint or Army terms are used and their definitions included in the text, those terms are italicized, and the number of the proponent manual follows the definition.

This manual is organized into three chapters and two appendixes. Chapter 1 discusses conducting site exploitation operations, with an emphasis on the operations process, the purposes for site exploitation, and the framework for executing site exploitation operations. In chapter 1, this manual establishes the new doctrinal definition for the term *site exploitation*. Chapter 2 discusses specialized Army assets that support site exploitation. Chapter 3 discusses considerations related to sensitive sites. Sensitive sites are described in terms of a broad range of risks and challenges, not just weapons of mass destruction. Appendix A discusses joint and national organizations that support site exploitation. Appendix B discusses evidence collection, handling, and documentation, to support units that must handle evidence without the help of trained law enforcement personnel.

This publication applies to the Active Army, Army National Guard (ARNG)/Army National Guard of the United Stated (ARNGUS), and United States Army Reserve (USAR) unless otherwise stated. This manual does not apply to site exploitation operations conducted by special operations forces.

United States Army Training and Doctrine Command (TRADOC) is the proponent for this publication. The preparing agency is the Combined Arms Doctrine Directorate, U.S. Army Combined Arms Center. Send written comments and recommendations on Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: Commander, U.S. Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-CD (ATTP 3-90.15), 300 McPherson Avenue (Building 463), Fort Leavenworth, KS 66027-1352. Send comments and recommendations by e-mail to leav-cadd-web-cadd@conus.army.mil. Follow the DA Form 2028 format or submit and electronic DA Form 2028.

This page intentionally left blank.

Chapter 1

Conducting Site Exploitation Operations

This chapter defines site exploitation and discusses the operational environment as it relates to site exploitation. Army forces conduct site exploitation operations in support of full spectrum operations. The brigade combat team is the primary Army unit that conducts site exploitation operations, in coordination with other military or civilian organizations. The purposes of a site exploitation operation guide all related actions. Army site exploitation forces plan, prepare, execute, and assess site exploitation operations using the operations process. Within this process, site exploitation forces execute operations based on a framework of four actions: search, collect, analyze, and disseminate.

SITE EXPLOITATION DEFINED

1-1. ***Site exploitation*** **is systematically searching for and collecting information, material, and persons from a designated location and analyzing them to answer information requirements, facilitate subsequent operations, or support criminal prosecution.** Site exploitation (SE) contributes to *exploitation*, defined as taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes (JP 1-02). A site, in general, is a location that potentially contains valuable information. Site exploitation operations doctrine describes a systematic and comprehensive approach to obtaining information of value from a site for exploitation.

1-2. Information at a site may take an unlimited variety of forms. In the context of search and collection, information encompasses all potential sources of *information*—defined as facts, data, or instructions in any medium or form (JP 3-13.1). Media can include commonly considered information sources, such as documents, computers, and recordings. Additionally, materials such as weapons, ammunition, equipment, chemicals, and supplies can be collected and analyzed. Furthermore, human sources can provide information. Generally speaking, SE forces search for and collect persons. Therefore, to encompass *all potential sources of information*, this discussion uses the acronym IMP to refer to information (in any medium or form), material, or persons that can be collected and analyzed to produce intelligence.

1-3. Searching, in the context of SE, refers to using systematic procedures and appropriate equipment to identify potentially valuable IMP, based on specific purposes (see paragraph 1-5). Collecting refers to gathering and preserving IMP identified as potentially valuable. Analyzing IMP on-site generally refers to determining the actual value and relevance of the IMP collected, in relation to operational purposes and to information and intelligence already known. Initially, SE forces analyze the IMP collected on-site. They transfer selected IMP off site for further analysis as needed.

1-4. Site exploitation not only provides a commander with tactical information, but it also may lead to the discovery of information with operational or strategic value. For this reason, SE operations must be understood in tactical, operational, and strategic contexts. Material at an exploitable site may include tactical weapons, materials for making bombs, or even weapons of mass destruction. Additionally, exploitable sites may contain evidence of war crimes or other information that meets a theater-specific definition of strategic importance.

1-5. Site exploitation operations doctrine emphasizes three purposes for SE operations—

- To answer information requirements (usually the commander's critical information requirements).
- To facilitate subsequent operations (already planned or not yet anticipated).
- To facilitate criminal prosecution by host-nation or international authorities (related to war crimes).

1-6. Analyzed information obtained from SE eventually becomes intelligence. The relationship between SE operations and intelligence collection necessitates coordination. The fusion of intelligence from multiple sources can reveal opportunities for subsequent operations. Regardless of the mission's specific purpose, all Army operations have the implied task of collecting and sharing information about the opponent and the operational environment.

THE OPERATIONAL ENVIRONMENT IN RELATION TO SITE EXPLOITATION

1-7. The *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Army commanders analyze their operational environment using the operational variables: political, military, economic, social, information, infrastructure, physical environment, and time (known as PMESII-PT). As part of their analysis, commanders consider how SE operations can contribute to the overall mission. Commanders develop an in-depth understanding of the operational environment and the enemy.

1-8. Based on analyzing the operational environment, a commander determines critical information requirements that may include questions such as—

- Where are the enemy's heavy forces and where is the enemy's main effort?
- What are the enemies command and control vulnerabilities?
- What insurgent cell is responsible for the increase in improvised explosive device and sniper attacks?
- What network is funding and providing resources to the insurgents?

1-9. The operational variables also facilitate analyzing the results of SE operations. Some examples from past SE operations include—

- Austrian-made .50-caliber sniper rifles originally sold to Iran for military use were apparently discovered later to be in use by threat forces in Iraq (political, military).
- Improvised-explosive-device design variations led to discovery of specific networks supporting the threat (political, military, and economic).
- Laptops recovered disclosed financial and internal workings of Al Qaida in Iraq (military, economic, social, infrastructure).

1-10. Site exploitation operations have historically been associated with eliminating weapons of mass destruction. However, SE operations can contribute to defeating a wide range of current and evolving threats. In Operations Iraqi Freedom and Enduring Freedom, SE operations emerged as a valuable tool to attack threat networks and gain tactical, operational, and strategic advantages. Therefore, doctrine considerations for SE include all sites likely to provide valuable information and help defeat the threat.

THE CHANGING NATURE OF THE THREAT

1-11. Four major types of threat are traditional, irregular, catastrophic, and disruptive. Traditional threats, consisting of conventional military capabilities possessed by nation-states, continue to be relevant. Opponents using unconventional, asymmetric methods, such as terrorism, pose irregular threats. Catastrophic threats involve the acquisition, possession, and use of weapons of mass destruction. Disruptive threats involve the use of new technologies to reduce U.S. advantages in key operational domains. These categories are helpful in describing threats but they do not define or limit the nature of any

specific enemy or adversary. Opponents may combine types of threat. (See FM 3-0 for a discussion of the types of threat.)

1-12. Opponents often operate in small cells from diverse locations, some well hidden within urban areas. Friendly forces are likely to discover their locations during cordon and search operations by small patrols. Site exploitation operations can quickly obtain and analyze information for exploitation. Opponents often use unconventional means such as improvised explosive devices and information operations in tactical and strategic attacks. Soldiers conducting SE operations may recover unconventional weapons, homemade explosives, and ammunition. Maneuver forces must be able to search for, collect, and analyze IMP on-site.

Operations Against Traditional Threats

1-13. Traditional operations require protection against a wide array of high-tech weapon systems and capabilities. In major combat operations, commanders consider the advantages deliberate SE operations can provide. Including specialized assets as part of the initial SE force expedites the collection and subsequent analysis of IMP. If specialized assets are not initially available, commanders' planning considerations include the capability to obtain them if the need arises.

Operations Against Irregular Threats

1-14. Many opponents of the United States are not nation-states, although some may be supported by hostile nation-states. Their methods of attack and influence are sometimes referred to asymmetric or unconventional. They may operate in urban areas and use easily available technologies.

1-15. When conducting intelligence preparation of the battlefield (IPB), commanders study enemy technological capabilities based on information secured during SE operations. Based on this information, they can maintain a catalog of technological signatures. Similarities between technologies recovered from multiple sites may indicate the presence and movement patterns of specific individuals based on their technological signature. The study of IMP collected may reveal whether the threat is receiving assistance from external sources and to what degree. Continued analysis of the IMP collected may also provide indicators of how adaptive the threat is to external pressures.

1-16. Included under the category of irregular threats are the activities of insurgents, guerrillas, and terrorists. Irregular threats sometimes use effective low-tech methods or niche technologies. Some of the most simply constructed improvised explosive devices are difficult to defeat. Feedback from SE operations may disclose the evolution of low-tech methods of attack.

Operations Against Catastrophic Threats

1-17. Catastrophic threats present the greatest risk to friendly forces and the homeland. Opponents are developing weapons of mass destruction to deter or directly attack U.S. forces. Numerous opponents claim to possess or have immediate access to chemical, biological, radiological, and nuclear material. The potential consequences require commanders to commit adequate resources to identify and defeat this threat.

1-18. Analysis of IMP collected during SE operations may disclose an opponent's capability to employ a catastrophic strike. The analysis may require the assistance of multiple agencies within the Department of Defense and other government agencies. Analyzed information provided quickly to the commander and staff may help prevent catastrophic attacks.

1-19. Small-unit commanders conducting SE operations related to catastrophic threats coordinate with their intelligence staff officer for information about their objectives and the results of past catastrophic threats discovered. If the commander requires access to more information, the intelligence staff officer can contact higher headquarters for additional planning details to enable deliberate planning and receipt of specialized assets.

Operations Against Disruptive Threats

1-20. Disruptive threats focus on using new technologies to compromise or degrade essential military or civilian systems such as computer networks. Networked information capabilities are among the greatest vulnerabilities of U.S. society. Enemies can attack and disable information networks by remote access. U.S.

forces conducting SE operations may discover disruptive threats during U.S. checkpoint or cordon and search operations.

ENEMY FORCES AT EXPLOITABLE SITES

1-21. Site exploitation forces anticipate and prepare to encounter enemy forces at a site. Defeating and destroying enemy forces often is the only way to secure a site for exploitation. However, SE forces must remain adaptable. On one hand, enemy forces may defend exploitable sites tenaciously. They may resist until they are destroyed. Other enemies may attempt to surrender, and some defenders may abandon the area to avoid confronting Army forces.

1-22. Because enemies place strategic value on exploitable sites, the most proficient enemy forces may be detailed to defend them. Often exploitable sites are defended in layers, with external defense assigned to police, territorial, or militia forces and internal security assigned to better-equipped and better-trained forces. As a result, Army forces engaged in operations at an exploitable site may first encounter limited or ineffective resistance. As Army forces approach the most valuable areas of the site, which they may not know about, enemy resistance may increase sharply.

1-23. Within or close to an exploitable site, Army forces may encounter civilians. Distinguishing enemies from innocent noncombatants may be difficult. Therefore, Army forces secure and safeguard both uniformed and civilian prisoners discovered at exploitable sites. They hold them or transfer them to a facility where qualified interrogators can determine their status and intelligence value. Military police support may be used whenever possible to assist with prisoner and detainee handling.

1-24. Commanders balance the resources for SE against resources available for other tactical missions. Higher-level headquarters planners clearly articulate mission priorities for subordinate units and provide supplies, equipment, and personnel to conduct SE during other tactical combat operations.

THE BRIGADE COMBAT TEAM AND SITE EXPLOITATION

1-25. The brigade combat team (BCT) is the primary Army unit tasked to perform SE. BCTs train, plan, rehearse, and implement SE tactics, techniques, and procedures. A SE mission may be an independent task or nested and executed as continuous and complementary tasks within the context of other tactical missions.

1-26. Maneuver BCTs are organized, trained, and equipped to conduct SE operations. Specific actions include information collection, initial analysis, intelligence development, and target development for subsequent missions. Based on combat information or intelligence available before a SE mission, a BCT may be augmented to enhance its organic collection and analysis capabilities. With augmentation, BCTs can perform more detailed and specialized analysis of IMP discovered at a site. Augmented BCTs can conduct or support the exploitation of a sensitive site (see chapter 3). In some cases, the BCT facilitates operations while specialized teams execute their respective SE tasks.

1-27. Maneuver enhancement brigades, other task-organized units, and select functional brigades perform tasks directly related to SE. Individual Soldiers within units executing SE may conduct detailed searches, detain persons, and conduct tactical questioning. They can then collect IMP that support information requirements. (FM 2-91.6 provides additional information on tactical-level information collection support to SE.)

1-28. Site exploitation operations rest on the idea that every Soldier is a sensor. Site exploitation operations encompass the actions of all forces conducting or supporting SE.

THE PURPOSES AND POTENTIAL RESULTS OF SITE EXPLOITATION

1-29. Site exploitation operations must not be viewed in isolation. They are an integral part of the overall mission. During planning, commanders clearly identify and articulate the purpose—or purposes—of the SE operation. Forces use the purpose(s) to guide all planning efforts, including planning for sharing the results of information analysis. Commanders ensure the staff considers the potential to facilitate subsequent

operations. Figure 1-1 shows the three general purposes for SEs missions in relation to execution and potential results.

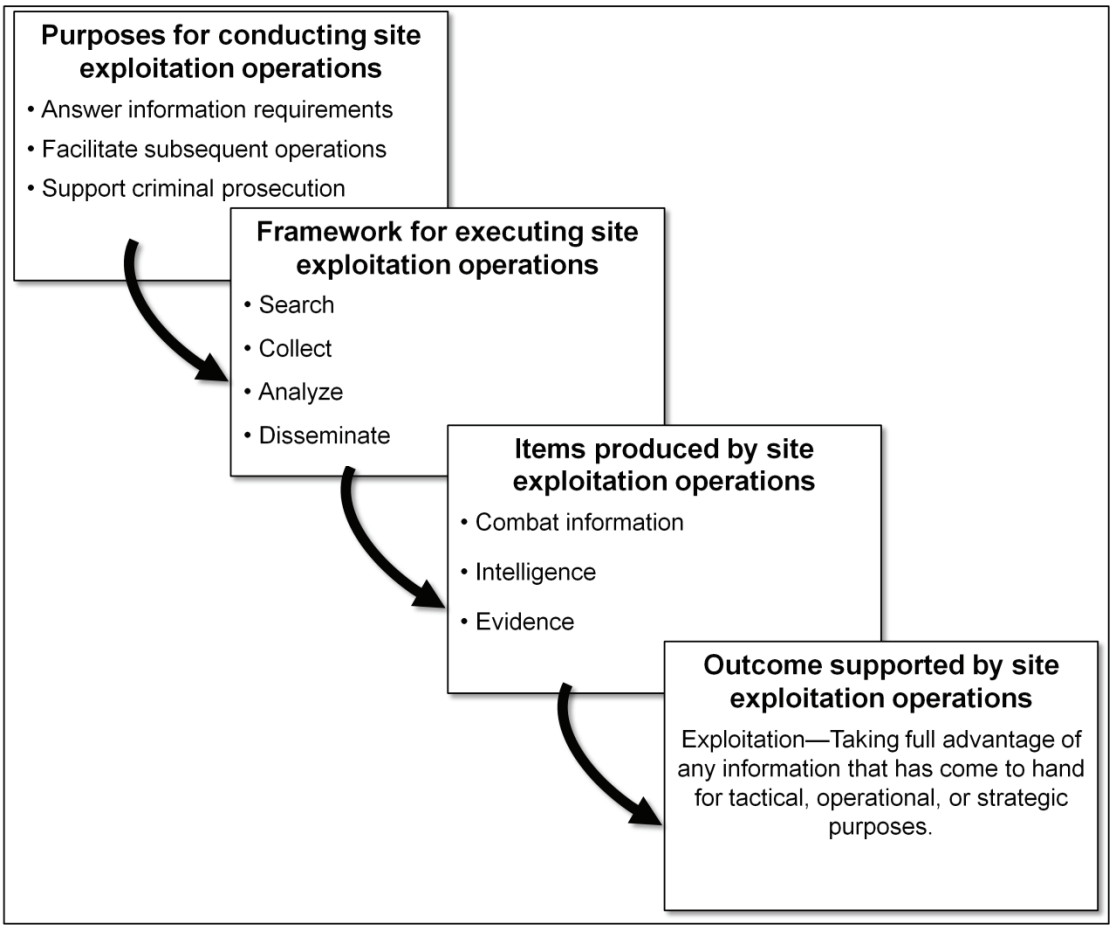

Figure 1-1. Site exploitation purposes, execution, and potential results

1-30. The framework for executing SE operations, briefly outlined in the second frame of figure 1-1, comprises four main actions—search, collect, analyze, and disseminate. The execution framework is further discussed in paragraphs 1-108 to 1-153. (Table 1-1, page 1-19, gives a more detailed outline.)

1-31. The information gained from SE is most valuable when used to facilitate subsequent operations. When forces effectively collect and process information to produce intelligence, they can execute subsequent operations using direct and focused targeting of an objective. Therefore, commanders plan to rapidly exploit any information gained, for the current operation and the next. Ideally, each SE mission leads to another SE mission. In addition, SE operations enable direct offensive action. Failure to recognize the relevance and timeliness of information can impede subsequent operations and must be avoided.

1-32. Targeting is linked to SE by providing information that, when analyzed, becomes intelligence. This intelligence leads to identifying new sites for exploitation, such as locations containing high value individuals, threat communication equipment and networks, weapons caches, or explosives production facilities. The commander and staff integrate the targeting process with SE to determine the best allocation of resources and to prioritize objectives.

1-33. Rapid analysis (either on or off-site) enables friendly force commanders to observe, orient, decide, and act faster than the enemy. Site exploitation teams analyze the collected information on-site if possible. In many instances, additional coordination between operations and intelligence staffs produces intelligence that will support future operations.

1-34. Joint, theater, and division assets can provide analysis, produce answers to information requirements, and support BCT targeting requirements. Therefore, commanders ensure tactical units have access to appropriate assets. They brief all tactical units on information requirements so they can recognize potential answers.

SITE EXPLOITATION IN FULL SPECTRUM OPERATIONS

1-35. Commanders integrate SE operations into full spectrum operations. Any operation can present opportunities for SE.

1-36. Site exploitation must be a continuously integrated effort between intelligence and operations staffs to defeat threat networks rapidly. Integration also extends to the actions of individual Soldiers at a given site. Commanders integrate efforts to analyze collected IMP, facilitate intelligence production, support effective targeting, and execute subsequent operations. This maintains seamless pressure against enemy forces. It allows friendly forces to collect additional information, subsequently weaken, and ultimately defeat threat networks.

1-37. During stability operations, Army forces may support stability tasks such as establishing civil control and establishing civil security. Site exploitation forces may collect evidence to support criminal prosecution for war crimes courts. The assessment, planning, preparation, and execution of SE operations related to criminal prosecution require special considerations regarding host-nation and international rules of evidence, law, and authority (see paragraphs 3-19 through 3-22). Whenever SE operations facilitate criminal prosecution, commanders consult a staff judge advocate.

1-38. Site exploitation operations have a considerable range in scale and complexity. A large operation might involve a division-level effort with an array of joint, interagency, intergovernmental, multinational, host-nation, commercial, and private organizations to exploit an entire town. A smaller operation might involve a section of Soldiers searching a single building or room. Regardless of the scale or complexity, commanders and staffs use the operations process: planning, preparing, executing, and assessing.

USING THE OPERATIONS PROCESS FOR SITE EXPLOITATION

1-39. This section discusses using the operations process in relation to SE operations. Forces use the operations process to integrate SE into full spectrum operations. Refer to FM 5-0 for a thorough discussion of the steps of the operations process.

ASSESSING THE SITE EXPLOITATION OPERATION

1-40. *Assessment* is the continuous monitoring and evaluation of the current situation, particularly the enemy, and progress of an operation (FM 3-0). During planning, preparation, and execution, commanders continually estimate the site's probability of answering information requirements. While planning the operation, a thorough assessment of the site helps commanders identify specific assets needed. This ensures that executing forces arrive at the site appropriately task organized and able to immediately collect and analyze IMP. It also expedites the development of information that will answer information requirements or be processed to produce further intelligence. During execution, commanders continually assess the performance of SE tasks. Commanders also assess the end results, such as enhanced ability to attack the threat network and achieve the desired end state. Commanders evaluate the effectiveness of the exploitation operation in relation to its purpose, the value of the information, and the subsequent intelligence produced.

1-41. Assessing a site is an inherent command and control action. A commander's assessment of a site's potential value, the capabilities needed to exploit it, and the associated risks may change at any time throughout the operation. A commander continuously assesses the site and redirects the operation as appropriate. Refer to chapter 6 of FM 5-0 for a thorough discussion of assessment as part of the operations process.

1-42. In general, commanders base the criteria for estimating a site's probability of answering information requirements on available intelligence. To determine a site's potential for exploitation, considerations include—

- Existing intelligence.
- Hazards at the site.
- Security concerns related to the site.
- Complexity or scope of the site (building or grounds).
- Suspected contents of strategic significance.
- Historical use of the site (its affiliation or employment).
- Location of the site.

1-43. The commander's assessment includes criteria for assessing the sensitivity of IMP the site may yield. For instance, a site is considered sensitive if it contain evidence of war crimes; research and production facilities involving chemical, biological, radiological, nuclear, and high-yield explosive materials; or breakthrough technologies used by the opponent. Specialized units or agencies not resident in the BCT tactical formation may be required to exploit the site. See Chapter 3 for a more detailed discussion of sensitive sites.

PLANNING THE SITE EXPLOITATION OPERATION

1-44. Commanders and staffs use the military decisionmaking process (MDMP) for planning, and small unit leaders use troop leading procedures to plan and prepare for SE operations. These processes provide universally understood and commonly used procedures as described in FM 5-0. Paragraphs 1-45 to 1-102 discuss selected concepts and processes as they relate to planning SE operations. Refer to chapter 2 of FM 5-0 for a thorough discussion of planning as part of the operations process. See appendix D of FM 5-0 for guidelines for commander's planning guidance. See appendix B of FM 5-0 for a thorough discussion of the MDMP.

Key Planning Concepts

1-45. Site exploitation planning requires technical and tactical competence and applying key planning concepts. This section discusses some of the key planning concepts outlined in FM 5-0 as they relate to SE. They include—

- Nested concepts.
- Sequencing operations.
- Control measures.
- Deliberate and hasty operations.
- Intelligence, surveillance, and reconnaissance.

Nested Concepts

1-46. Purpose unifies all elements of battlefield organization by focusing all actions. In general, commanders organize forces according to a mission's overall purpose by determining whether each unit's operation will be decisive, shaping, or sustaining. Site exploitation operations are shaping operations that, when effectively executed, facilitate operational and strategic success.

1-47. Site exploitation operations are nested within the higher headquarters concept of operations. Commanders conducting operations that include SE ensure that subordinate unit missions are unified and integrated by task and purpose. For example, conducting shaping operations such as a cordon and search or a raid can obtain information and intelligence that facilitate subsequent attack of the threat network.

1-48. The commander ensures the concept of operations clearly describes the SE scheme of maneuver and expresses how each element will cooperate to accomplish the mission.

Sequencing Operations

1-49. Based on the availability of resources—such as time, forces, and specialized assets—commanders synchronize subordinate SE actions in time, space, and purpose. Site exploitation operations usually follow a general sequence (see paragraph 1-108). Planning for the mission may require phasing linked to the transitions from other tactical tasks, based on forces available and the threat.

1-50. Based on the level of protection required to thoroughly search for and collect IMP, forces may execute any number of tactical tasks early in execution. These tasks might include isolating, controlling, or seizing an objective. Portions of the forces that support the initial protection tasks often perform the search and collection tasks. When applicable, maneuver forces conduct tactical tasks (cordon, secure, and isolate) to protect a site before other forces begin searching for and collecting IMP. After maneuver forces complete their tasks, units such as forensic collection units or chemical, biological, radiological, and nuclear forces may begin their tasks. When availability of these types of assets is limited, commanders may sequence their support across several phases or components of an operation.

1-51. Based on uncertainty in the operational environment, commanders maintain flexibility in their planning. Commanders consider branch plans or sequels within base plans. Branch plans facilitate changing the mission, disposition, orientation, or direction of movement based on anticipated events. Unforeseen events can require additional resources. Examples of unforeseen events that might require flexibility include the discovery of—

- Chemical, biological, radiological, nuclear, and high-yield explosive threats.
- Significant environmental hazards (hazardous materials or waste).
- High-value individuals.
- External disruptions, such as enemy attacks, that require protecting the site until specialized teams arrive to neutralize or reduce the threat.
- A large munitions or explosives cache.
- IMP that meet the criteria for a sensitive site (see chapter 3).

1-52. Sequels follow current operations and are developed based on anticipated outcomes. One example is collecting specific information that leads to immediately exploitable targets.

Control Measures

1-53. Planners develop and recommend control measures for each course of action (COA) being considered. Control measures provide the means for the commander to direct SE actions. These measures establish responsibilities to subordinate elements and outline limits that can prevent loss or destruction of relevant information and potential intelligence. Control measures are either permissive or restrictive. Permissive control measures allow SE elements freedom of action and limit the requirement to refer to higher headquarters for permission. Examples include apprehension parameters. Restrictive SE measures might prohibit forces from entering specific areas of a site to prevent contamination of material by Soldiers or the contamination of Soldiers from suspected chemical, biological, radiological, or nuclear material.

Deliberate and Hasty Site Exploitation Operations

1-54. FM 3-90 describes deliberate and hasty operations. A *deliberate operation* is an operation in which a commander's detailed intelligence concerning the situation allows him to develop and coordinate detailed plans, including multiple branches and sequels. He task organizes his forces specifically for the operation to provide a fully synchronized combined arms team. He conducts extensive rehearsals while conducting shaping operations to set the conditions for his decisive operation (FM 3-90). A *hasty operation* is an operation in which a commander directs his immediately available forces, using fragmentary orders, to perform actions with minimal preparation, trading planning and preparation time for speed of execution (FM 3-90).

1-55. A deliberate SE operation is based on effective targeting and supported by a commander's detailed intelligence or information. Commanders and staffs apply the operations process to ensure subordinate elements are organized and equipped to exploit the targeted objective. Such action facilitates a continuous cycle of exploitation opportunities.

1-56. The main difference between deliberate and hasty operations is the time available for planning and preparation. Commanders assess their operational environment using the mission variables of mission, enemy, terrain and weather, troops and support available, time available and civil considerations (METT-TC). They task organize forces to ensure they take advantage of unexpected SE opportunities. They train, equip, and organize forces to maintain flexibility. They bear in mind that regardless of the time available, any SE opportunity has the potential to yield answers to information requirements and other relevant information. During execution, seemingly benign missions can present unexpected opportunities.

1-57. As subordinate units encounter opportunities, their commanders initiate hasty SE operations. Hasty SE operations support tactical, operational, or strategic objectives no less than deliberate operations. If a hasty SE operation identifies IMP of significant intelligence value, a commander may choose to allocate additional time to the operation and transition to a deliberate operation.

1-58. When planning for SE missions in a time-constrained environment, commanders assess the situation, refine their situational understanding, and direct the staff to perform the MDMP steps needed to support SE decisions. Commanders rely on more intuitive decisionmaking to take advantage of hasty SE opportunities.

Intelligence, Surveillance, and Reconnaissance

1-59. Intelligence, surveillance, and reconnaissance (ISR) synchronization and integration include—

- Analyzing information requirements and intelligence gaps.
- Evaluating the capacity of available assets internal and external to the organization.
- Prioritizing ISR assets controlled by the organization for collecting answers to the commander's critical information requirements (CCIRs).
- Identifying gaps those assets cannot fulfill.
- Requesting support from adjacent and higher headquarters to fill unresolved collection requirements.

1-60. Integrated ISR operations enable the commander and staff to confirm or deny assumptions made in planning for SE operations. ISR answers information requirements to improve situational understanding. ISR synchronization and integration begin early in planning. Ideally, this enables commanders to obtain information and intelligence related to SE decisions during COA development. This allows the commander to make necessary changes, such as task organizing the search element, or adding detainee collection points based on the estimated number of persons on the site. ISR tasks related to SE sometimes lead to executing branch plans or abandoning a mission.

The Commander's Role in Planning Site Exploitation

1-61. Commanders visualize, describe, and direct operations; this includes overseeing the staff's planning and orders production. (FM 6-0 discusses the leader's role in planning and orders production in detail.) Visualization includes envisioning the SE purpose or purposes and the current state of friendly forces in relationship to the enemy and the environment. Considerations include—

- The size of the isolation force in respect to the threat.
- The capability of the search element in relation to—
  - Anticipated information, people, and cultural and natural resources at the site.
  - The possibility of hazardous material adversely affecting Soldier health.
  - Other anticipated material at the site.
- Whether the environment is permissive or nonpermissive.

After visualization, commanders describe their guidance through articulating intent, planning guidance, and initial CCIRs.

The Staff's Role in Planning Site Exploitation

1-62. The staff focuses on assisting the commander with making decisions and developing effective plans and orders. The staff initially performs mission analysis to develop the information the commander requires to understand the situation and mission. (FM 5-0 discusses mission analysis in more detail.) The staff performs the following critical tasks during planning:

- Develop and maintain the running estimate.
- Identify specified and implied tasks.
- Identify constraints.
- Identify key facts and assumptions.
- Perform IPB.
- Formulate a concept of operations and a concept of support in line with the commander's intent.
- Develop the scheme of maneuver to support the approved COA.
- Prepare, authenticate, and distribute their portion of the plan or order, annexes, estimates, and appendixes.

1-63. The appropriate coordinating and special staff officers provide recommendations and advice to the commander and operations officer on the search-related capabilities of their respective supporting organizations, such as—

- Capabilities and limitations of specialized assets such as chemical, biological, radiological, and nuclear units, explosive ordnance disposal units, and technical intelligence (TECHINT) units.
- Document and media exploitation support capabilities.
- Human intelligence collection capabilities (to include tactical questioning and interrogation).
- Capabilities of host-nation authorities or multinational military partners.
- Rules of engagement or environmental and hazardous materials laws that fall under the purview of the legal officer.
- Capabilities of organic forces and external support.

1-64. Organizations may designate search advisors and coordinators as additional duty positions and provide them with additional training to support SE operations. Search advisors and coordinators are not recognized positions within the BCT's modified table of organization and equipment.

1-65. Paragraphs 1-66 to 1-102 discuss selected considerations for SE in relation to portions of the MDMP:

- Receipt of mission.
- Mission analysis.
- COA development.

Receipt of Mission

1-66. Planning for a SE mission may be initiated—

- In anticipation or receipt of a new mission.
- As a branch or sequel to an ongoing operation.
- As a part of a base order.
- As a part of a unit standing operating procedure.

1-67. As previously discussed, one of the purposes of SE is to facilitate subsequent operations. Successful SE actions support the commander's decisionmaking by identifying potential targets. The staff uses the information gained from SE to help the commander to anticipate subsequent SE missions.

Running Estimates

1-68. Before conducting mission analysis, the staff evaluates and refines the status of friendly forces and resources. The staff continually maintains a running estimate throughout the operations process. Updates may include the status or availability of specialized support such as—

- Document and media exploitation assets.
- Military working dog teams.
- Environmental assets.
- Linguists.
- Forensics laboratories and facilities.

Updates also include the availability of equipment, such as biometric identity management tools, remote detection assets, and language translation tools.

Initial Assessment

1-69. Time constraints are the focus of the initial assessment. Time constraints significantly influence SE planning in relation to the perishable nature of the information or intelligence that initiated the SE mission. The commander and staff must receive and develop information quickly enough to interrupt the threat's decision cycle.

Initial Guidance

1-70. The commander provides initial guidance (not to be confused with commander's initial planning guidance during mission analysis) that outlines multiple factors. Key to SE operations, the initial guidance provides the operational time line and the initial information requirements.

1-71. Commanders develop their initial guidance based on initial visualization. Commanders visualize the SE mission and provide guidance to the staff while still providing the latitude to explore different options based on the time available for planning. Initial guidance focuses on ISR considerations required to develop COAs that will meet the desired end state.

1-72. Commanders integrate information engagement into the operations process from its inception. Information engagement actions are nested with higher headquarters intent and any applicable strategic guidance. The commander's initial guidance regarding information engagement informs the staff on how to integrate and synchronize information engagement actions with other operational actions. Commanders consider how proposed actions might affect the operational environment in relation to the overarching information engagement plan.

Mission Analysis

1-73. The commander and staff conduct mission analysis to enable better visualization of the operation. The process and products derived from mission analysis help commanders refine their situational understanding. Mission analysis is a 17-step process outlined in FM 5-0. Paragraphs 1-74 to 1-97 describe selected mission analysis steps in relation to SE planning requirements. Refer to Figure B-2 of FM 5-0 for a complete list of the steps for mission analysis.

Analyze the Higher Headquarters Order

1-74. The commander and staff analyze the higher headquarters order and guidance. This helps them determine how the unit mission is nested with the higher headquarters mission, commander's intent, and concept of the operation. The commander and staff should determine how effective exploitation of the site supports higher headquarters operational and strategic objectives.

Conduct Initial Intelligence Preparation of the Battlefield

1-75. Commanders and staffs conduct IPB continuously to enhance SE planning. The four steps of the IPB process are—

- Step 1—Define the operational environment**.**
- Step 2—Describe the environmental effects on operations.
- Step 3—Evaluate the threat**.**
- Step 4—Determine the threat COAs**.**

The following paragraphs discuss some considerations related to the IPB process and SE planning. (See FMI 2-01.301 for more information about IPB.)

1-76. Step 1 includes identifying the characteristics and limits of the area of operations. During this step, commanders and staffs identify gaps in information pertinent to initial ISR planning.

1-77. Step 2 includes identifying limitations or requirements regarding size of buildings, number of rooms, scale and security of an area, and any environmentally significant aspects. In addition, SE operations are normally executed near a civilian population and involve various elements of the civilian infrastructure. Therefore, when planning SE operations, staffs give special consideration to the categories of civil considerations: areas, structures, capabilities, organizations, people, and events (ASCOPE). (See FM 3-24.2 for guidance on using civil considerations during planning.)

1-78. In step 3, the staff analyzes recent threat tactics, techniques, and procedures in relationship to the effects on the battlefield to determine what tactics, techniques, and procedures the opponent uses. Examples of SE considerations include the opponent's use of women and children as couriers, false walls in buildings, or storing weapons and material inside buried containers.

1-79. Step 4 includes determining how the threat will act or react on the site. This is critical to determining friendly COAs that will prevent damage to the site's contents (for example—*upon identification of the isolation force, the threat is expected to employ snipers to harass friendly forces*).

Determine Specified, Implied, and Essential Tasks

1-80. Site exploitation may be a specified task in the higher headquarters operation order within the assigned mission, tasks to subordinates, or other coordinating areas. Assigned tasks related to SE might include—

- Capture high-value individuals.
- Search an area, building, persons, or vehicles.
- Process persons and material in accordance with evidentiary requirements.
- Review the information requirements.

1-81. Normally, SE is an implied task based on supporting the specified tasks or mission objectives. The requirement to collect information, answer CCIRs, conduct on-site analysis, and develop the information gained is implied in all operations when not directed as a specified task. Site exploitation operations may include implied tasks such as evidence preservation, biometric enrollment, and forensic collection, which are supporting tasks that must be completed to meet the purpose of the operation.

1-82. Site exploitation tasks, whether specified or implied, may be essential tasks. Essential tasks are always included in the mission statement. When SE is an essential task, at a minimum it is depicted as an on-order mission. Examples of mission statements related to SE are—

- On order, conduct a cordon and search to locate material related to improvised explosive devices for technical analysis.
- On order, conduct SE to gain combat information supporting operational objectives.

Review Available Assets

1-83. Basic planning involves analyzing the organizational structure and supporting (direct and general) assets available to perform the task. Site exploitation requires a clear understanding of the personnel

available, along with their level of training, to determine their capabilities in support of SE tasks. For example, tactical questioning may require personnel trained in direct questioning, the employment of a linguist, or incorporation of certified human intelligence collectors trained in interrogation. For certain search-related tasks, mission requirements determine the required training level of forces. Maneuver Soldiers trained in search tasks provide a different level of capability than an engineer squad trained in specialized search techniques and equipment. Environmental concerns identified may require personnel trained specifically on environmental issues and hazardous materials tactics, techniques, and procedures. Additionally, the equipment available, such as biometric identification tools, void anomaly detectors, or ground-penetrating radar, affects COA development. Commanders must consider the time available for SE planning and the time sensitivity of the IMP to be exploited. The availability of supporting agencies to provide technical analysis, forensic collection, and render-safe capabilities influence planning and COA development. Commanders, coordinating staffs, and liaison officers help identify capabilities and limitations of the assets associated with their respective area of expertise.

Determine Constraints

1-84. A *constraint* is a restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action a subordinate commander has for planning (FM 5-0). Examples of constraints for SE planning include, but are not limited to rules of engagement, search restrictions relating to males or females, and rules for the use of force. Constraints can affect COA development of both the parent unit and its subordinate elements. Constraints should be included as tasks or coordinating instructions in operations orders to account for the impact on planning and execution.

Identify Critical Facts and Assumptions

1-85. Facts are verifiable information that forms a foundation for the development of solutions. For planning, an assumption is information accepted as potentially true in the absence of fact and is essential to continue planning. The commander and staff attempt to confirm or deny the validity of their assumptions. For planning, assumptions are treated as facts. Examples of assumptions for SE operations may include—

- Boobytraps will be present on the site.
- The threat will attempt to conceal its identity.
- The building will contain hidden compartments.
- Persons or material collected will have intelligence and prosecutorial value.

Perform Risk Assessment

1-86. Composite risk management, as outlined in FM 5-19, involves a 5-step process for identifying, assessing, and controlling risk by balancing risk cost with mission benefits. Composite risk management begins during mission analysis and continues throughout the operations process. The 5 steps are—

- Identify hazards.
- Assess hazards to determine risk.
- Develop controls and make risk decisions.
- Implement controls.
- Supervise and evaluate.

1-87. The commander and staff assess two kinds of risk: tactical and accidental. Tactical risks relate to those posed by the threat, such as boobytrapped doors, improvised explosive devices, and sniper fire. Accidental risks encompass all other risks, such as the risk posed by the presence of civilians or limited visibility. Commanders and staffs consider risk to their force when assessing and analyzing the threat.

Determine the Commander's Critical Information Requirements

1-88. CCIRs and other information requirements drive ISR planning. They focus collection efforts on answering the information requirements critical to mission planning and execution. CCIRs are usually time-sensitive, especially when related to SE operations. Once a COA is selected, CCIRs and subsequent ISR tasks should be further refined to support the commander's decisionmaking. For example, if ISR

resources identify chemical, biological, radiological, nuclear, or high-yield explosive materials, a branch plan may be executed requiring a different approach or task organization.

1-89. CCIRs should be specific enough to answer the information management priorities. CCIRs fall into two categories: priority intelligence requirements (PIRs) and friendly force information requirements (FFIRs).

1-90. PIRs identify the information about the enemy, terrain and weather, and civil considerations that the commander considers most important. Lessons from recent operations show that intelligence about civil considerations may be as critical as intelligence about the enemy. Thus, all staff sections may recommend information about civil considerations as PIRs (FM 3-0). PIRs related to a building being exploited can answer questions such as—

- What is the floor plan for the building?
- Where are the improvised explosive devices along the route to the building?
- Where are the explosives in the building?
- What is the civilian presence in the building?
- What is the attitude of the local populace towards friendly forces?
- What environmental hazards are present that will adversely affect the health and well-being of the Soldiers conducting the exploitation?

1-91. FFIRs identify the information about the mission, troops and support available, and time available for friendly forces that the commander considers most important (FM 3-0). FFIRs related to SE can answer questions such as—

- What is the status of the cordon force?
- What is the location of the weapons intelligence team?
- What is the response time for the quick reaction force and explosive ordnance disposal?
- Where are the local law enforcement facilities?

1-92. Commanders direct the staff and subordinates throughout the operations process. During the MDMP, commanders direct the staff during COA development, analysis, comparison, and selection by providing guidance and criteria to the staff on how the SE operation should develop.

Determine Essential Elements of Friendly Information

1-93. An *essential element of friendly information* is a critical aspect of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation, and, therefore, must be protected from enemy detection (FM 3-0). Examples of essential elements of friendly information for SE operations include forensic collection, remote detection, and signal intercept capabilities.

Determine the Initial Intelligence, Surveillance, and Reconnaissance Plan

1-94. When conducting SE operations, the ISR plan links the collection effort to the commander's information requirements. Often, time constraints shape the need for information. Within a site, identifying areas of interest helps establish the scope of the collection effort. Considerations may include the scale and complexity of the site, confirmation or exclusion of the presence of weapons of mass destruction, booby traps, hostile forces, or civilians. The ISR plan articulates the last time information is of value to the search element to prioritize the collection effort.

Write the Restated Mission

1-95. Site exploitation operations may be the primary task of a unit or element and a supporting task to the overall unit commander's mission. When SE is a critical task, it is in the unit's mission statement either as the primary task or as an on-order mission after the completion of the primary enabling task. For example, as the primary essential task, the mission statement may read, "Not later than 220600Z Nov 09, 1BCT conducts SE of the suspected IED factory on objective Raiders to facilitate the analysis of the information, material, and persons located at the factory." As a subsequent or on-order essential task, the mission

statement may read, "Not later than 190500 Oct 09, B Troop (+) conducts a raid on objective Tiger to capture the high-value individuals conducting sniper attacks on multinational forces. On order, conduct SE on objective Tiger to collect information for subsequent intelligence analysis and prosecution."

Develop the Initial Commander's Intent

1-96. The initial commander's intent for missions or operations including SE specifies the purpose of the collection effort and the end state for the information analysis. It focuses subordinate elements on rapidly collecting and developing information to support decisionmaking at the lowest level. The commander provides a clear and concise statement of the SE team's tasks and objectives. When SE is nested within another tactical mission, such as a raid, the commander articulates the purpose of the overall mission. This includes what potential IMP the mission will gain and how the force intends to rapidly exploit it. Key tasks relating to SE describe what the force must do to achieve the desired end state. Key tasks may include—

- Cache search.
- Evidence documentation.
- Tactical questioning or human intelligence collection.
- Render-safe procedures.
- Biometric enrollment.
- Forensic collection.
- Environmental evaluation for cultural and natural resources and hazardous materials.

1-97. Finally, after mission analysis commanders focus the staff on COA development, analysis, and comparison to facilitate accomplishing the key SE tasks. Commanders give guidance that focuses efforts within the SE purposes. The decisive point at the tactical level may be the capture of a high-value individual. The decisive point at the operational level may be identifying the leadership of a threat network or cell or reducing insurgent-related activity in a specific region. Regardless, the commander guides the staff toward application of maximum combat power or resources against the decisive point. (See FM 3-0 for more information relating to decisive points.)

Course of Action Development

1-98. After commanders approve the mission statement and initial intent, they provide the staff guidance for COA development. Whether SE is the primary mission, or it is planned as a subsequent or secondary task, COA development for SE follows the same considerations outlined in FM 5-0. Site exploitation COA development must synchronize and simultaneously apply combat power. The task organization of the SE element meets the unique mission requirements. When establishing the support relationships, commanders consider the supporting distance for specialized supporting agencies. These specialized agencies might include explosive ordnance disposal teams; TECHINT teams; forensic collection teams; and chemical, biological, radiological, and nuclear units.

1-99. Feasible COAs ensure sufficient resources exist to accomplish the mission. The protection force must be large enough to prevent interference with the search element. The search element must have sufficient personnel, time, and material to effectively search and identify appropriate IMP on the site based on scale and complexity.

1-100. The commander develops the concept of operations to describe how the SE mission will be accomplished. The concept of operations helps ensure that missions or tasks match the capabilities of the exploitation force. The concept of operations outlines shaping operations such as isolating a site, clearing hazards, and information engagement.

1-101. When developing COAs, the commander and staff array their forces and task-organize teams to perform the specific SE tasks. The commander may choose to task-organize organic and augmented assets into a SE team to better focus the capabilities of the force. An example of a task-organized exploitation team is diagrammed in figure 1-2.

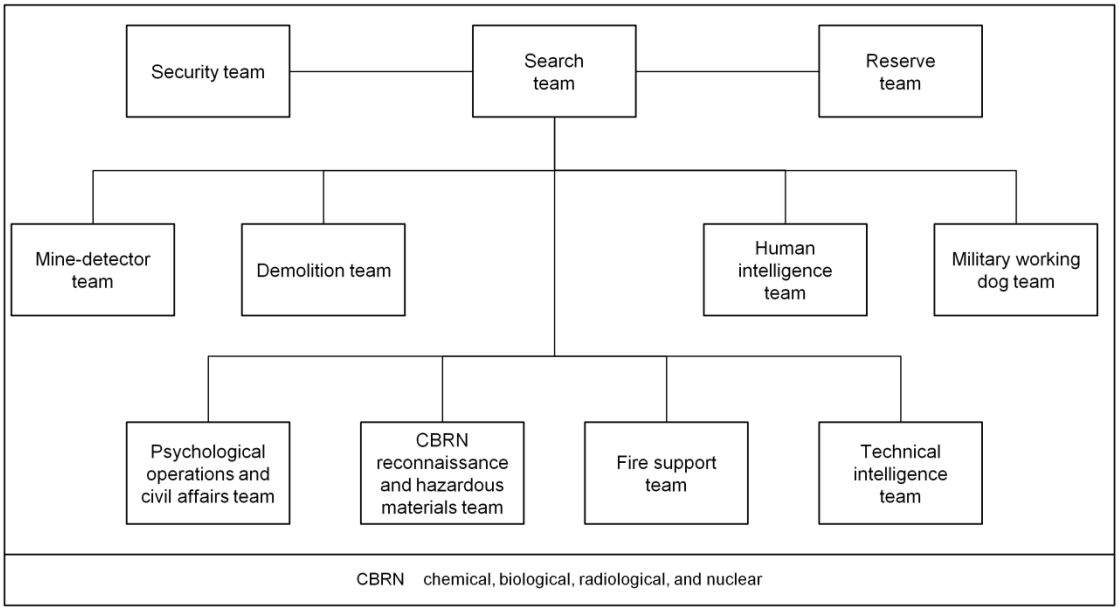

Figure 1-2. Example of a search element task-organized for site exploitation

1-102. The staff uses war-gaming to effectively synchronize the SE effort and ensure the appropriate decision points are identified to assist the commander during execution. At a minimum, when available time is limited, the staff war-games SE actions using the box technique to focus on specific SE actions. They evaluate actions on the site in relation to the threat; the known or assumed IMP contained on the site; and the time–distance relationships to specialized agency response teams. Additionally, the staff evaluates and identifies subsequent actions such as site disposition requirements or sequels driven by information gained from successful SE. Appendix B of FM 5-0 gives all steps of the MDMP. Appendix E of FM 5-0 provides formats for plans and orders. Appendix F of FM 5-0 discusses task organization.

PREPARING FOR THE SITE EXPLOITATION OPERATION

1-103. *Preparation* consists of actions performed by units to improve their ability to execute an operation. Preparation includes, but is not limited to, plan refinement; rehearsals; intelligence, surveillance and reconnaissance; coordination; inspections; and movement (FM 3-0). Site exploitation operations follow the same preparation requirement regardless of the mission source. When a higher headquarters assigns a mission to a subordinate organization, parallel planning and preparation are based on guidance from the commander. Refer to chapter 4 of FM 5-0 for a thorough discussion of preparation.

1-104. Parallel planning takes place at various levels before higher headquarters planning is complete so initial preparations can get under way quickly. As previously stated, commanders begin to plan a SE operation upon receipt of a mission from higher headquarters, in anticipation of receiving a new mission, or as derived from an ongoing operation.

1-105. Surveillance is integrated with SE. The commander directs surveillance to systematically observe an area and collect information. Surveillance may provide information supporting decision points for initiating exploitation-related actions such as a cordon and search operation. It is important for the staff to determine the mission-specific surveillance needs and add those requirements to the ISR synchronization process.

1-106. Directed reconnaissance supports SE by answering information requirements, by confirming or denying the existence of a threat, and by potentially providing intelligence. During the MDMP, the staff supports the commander with the initial ISR plan that includes appropriate reconnaissance tasks. The requirements initially determined upon receipt of the mission drive the collection effort. As the plan is developed and completed, the focus of the collection effort may change based on the commander's

assessment of the situation, requiring subsequent changes to the ISR plan. The focus for reconnaissance may be to determine the best opportunity to execute SE, based on established criteria.

1-107. The complexity of SE operations and the volume of events and resources linked during execution require directed rehearsals to ensure coordination. Commanders conduct rehearsals to ensure subordinates understand their role in the SE operation in relation to other elements. Examples of SE tasks that may require rehearsals are—

- Establishment of initial protection and control points within the area to be searched.
- Coordination of host-nation persons.
- Documenting search and collection results.
- Specific tactical questioning of women and children based on intelligence and local customs.
- Biometric enrollment.
- Evidence handling procedures.
- Transfer or handover of detainees and material.
- Search execution.

EXECUTING THE SITE EXPLOITATION OPERATION

1-108. When a commander determines a site is likely to contain valuable information, execution proceeds according to this general framework:

- Search.
- Collect.
- Analyze.
- Disseminate.

Site exploitation actions normally progress through this general sequence, illustrated in figure 1-3. First, SE forces search a site. After searching, they collect IMP with potential value. Forces then analyze collected IMP—on-site, if possible, particularly if the IMP are likely to provide answers CCIRs. Forces may transfer select IMP to a facility with capability to conduct analysis and produce intelligence. Commanders ensure that information and intelligence produced are disseminated to appropriate friendly force organizations for *exploitation*: taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes (JP 1-02). As illustrated in figure 1-3, this leads to a continuous cycle intelligence–driven operations. Paragraphs 1-110 to 1-153 discuss the execution framework in more detail. Refer to chapter 5 of FM 5-0 for a thorough discussion of execution as part of the operations process.

1-109. Some SE actions overlap. For example, while forces collect IMP, a certain amount of searching may be ongoing. Analysis may indicate that additional IMP should be collected. Assessment is continuous throughout. In some instances, a commander's assessment of a site's status or potential may change before all actions are completed. When the commander determines a site is no longer exploitable, the commander ceases that operation and transfers control of the site to the appropriate entity.

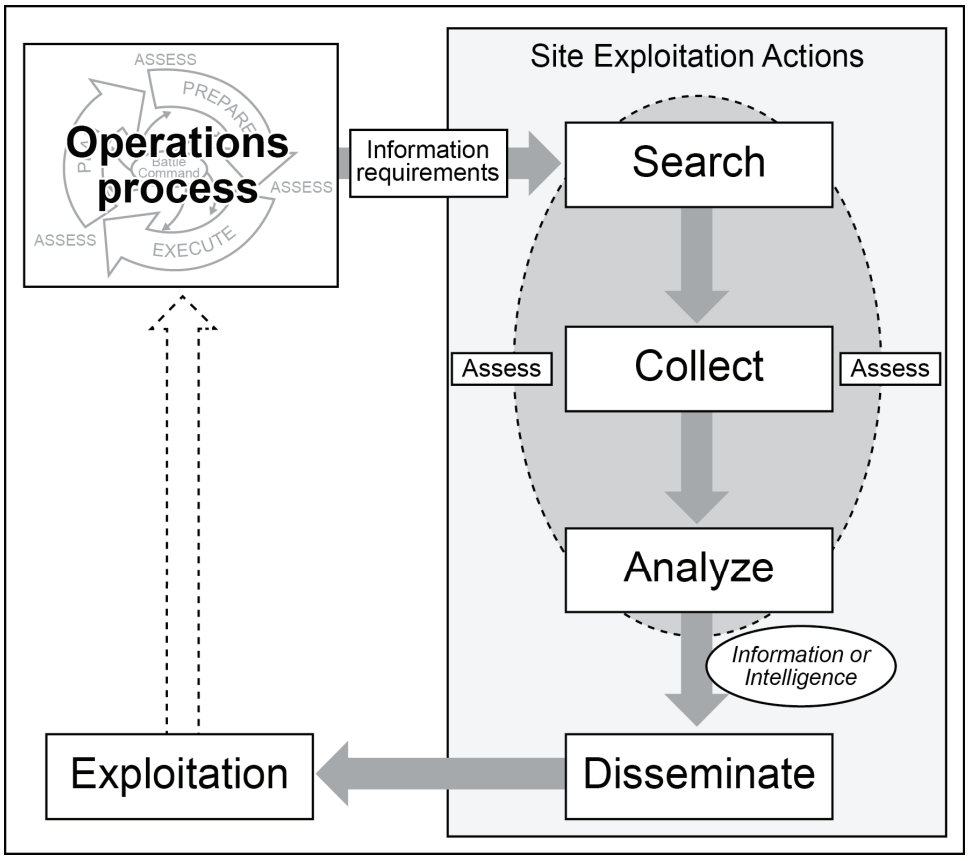

Figure 1-3. The site exploitation execution framework

1-110. The four general actions described above—search, collect, analyze, and disseminate—form a logical framework for organizing mission-specific SE tasks. Some examples of specific tasks that can be organized within this framework are—

- Collect fingerprints, electronic data, weapons, and other physical evidence.
- Conduct tactical questioning and interrogation of detainees.
- Analyze the tactics, techniques, and procedures the enemy used at the exploitation site.
- Enter information into the Distributed Common Ground System–Army or other intelligence conduits as applicable.
- Advise subordinate commanders on improvised explosive device designs found to be used by the enemy.

Table 1-1, page 1-19, expands the execution framework to show the subordinate actions each main action normally includes.

Table 1-1. Expanded site exploitation execution framework

- Search the site:
  - Locate the site.
  - Protect the site.
  - Conduct a site search.
- Collect information, material, and persons (referred to as IMP):
  - Collect potentially valuable IMP.
  - Preserve the site and the IMP collected.
  - Transfer control of the site.
- Analyze the collected IMP.
  - Analyze the collected IMP on-site.
  - Transfer IMP indicated for further processing.
  - Analyze the transferred IMP off-site.
- Disseminate information and intelligence.
  - Establish connectivity with intelligence organizations.
  - Share data, information, and intelligence, through appropriate channels.

Search the Site

1-111. In the context of SE operations, to search a site refers to systematically examining the site so that all areas pass within the view of SE team members. Forces ensure potentially valuable items are identified and preserved. To search the site, Soldiers perform the following actions:

- Locate the site.
- Protect the site.
- Conduct a site search—
  - Recognize all potential sources of valuable IMP.
  - Consider all potentially valuable IMP for further analysis.

The following paragraphs discuss these actions in detail.

Locate the Site

1-112. Maneuver forces move to and locate (or confirm the location of) the exploitable site through standard reconnaissance efforts. Based on ISR, normally, the SE force receives an accurate location or description of the site. In instances where the available information is general, the maneuver force locates the targeted site through tactical operations, employing systematic search techniques commensurate with the situation. In some instances, a unit may discover an unanticipated site that appears to support information requirements while executing another tactical mission. Units may obtain initial confirmation using unmanned aerial systems, signals intelligence, human intelligence, or other technical means.

Protect the Site

1-113. Commanders establish and maintain protection of the site throughout the execution of any SE operation. The element designated to protect the site must prevent interference with the search element. Elements responsible for protection of the site normally perform one of the following tasks: seize, secure, cordon, control, contain, isolate, or clear. Units apply the appropriate tactical methods such as inner and outer cordons, traffic control points, or a combination of methods and tasks to control the site for subsequent exploitation.

1-114. Units may encounter complex sites where it is tactically imprudent to secure or clear an area without expert assistance. Such assistance may include explosive ordnance disposal teams; military working dog teams; or chemical, biological, radiological, and nuclear units. For example, a unit may

encounter a building suspected of containing biological warfare agents. Unit leaders may suspect that hostile persons are inside a building that contains information of value. However, the unit may need to isolate or contain the site and seek technical advice from subject matter experts before securing the site for the search element. In some cases, a unit secures a site and simply waits for additional support.

1-115. Based on various factors, such as booby traps and environmental hazards, the search element employs appropriate internal security procedures. After removing any adversaries from the site and clearing hazards, security units secure access to the site to prevent destruction of information, which the search element may collect and subsequently evaluate.

Conduct a Site Search

1-116. Soldiers conduct a visual and equipment-aided site search. When conducting a site search, search teams ensure all contents of the site pass within the view of the Soldiers conducting the search. (FMs 3-90.119, FM 3-34.210, and FM 3-19.13 describe tactics, techniques, and procedures for searching individuals, areas, vehicles, and occupied and unoccupied buildings.)

1-117. Commanders' primary considerations for conducting a site search include—

- Mitigating risk.
- Using systematic search procedures to ensure that all IMP of value are discovered.
- Minimizing the time on-site in relation to security considerations.
- Minimizing the destruction of property.

Before applying invasive search techniques and collection actions, forces thoroughly document the site and its contents. Complete documentation may include written or oral descriptions, sketches, photographs, or video recordings. This documentation forms a record of the starting point for search actions.

1-118. A search can support host-nation or international authorities prosecuting criminals. Forces engaged in search operations must act, and be seen to act, in accordance with international and national laws to maintain legitimacy.

1-119. Commanders integrate tactical questioning of persons located on or around the site with the search effort. The information obtained can focus the search effort. Conversely, a search can facilitate a line of questioning based on the items identified during the search. When time is short, units screen detainees to determine which to question. Expedited tactical questioning may lead to subsequent operations.

1-120. Any trained Soldier, within legal guidelines, can conduct tactical questioning. Soldiers must be trained to conduct tactical questioning according to DODD 3115.09:

- Paragraph 3.d. (1): At a minimum, personnel who conduct, support, or participate in tactical questioning shall be trained in the law of war and humane treatment standards.
- Enclosure 2, Para. 7.d.: [Secretaries of the Military Departments shall] Provide training on the conduct of tactical questioning for appropriate personnel.
- Enclosure 2, Para. 9. e.: Commanders of the combatant commands plan, execute, and oversee combatant command intelligence interrogation operations, detainee debriefings, and tactical questioning in accordance with this Directive.

1-121. In addition to tactical questioning, commanders make effective use of human intelligence personnel to interrogate individuals. Only human intelligence collectors and other trained and certified personnel following established guidelines can interrogate individuals. Integrating human intelligence collection with the search effort leads to more rapid delivery of intelligence and information. This supports current and subsequent operations.

1-122. It is often difficult to recognize items of value. Therefore, commanders train Soldiers to recognize IMP with potential information, intelligence, or evidentiary value in conjunction with appropriate criteria. Soldiers use their cognitive skills along with systematic procedures and appropriate equipment to identify valuable items. Commanders provide training to further develop Soldiers' skills. They develop standing operating procedures, training products that support how to identify indicators, and other aids that help Soldiers recognize answers to information requirements. Commanders provide clear and specific criteria to

facilitate recognition; they require every Soldier to be a sensor. Commanders focus a search by articulating the mission's purpose.

Collect Information, Material, and Persons

1-123. After identifying potentially valuable IMP, units collect and preserve them. SE forces use systematic procedures to gather, safeguard, and maintain items for analysis. Finally, once the IMP are collected and preserved, commanders transfer control of the site to the appropriate entity. In the context of SE operations, Soldiers perform the following actions related to collecting IMP:

- Collect the potentially valuable IMP.
- Preserve the site and the IMP collected.
- Transfer control of the site.

Collect the Potentially Valuable IMP

1-124. Initially, forces document the contents of a site before collecting anything. Documentation is ongoing during collection and may include photographs, video or audio recordings, appropriate forms, and chain-of-custody procedures. Forces strictly adhere to procedures that ensure accurate documentation, including using appropriate media and official forms. When a situation requires speedy collection, a commander may consider sacrificing accuracy. However, choosing speed over the accurate documentation of IMP may mean items cannot be properly analyzed or are rendered inadmissible as evidence.

1-125. Forces handle IMP discovered during the search to preserve their integrity for further analysis. They avoid corrupting the items. Tactics, techniques, and procedures; unit standing operating procedures; rules of engagement; and host-nation requirements must be followed to ensure the IMP collected support analysis, criminal prosecution, or both. Potential forensic value, chain of custody, evidentiary procedures, and time available all influence collection priorities and procedures. (See appendix B for specific considerations for evidence handling.)

1-126. Commanders and staff determine the priorities for collection before executing the operation. Commanders set priority guidelines based on the mission's purpose and the information requirements. Applying these priorities during collection is sometimes known as triage. In general, during triage, units prioritize IMP for collection based on their information value, time-sensitivity, and perishability. For example, collection priorities might include—

- Items of immediate tactical value.
- Perishable evidence that can be altered or contaminated over time or by the elements despite protective measures.
- Items that may impede the overall search.
- Items of command significance.

1-127. Forces conduct prioritization at all levels. In the context of SE, prioritization encompasses a critical review of the IMP at the site to determine the priority for exploitation and the ultimate output required from exploitation methods. The commander determines which IMP to evacuate to higher-level exploitation facilities. Organizations providing technical support for analysis, such as explosive ordnance disposal and forensic labs, assist with the prioritization during the first technical assessment of the items. Forces prioritize efforts at every step of the operation and keep a record their decisions.

Preserve the Site and the IMP Collected

1-128. Preservation refers to protecting a site and its contents from damage, loss, or change. In general, the degree of preservation required depends on several considerations. These considerations include the—

- Purpose of the operation.
- Sensitivity of the site.
- Significance of the site.

1-129. Usually, the standard for preserving a site's contents is highest when those contents can facilitate criminal prosecution. Any potential evidence related to criminal prosecution must be kept intact. During

stability operations, supporting war crimes courts and tribunals is a primary stability task related to establishing civil control. Establishing civil control also includes protecting and securing key facilities such as places of religious worship, cultural sites, critical infrastructure, natural resources, and strategically important institutions. Examples include government or medical buildings, banks, museums, and military facilities.

1-130. In addition, Army forces help establish civil security by supporting identification programs. Examples of essential stability tasks related to civil security are securing facilities, documenting and preserving evidence, and securing documents relating to personal identification, property ownership, court records, and voter registration. (See FM 3-07 for more information about stability tasks.)

1-131. Commanders address preservation requirements in the operation order. Throughout execution, commanders ensure exploitation forces follow procedures precisely to preserve items discovered during SE operations. Commanders establish positive control of the site to limit access and minimize movement of people. They also establish control measures to avoid inadvertent destruction of evidence and to preserve the value of information obtained. The search element takes every precaution to preserve information or potential evidence in its original state until its transfer to the appropriate entity. (See appendix B.)

Transfer Control of the Site

1-132. After collecting valuable IMP from the site, forces transfer control of the site itself to another entity. (Paragraphs 1-141 to 1-144 discuss transferring the IMP collected.) Transfer of a site is usually a planned and orderly handover to an appropriate group or individual. Commanders assess the situation and the site's condition before determining how to transfer the site. Transfer of a site also includes considerations related to damage caused by SE forces, the requirements of ongoing operations (such as tempo or immediate threat to SE forces), and threats or hazards posed to civilians or military forces by the site.

1-133. If SE forces have changed, removed, or damaged any private or host-nation property, commanders consider the legal implications. Site exploitation forces document damage they have caused to sites. They ensure property owners have the opportunity to resolve claims through legal means. Forces use the minimum force to accomplish the mission; however, property damage may still occur. Commanders include host-nation and local authorities to determine the severity of the damage and record a collective understanding as to what remediation is expected.

1-134. A site may not yield anticipated intelligence or show evidence of enemy activity. In such cases a commander may decide to transfer the site back to the legal occupant or other host-nation personnel. Site exploitation forces take care to return the site as it was found, as much as reasonably possible. In limited circumstances, the commander may decide to simply abandon the site, depending on current operational requirements.

1-135. Specialized units or agencies may need to conduct the neutralization at certain sites, such as those containing chemical, biological, radiological, and nuclear threats. Normally they remove all hazardous material from the site and manually destroy the specific opponent equipment. The commander may decide to destroy a site when it poses a major threat to the civilian population or friendly forces.

1-136. A unit may initiate a SE operation and then be required to hand over the mission to another organization. In such a case, the on-site commander conducts a thorough mission briefing of all Soldiers involved in the operation to ensure no loss of continuity. The commander directs collected IMP be transferred to the gaining unit using established protocols to maintain chain of custody.

Analyze the Collected Information, Material, and Persons

1-137. In the context of SE, analyzing the collected IMP refers to using appropriate means to evaluate them and deduce their probable meaning, in relation to the operation's purpose or purposes. To analyze the collected IMP, Soldiers perform the following actions:

- Analyze collected IMP on-site.
- Transfer IMP indicated for further processing.
- Analyze the transferred IMP off site.

1-138. Forces conduct initial analysis on the site using organic capabilities. If necessary, they transfer selected items to a lab or other facility located away from the site or even outside the theater of operations.

Analyze the Collected IMP on-site

1-139. Site exploitation teams analyze IMP on-site to answer to CCIRs. Soldiers immediately report and track on-site information that contributes to planning and decisionmaking or is highly perishable.

1-140. Augmentation from specialized assets enhances on-site analysis and development of intelligence. This supports subsequent operations such as a raid or attack. For example, a SE force can be augmented with TECHINT support, trained post-blast analysis explosive ordnance disposal personnel, human intelligence collection teams authorized to conduct interrogation, or forensic collection agencies.

Transfer IMP Indicated for Further Processing

1-141. After the initial on-site analysis, units transfer IMP identified as having possible intelligence value for additional processing. Forces that collect IMP ensure safe handling and transfer of the IMP beyond the organization. Units establish standing operating procedures to describe transfer procedures. Procedures include positive control measures and chain of custody for the IMP collected at the site. Forces establish and follow a protocol when transferring anything to an external source for further analysis.

1-142. Site exploitation units transport persons detained during SE operations to the appropriate facility for interrogation by trained interrogation teams. Documenting transfer of custody, identifying associated personal effects, and identifying collected material during the search support further processing and production of intelligence.

1-143. Site exploitation forces make a record of collected documents and media—such as computer hard drives and thumb drives. They deliver them to the appropriate document and media exploitation (sometimes known as DOMEX) element. This element transfers documents and media onto various database formats suitable for analysis and production of intelligence.

1-144. Forces document and deliver material such as weapons, explosives, and other technical threat items to the appropriate TECHINT organization. Higher headquarters may establish a center, such as a captured materiel exploitation center, to process captured threat items. Technical intelligence elements and special teams or working groups established by combatant commanders provide specialized technical analysis support. For example, during Operation Iraqi Freedom, United States Central Command established ad hoc organizations such as Joint Task Force–Troy to provide technical analysis of captured materiel used for improvised explosive devices.

Analyze the Transferred IMP Off Site

1-145. In addition to the on-site analysis, further analysis of selected IMP continues off-site. Site exploitation forces promptly pass on potentially valuable information to all appropriate organizations through normal intelligence channels. Intelligence organizations analyze the IMP to produce intelligence.

1-146. The intelligence process is generally the same both on and off the site. However, forces conducting analysis off site usually have access to intelligence reachback capabilities and depth of expertise beyond those normally found at the BCT level.

1-147. Following analysis, commanders assess information and materials collected to determine their final disposition. Based on the assessment, the commander initiates the final transfer of information and materials. This can include—

- Destruction.
- Long-term storage and maintenance.
- Transfer to other organizations.
- Return to appropriate host-nation person or group.

Disseminate Information and Intelligence

1-148. Dissemination involves distributing relevant information from one person or place to another in a usable form. In the context of SE, Soldiers perform the following actions to disseminate information and intelligence:

- Establish connectivity with intelligence organizations.
- Share data, information, and intelligence through appropriate channels.

Various organizations—such as forensic facilities, document and media exploitation teams, and TECHINT elements convert the collected information into useable form to share and analyze with the goal of developing intelligence.

Establish Connectivity

1-149. Effective dissemination requires connectivity with supporting intelligence organizations. Brigades establish access to databases and information portals that facilitate self-service of information requirements by commanders and their staffs. The staffs follow up with supporting agencies to capitalize on the information processed from tactical operations.

1-150. A database provides a bridge allowing different systems with different purposes to work together. For example, *Harmony* is the national intelligence database for foreign document and media exploitation and translations management. It is the single, comprehensive bibliographic reference for all available primary source foreign technical and military documents and their translations. The Harmony database supports tactical through strategic users, and is available to all units with access to the SECRET Internet Protocol Router Network, Joint Worldwide Intelligence Communications System, or StoneGhost networks. Through a common database, multiple applications can simultaneously use the same data for different purposes at different echelons.

Share Data, Information, and Intelligence Through Appropriate Channels

1-151. Commanders do not assume that dissemination of analyzed information is automatic. BCTs and subordinate organizations submit requests for information or coordinate with liaison personnel to obtain information from or share it with various intelligence resources and higher headquarters.

1-152. Most TECHINT data is distributed using the Distributed Common Ground System–Army, the Army's battle command intelligence network, at multiple security levels. Initial TECHINT reports flow through the maneuver intelligence staff officer or assistant chief of staff, intelligence, or other the reporting channels. Other intelligence channels include a joint captured materiel exploitation center, interagency networks, and intelligence networks in the continental United States.

1-153. Common databases provide powerful tools for transforming data into the information and knowledge required for decisions. Data in a database can be stored, organized, and queried to support further analysis based on models reflecting commanders' decision-making needs. For example, software applications can compare data collected from a series of improvised explosive device detonations to determine similarities between events and identify commonalities in support of link and pattern analysis.

Chapter 2

Specialized Support Assets for Site Exploitation

The brigade combat team may obtain augmentation to support numerous specialized requirements. This chapter discusses Army assets commanders are likely to use for task-organizing site exploitation teams; it does not provide an exhaustive list. In addition, commanders may create ad hoc organizations based on their specific mission and operational environment.

BRIGADE COMBAT TEAM ASSETS TO SUPPORT SITE EXPLOITATION

2-1. The brigade combat team (BCT) has organic assets that may be tasked to conduct or assist in conducting a site exploitation (SE) mission. However, there are relatively few Soldiers with specialized skills, and most are assigned to a brigade special troops battalion (BSTB). The commander and staff use the composite risk management process to determine the risk of using organic specialized assets with limited availability to support SE missions. The BCT staff then receives additional guidance from the commander regarding integrating organic specialized assets into SE operations.

2-2. The BCT's SE team may be augmented with enablers external to the BCT. The SE team is task organized to meet any special requirements depending on mission variables. Teams exploiting sites containing hazardous or sensitive materials require augmentation. For example, a mission to exploit a bombmaker's workshop would require an explosive ordnance disposal team to render safe any devices before SE operations commence. See chapter 3 for more information about sensitive sites.

2-3. In full spectrum operations, commanders balance the risk of using limited resources for a SE operation versus continuing the tactical mission. Time is a significant factor when conducting SE operations with organic assets. Using specialized assets for a brief period to determine a site's potential to yield valuable information is not likely to degrade the capabilities of the BSTB or BCT. However, when using specialized assets for an extended period may, the commander and staff periodically re-assess the risk.

SUPPORT FOR ENVIRONMENTAL CONSIDERATIONS

2-4. Environmental considerations have several implications for SE operations. These considerations affect all levels of war. Commanders and their staffs consider how their missions might affect the environment; they avoid unnecessary environmental damage. They understand the strategic, operational, tactical, and ethical requirements of environmental protection. The engineer coordinator advises the commander on environmental issues. Working with other staff officers, the engineer coordinator determines the impact of operations on the environment.

2-5. Environmental damage is an inescapable consequence of combat operations. However, the revolution in military technology has made it possible to minimize the collateral damage from legitimate military operations. It is seldom necessary to obliterate terrain to achieve the desired military effect. It is imperative that organizations develop additional environmental procedures to support SE operations. Forces practice routine environmental protection measures during execution. Actions required during or after operations may include—

- Conducting remediation operations after the discovery of toxic industrial chemicals.
- Integrating force health protection considerations in densely populated areas that are impacted by SE operations.
- Responding to environmental terrorism or sabotage.
- Working within the limitations brought about by environmental considerations.
- Remedying adverse environmental impacts as a part of the exit strategy.

For further information concerning environmental considerations in military operations, see FM 3-34.5.

SUPPORT FOR CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR REQUIREMENTS

2-6. Exploitation of a site containing chemical, biological, radiological, and nuclear (CBRN) materials is complex due to technical demands and the numerous program and infrastructure components that must be addressed. The challenges are compounded by political, military, humanitarian, and environmental considerations. Commanders planning a SE mission involving CBRN materials must understand the range of capabilities required to address them. In addition, commanders must be familiar with the military and civilian organizations that have roles in accomplishing or overseeing various aspects of the mission (see appendix A).

2-7. Units conducting SE at sites with CBRN materials need proper technical assets to conduct assessments. These assessments determine exactly what types of materials are at the site and what types of capabilities are needed for rendering safe and the disposing of contaminated materials found on-site.

2-8. Tasks related to CBRN materials include locating, identifying, and securing materials, weapons, equipment, persons, and infrastructure to create forensic evidence. (A site with CBRN materials may be considered a crime scene.) Locating and securing a site with CBRN materials requires robust intelligence support. It also requires task-organized forces capable of maneuvering in all environments, from combat to permissive conditions and across varied terrains. For certain sites, a hasty or deliberate attack against enemy forces may be necessary, requiring ground combat forces and supporting indirect fire or close air support.

2-9. Forces conducting SE at a site with CBRN materials may be required to collect and process hazardous materials. Commanders ensure forces have the technical knowledge and tactical skills to conduct detection and decontamination of persons and equipment. Furthermore, if security support is not immediately available, forces conducting SE may be required to protect the site from enemy attempts to recapture or remove valuable items or individuals.

2-10. During planning, commanders must estimate and prioritize the full range of requirements. This includes determining the number of sites, the types of sites, and the tasks that must be accomplished compared against the qualified personnel, resources, and time available.

2-11. BCTs possess limited CBRN mitigation capabilities. BCTs usually conduct operations involving CBRN materials in conjunction with multinational military and civilian partners. Many of these partners have developed niche capabilities in detection, decontamination, and destruction of CBRN agents.

Chemical, Biological, Radiological, and Nuclear Reconnaissance Platoon

2-12. The CBRN platoon provides CBRN reconnaissance, surveillance, and limited consequence management support to the BCT. A CBRN reconnaissance platoon is assigned to the BSTB for infantry and heavy BCTs. A CBRN reconnaissance, surveillance, and target acquisition squadron is assigned to the Stryker BCT. These platoons vary by crew size, assigned equipment, and mobility platform. Table 2-1 shows an abbreviated list of the CBRN reconnaissance platoon's capabilities related to SE.

Table 2-1. Some site exploitation capabilities of the CBRN reconnaissance platoon

- Dismounted CBRN reconnaissance.
- Detecting and assessing CBRN hazards through reconnaissance, surveys, and surveillance.
- Providing early warning of contamination at exploited sites.
- Presumptively identifying known agents and materials found on the site.
- Coordinating evacuation of CBRN samples.
- Engaging level-I threats (a small enemy force that can be defeated with a unit's organic resources).

2-13. Knowing the agent, delivery system, and other items helps the commander take appropriate offensive and defensive actions. To support this knowledge, CBRN reconnaissance units possess limited sampling capabilities as part of their normal operations. Regardless of what type of CBRN unit is assigned to the BCT, the collection, reporting, and administrative procedures pertaining to sampling operations are similar. Laboratory analysis identifies the sample, agent characteristics, toxicity, persistency, hazards to personnel, decontamination procedures, and first aid procedures.

Chemical, Biological Sampling Operations

2-14. The chemical officer assigned to the BCT coordinates with the intelligence staff officer for chemical or biomedical sampling operations. The intelligence staff officer is the primary staff responsible for control of chemical and biological sampling operations within the area of operations. The intelligence staff officer coordinates with the operations staff officer, command surgeon, and the area of operations chemical officer to plan missions for chemical and biological sampling assets. Typically, the assigned CBRN unit with the BCT is the only authorized, trained, and equipped element to collect chemical or biological samples.

2-15. Biomedical samples taken from affected individuals or corpses normally are collected by—

- Battalion-level medical units.
- Division-level medical treatment facilities.
- Major hospitals.
- Evacuation hospitals.
- CBRN reconnaissance units (assisted by medical personnel).

ENGINEER ASSETS

2-16. Each of the combined arms battalions in a heavy BCT or in a Stryker BCT has an engineer company. The infantry BSTB has an engineer company. The engineer company organic to the BSTB consists of a headquarters section, two combat engineer platoons and an obstacle reduction section. The engineer company is capable of—

- Assessing and marking of unsafe structures on the site.
- Supporting exploitation by assisting mobility and site access.
- Identifying and preparing barriers to isolate the site, particularly when the site is located in or near an urban area.
- Clearing sites using mine detection systems.
- Identifying environmental hazards.

GEOSPATIAL ASSETS

2-17. Geospatial assets organic to the BCT can assist with SE by providing maps. For complex operations, the engineer coordinator or the intelligence staff officer in the BCT staff can obtain division- or higher-level geospatial support. For example, support is available through the Facilities, Infrastructure, and Engineering Systems (known as FIRES), a program of the National Ground Intelligence Center. FIRES is the national database for architectural drawings and blueprints of facilities, infrastructures, and engineering systems of operational or intelligence interest to the U.S. government. The images are retrievable by any

governmental agency that has a need for such information. FIRES could be extremely helpful when exploiting structures of strategic importance.

MILITARY INTELLIGENCE

2-18. The military intelligence company conducts intelligence, surveillance, and reconnaissance (ISR) analysis, intelligence synchronization, and human intelligence collection. The military intelligence company supports the BCT and its subordinate commands through collecting, analyzing, and disseminating intelligence information and products. It provides continual input for the commander through maintaining the threat portion of the common operational picture. It provides analysis and intelligence synchronization support to the BCT intelligence staff officer. The military intelligence company also collaborates with the BCT operations staff officer in integrating ISR tasks and coordinating requirements and human intelligence operations as directed by the BCT operations staff officer and the counterintelligence and human intelligence staff officer. The military intelligence company contains an analysis and integration platoon, a tactical unmanned aircraft system platoon, and a ground collection platoon.

The Military Intelligence Company Analysis and Integration Platoon

2-19. The analysis and integration platoon provides the BCT intelligence staff officer analytical support. The ISR requirements section and the situation and target development section co-locate with the brigade command post and are under operational control of the BCT intelligence staff officer. They provide the BCT intelligence staff officer automated intelligence processing, analysis, and dissemination capabilities as well as access to the intelligence products of higher echelons.

2-20. The analysis and integration platoon is the brigade intelligence staff officer's principal support organization for general military intelligence, target intelligence, and ISR management. They are all-source, multidiscipline intelligence organizations with organic analysis, management, and information technology capabilities to perform these tasks across full spectrum operations. Analysis and integration platoon intelligence products and databases support the intelligence staff officer in—

- Advising the brigade commander and staff.
- Analyzing and presenting the current threat situation.
- Analyzing and war-gaming future threat courses of action.

2-21. The analysis and integration platoon uses its Distributed Common Ground System-Army database to track and analyze threat information, including threat movement and threat combat effectiveness. Using the Distributed Common Ground System-Army database, platoon personnel pull intelligence and relevant information from external intelligence organizations to enhance analysis, understanding, and reporting. The platoon uses this system to create graphic and textual products that depict the results of its analysis. The analysis and integration platoon shares its information and conclusions with the brigade, its subordinate element's intelligence staff officer, and higher and lateral echelon intelligence organizations. The analysis and integration platoon responds to the information requirements of the intelligence staff officer and requests for information from intelligence staffs throughout the brigade.

2-22. The analysis and integration platoon develops, manages, and communicates all-source and multidiscipline intelligence. As with all military operations, the analysis and integration platoon leader must review platoon organization based on the factors of METT-TC (mission, enemy, terrain and weather, troops and support available, time available, civil considerations) to ensure the proper personnel, equipment, and support are in place to execute each mission.

The Military Intelligence Company Tactical Unmanned Aircraft System Platoon

2-23. The tactical unmanned aircraft system platoon provides the commander real-time visual imagery in support of reconnaissance and targeting operations. The platoon's aircraft can deliver imagery for planning purposes as well as for ongoing operations. This imagery gives a commander a number of capabilities, including—

- Enhanced situational awareness.
- Target acquisition.
- Enhanced force protection.

The Military Intelligence Company Ground Collection Platoon

2-24. The ground collection platoon contains the BCT's signals intelligence and human intelligence collection assets. During operations, it is extremely likely these assets will be assigned across the brigade's area of operations. They may be tasked to support subordinate brigade elements. The Prophet control section provides mission management, correlates direction-finding data, and reports combat information on threat emitter activity and position. The operational management team and human intelligence collection teams provide the BCT with an organic capability to conduct human intelligence collection. The human intelligence capability is directed toward assessing the enemy and civil considerations to answer the BCT commander's information requirements.

2-25. Signals intelligence is intelligence-gathering by interception of signals, primarily between people (communications intelligence) or between machines (electronic intelligence), or a combination of the two. Communications intelligence may provide some or all of the following:

- Who are transmitting and what their locations are. (If the transmitter is moving, it is possible to plot the signal against location.)
- The transmitter's relationship or function within an organization.
- The frequencies used and other technical characteristics of the transmission.
- The time and duration of the transmission (and the schedule if it is a periodic transmission).
- If the transmission is encrypted and if it can be decrypted.
- If it is possible to intercept a signal transmitted in clear text or obtain it through cryptanalysis, communications intelligence can determine the language used in the communication and provide a translation.
- The addresses, if retrievable from the message. This may include communications intelligence (such as a confirmation of the message or a response message), electronic intelligence (such as a navigation beacon being activated) or both.
- Information on the location and signal characteristics of the responder.

2-26. The military intelligence company's electronic warfare capability dwells in the Prophet section of the ground collection platoon. The Prophet section conducts electronic warfare operations. Prophet collection teams detect, locate, and track threat communications emitters to include frequencies used to initiate improvised explosive devices. This information becomes part of the common operational picture and enables the commander to array electronic warfare assets accordingly. If capable of electronic attack, the teams deliver nonlethal effects (such as jamming) against selected improvised explosive devices to deny, disrupt, and delay the threat's ability to target friendly forces. Whether operating independently or as part of a direction-finding baseline, the teams position themselves where they can detect threat emitters and communicate with the multisensor control team.

2-27. The human intelligence collection section has one operational management team and three human intelligence collection teams. The human intelligence collection teams are task organized and placed based on METT-TC to fulfill the commander's critical information requirements. The BCT's human intelligence assets are most effective in a small-scale contingency and are an excellent resource to augment an SE team.

2-28. Well-focused and synchronized human intelligence can provide the BCT commander and staff with an enhanced understanding of the threat. Operations in a small-scale contingency rely heavily on extensive

and continuous interpersonal contact throughout the area of operations. However, human intelligence collection teams must be prepared to conduct operations across the spectrum of conflict.

2-29. Human intelligence collectors working in conjunction with SE operations contribute to developing an understanding of the current situation by questioning local inhabitants and debriefing friendly forces. They also conduct tactical questioning and interrogation of detained persons at the exploited site before their transfer to holding facilities. Additionally, they conduct document and media exploitation. Site exploitation units provide human intelligence collectors with pertinent point-of-capture data for all information, material, and persons (IMP) acquired from a site. (See paragraph 1-2 regarding potential sources of information at a site.) Human intelligence collection teams use the point-of-capture information to exploit the IMP for intelligence.

2-30. Products and intelligence derived from document and media exploitation can be a significant force multiplier for the commander. Document and media exploitation must be conducted with sufficient speed and accuracy to satisfy the commander's critical information requirements and enable operations that interrupt the enemy's decision cycle. All Soldiers must be able to correctly identify and collect IMP for further exploitation to avoid the inadvertent loss of valuable information.

MILITARY POLICE

2-31. The BSTB headquarters company contains a military police (MP) platoon. This MP platoon has the potential for fulfilling limited security and forensic missions in support of SE operations. Its capabilities include—

- Isolating and securing the site by establishing a restricted perimeter, providing access control, and preventing evidence destruction.
- Conducting site searches and evidence collection and management activities. (See Appendix B for details about evidence collection.)
- Conducting the initial assessment of suspected mass graves, torture chambers, and war crimes sites.
- Segregating and processing personnel encountered at the site and evaluating them for possible detention and interrogation.
- Processing captured documents and equipment.
- Conducting police intelligence operations through the collection of police information.
- Conducting crowd control operations.

2-32. The criminal investigation division (CID)—

- Deploys highly trained special agents and support personnel, including computer crimes specialists.
- Operates a certified forensic laboratory, a protective services unit, and polygraph services.
- Conducts criminal intelligence collection and analysis.
- Operates a variety of other services associated with law enforcement activities.

2-33. Additional MP assets may be required once a site has been secured by the organic MP unit. MPs have many potential roles. Mission planners coordinate and allocate support from the MP and criminal investigation division (CID), based on the type of site and anticipated conditions.

2-34. Some MP support capabilities include—

- Providing access control at captured intelligence facilities or sites related to CBRN materials.
- In coordination with CID, investigating mass graves, torture chambers, and other war crimes sites.
- Evaluating personnel on-site for possible detention and interrogation. (CID agents also may be needed to interview suspects or collect witness statements).
- Assisting in establishing a chain of custody for material captured at the site.

(When material collected will be used in legal proceedings, a proper chain of custody for evidentiary purposes must be established. See appendix B.)

EXPLOSIVE ORDNANCE DISPOSAL ASSETS

2-35. The BCT usually requires explosive ordnance disposal support for destruction of ammunition, and rendering safe improvised explosive devices (IEDs) and unexploded explosive ordnance. Explosive ordnance disposal capabilities are not organic to the BCT. However, higher headquarters usually provides explosive ordnance disposal augmentation to support BCT operations. Usually, one explosive ordnance disposal company is attached to each deployed BCT; the company is then attached to the BSTB.

2-36. The explosive ordnance disposal company is the only force equipped, manned, and trained to positively identify, render safe, and dispose of U.S. and foreign CBRN and explosive ordnance and improvised explosive devices. The explosive ordnance disposal company conducts SE and technical intelligence (TECHINT) collection and analysis of explosive ordnance and components. Tactical commanders must plan for explosive ordnance disposal support, when possible. Explosive ordnance disposal support is likely to be a limited commodity with high demand.

2-37. When explosive ordnance disposal cannot be integrated into the SE team, senior tactical commanders plan for the movement of explosive ordnance disposal teams to sites requiring special support. Explosive ordnance disposal teams can provide the ability to—

- Identify and collect ordnance, IEDs, and related components.
- Conduct render-safe procedures on ordnance and IEDs.
- Conduct disposal procedures on ordnance and IEDs.
- Conduct ordnance technical intelligence operations.
- Conduct post-blast analysis.

ADDITIONAL BRIGADE-LEVEL ASSETS FOR SITE EXPLOITATION

2-38. Some search missions present hazards to personnel and require solutions to mitigate the risk of harm. Other search missions such as area search are time consuming and may require more time than is available with organic equipment. These missions require specialized assets such as robots or search dog teams to protect Soldiers or help them search thoroughly and quickly.

TACTICAL MOBILE ROBOTS

2-39. During recent operations, tactical mobile robots have supported nearly every warfighting function. When equipped as multifunctional platforms, robots may be a huge force multiplier to a unit involved in SE. Robots can be fitted with a wide variety of cameras, sensors, and tools. This allows otherwise hazardous tasks to be performed safely from a secure location via remote control. Originally designed to assist in the identification and neutralization of explosive ordnance, robots can be modified to provide a wide range of capabilities. A few of the tasks that can be performed by a robot via remote control are—

- Area, building, and vehicle search.
- Detecting hazardous material.
- Neutralization of unexploded ordnance and unidentified explosive hazards.
- Moving weapons and other heavy payloads.

SPECIALIZED SEARCH DOG TEAMS

2-40. A specialized search dog team consists of one trained dog and one school-trained handler. Specialized search dog teams are controlled by MPs and engineers. The mission of the specialized search dog team is to support SE operations by detecting firearms, ammunition, and explosives in—

- Buildings (occupied, unoccupied, or derelict).
- Vehicles (cars, trucks, trains, ships, boats, or aircraft).
- Open areas (fields, islands, woods, hedgerows, or embankments).

SITE EXPLOITATION ENABLERS AT ECHELONS ABOVE BRIGADE

2-41. Additional specialized assets can be requested through brigade and higher headquarters to assist SE operations. These enablers are not readily available to the BCT commander and must be requested with sufficient justification to warrant their assistance. Examples of enablers that can be requested are special operations forces and the Asymmetric Warfare Group. In addition, in certain areas of operations, ad hoc organizations may be available to support SE.

ARMY SPECIAL OPERATIONS FORCES

2-42. Special operations forces are critical in meeting the challenges of the BCT in today's operational environment. They offer capabilities that are not only rapidly deployable but also uniquely flexible across full spectrum operations. Army special operations forces include special forces, rangers, special operations aviation, civil affairs, and psychological operations.

2-43. Special operations forces can reinforce, augment, and complement conventional forces. They can operate independently in missions that demand small, discrete, highly trained forces. Army special operations forces are unique in their ability to mesh with indigenous forces; this is a tremendous force multiplier for SE.

2-44. Special operations forces may be tasked with SE missions. These missions have a global impact on the joint force commander's campaign because they provide deeper intelligence on enemy activity. These missions are highly sensitive, and the slightest contamination of evidence may compromise the mission. Special operations forces are exceptional combat multipliers and provide effects that are central to the success of the BCT.

ASYMMETRIC WARFARE GROUP

2-45. The Asymmetric Warfare Group is a special mission unit that provides operational advisory assistance to Army and joint force commanders. The Asymmetric Warfare Group assists both in predeployment and within the area of operations. This assistance enhances the combat effectiveness of the operating force and enables the defeat of asymmetric threats. It also provides key observations for senior leaders and advises senior leaders on policy and resource decisions.

2-46. The Asymmetric Warfare Group deploys and sustains its forces worldwide to observe, assess, and analyze information about the evolving security environment, including emerging asymmetric threats. These observations are assessed and disseminated through globally postured advisory assistance elements in support of Army and joint force commanders. The Asymmetric Warfare Group further assists in the identification, development, integration, and transition of materiel and nonmaterial solutions for SE.

EXAMPLE OF AN AD HOC ORGANIZATION

2-47. On example of an ad hoc organization was known as a joint task force for elimination of weapons of mass destruction. It provided on-site weapons of mass destruction (WMD) and chemical, biological, radiological, nuclear, and high-yield explosives expertise. Some of its capabilities were—

- Deployable WMD coordination elements.
- Deployable nuclear disablement teams.
- A mobile analytical laboratory for chemical, biological, and radiological analysis.

SUPPORT FROM NON-ARMY ENTITIES

2-48. A commander may also request support from other government agencies or departments in the area of operations. A list of organizations available to support SE operations is in appendix A.

TECHNICAL INTELLIGENCE SUPPORT FOR SITE EXPLOITATION

2-49. The 203d Military Intelligence Battalion is the only TECHINT battalion for the Army. The 203d Military Intelligence Battalion is the link between the scientific and TECHINT community and the operational commander. The mission of the 203d is to deploy worldwide to support strategic- through tactical-level TECHINT requirements. The 203d Military Intelligence Battalion establishes a captured materiel exploitation center (CMEC) for the joint task force commander, under the theater military intelligence brigade. The 203d fulfills Army TECHINT requirements stated by the National Ground Intelligence Center and battlefield commanders. (See FM 2-22.401 for more information on the CMEC.)

2-50. The responsibilities of the 203d are—

- Support U.S. Army Intelligence and Security Command's foreign materiel acquisition and foreign materiel exploitation activities, as directed.
- Analyze and exploit TECHINT-related captured enemy documents and media.
- Report on the capabilities and limitations of enemy combat materiel.
- Recommend countermeasures on threat technological advantages.
- Supervise evacuating items of TECHINT interest.
- Provide task-organized battlefield TECHINT teams to the supported command.
- Provide weapons TECHINT expertise.

2-51. Other technicians and specialists in disciplines such as medical, explosive ordnance disposal, and engineering may augment the CMEC. When subject matter experts from other Services augment the CMEC, it becomes a joint CMEC. When subject matter experts from other nations augment it, the CMEC becomes a multinational joint CMEC (usually known as a combined CMEC). The CMEC is the central location for the collection, safeguarding, identification, battlefield exploitation, reporting, and evacuation of captured enemy materiel that has intelligence value.

2-52. After the TECHINT unit takes custody of captured enemy materiel at a site, it begins the intelligence analysis. The TECHINT team determines which IMP require transfer for off-site analysis and prepares the items for transport. Analysts use a checklist and standing operating procedures established by the CMEC. TECHINT teams determine and coordinate the final disposition of the captured enemy materiel.

TECHNICAL ESCORT UNIT

2-53. The technical escort unit is capable of no-notice deployments. It can provide advice, verification, sampling, detection, mitigation, render-safe, decontamination, packaging, escort, and remediation of chemical and biological devices or hazards worldwide in support of TECHINT.

MANEUVER ENHANCEMENT BRIGADE

2-54. The maneuver enhancement brigade is designed as a command and control headquarters with a robust multifunctional brigade staff optimized to conduct maneuver support operations. Maneuver support

operations integrate key protection and mobility capabilities, tasks, and systems to assure freedom of action for the supported force. The maneuver enhancement brigade contains no organic units other than its organic headquarters and headquarters company, signal network support company, and brigade support battalion. The maneuver enhancement brigade can provide unique and critical capabilities to BCT commanders.

2-55. The maneuver enhancement brigade staff includes CBRN, engineer, and MP functional operations and planning cells. Each maneuver enhancement brigade is uniquely tailored with augmentation for its directed mission. A maneuver enhancement brigade typically includes a mix of several types of battalions and separate companies and may include civil affairs, CBRN, engineer, explosive ordnance disposal, and MP units. It may be augmented with MI assets and possibly a tactical combat force when assigned an area of operations with a level-III threat.

2-56. The four primary mission sets performed by the maneuver enhancement brigade include—

- Maneuver support operations.
- Support area operations.
- Consequence management operations.
- Stability operations.

See FM 3-90.31 for additional information about the maneuver enhancement brigade.

Chapter 3

Considerations for Sensitive Sites

This chapter discusses characteristics of sensitive sites and related challenges. The considerations discussed in this chapter include task-organizing for sensitive sites and terminating operations.

CHARACTERISTICS OF SENSITVE SITES

3-1. In general, the information, materials, or persons (IMP) a sensitive site contains could cause embarrassment, compromise, or threat to United States security or national interests. (See paragraph 1-2 regarding potential sources of information at a site.) Therefore, a sensitive site requires special considerations and actions. Criteria for determining that a site is sensitive are based on formally promulgated national- and theater-level guidance. In a given operation, the commander normally provides clear and precise criteria for identifying sensitive sites in a fragmentary order. A sensitive site can present unusual risks or hazards to military and civilian personnel. The IMP at a sensitive site may possess high technological, cultural, or monetary value. Exploiting a sensitive site may require a force with special capabilities to search for, collect, and analyze IMP. If a commander determines that IMP at a sensitive site do not support military information requirements, the commander transfers control of the site to the appropriate host-nation authorities.

EXAMPLES OF SENSITIVE SITES

3-2. Planning for sensitive sites is challenging—no complete list of sensitive site types is possible. Sensitive sites seldom fit neatly into categories, and their discovery is often unexpected. The uncertainty of war guarantees that new and unique sites will continue to be discovered. However, some types of sites have common characteristics that make planning for them somewhat predictable. Some examples of sensitive sites are—

- Chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) facilities.
- Locations containing evidence of war crimes, such as mass graves, illegal detainment facilities, and clandestine command and control facilities.
- Terrorist training camps.
- Prisoner of war locations.
- Research and production facilities involving breakthrough technologies.
- Government buildings and infrastructure of strategic value.
- Official government residences.
- Sites suspected of harboring enemy leaders or other highly sought-after persons.

PLANNING FOR COMPLEX SITES

3-3. The size and complexity of some sensitive sites may require multiple teams of specialists. The headquarters committing the teams (for example, the joint task force commander) designates a single site exploitation (SE) team coordinator for all teams exploiting the site. In rare instances where multiple exploitation teams arrive without a designated leader, the senior tactical commander should coordinate SE operations. See paragraphs 3-23 to 3-25 for more information on task-organizing a team to exploit a sensitive site.

3-4. Commanders must ensure Soldiers have sufficient command guidance to exercise individual initiative and maintain accountability. Even a task organized sensitive SE team conducting deliberate operations based on accurate intelligence may encounter unanticipated situations. Early in World War II,

for example, Army forces uncovered large caches of stolen art treasures hidden by the Nazi Party. A lack of guidance about safeguarding these sites resulted in Soldiers looting the contents. Teams were eventually created and procedures established for recovering stolen works of art and maintaining accountability.

SPECIAL RISKS TO MILITARY AND CIVILIAN PERSONNEL

3-5. Sensitive sites often pose special risks. Site exploitation operations may occur at locations where weapons of mass destruction were produced. Sites may contain toxic industrial chemicals. Environmental conditions determine the requirement for protective equipment. However, using protective equipment can negatively affect a team's efficiency and pace. The commander prioritizes and analyzes the environmental risks associated with a SE operation. Protecting Soldiers remains one of the commander's highest priorities.

3-6. Commanders carefully consider the effects of the operation on noncombatants. They develop guidance in case operations at the site expose noncombatants to chemical or biological hazards. Proximity of noncombatants to the sensitive site may require placing equipment for detecting toxic chemical or materials. This may lead to a request to the Provost Marshal or host-nation authorities to relocate displaced civilians outside the hazardous area.

3-7. Unless otherwise directed, units treat persons found inside a site as detainees. Forces search, silence, segregate, safeguard, tag, and evacuate detainees to a facility where qualified intelligence personnel can interrogate them and determine their status.

3-8. Combat in and around sites with hazardous chemicals or materials may expose friendly forces to the unintended release of toxic materials from the site. The danger to friendly forces is dramatically increased if the enemy threatens to release toxic biological or chemical agents or explode a radiological dispersal device. During planning, commanders and staffs consider tactics, techniques, and procedures for offensive combat operations in a CBRNE environment if toxic industrial chemicals or materials are suspected.

DELIBERATE AND HASTY OPERATIONS FOR SENSITIVE SITES

3-9. Sensitive site operations may be deliberate or hasty (see paragraphs 1-54 to 1-58). In deliberately planned sensitive site operations, the commander provides the SE team detailed criteria for recognizing appropriate IMP, usually in a fragmentary order. The preliminary information leading to the operation may come from intelligence sources and allow sufficient time for task-organizing a team.

3-10. Hasty sensitive site operations usually follow deliberate, tactical SE operations. Units conducting deliberate, tactical SE seek answers to specific information requirements. Commanders also provide them criteria for recognizing sensitive sites. Tactical units report the discovery of sensitive IMP immediately. When the presence of sensitive IMP is confirmed, the commander designates the site as sensitive and initiates hasty sensitive site operations.

3-11. Soldiers apply the commander's criteria to assess the information value and sensitivity of IMP they encounter during tactical missions. However, the commander's planning is based on anticipated discoveries. In combination with the commander's criteria, Soldiers must use their instincts and professional judgment upon contact with something unexpected. Units are likely encounter IMP that do not fit neatly into the commander's criteria for sensitive sites.

3-12. The discovery of a sensitive site is of immediate interest to the area of operations' chain of command. The unit on-site provides an immediate report with as much detail as feasible—the discovering commander balances the need to report details quickly against the apparent risks. Excessive haste, for example, may lead to casualties from enemy action. Excessive caution, however, may allow the enemy to improve and reinforce defenses or succeed in removing key personnel and equipment.

3-13. Tactical units discovering a potentially sensitive site perform the actions listed below and take other actions as appropriate for the nature of the site:

- The unit commander—
  - Initiates actions for securing the site.
  - Initiates a survey and assessment of the site's contents.
  - Requests guidance from higher headquarters immediately after the initial assessment.
- The unit—
  - Secures the site and eliminates any armed resistance.
  - Records (in writing or with photographs or video, as appropriate).
  - Safeguards the site's IMP.
  - Reports, as accurately as possible, the IMP and the conditions found at the site.

The tactical rule is this: *when in doubt, secure it and report it.* A higher headquarters receiving a report of an unusual site reports to the joint force commander on the nature of the discovery and requests support for determining the value and sensitivity of the site.

SPECIAL CHALLENGES FOR SENSITIVE SITES

3-14. This section highlights selected examples of sensitive sites that pose special challenges. The subsequent section discusses task organizing for sensitive sites. Sensitive sites pose significant challenges for any unit, especially if the sites are industrial facilities. The quantity, concentration levels, or possibly unknown nature of the materials may exceed the capabilities of a tactical unit. In these cases, tactical units seize, secure, and preserve the integrity of the site pending arrival of qualified personnel to exploit the site or provide a reach-back capability. Commanders anticipate and prepare for any special support requirements. This section discusses two general categories:

- Research and development facilities (usually related to CBRNE materials).
- Sites with evidence of war crimes.

RESEARCH AND DEVELOPMENT FACILITIES

3-15. In addition to offices and laboratories, research and development facilities can include testing, equipment, and storage facilities. Research and development facilities study new materials, equipment, and techniques for their future employment. Facilities that conduct defensive research typically possess some quantity of chemical or biological agents that may be a toxic hazard to the SE force. Levels of sophistication can vary widely, from rudimentary to highly sophisticated. Site exploitation units exercise great caution, as the presence new, novel, or especially dangerous agents could have disastrous consequences.

3-16. Testing facilities are usually operated in conjunction with research and development facilities. Testing facilities may be open-air or enclosed in a protected building. Open-air sites can present residual hazards for personnel in or near them. Many of these sites are associated with storage facilities that present additional hazards. Missile engine testing facilities and missile engine test stands, for example, can yield information about the size of rocket motors or missile engines being tested. This information may also help friendly forces calculate enemy weapons specifications, such as maximum payloads and missile range.

3-17. Equipment facilities can provide valuable information regarding the direction and sophistication level of the enemy's militarization efforts. Storage facilities can contain hazardous chemical, biological, radiological, or other toxic materials. These materials can provide valuable information regarding the direction and sophistication level of the enemy's militarization of commercial products. These sites may range from state-of-the-art armored bunkers to materials buried in an underground cache. Units approach all storage sites with caution.

3-18. Facilities and equipment associated with CBRNE research, development, and production can provide valuable information regarding the direction and sophistication level of an enemy's weapons of mass destruction (WMD) efforts. Information gained from these sites can produce intelligence in areas such as the focus of research activities, intended WMD use, and noncompliance with treaties or other international

agreements. Items of interest can include computers and electronic storage media, paper files, blueprints, drawings, and key personnel that can provide further information and insights regarding the site's activities. Ideally, the initial analysis of a sensitive site provides timely intelligence to commanders at the tactical level that can be readily exploited.

SITES WITH EVIDENCE OF WAR CRIMES

3-19. A war crime is any violation of the Law of War by any person or persons, military or civilian. The Law of War is derived from two principal sources. One is lawmaking treaties or conventions such as The Hague and Geneva Conventions. The other is a body of convention firmly fixed by the customs of a nation and recognized by authorities on international law. (See DA Pam 27-1 and FM 27-10.)

3-20. There is no standard description of a site with evidence of war crimes. Guidance for the tactical commander as to what is defined as a war crime site may be found in theater or command operations orders. Only U.S. government and international legal officials can determine if a site contains evidence of a war crime.

3-21. Tactical units may be the first to discover a location at which suspected war crimes may have been committed. During World War II, the Vietnam War, Operation Iraqi Freedom, and smaller-scale contingencies such as Bosnia, Columbia, and Rwanda, Army forces discovered many war-crimes locations. In some cases, units overran prisons and concentration camps. In others, local inhabitants led Soldiers to mass graves and torture facilities.

3-22. A unit that discovers a site that potentially contains evidence of war crimes conducts the following activities:

- The unit commander—
  - Initiates actions for safeguarding and preserving the site.
  - Ensures members of the unit record the scene with video, notes, sketches, and photographs.
  - Requests guidance from higher headquarters after making an initial assessment.
- The unit—
  - Secures the site and eliminates any armed resistance.
  - Separates and safeguards captured enemies from other persons at the site.
  - Reports, as accurately as possible, the conditions and indicators at the site.
  - Assists any survivors or victims.

Ideally, units conduct these activities in sequence. In practice, however, circumstances at the site may lead to ongoing, overlapping, and simultaneous actions. Safeguarding the scene from undue change is a primary activity—preserving any evidence of war crimes is ongoing during the search of the site. (See appendix B for information about handling evidence.)

TASK-ORGANIZING FOR SENSITIVE SITES

3-23. A commander task-organizes an exploitation team specifically for each sensitive site. The commander determines the appropriate task-organization based on prior knowledge of the sensitive site, terrain, infrastructure, and enemy security. The composition of a team depends on the nature of the site and also on the available resources. Properly task-organized teams possess the expertise to exploit the site while eliminating any threat posed by material found inside. A team may consist of Army, joint, and interagency personnel. A unit must coordinate the necessary interagency support for the exploitation. For a list of supporting non-Army organizations, see appendix A.

3-24. A commander task-organizes assets for deliberate exploitation operations before operations begin. Depending on the nature of a campaign, the joint force land component commander may form one or more special-purpose forces for the types of sensitive sites anticipated. In a hasty exploitation operation, a tactical unit may secure the site initially, followed by a team the commander rapidly organizes and deploys. Sensitive site teams almost always consist of a combination of military and interagency experts.

3-25. During Operation Iraqi Freedom, U.S. Central Command formed an ad hoc sensitive SE task force drawing on specialized CBRNE and associated technical expertise from across the Department of Defense.

Team members were drawn from the Defense Threat Reduction Agency, Defense Intelligence Agency, and explosive ordnance disposal and technical escort unit elements. The task force also received interagency attachments from the Central Intelligence Agency and Department of Justice. This task force was known as the 75th Exploitation Task Force. The task force established mobile exploitation teams based on any unique requirements identified during intelligence preparation of the battlefield. For example, Mobile Exploitation Team Alpha was augmented with a team of nuclear experts from the Defense Threat Reduction Agency to conduct the exploitation mission at the military-industrial complex near the city of Karbala, Iraq.

TERMINATING OPERATIONS AT A SENSITIVE SITE

3-26. Terminating operations at a sensitive site is extremely complex, even after the analysis has been completed and munitions rendered safe. Numerous specialized assets may be required to safeguard, prepare for movement, and transport the munitions to a secure location (see chapter 2 for more information regarding transferring control of a site). Before terminating operations at a sensitive site, commanders obtain guidance from higher headquarters regarding appropriate treatment of the site and its contents.

3-27. Exploitation of a sensitive site can be expected to be under the intense scrutiny of the host-nation government and perhaps the international news media. Sensitive site operations must show appropriate regard for private and host-nation property. The staff planning for sensitive site operations must engage host-nation authorities and the news media early in the operation.

3-28. In general, forces restore an exploited sensitive site to its original condition if possible and appropriate. The level and expediency of restoration depend on the level of force that was used during the exploitation and any hazards at the site.

3-29. Site exploitation forces may need to disable or destroy munitions found on-site, such as military ordnance or large stocks of homemade explosives. In some cases, exploitation may involve the complete destruction of facilities and equipment. Additionally, forces may have removed documents, records, and electronic storage media from the site for analysis. Forces maintain accountability of all items removed.

This page intentionally left blank.

Appendix A

Non-Army Support for Site Exploitation

The brigade combat team conducting site exploitation can obtain additional support from governmental and military organizations regardless of its area of operations. This appendix briefly describes several non-Army intelligence and forensic organizations that support site exploitation to enhance commanders' awareness and facilitate coordination.

INTERAGENCY COORDINATION

A-1. Interagency relationships are ones of coordination and mutual support, not direction. A commander may request support. The degree to which other government agencies or departments can or will provide support depends on federal statutes, policy decisions, resources, and memorandums of agreement and understanding. Commanders plan collaboratively to identify where and how they and other government agencies or departments can work together. Together, they provide mutually beneficial support through the Office of the Secretary of Defense and the joint staff to develop standing relationships with the requisite organizations.

A-2. Successful site exploitation (SE) operations coordinate with Department of Defense (DOD) and other government agencies. Often, the joint force commander supports another government agency; that organization may support a partner nation or intergovernmental organization. In particular, SE operations require significant interagency and intergovernmental coordination. Commanders may use a joint interagency coordination group or a joint interagency task force to coordinate the agencies operating in the operational area.

JOINT INTERAGENCY COORDINATION GROUP

A-3. A joint interagency coordination group enables coordination of interagency activities based on exist-in agreements. This group performs a liaison function enabling civilian and military operational planners to establish regular, timely, and collaborative working relationships. Originally formed to coordinate counterterrorism activities, joint interagency coordination groups can expand to cover all interagency coordination requirements such as SE. Commanders ensure joint interagency coordination group personnel coordinate with their parent agencies' subject matter experts. These experts understand their agencies' authorities, capabilities, and capacity to assist in given situations.

JOINT INTERAGENCY TASK FORCE

A-4. The joint interagency task force exercises tactical control over assigned elements when conducting a mission. Joint interagency task forces derive their authority from an interagency memorandum signed by the head of each participating department or agency. Joint interagency task forces currently lack authority to interdict weapons of mass destruction.

A-5. Commanders identify tasks requiring interagency support early in the planning process. These tasks may encompass diplomacy, economics, law enforcement, and information required from civilian agencies. For example, in support of SE, a commander may require national intelligence assets and Department of Justice engagement during the conduct of SE operations.

OVERVIEW OF THE U.S. INTELLIGENCE COMMUNITY

A-6. The U.S. intelligence community comprises many government and intelligence oriented organizations. Together they form a team capable of leveraging skill sets unique to each organization

without having to maintain those assets individually. Paragraphs A-7 through A-37 discusses organizations that commonly support SE operations.

DIRECTOR OF NATIONAL INTELLIGENCE

A-7. The Director of National Intelligence serves as the head of the intelligence community. This director oversees and directs the implementation of the National Intelligence Program and acts as the principal advisor to the President, National Security Council, and Homeland Security Council for intelligence matters.

A-8. The Intelligence Reform and Terrorism Prevention Act of 2004 outlines the duties of the Director of National Intelligence. The Director's duties are to—

- Ensure that timely and objective national intelligence is provided to the President, the heads of departments and agencies of the executive branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and the Congress.
- Establish objectives and priorities for collecting, analyzing, producing, and disseminating national intelligence.
- Ensure maximum availability of and access to intelligence information within the intelligence community.
- Oversee coordination of relationships with the intelligence or security services of foreign governments and international organizations.
- Ensure the most accurate analysis of intelligence comes from all sources to support national security needs.

A-9. The Director of National Intelligence has six mission managers. These mission managers oversee all aspects of intelligence related to their focus areas:

- Iran, led by the mission manager for Iran.
- North Korea, led by the mission manager for North Korea.
- Cuba and Venezuela, led by the mission manager for Cuba and Venezuela.
- Counterterrorism, led by the director of the national counterterrorism center.
- Counterproliferation, led by the director of the national counterproliferation center.
- Counterintelligence, led by the director of the national counterintelligence executive.

A-10. In each area, mission managers understand the requirements of intelligence consumers; provide consistent overall guidance on collection priorities, integration, and gaps; assess analytic quality, capabilities, and gaps; share intelligence information on the target; and recommend funding, investment, and research and development resource allocations.

CENTRAL INTELLIGENCE AGENCY

A-11. The Central Intelligence Agency provides national security intelligence to the President through the Director of National Intelligence. The Director of Central Intelligence Agency also serves as the national human intelligence manager.

A-12. To accomplish the mission, Central Intelligence Agency works closely with the rest of the intelligence community and other government agencies. Together they ensure that intelligence consumers—whether administration decisionmakers, diplomats, or military commanders—receive the best intelligence possible. The Central Intelligence Agency is organized into four mission components called directorates. These directorates carry out the intelligence process—the cycle of collecting, analyzing, and disseminating intelligence. The directorates include—

- The National Clandestine Service.
- The Directorate of Intelligence.
- The Directorate of Science and Technology.
- The Directorate of Support.

A-13. The National Clandestine Service is the clandestine arm of the Central Intelligence Agency. Its core mission is to support our country's security and foreign policy interests by conducting clandestine activities to collect information that is not obtainable through other means. The information the collected is reviewed for reliability before its dissemination to decisionmakers. This directorate also conducts counterintelligence activities abroad and special activities as authorized by the President.

A-14. The Directorate of Intelligence supports the President, administration decisionmakers, the Congress, Pentagon planners, law enforcement agencies, and negotiators. This directorate provides timely, comprehensive all source intelligence analysis on national security issues. The Directorate of Intelligence into-grates, analyzes, and evaluates information collected through clandestine and other means, including open sources, to generate value added insights. By working closely with the National Clandestine Service and other collectors, this directorate enhances the quality and timeliness of intelligence support.

A-15. The Directorate of Science and Technology works closely with the National Clandestine Service and Directorate of Intelligence to access, collect, and exploit critical intelligence. This directorate applies innovative scientific, engineering, and technical solutions. By maintaining extensive contacts with national scientific and technical communities, this directorate can rapidly assemble experts from many fields to bring the technological prowess of the United States to solve pressing intelligence and national security issues.

A-16. The Directorate of Support provides integrated, mission critical support to the entire intelligence community. This directorate's core support disciplines include human resources, financial and logistic operations, medical support, contracts and acquisitions, security, secretarial and administrative support, facilities, and integrated information technology support.

DEFENSE INTELLIGENCE AGENCY

A-17. Defense Intelligence Agency is a major producer and manager of foreign military intelligence for DOD and is a principal member of the U.S. intelligence community. This agency provides timely, objective, all source military intelligence to decisionmakers, to U.S. armed forces around the world, and to the U.S. intelligence community and force planners. This intelligence counters various threats and challenges across the spectrum of conflict.

A-18. To support all source analytical efforts, Defense Intelligence Agency directs and manages DOD in-diligence collection requirements for the various intelligence collection disciplines. These disciplines include measurement and signature intelligence, imagery intelligence, and signals intelligence.

A-19. Defense Intelligence Agency manages various national and DOD activities related to measurement and signature intelligence. Such intelligence is technically derived information that measures, detects, tracks, and identifies unique characteristics of fixed and dynamic targets. Measurement and signature intelligence technologies allow DOD to confidently monitor arms control agreements, to make smart weapons even smarter, and to support protection and missile defense efforts effectively.

A-20. To support DOD efforts in the global war on terrorism, Defense Intelligence Agency established the Joint Intelligence Task Force for Combating Terrorism to consolidate and produce all source terror-ism related intelligence. This task force leads and manages the DOD counterterrorism intelligence effort and exploits all sources of intelligence to warn U.S. forces and to support offensive counterterrorism opera-tins.

It collects, analyzes, and shares intelligence with military commanders, government officials, and other intelligence agencies.

A-21. Defense Intelligence Agency also serves as the executive agency for the U.S. intelligence community's prisoner of war and missing in action analytic cell. This unit provides actionable, national level intelligence support to locate missing, isolated, evading, or captured U.S. military or U.S. government personnel.

A-22. Defense Intelligence Agency's underground facility analysis center houses the nation's intelligence and other technical resources. It coordinates the intelligence community's efforts to detect, identify, and assess buried underground facilities and their associated programs worldwide.

A-23. Defense Intelligence Agency's Missile and Space Intelligence Center is the DOD authority on the man portable air defense system. It develops scientific and technical intelligence on foreign missile systems such as:

- Short-range ballistic missile system.
- Surface to air missile system.
- Antitank guided missile system.
- Antiballistic missile system.
- Ground based antisatellite system.
- Associated command and control systems.

A-24. Defense Intelligence Agency's National Center for Medical Intelligence provides medical profiles of foreign countries. It assesses real and potential health hazards to support U.S. forces worldwide to include humanitarian operations.

A-25. To support the growing demand for intelligence agility and global collaboration, Defense Intelligence Agency maintains the Joint Worldwide Intelligence Communications System. This system incorporates advanced networking technologies that permit a secure, high bandwidth system providing video teleconferencing and data exchange for the entire intelligence community.

A-26. Defense Intelligence Agency also assumes responsibility for managing intelligence information technology for the combatant commands. This initiative creates greater efficiency and promotes information sharing. It also encourages a single DOD data standard for information metadata tagging and ensures that every DOD system will track, tag, and store data the same way. This consolidated resource management ensures an even more integrated and interoperable intelligence information architecture.

DEPARTMENT OF HOMELAND SECURITY'S OFFICE OF INTELLIGENCE AND ANALYSIS

A-27. Intelligence in Department of Homeland Security consists of the Office of Intelligence and Analysis and intelligence offices located within Department of Homeland Security operational components. These offices focus on five principal areas: improving the quality and quantity of its analysis, integrating the intelligence elements of the department, sharing threat information and assessments with state and local governments and the private sector, ensuring Department of Homeland Security is an effective member of the national Intelligence Community, and strengthening relations with Congress.

A-28. Department of Homeland Security intelligence analysts not only track terrorists and their networks but also assess threats to U.S. critical infrastructures, bio and nuclear terrorism, pandemic diseases, threats to our borders (air, land, and sea), and radicalization within U.S. society.

NATIONAL GEOSPATIAL INTELLIGENCE AGENCY

A-29. The National Geospatial Intelligence Agency provides timely, relevant, and accurate geospatial intelligence in support of national security objectives. Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth.

A-30. Information collected and processed by National Geospatial Intelligence Agency is tailored for customer specific solutions. By giving customers ready access to geospatial intelligence, the National

Geospatial Intelligence Agency provides support to civilian and military leaders and contributes to the state of readiness of U.S. forces. This agency also contributes to humanitarian efforts such as tracking floods, tracking fires, and keeping the peace. The agency ensures access to geospatial intelligence and provides tailored, customer specific geospatial intelligence analysis, services, and solutions.

A-31. The National Geospatial Intelligence Agency's strategy supports operational readiness through a set of geospatial foundation data. These may include controlled imagery, digital elevation data, and selected information. This information can be readily augmented and fused with other spatially referenced information such as intelligence, weather, and sustainment data. The result is an integrated, digital view of the mission space.

NATIONAL RECONNAISSANCE OFFICE

A-32. The National Reconnaissance Office is the nation's eyes and ears in space. The National Reconnaissance Office aims to—

- Be a foundation for global situational awareness.
- Provide intelligence on timelines that are responsive to user needs.

A-33. To meet these goals, the National Reconnaissance Office—

- Addresses the new intelligence imperatives of present and future operational environments.
- Shifts focus to producing value added information and not increasing volumes of data.
- Manages its systems as a single, integrated architecture focused on multidisciplinary solutions to intelligence problems.
- Recognizes that its ground-based capabilities are as critical as collection in meeting the need for actionable intelligence.
- Places equal priority and programmatic emphasis on quick turnaround support to intelligence and defense users as it does on long term, system acquisition.

A-34. The National Reconnaissance Office collaborates closely with National Security Agency/Central Security Service, National Geospatial Intelligence Agency, Central Intelligence Agency, U.S. Strategic Forces Command, Army, Navy, and Air Force, as well as other intelligence and defense organizations.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

A-35. The National Security Agency/Central Security Service is the nation's cryptologic organization that coordinates, directs, and performs highly specialized analysis to produce foreign intelligence to protect U.S. information systems. A high technology organization, the National Security Agency/Central Security Service is at the forefront of communications and information technology. The National Security Agency/Central Security Service is also one of the most important centers of foreign language analysis and research within the U.S. government.

A-36. The National Security Agency/Central Security Service has two strategic missions that relate to SE: signals intelligence and information assurance. Signals intelligence is the exploitation of foreign signals for national foreign intelligence and counterintelligence purposes. Information assurance is the protection of U.S. intelligence community and allied information through technical solutions, products, and services, and defensive information operations.

A-37. The National Security Agency/Central Security Service has remained agile and responsive to an increasingly dynamic set of customer demands. Terrorism, narcotics trafficking, organized crime, counterintelligence, and asymmetric threats are just a few of the issues facing U.S. strategic interests. U.S. forces are more likely to be involved in multinational warfare, regional conflicts, peacekeeping operations, and non-traditional operations than in the past. The rapid growth of global information technology makes the National Security Agency/Central Security Service's missions of signals intelligence and information assurance more significant. To meet these emerging challenges, the National Security Agency/Central Security Service has embarked on an ambitious strategy to increase its agility with a service-based architecture that includes a re engineered cryptologic system that provides interoperability and connectivity

with our customers. This mandate for change firmly establishes signals intelligence and information assurance as major contributors to information superiority for U.S. warfighters and decisionmakers.

ARMED FORCES INTELLIGENCE (NON ARMY)

A-38. Each branch of the armed forces is staffed with an intelligence capability tailored to the mission it is tasked with executing. Although some overlap in common capabilities exists, each of the Services has niche intelligence functions that provide the answer to many of the intelligence requirements levied by commanders in the field.

MARINE CORPS

A-39. Within Marine Corps doctrine, intelligence is considered the foundation on which the operational effort is built and the premise on which all training, doctrine, and equipment are developed. Intelligence encompasses the policy, planning, direction, collection, processing, dissemination, and use to meet Marine Corps missions in maritime, expeditionary, land, and air warfare.

A-40. The Marine Corps participates in three component programs of the National Intelligence Program:

- The Consolidated Cryptologic Program.
- The Foreign Counterintelligence Program.
- The General Defense Intelligence Program.

A-41. The Consolidated Cryptologic Program funds the majority of Marine Corps participation in the National Security Agency/Central Security Service activities worldwide. The Foreign Counterintelligence Program provides Marines to the Naval Criminal Investigative Service for counterintelligence activities. The General Defense Intelligence Program funds Marine Corps participation in the Defense Human Intelligence Service, combatant command staff; manning of the Joint Intelligence Center and Joint Analysis Center; and Defense Intelligence Agency distributed production functions of the Marine Corps Intelligence Activity.

NAVY

A-42. The Navy intelligence organization is known as the Office of Naval Intelligence. It supports a variety of missions including U.S. military acquisition and development, counterterrorism, counterproliferation, counternarcotics, customs enforcement and, through partnerships and information sharing agreements with the U.S. Coast Guard and U.S. Northern Command, Homeland Security and Homeland Defense.

A-43. The Navy's cryptologic professionals, who form the maritime component of the Unified Cryptologic System, are fully integrated with the Navy's warfighting organizations, from major combatants to fleet command staffs. This integration includes Navy and national cryptologic field locations worldwide.

AIR FORCE

A-44. Air Force intelligence also provides the nation with technical collection against foreign ballistic missile development using a global network of airborne, shipborne, and ground based collectors.

A-45. The Air Force is the executive agent for technical analysis of opponent aircraft, long-range ballistic missiles, and space-based technologies. Air Force intelligence, surveillance, and reconnaissance provides persistent surveillance, available worldwide and on demand providing an unmatched asymmetric advantage. The Air Force achieves these capabilities by increasing its investment in measurement and signatures intelligence to identify specific threats.

COAST GUARD

A-46. The Coast Guard is a military, multimission, maritime Service within the Department of Homeland Security. Coast Guard missions are executed in any maritime region in which maritime interests may be at risk, including international waters and America's coasts, ports, and inland waterways.

A-47. Because the Coast Guard employs unique expertise and capabilities in the maritime environment—in domestic ports, coastal waters, offshore regions, and even in foreign ports—where other U.S. government agencies typically are not present, the opportunity exists to collect intelligence that supports not only Coast Guard missions, but other national security objectives as well.

A-48. The Coast Guard's Intelligence and Criminal Investigations Program includes its National Intelligence Element, the Criminal Investigations Service, the Counterintelligence Service, and the Cryptologic Service. Its mission is to direct, coordinate, and oversee intelligence and investigative operations and activities that support all Coast Guard objectives by providing actionable (timely, accurate, and relevant) intelligence, to strategic decisionmakers, as well as operational and tactical commanders. The Coast Guard's Intelligence and Criminal Investigations Program also supports the National Strategy for Homeland Security and applicable National Security objectives.

A-49. The Coast Guard's role is the lead federal agency in maritime homeland security. That role includes missions related to port security, search and rescue, maritime safety, counternarcotics, alien migration interdiction, living marine resources protection, and homeland security. The Coast Guard stands ready to protect the nation and provide unique intelligence to ensure that the ports, waterways, and coasts remain safe and secure.

SUPPORTING FORENSIC ORGANIZATIONS

A-50. Forensics refers to using m multidisciplinary scientific processes to establish facts. Multidisciplinary scientific processes include, but are not limited to, the following disciplines:

- Latent prints.
- Firearms and tool marks.
- Deoxyribonucleic acid (DNA).
- Forensic medicine.
- Forensic documents.
- Computer forensics.
- Trace material.
- Fire debris.
- Forensic chemistry (includes hazardous materials and their projected use or purpose).
- Impressions.
- Forensic engineering (includes environmental engineering).
- Electronic exploitation.
- Video and photographic analysis.
- Forensic anthropology.
- Chemical, biological, radiological, nuclear, and high yield explosive (CBRNE) forensics.

A-51. The Federal Bureau of Investigation (FBI) provides forensic support for DOD. The FBI's Terrorist Explosive Device Analytical Center exploits improvised explosive devices (IEDs) of interest for usable intelligence.

A-52. The Armed Forces Medical Examiner and the Armed Forces DNA Identification Laboratory are the lead agencies for forensic pathology, forensic toxicology, mortality surveillance, and DNA technology. Their system is recognized as the world's leading forensic investigation service.

A-53. The Joint POW/MIA Accounting Command is a standing joint task force within the U.S. Pacific Command. Its Central Identification Laboratory investigates leads and recovers and identifies Americans who were killed in action but never brought home. This organization closely coordinates with other U.S. agencies, including the Defense Prisoner of War/Missing Personnel Office, Department of State, the Joint Staff, U. S. Pacific Command, Defense Intelligence Agency, the Armed Forces Medical Examiner, and Armed Forces Institute of Pathology.

A-54. Defense Threat Reduction Agency provides tools and services for DOD. Defense Threat Reduction Agency supports SE in the fields of protection and technology development.

A-55. National Ground Intelligence Center's mission is to produce all source analysis for biometrics to on the ground individuals and provide training for deploying units. National Ground Intelligence Center works closely with Armed Forces DNA Identification Laboratory and the FBI's Terrorist Explosive Device Analytical Center to get the information into an operational area and make any available matches.

A-56. The mission of the Naval Criminal Investigation Service is to provide investigation and intelligence services and forensic support through major crime-scene response teams and consultant programs. The Naval Criminal Investigation Service is experienced in crime-scene processing. It is developing expeditionary laboratory facility capability.

A-57. The FBI created the National Media Exploitation Center in 2001. The National Media Exploitation Center coordinates FBI, Central Intelligence Agency, Defense Intelligence Agency, and National Security Agency/Central Security Service efforts to analyze and disseminate information obtained from documents and media seized by the U.S. military and intelligence community in foreign lands.

DEVELOPING MULTIAGENCY AD HOC ORGANIZATIONS

A-58. Commanders draw on capabilities from existing organizations, and when necessary they develop ad hoc teams to meet the requirements of their missions. They draw on any number of assets from a variety of military and nonmilitary entities, and some of these teams are relatively long-standing. For example, explosive ordnance disposal forces can advise commanders at all levels on ordnance, precursor chemicals, homemade explosives, unexploded ordnance, and first seen ordnance. Explosive ordnance disposal forces are the only forces equipped, manned, and trained to positively identify, render safe, and dispose of U.S. and foreign ordnance and IEDs (including CBRN materials).

A-59. An SE team may consist of qualified explosive ordnance disposal, law enforcement, and intelligence capabilities. These individuals are linked to brigade combat teams for support related to IEDs. They provide technical intelligence tactics, techniques, and procedures, and they support targeting and material solutions. Their critical tasks are scene investigation, analytical support, and advice to the local commander.

A-60. The Multi National Corps–Iraq developed an ad hoc organization to conduct the functions of a forensic exploitation battalion. A forensic exploitation battalion is an example of a nondoctrinal design focused on meeting the immediate needs of the commander for conducting SE. The forensic exploitation battalion provided command and control for what was known as joint expeditionary forensic facilities. The forensic exploitation battalion provided Multinational Corps–Iraq and subordinate commands with responsive, time sensitive forensic analysis and exploitation. The joint expeditionary forensic facilities were relocatable laboratories (trailers, shelters, or buildings) that performed processing, analyses, and exploitation of non-IED forensic material. They disseminated information and supported reach back coordination among laboratories, deployed elements, and sites being exploited.

Appendix B

Evidence Collection, Handling, and Documentation

Normally, trained law enforcement personnel or military police search for, collect, and manage evidence of crimes. This appendix provides guidelines for occasions when operations require Soldiers not trained in law enforcement to collect and handle evidence.

TESTIMONIAL AND PHYSICAL EVIDENCE

B-1. Successful prosecution of individuals depends on gathering and evaluating evidence, both testimonial and physical. Sworn statements are not required for testimonial evidence. Testimonial evidence is often used to obtain background information that gives meaning to the physical evidence collected. Physical evidence, such as weapons and fingerprints, is obtained by site exploitation (SE) operations. Further evidence comes from exploiting any leads discovered by SE operations and developing information obtained. More than the collection of evidence is required for a successful prosecution. The evidence must withstand intense scrutiny and be admissible in court. This requires systematic procedures for collecting, handling, and documenting evidence.

PRE-ENTRY BRIEFING TOPICS

B-2. Leaders thoroughly brief Soldiers before a SE mission. Table B-1 outlines key items to include in the pre-entry briefing.

Table B-1. Guidelines for topics to include in the pre-entry briefing

Safety concerns:

- Structural considerations (engineering faults, structural integrity).
- Hazardous materials (such as chemical and radiological materials and devices or toxic industrial chemicals and materials).
- Biohazards (such as toxins, decaying bodies, or diseases endemic to the site).
- Insurgents, criminals, or local populace.

A full description of the evidence being sought.

How the evidence may be hidden or discarded.

How to identify items that will provide valuable physical evidence.

What to do when a piece of evidence is discovered:

- Refrain from touching or removing the item if possible.
- Use personal protective equipment such as latex or nonporous gloves if they must touch an item.
- Immediately inform the supervisor.
- Protect the area until relieved.

ESTABLISHING SITE SECURITY

B-3. The designated security force establishes a perimeter to provide 360-degree security and control access to the area. They only allow necessary personnel to enter the area where evidence is being collected so the chances of contaminating potential evidence are reduced. When a building or room is left unsecured by evidence collection actions, forces ensure measures are taken to protect the interior's contents.

B-4. Once a perimeter is established, entrance to and exit from the scene are from the same egress point, not from any other location. This is especially important when securing an external or open area as a crime scene.

INITIAL ACTIONS UPON ENTRY INTO THE SITE

B-5. Initial actions are to observe and record. Soldiers note all items, their condition, and their location, preferably without entering critical areas of the scene. The position of items in relation to each other and any persons present at the site, if any, can be as important to a case as the items themselves. This is a reason to photograph the scene to record the placement of information, material, and persons within the site.

B-6. If the SE is expected to be lengthy, units set aside an administrative area close by, but outside the critical area. The establishment of an administrative area within the security perimeter but exterior to the exploitation area reduces the chances of contamination of the scene. It also provides a place for—

- Trash generated during the mission.
- Equipment not in immediate use.
- Personnel to take work or smoke breaks.

B-7. Evidence may not always be very large or obvious, such as an explosives cache. Soldiers at the site need to remember physical evidence can be composed of materials in either gross or trace quantities. Each Soldier must remember materials collected during the SE may be examined and analyzed for potential value. For this reason, Soldiers must treat all items as though they have evidentiary value until proven otherwise.

B-8. Common examples of physical evidence are shown in table B-2, page B-3. In addition to items such as those shown in table B-2, Soldiers note and record environmental aspects including hazards and historical or cultural evidence according to standing operating procedure.

Table B-2. Examples of physical evidence

Fingerprints. Positive identification can be obtained from—

- Nonporous, smooth surfaces (such as coffee cups, weapons, or personal gear).
- Paper documents.
- Fluids (such as blood or paint).

DNA. Positive identification can be obtained from—

- Blood.
- Hair.
- Fibers.
- Semen.
- Saliva (on items such as cigarette butts, drinking containers, eating utensils, or envelopes).
- Perspiration (items such as clothing or bed sheets).
- Skin, organs, or other body parts.

Documents. Hard copy, paper documents may contain—

- Exploitable information of tactical value.
- Fingerprints.
- DNA.

Weapons. Links to crimes, incidents, or people may include—

- Fingerprints.
- Individual (weapon) markings.
- DNA.

Electronics. Information and positive identification can be found on—

- Computers.
- Flash drives.
- CDs.
- Removable hard drives.
- Cell phones.
- Pagers.
- Personal data assistants.
- Global positioning systems.

Post blast fragments. Fragments can yield fingerprints or tool marks that tie a device to a particular builder or organization and may include—

- Time and ignition devices or parts.
- Delay mechanisms.
- Switches.
- Blasting caps.
- Matches.
- Fuse lighters.
- Circuit boards
- Batteries or other sources of electric current.

B-9. This appendix does not attempt to give a detailed or prescriptive description of searching. The following limited discussion of searching provides context for collecting and handling physical evidence.

B-10. During a preliminary walk through, Soldiers note obvious items of evidence to be collected. However, leaders first determine how items will be collected and processed. Leaders define the method to use, what items should be collected, and associated tasks. If the exploitation mission extends beyond the immediate site, additional Soldiers may be requested from other units.

B-11. A successful SE operation produces a comprehensive and nondestructive accumulation of all available physical evidence within a reasonable amount of time, minimizes movement, and avoids unneeded disturbance. Forces use one or more of the following search methods:

- Circle search.
- Grid search.
- Zone or sector search.

B-12. Any of the searches are acceptable as long as the search is methodical and systematic. The search method chosen to collect evidence depends on the intent of the search and by the area to be covered. For example, in rooms, buildings, and small outdoor areas, a systematic circle search is often used. The circular method can be done one of two ways: starting from the inside and working out in a circular motion, or starting on the outside and working in. If the most evidence appears to be inside, then searchers work from the inside out.

B-13. In large outdoor areas, a grid search may be useful. The searchers mentally divide the area into strips about 4 feet wide, identifying a main area to begin the search. They begin at one corner of the main area and move back and forth from one side to the other. Then the searchers moves from end to end in the same manner.

B-14. The zone or sector methods refer to searching an area in smaller, more manageable pieces. Forces initiate the search from the immediate area of importance, followed by adjoining and other areas. This search works best for larger areas when more people are available. Both indoor and outdoor areas may be searched using the zone or sector method.

COLLECTING AND PROCESSING EVIDENCE

B-15. Collecting evidence is usually done after a preliminary search has been completed and photographs taken. However, forces give priority to two types of evidence: fragile evidence and perishable evidence. Fragile evidence is the smallest trace amounts of an item (such as hair or fiber) which is resilient but must be protected from loss. Perishable evidence (such as blood or bodily fluids) will change over time despite protective measures. These types of evidence must be collected immediately while adhering to established collection procedures.

B-16. Leaders ensure major evidence is collected, photographed, marked, and recorded in the most logical order based on the need to conserve movement. They give careful consideration to how and where identification marks are placed on items. Unnecessary damage or destruction of items of personal property that may ultimately be returned to the owner is prohibited.

B-17. Forces carefully mark items that may require future laboratory examination for latent prints. To avoid defacing or damaging such items, identification markings should be as inconspicuous as possible or the item should be placed in a container that is sealed and the container marked for identification. Additionally, if marking the evidence itself is not possible or practical due to reasons such as value, size, or quantity, forces place the evidence in an evidence container and then seal and mark it for identification.

B-18. After an item has been collected and marked, Forces record in a notebook its description (verbal and sketch, if necessary), the date and time of discovery, and whether or not it was placed in a container (see AR 195-5). Forces ensure authorization is obtained before damaging or partially destroying an item when necessary to obtain an important piece of evidence. For example, forces obtain authorization before cutting away a piece of upholstery to collect a patch stained with blood or removing a section of a wall to collect fingerprints or tissue samplings.

PHOTOGRAPHS OF EVIDENCE

B-19. It is not always possible or practical to bring a piece of evidence into judicial proceedings. Photographic media, x-rays, replicas of hazardous material, sketches, and graphs are examples of demonstrative evidence. Demonstrative evidence is evidence consisting of a representation of the actual piece of evidence to establish context among the facts presented in a case. A demonstrative exhibit must accurately represent the actual object at the relevant time of collection.

B-20. Units take as many photographs as possible of as much evidence as possible. The photographs are used to show the judges what happened and where it happened. Photographs aid the witnesses when testifying. Photographs provide an accurate representation of the scene as found and a permanent record of fragile and perishable evidence. A picture is worth a thousand words. Table B-3 lists specific guidelines for photographing evidence.

Table B-3. Guidelines for photographing evidence

Photographs must—

- Be clear, sharp, and free of distortion.
- Be taken from a stable position at eye level (average height).
- Include the date, time, and location when photographs were taken. (Digital cameras must be correctly programmed for the date and time.)
- Be processed by the unit intelligence section if not taken with digital cameras.

Take photographs of—

- 360-degree exposure of the entire area, room, or four corners.
- Each piece of suspected evidence, with and without measuring device (small ruler).
- Close-ups in which the evidence will fill the frame.
- Victims, suspects, and witnesses.
- The crowd and any vehicles in the area.
- A reference point of view depicting the physical dimensions of the site, building, and items collected.
- A broad point of view that establishes the location of the crime scene by including landmarks or reference points.
- Anything that may be considered evidence (such as weapons, ammunition, money, or detonators). (If ever in doubt, photograph it; more is better than less.)
- Detainees with the evidence that associates them with the illegal activity (in the same picture) at the location in question. Display under the detainee's face in the photograph name; father's name (if appropriate, for identification); village; tribe; date of birth; objective, building, and room; and date of photo.

Follow established guidelines for photographs showing—

- Weapons of mass destruction.
- Toxic industrial chemicals.

SKETCHING THE LAYOUT OF EVIDENCE FOUND AT A SITE

B-21. To create a record showing exactly where evidence was found, SE forces sometimes draw sketches depicting a site in detail. Sketches include written names or descriptions of items either in or below the sketch. Figure B-1 shows an example of a sketch drawn before collecting evidence.

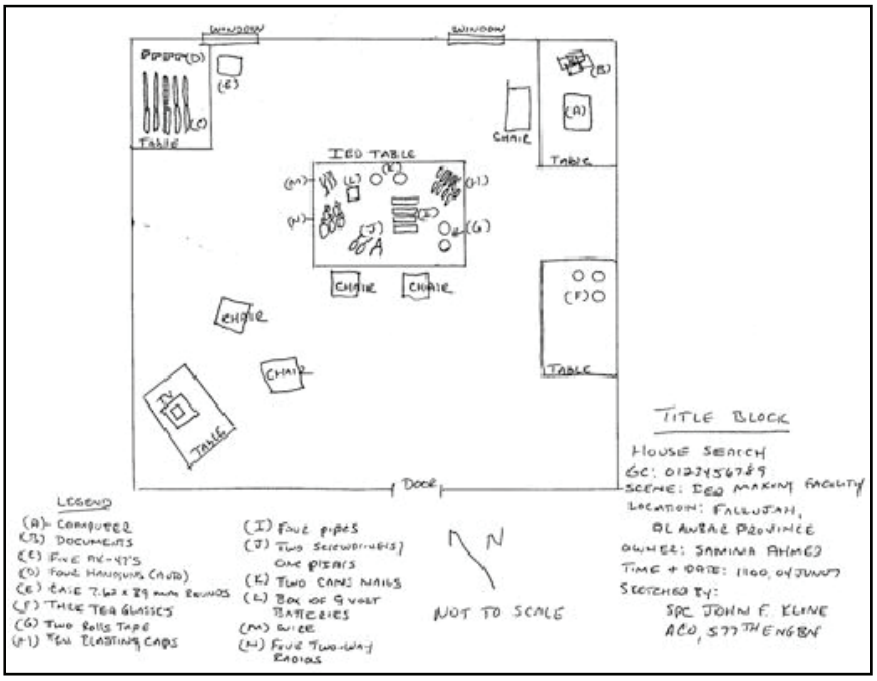

Figure B-1. Example layout sketch drawn before collecting evidence

Table B-4 lists guidelines for creating a sketch.

Table B-4. Guidelines for drawing sketches

• Sketches are used to assist in recalling the layout of a scene. • The sketch should support the photographs. • Items are not to scale but should be appropriately sized. • Reference where the detainees and evidence were found in relation to the scene. • Use a Global Positioning System (GPS) for additional accuracy • Number the rooms counterclockwise (or clockwise if more appropriate). • Number each of the walls within a room beginning with the wall immediately adjacent to right of the door as number 1 and continue counterclockwise until all walls are numbered. • Consider drawing a grid, either within the site's boundaries or to show the site's relationship to the area. • Reference landmarks, cities, villages, and key points of interest. (Show the direction of north and a grid.)

DETAINEES AND ASSOCIATED EVIDENCE

B-22. If individuals on the site are found with evidence and equipment such as weapons, forces detain the individuals. Forces tag the detainees and the equipment using a DD Form 2745(Enemy Prisoner of War (EPW) Capture Tag). Forces account for the evidence on DA Form 4137(Evidence/Property Custody Document). Forces maintain and transport evidence along with the detainee to maintain its association with the detainee. This includes photographs showing the evidence and the detainee in the same picture.

B-23. The guidelines for initial handling of detainees are sometimes known as *the five Ss and T*. Table B-5 lists these guidelines.

Table B-5. Guidelines for initial handling of detainees

Search: Conduct a thorough search of the individuals for weapons and documents.
Silence: Do not allow detainees to communicate with one another, either verbally or with gestures.
Segregate: Keep civilians and military separate and further divide them by rank, gender, and nationality, ethnicity, or religion.
Safeguard: Provide security for and protection for the enemy prisoners of war and detainees.
Speed: Move detainees to the rear as quickly as possible.
Tag: Ensure detained individuals are tagged with DD Form 2745. The tag is distributed as follows: • Part A remains with the captive. • Part B is maintained with the capturing unit. • Part C remains with the captive property.

FATALITIES AT A CRIME SCENE

B-24. In general, military forces leave civilian fatalities and their surroundings undisturbed. If appropriate law enforcement personnel are available, they conduct a detailed search of the body before removal, according to casualty disposition policy. Available law enforcement personnel may also—

- Search for and collect trace evidence.
- Collect post-mortem fingerprints or, at least, photograph and protect fingerprints from contamination (using paper bags) before the body is removed (see AR 195-5).

B-25. If a human death is involved under suspicious or unknown circumstances and is not directly combat related, the search area must include the area from the point of entry of the scene to the body and a preliminary search of the body.

B-26. After all search operations have been completed, forces take fingerprints of investigators and other personnel who had access to the scene. These are sometimes known as elimination prints.

HANDLING AND DOCUMENTING EVIDENCE

B-27. Commanders ensure that—

- Every precaution is taken to properly handle evidence during collection and preserve the evidence in its original state until its final disposition.
- Acquired evidence is properly tagged and documented before it is submitted to the evidence custodian.
- Security of evidence is maintained, according to chain of custody and transportation requirements.
- When touching items of potential evidence, forces remain mindful of how they may have been handled by the suspect. Forces avoid touching those areas the suspect touched.

PRESERVING EVIDENCE

B-28. Preserving evidence requires protecting it from change. Organic materials always undergo some change and inorganic materials may undergo change from weather or other unavoidable actions. Table B-6 shows guidelines Soldiers follow to minimize change during evidence handling.

Table B-6. Guidelines for minimizing change to evidence

- Wear rubber gloves during searches and handling of evidence.
- Handle the evidence as little as possible and prevent accidental scratches or bending. If evidence is touched and fingerprints are left, that fact should be noted and lab personnel informed.
- Use only clean containers to collect and store evidence. This reduces the chance of chemical or bacterial contamination. Containers should also be air tight to prevent spillage, evaporation, and seepage.
- Clean, suitable containers may include paper bags, heat-sealed bags, pillboxes, envelopes, or jars.
- Avoid cross contamination, such as placing a piece of evidence that will be examined for paint in contact with other painted surfaces at the crime scene.
- Wear personal protective equipment such as a surgical mask to avoid cross contamination caused by talking, sneezing, and coughing.
- Change gloves between collections of samples in different areas.
- Ensure evidence that requires special considerations such as refrigeration is not left unattended in an unsuitable environment.

B-29. When encountering electronic devices, forces on-site do not attempt to retrieve data. Table B-7 lists guidance for handling electronic devices.

Table B-7. Guidelines for handling electronic devices

Desktop computer:
- Do not turn a desktop computer off.
- Disconnect the power cord from the back of the computer.

Laptop computer:
- Do not turn a laptop computer off.
- Disconnect the power cord from the back of the computer.
- If laptop does not turn off when disconnected, remove the battery.

PDAs and cell phones:
- Leave them as found, whether on or off. (Turning them off could enable a password.)
- Collect all cords.
- Keep them charged if possible or have them analyzed as soon as possible.

Other removable media devices:
- Collect compact disks, digital video disks, secure digital cards, memory sticks, etc.
- Keep media away from magnets, radios, and transmitters.

B-30. When encountering possible DNA evidence, forces take special precautions. Table B-8, page B-9, gives guidelines for handing DNA evidence.

Table B-8. Guidelines for handling DNA evidence

- Secure DNA evidence in paper bags or envelopes.
- Allow wet fluids, such as bloodstained materials, to air-dry before placing them in a dry and clean paper bag.
- Keep evidence that may contain DNA dry and at room temperature.
- Do not try to scrape or swab blood or saliva.
- Never place possible DNA evidence in plastics bags or allow exposure to heat. (This may produce undesirable moisture that would damage the DNA.)

TAGGING EVIDENCE

B-31. Forces tag evidence at the scene as it is being collected or at the place where it is received. Forces attach a self-adhesive DA Form 4002 (Evidence/Property Tag) to each item of evidence or evidence container at the earliest opportunity to identify and control it. A DA Form 4002 is attached directly to the item of evidence or evidence container, or it may be affixed to a blank shoe tag, which is attached to the item. Merely attaching a completed DA Form 4002 to an item of evidence does not meet the requirements of AR 195-5. Each item of evidence or sealed evidence container must also be marked itself for future identification. If evidence is placed in a heat-sealed bag, the tag on the bag may replace the adhesive label.

B-32. The DA Form 4002 is the tag attached to the evidence or evidence container. It is not to be confused with DA Form 4137. DA 4137 is used to maintain the chain of custody—documentation of every transfer—and serves as an inventory and accountability record for the evidence.

B-33. When like items are grouped together (such as a box containing tools), only one DA Form 4002 is used. There is no need to remove or mark each individual item. The box or container is collected as one item and placed in a container that is then sealed. The container is marked with the time, date, and initials representing the appropriate indicator. A DA Form 4137, in this situation, is annotated *sealed container received, contents not inventoried* (or *SCRCNI*).

B-34. Each Soldier is responsible for the care, safekeeping, and preservation of evidence under his or her control. When a piece of evidence is acquired, a DA Form 4137 must be prepared. Regardless of how evidence is obtained, forces inventory and account for all physical evidence on DA Form 4137. This form serves as a receipt for the piece of evidence, lists the names of the individuals that were in its chain of custody, and is the authority and witnessing document for its final disposition or destruction.

SWORN STATEMENTS AND WITNESS TESTIMONY

B-35. Forces use DA Form 2823 (Sworn Statement) when completing statements from witnesses. The primary purpose of sworn statement collection is for host-nation prosecution. Forces collect as many corroborating statements from host-nation citizens as possible to aid prosecution. The statements should address who, what, when, where, why and how in relation to the events. In addition, forces collect statements that support any photographs and evidence taken at the site.

B-36. The DA Form 2823 must accurately and adequately explain the details of the detainment or capture. This information on form explains the conduct, behavior and associations of the detainees. Detailed information on this form facilitates the eventual interrogation of these individuals.

EVIDENCE COLLECTION POINT

B-37. Once evidence has been identified, assessed, sketched or photographed in place, and subsequently collected, forces move it to a central evidence collection point. Leaders designate the central evidence collection point to facilitate the positive control of the evidence and confirmation of evidence tags' accuracy. Using a central evidence collection point helps forces remove evidence safely and securely.

B-38. The evidence collection point is manned by senior personnel who understand the gravity of their duties. Any failure to maintain accurate recording and chain-of-custody procedures may lead to the eventual release of a criminal. The senior personnel directing the activities at the evidence collection point

are responsible for maintaining the chain of custody until the evidence is released to the appropriate evidence custodian.

TRANSFER OF EVIDENCE AND DA FORM 4137

B-39. When evidence is transferred, forces annotate and transfer the proper documentation along with the evidence. An original and three copies of a DA Form 4137 are completed and updated as custody changes for a piece of evidence. The importance of keeping accurate and complete custody documents cannot be overemphasized. Forces type entries or print them in ink. They submit the original and first two copies to the evidence custodian for his or her files. The third copy is placed in the official case file. Forces give special attention to completing the following portions thoroughly:

- Administrative section.
- Description of articles section.
- Chain of custody section.
- Purpose of change of custody column.

Administrative Section

B-40. In the administrative section, forces write the reason, time, place, and date evidence was obtained.

Description of Articles Section

B-41. In this section, forces describe the evidence accurately and in detail. For example, information for a piece of equipment would include the name or number of the model, the serial number, the item's condition, and any unusual marks or scratches. Forces enter the quantity of collections of loose items if known. Sometimes a quantity cannot be determined because an item is hard to measure or subject to change. Forces estimate as closely as possible, sometimes describing approximate weight, volume, or size. For items such as glass fragments or crushed tablets, forces enter appropriate descriptions, such as a*pproximately 50*. They may enter *undetermined* or *unknown* if no quantity can be estimated.

Chain of Custody Section

B-42. When any change of custody occurs, the Soldier in control of the evidence at that time notes the change in custody on all copies of the DA Form 4137. The signature, printed name, and grade or title of the individual from whom the evidence was initially taken (if applicable) is noted in the *release by* column. If the individual refuses or is unable to sign, the Soldier records *refused* or *unable to sign* in the signature block. If the evidence was found by a search team member or the owner cannot be determined, the Soldier records *N/A* (not applicable) in the signature block.

Purpose of Change of Custody Column

B-43. The evidence custodian writes *received by evidence custodian* in this block. All others write *evaluation of evidence*. If the evidence is nonfungible (readily identified, marked distinctively, or with individual characteristics [AR 195-5]) and sealed in a container, then the custodian writes s*ealed in a [state the type of container]*. When custody of sealed evidence is received but not inventoried, the next evidence custodian marks the chain of custody form *sealed container received; contents not inventoried,* (or *SCRCNI*).

STORING EVIDENCE

B-44. Forces store acquired evidence in a key-locked field safe or other high-security container for temporary storage outside of normal duty hours. An evidence custodian is responsible for evidence when it is not under the control of authorized personnel involved in the investigation (for example, trial counsel). Forces ensure evidence that requires special considerations, such as refrigeration, is not left unattended in an unsuitable environment.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

ATTP	Army tactics, techniques, and procedures
BCT	brigade combat team
BSTB	brigade special troops battalion
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CCIR	commander's critical information requirement
CID	criminal investigation division
CMEC	captured materiel exploitation center
COA	course of action
DA	Department of the Army
DNA	deoxyribonucleic acid
DOD	Department of Defense
DODD	Department of Defense Directive
FBI	Federal Bureau of Investigation
FFIR	friendly force information requirement
FIRES	Facilities, Infrastructure, and Engineering Systems
FM	field manual
IED	improvised explosive device
IMP	information, material, and persons
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
JP	joint publication
MDMP	military decisionmaking process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, civil considerations (mission variables)
MIA	missing in action
MP	military police
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, time (operational variables)
POW	prisoner of war
SE	site exploitation
TECHINT	technical intelligence
WMD	weapons of mass destruction

SECTION II – TERMS

***site exploitation**

Systematically searching for and collecting information, material, and persons from a designated location and analyzing them to answer information requirements, facilitate subsequent operations, or support criminal prosecution.

References

REQUIRED PUBLICATIONS

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

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 12 April 2001.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: <http://www.dtic.mil/doctrine/new_pubs/jointpub.htm.>

DODD 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning.* 9 October 2008.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 07 October 2004.

JP 3-0. *Joint Operations*. 17 September 2006.

JP 3-13.1. *Electronic Warfare*. 25 January 2007.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: <http://www.army.mil/usapa/doctrine/Active_FM.html>.

AR 195-5. *Evidence Procedures*. 25 June 2007.

DA Pam 27-1.*Treaties Governing Land Warfare*. December 1956.

FM 2-22.401. *Multiservice Tactics, Techniques, and Procedures for Technical Intelligence Operations*. 9 June 2006.

FM 2-91.6. *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*. 10 October 2007.

FM 3-0. *Operations*. 27 February 2008.

FM 3-07. *Stability Operations*. 6 October 2008.

FM 3-19.13 (FM 19-20). *Law Enforcement Investigations*. 10 January 2005.

FM 3-24.2 (FM 90-8, FM 7-98), *Tactics in Counterinsurgency*. 21 April 2009.

FM 3-34.210 (20-32). *Explosive Hazards Operations*. 27 March 2007.

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

FM 3-90.31. *Maneuver Enhancement Brigade Operations*. 26 February 2009.

FM 3-90.119 (FMI 3-34.119). *Combined Arms Improvised Explosive Device Defeat Operations.* 21 September 2007.

FM 3-34.5. *Environmental Considerations in Military Operations*. 6 July 2010.

FM 5-0. *The Operations Process*. 26 March 2010.

FM 5-19 (FM 100-14). *Composite Risk Management*. 21 August 2006.

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

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

FMI 2-01.301. *Specific Tactics, Techniques, and Procedures and Applications for Intelligence Preparation of the Battlefield.* 31 March 2009.

OTHER PUBLICATIONS

Intelligence Reform and Terrorism Prevention Act of 2004. PL 108-458. 17 December 2004.

PRESCRIBED FORMS

None.

REFERENCED FORMS

DA forms are available on the APD website (www.apd.army.mil). DD forms are available on the OSD website (www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm).

DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

DA Form 2823. *Sworn Statement*.

DA Form 4002. *Evidence/Property Tag*.

DA Form 4137. *Evidence/Property Custody Document*.

DD Form 2745. *Enemy Prisoner of War (EPW) Capture Tag.*

Index

Entries are by paragraph number unless stated otherwise.

ATTP 3-90.15 (FM 3-90.15)
8 July 2010

By order of the Secretary of the Army:

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

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1019408

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve: Not to be distributed; electronic media only.