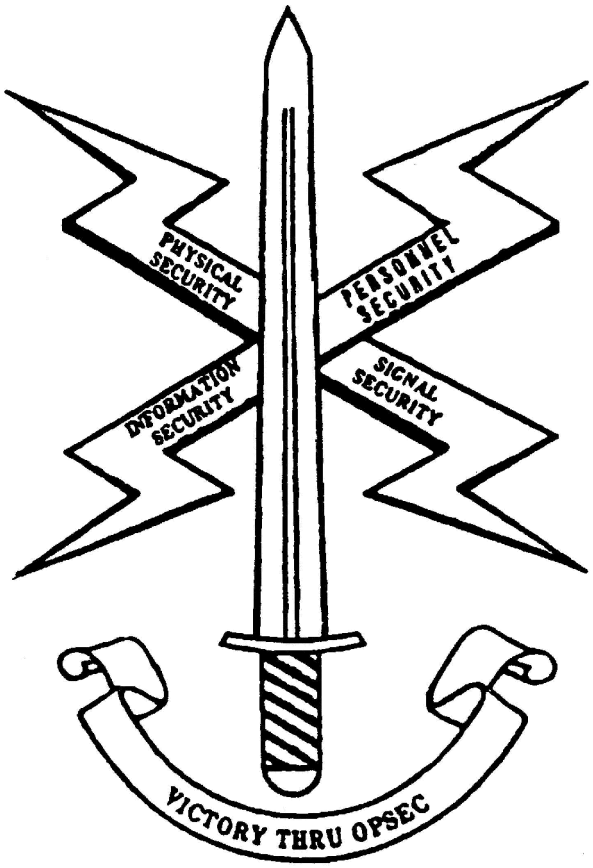
SUBCOURSE
IT 0464

EDITION
B

US ARMY INTELLIGENCE CENTER

OPERATIONS SECURITY



THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT
ARMY CORRESPONDENCE COURSE PROGRAM

AIPD

READINESS/ PROFESSIONALISM THRU GROWTH

OPERATIONS SECURITY

Subcourse Number IT 0464

EDITION B

U.S. Army Intelligence Center
Fort Huachuca, AZ 85613-6000

5 Credit Hours

Edition Date: June 1999

SUBCOURSE OVERVIEW

This subcourse is designed to teach you the basic procedures involved with implementing the US Army's operations security (OPSEC) program. Contained within this subcourse is instruction on the OPSEC Planning Sequence, why OPSEC must be practiced by all members of the Army to include Department of the Army (DA) civilians and contractors, and how the success or failure of OPSEC directly influences the accomplishment of the unit's mission.

There are no prerequisites for this subcourse.

This subcourse reflects the doctrine which was current at the time the subcourse was prepared. In your own work situation, always refer to the latest publications.

Unless stated otherwise, masculine nouns and pronouns do not refer exclusively to men.

TERMINAL LEARNING OBJECTIVE

ACTIONS:	You will identify all components of the OPSEC Planning Sequence, conduct analysis of collected OPSEC data, identify gaps in the OPSEC data base, conduct vulnerability assessment and risk analysis, develop and document OPSEC measures, implement OPSEC measures, and determine OPSEC evaluation procedures.
CONDITIONS:	You will be given narrative information and extracts from AR 530-1 and FMs 34-1 and 34-60.
STANDARD:	You will initiate an OPSEC program in accordance with the provisions of AR 530-1.

TABLE OF CONTENTS

LESSON

OPERATIONS SECURITY INSTRUCTIONAL CONTENT

CRITICAL TASKS: 301-372-2015
301-372-2012
301-372-2017
301-372-2020
301-372-2100
301-372-2151
301-372-2200
301-372-2400
301-372-2404
301-372-3017
301-372-3019

01-3381.41-4004
01-3397.45-5002

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn how to systematically implement and evaluate a viable OPSEC program that is relevant and pertinent at all DA echelons.

TERMINAL LEARNING OBJECTIVE:

TASKS: Identify all components of the OPSEC Planning Sequence, conduct analysis of collected OPSEC data, identify gaps in the OPSEC data base, conduct vulnerability assessment and risk analysis, develop and document OPSEC measures, implement OPSEC measures, and determine OPSEC evaluation procedures.

CONDITION: You will be given narrative information and extracts from AR 530-1 and FMs 34-1 and 34-60.

STANDARD: You will initiate an OPSEC program in accordance with the provisions of AR 530-1.

REFERENCES: The material contained in this lesson was derived from the following publications:

AR 530-1, Operations Security, 3 Mar 95.
AR 361-20, US Army Counterintelligence Activities, Apr 87.
FM 34-10, Division Intelligence and Electronic Warfare Operations, Nov 86.
FM 34-60, Counterintelligence, Oct 95.
FM 100-5, Operations, Jun 93.
FM 101-5, Staff Organization and Operations, May 97.
TRADOC PAM 525-6, Operations Security, May 81.
JCS Pub 18, Operations Security, Dec 82.
Joint Pub 3-57, Joint Doctrine For OPSEC, 24 Jan 97

INTRODUCTION

The Deputy Chief of Staff for Operations (DCSOPS), G3/S3, has primary staff responsibility for OPSEC. However, to be totally successful in denying information concerning friendly operations to the enemy's all-source intelligence collection effort, OPSEC must be a joint effort of both the operations personnel and the intelligence personnel within a command. It is essential that you have a good understanding and working knowledge of the OPSEC Planning Sequence and the role you will play in support of that process.

This lesson has two parts:

Part A: Introduction to OPSEC.

Part B: OPSEC Planning Sequence.

After each part, there is a practice exercise. Answer all the questions on each practice exercise and check your answers. Do NOT go on until you answer all questions correctly.

PART A: INTRODUCTION TO OPSEC

Operations Security (OPSEC) as outlined in US Army doctrine is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC is not an overall management program. (OPSEC and other security programs such as information, signals, and documents coupled with the security disciplines such as Human Intelligence (HUMINT), Signals Intelligence (SIGINT), or Imagery Intelligence (IMINT) are all involved with protection of information.) However, the principal characteristics that distinguish OPSEC from other related programs are its broad scope and concern with all exploitable information, not just classified.

OPSEC is described in AR 530-1, as "The process of denying adversaries information about friendly capabilities and intentions, by identifying, controlling, and protecting indicators associated with planning and conducting military operations and activities. Its ultimate objective is to prevent an enemy from obtaining sufficient information to predict, and thus be able to degrade, friendly operations or capabilities."

For you to fully understand and properly implement OPSEC in your unit, or assist a supported command in developing its own OPSEC program, you should read and have on hand the following references:

- AR 530-1, dated 3 March 1995, "Operations Security", outlines the minimum standards for command's OPSEC program by stating the regulatory requirements for such programs. It also outlines requirements to be fulfilled by major commands (MACOM) and Department of the Army (DA) level agencies. This regulation also discusses the relationship between OPSEC and other US Army security programs such as physical security, electronic security, and military deception.

- TRADOC Pam 525-6, dated 1 May 1981, "Operations Security", provides a basic "how to" for implementing some of the regulatory requirements. This document may prove useful to planning staffs. It was issued prior to the development of FM 34-60 and was one of the documents that assisted the OPSEC planning process.

- FM 34-1, dated 24 September 1994, "Intelligence and Electronic Warfare Operations (IEW) ", discusses some specific OPSEC functions and considerations as they relate to IEW operations.

- FM 34-60, dated 3 October 1995, "Counterintelligence", describes counterintelligence (CI) functions to include information on the OPSEC process. FM 34-60A(S), details specific counter-HUMINT, counter- SIGINT, and counter-IMINT measures, and how these operations tie into the overall OPSEC planning cycle.

- JCS Pub 18, dated December 1982, "Operations Security", provides joint policy and guidance for OPSEC for use by the military departments and services. Unified and specified commands, defense agencies, and joint activities as needed in the conduct of daily activities, in preparation of their respective plans and functions.

As already stated, AR 530-1 is the basic regulatory guidance for the establishment and conduct of OPSEC programs. Some of the basic requirements for the DA are as follows:

- All commanders will establish OPSEC as a command emphasis item.

- All commanders will ensure that appropriate OPSEC measures are implemented for all operations, exercises, and activities.

- All commanders (down to battalion level), will appoint an organizational OPSEC officer (commissioned officer, warrant officer, E-6 or above, or GS-7 or above).

- All commanders will ensure that command OPSEC programs are examined during Inspector General (IG) Inspections, or other command inspection visits.

- All commanders will institute command-wide OPSEC training.

- An OPSEC Annex is required to support plans for operations, exercises, technology, or other activities that are of interest to foreign intelligence.

As with any military program, the commander has overall responsibility for OPSEC within his/her command. We have already discussed the need for the commanders emphasis so that the program will be effective. Even though the commander has overall responsibility, the staff responsibility for OPSEC is passed down to the G3/S3. This is because OPSEC is an operations function.

This does not mean that the G2/S2 has no OPSEC mission. On the contrary, most of the OPSEC functions at Echelons Corps and Below (ECB) will be shared equally by the G3/S3 and the G2/S2. As we discuss the OPSEC Planning Sequence, we will clearly define who does what along with how the two staffs must work together. The OPSEC Management and Analysis Section, under current Tables of Organization and Equipment (TO&E), has been broken down into the OPSEC staff element and CI analysis section-one working for each staff section instead of concentrating all OPSEC assets under the G2/S2. Under the Army of Excellence (AOE) TO&E, these two sections have been established at the division and corps levels. Some units, although not under AOE, have nevertheless established these two sections. The majority of OPSEC related tasks at division and corps will be performed by these elements. Specific duties are as follows:

1. OPSEC Staff Element: The OPSEC Staff Element is provided to assist the G3 in fulfilling the unit's OPSEC responsibilities. This section performs the overall management and supervision of OPSEC within the command. It works closely with the CI Analysis Section to develop and implement an effective OPSEC program. The OPSEC Staff Element is also responsible for preparing, updating and disseminating the unit's OPSEC Standing Operating Procedures (SOP). They will also develop, implement and super- vise OPSEC training programs within the command. The chief of the OPSEC Staff Element will normally be designated as the unit's OPSEC officer. This then becomes a primary function rather than an additional duty.

2. CI Analysis Section: The CI and C-HUMINT multidiscipline assets of the analysis and control element (ACE) are under the staff supervision of the G2 at theater, corps, and division levels. Theater ACE staffing is provided from the operations battalion of the theater MI brigade. Corps ACE staffing is provided from the corps MI brigade headquarters and operations battalion. Division ACE staffing if provided by personnel assigned to the headquarters company of the divisional MI battalion. In addition to CI personnel, an all-source mix of single discipline analysts is sometimes required for interpretation to produce the CI analytical products required for interpretation to produce the CI analytical products required by the commander at each echelon. CI products are also critical to the function of the G3 OPSEC and deception cells as well. This section provides valuable input to the unit's OPSEC program by working closely with the OPSEC Staff Element during the OPSEC Planning Sequence. They provide the intelligence related support to the OPSEC program by identifying and assessing the risks that hostile foreign intelligence collection will have on the outcome of friendly unit operations.

As intelligence personnel, you may find yourself assigned to either of the above sections. To perform efficiently, you must be the expert on how the OPSEC Planning Sequence works. As a recommended additional resource to assist the above sections with OPSEC duties as well as providing support to OPSEC at other echelons, an OPSEC Committee should be established.

3. OPSEC Committee: Although the OPSEC committee is not a regulatory requirement, it is a good idea to set one up to assist in the effective performance of OPSEC duties. Representatives with expertise in all areas of the command should be included in all committee activities. Each primary staff and all sub-staff elements must be represented. This allows for better coordination of OPSEC activities throughout the command. It also provides a valuable source for outside assistance.

The above staff sections and personalities have certain responsibilities assigned to them, all of which we will discuss later. The key to successful OPSEC, as we will soon see, is to get everybody involved. No matter what their job is, every person does have some responsibility for OPSEC.

LESSON

PRACTICE EXERCISE

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows.

1. The ultimate objective of OPSEC is to

_____

_____

2. Name three OPSEC requirements as stated in AR 530-1.

   A.

   B.

   C.

3. The _____ is provided to assist the G3 in fulfilling the units OPSEC responsibilities.

4. The CI Analysis Section, under the direct supervision of the _____, is part of the theater, corps and division level ACE.

5. Although the OPSEC Committee is not a _____, it is a good idea to set one up to assist in the _____ of OPSEC duties.

LESSON

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item	Correct Answer Feedback
1.	To prevent an enemy from obtaining sufficient information to predict, and thus be able to degrade, friendly operations or capabilities. (page 1-3, para 8).
2.	See page 1-4.
3.	OPSEC Staff Element. (page 1-5, para 2).
4.	G2. (page 1-5, para 3).
5.	Regulatory requirement; effective performance (page 1-5, para 5).

PART B: OPSEC PLANNING SEQUENCE STEP 1

The OPSEC Planning Sequence is a systematic process encompassing all aspects of security and common sense. It involves continuous planning, data collection, analysis, reporting, and execution of orders and instructions. The planning sequence is cyclic in nature, taking into consideration the changing nature of both the threat and friendly vulnerabilities. It should be applied to all US Army operations, elements in garrison, field training exercises in peacetime, and operations in wartime. We will discuss in great detail the recommended steps that can be followed to provide good OPSEC. Although not all inclusive, they do serve as a point of departure. Keep in mind that these steps may be brief or in detail, depending on the complexity and sensitivity of the activity.

STEP 1: PREPARE AN OPSEC ESTIMATE OF THE SITUATION.

OPSEC Estimates: An OPSEC Estimate would be prepared as soon as it is known that an operation or activity is to be undertaken and periodically during the planning, preparation, and execution phases. The general planning problem is how to gain advantage and avoid harm from inevitable adversary assessments about friendly intentions and military capabilities. Therefore, an OPSEC data base must be developed. Before a unit can implement the other 6 steps within the OPSEC Planning Sequence and develop OPSEC measures, it is necessary to develop the OPSEC data base. It contains the hostile intelligence service (HOIS) collection threat and the friendly force profile. A comprehensive OPSEC data base is absolutely essential if effective analysis is to occur. We must develop detailed information on both the threat and friendly force. The OPSEC data base is developed from pattern analysis of recent operations, operations orders, readiness plans, study directives, signals operating instructions (SOI) counterintelligence reports along with similar documents and details relevant to the operation or activity. Without this information, the planning sequence may as well stop because the operation or activity will only be applying OPSEC haphazardly and most likely will not be protecting the key friendly indicators. All staff elements contribute to the development of the data base. All data contained in both parts of the OPSEC data base which identify the hostile intelligence collection threat and identify the friendly force profile must be systematically organized and cross-referenced for quick access and easy use. Discussed later in the text a some methods for systematically organizing and cross-referencing which will assist in conducting OPSEC analysis, developing effective OPSEC measures, and ultimately protecting friendly indicators.

Identify the Hostile Intelligence Collection Threat: Identifying the hostile intelligence collection threat is the first part of the OPSEC data base. This is an intelligence function performed by the CI Analysis Section (See Figure 1-1). They are responsible for developing and maintaining the hostile intelligence collection capabilities portion of the OPSEC data base.

They must coordinate with the G2, the All-Source Production Section (ASPS), and the ACE for the collection and processing of information for inclusion in this portion of the data base.

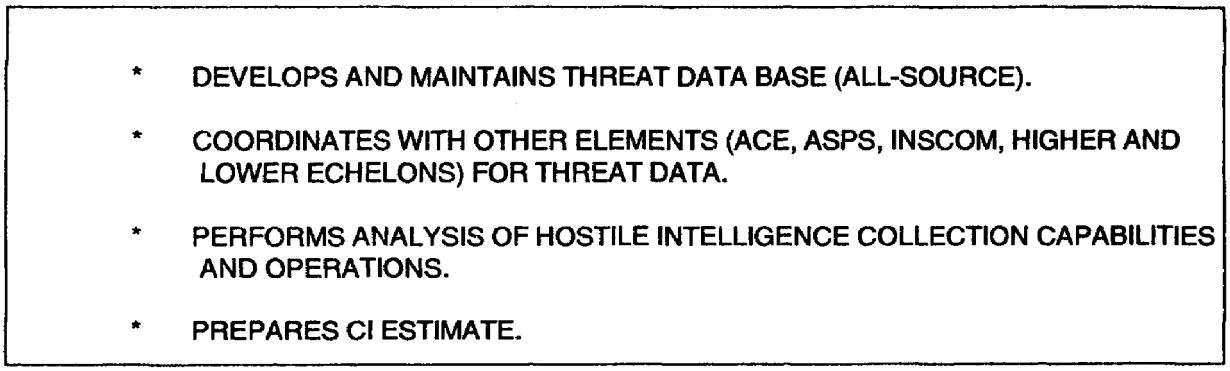


Figure 1-1. CI Analysis Section.

The ASPS already maintains a threat data base which contains all information on the opposing enemy unit(s). For OPSEC purposes, we are interested only in their intelligence collection threat capability. So naturally, the first place counterintelligence (CI) personnel should go for this type of information is the ASPS. The ASPS will provide the majority of the threat information for the OPSEC data base. This information can be used as a basis for developing further information from other sources. The threat data will be as detailed as possible and will not only contain in- formation on who is collecting against friendly forces and how they are doing it, but also with what types of collectors and their actual capabilities. Once the information is collected from the various sources, the CI Analysis Section analyzes it as it applies to OPSEC in order to form an assessment of the hostile collection capability.

The intelligence collection threat facing the US Army today is all-source, multidisciplined and extremely aggressive. As you already know, the Intelligence collection threat can be broken down into three basic disciplines: Human Intelligence (HUMINT); Signals Intelligence (SIGINT); and Imagery Intelligence (IMINT). It is absolutely essential that the CI Analysis Section develop and maintain the data base with the threat targeted against your unit. Consider the unit's current location and contingency mission to determine the requirements. If the unit is facing North Korea, the data base will naturally contain the appropriate threat posed by them. In some cases, the data base will deal with US equipment and tactics being used by former Allies. So, when we state that the hostile threat is multidisciplined, we mean that all three collection disciplines are meshed together to provide a clear picture of the units operations from all points of view.

Additionally, one discipline is used to complement another. The expression all-source means that collection systems, ranging from highly technical overhead platforms, to less technical ground based systems, down to the human eye, are tapped to provide Intelligence information. A quick study of these disciplines will provide the unit with a basis to properly analyze this enormous threat in order to determine the nature, scope, and magnitude of the enemy's intelligence collection means targeted against friendly forces.

Human Intelligence: HUMINT is simply the collection of information using human sources. Hostile governments consistently utilize varied HUMINT techniques to collect information on friendly forces. Some of the methods, although completely overt in nature, nevertheless yield tremendous returns. Examples of human sources include, but are not limited to, the following:

- Representatives of foreign governments: These sources include diplomats, military attaches, other embassy personnel and United Nations employees.

- Foreign students and scientists: it is well known that HUMINT collectors have been inserted into countries using the above named positions. Attendance at scientific trade shows and conferences provide additional opportunities for collection activities to occur.

- Merchant sailors: Soviet merchant ships literally make thousands of port calls in the US and allied countries each month. They are routinely given 29 day visas at their first port of embarkation in the US, thus they are able to travel freely anywhere in the country without any restrictions or limitations.

- Open source: The most readily available source of HUMINT derived intelligence information comes from the wide variety of open source printed material put out in the US and other allied countries. A great deal of information can be collected through the US Government Printing Office and a number of publication clearing houses.

In time of war, CI personnel must also be concerned with the intelligence collection potential of many additional human sources. Some of these sources include: enemy reconnaissance patrols, observation posts, listening posts, and special purpose forces. All of these perform Intelligence collection missions, and can provide valuable information to the enemy commander. Line crossers and refugees provide additional means to infiltrate trained intelligence agents into friendly territory, as well as providing hostile intelligence collection services with a huge wealth of individuals to recruit from.

Signals Intelligence: SIGINT collection encompasses four basic subcategories: communications intelligence (COMINT), electronics intelligence (ELINT), and foreign instrumentation intelligence (FISINT). COMINT is information derived from the study of intercepted electromagnetic communications. COMINT probably has the greatest impact on our daily lives due to our dependency on telephones and radios. ELINT is electronics Intelligence derived from noncommunications electromagnetic radiations from equipment such as radars and navigation beacons. FISINT is derived from the intercept and analysis of electronically transmitted data containing measured parameters of performance, either mechanical or human. Measurement and signature intelligence (MASINT) is scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification or measurement. SIGINT poses a serious threat to the Department of the Army (DA). Modern technology has elevated its effectiveness to a point where virtually all electromagnetic communications, including telephone and radio conversations, are highly vulnerable to hostile intelligence intercept. For OPSEC data base purposes, it is easier to gather very specific information on the SIGINT threat than it is with the HUMINT threat because of the different types of collectors. In order to effectively perform the unit's OPSEC duties, the data base must contain specifics on the hostile collection systems such as frequencies, accuracy, ranges, and so on. SIGINT collectors include-

- Fishing trawlers: Many fishing trawlers are actually sophisticated SIGINT collectors. They commonly patrol waters in and around our fleet task forces.

- Merchant fleet: The same merchant fleet mentioned earlier also possesses a significant SIGINT collection capability. The SIGINT collectors can operate as these ships enter and depart the port area, as well as over a period of several days while the ship is anchored in port to load and unload cargo.

- Overhead platforms: Other sources of valuable SIGINT collection include satellites, Aeroflot, civilian charter aircraft and even small private aircraft.

- Embassies: These facilities are located, and not by accident either, in key areas where nearly 100% of the country's microwave communications can be intercepted by SIGINT collectors.

In addition to all of the above sources for SIGINT collection, any enemy which we might face in a future conflict will be equipped with tactical direction finding, intercept, and monitoring equipment. This equipment will also include that which is necessary to degrade or destroy command and control capabilities of a unit, such as jamming. The wartime CI individual must obtain and use very detailed information in order to effectively counter the hostile SIGINT threat.

Imagery Intelligence: IMINT is also a valuable collection means available to hostile intelligence collectors. IMINT can be obtained from land, sea, air and space platforms. The most serious threat from hostile IMINT resources at the strategic level stems from photo reconnaissance satellites. At the tactical or field combat level, airborne collection possesses the greatest MINT threat. Imagery equipment is constantly being improved technically and used in combination with sensors to enhance the quality and timeliness of the intelligence product. Hostile IMINT collection occurs on a daily basis. No friendly unit or activity is immune from hostile prying IMINT collectors.

Sources of Information: Now that you have a better understanding of the hostile threat, you need to know where to obtain all the information for the data base. Remember that the data base must be sufficient in detail and periodically updated to remain current. You must coordinate the intelligence collection process at the tactical and strategic levels. As mentioned earlier, this is begun by going to the ASPS and getting everything available on the hostile intelligence collection threat. It must then be decided where the gaps in the intelligence holding are and attempt to fill them. This can be accomplished by tasking support units through the G2/S2 section. There are any number of sources available for collection of this information. Many of these sources will be readily available in the division or corps area to which you are assigned: For example, the Aerial Exploitation Battalion, interrogation and CI teams, ground sensors, as well as any SIGINT and HUMINT collection elements. In addition to the above intelligence assets, there are many other sources for current information. These include the Military Police (MP), artillery elements, reconnaissance patrols and engineers. If tactical elements cannot collect the information needed, there are many strategic sources available. These sources include: Intelligence and Security Command (INSCOM)(both local and their HQ), Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) along with other sister services. Daily, weekly and periodic reports generated by these agencies are available for review, usually at the local Special Security Office (SSO). The key to the successful collection of threat data is to establish a viable liaison program with applicable agencies and individuals.

Management of the data base: A comprehensive data base is absolutely essential if effective analysis Is to occur. There is an abundance of threat data available. As such, success in identifying the hostile intelligence collection threat is based more on organizing and maintaining the data base than on collecting threat information. There are a variety of methods available which can be used by the analyst. Listed below are a few of the recommended methods for maintaining the threat data base.

- Card files: Maintain all information on 3x5 or 5x8 index cards; cross referencing all information on collectors, names of individuals and organizations, affiliations, locations, incidents and so on. Cards will be kept on all types of collectors to include actual capabilities to collect. Cards can be used for doctrinal and actual information. Individual cards should be maintained for each new piece of information obtained with the cross-referenced notations of similar or related cards. This method is time consuming but it will provide quick access to large volumes of related information.

- Threat book: Using much the same technique as discussed with the card files, maintain a threat book containing all of the threat information. Maintain separate sections of the book for the HUMINT, SIGINT, and IMINT threats. The key difference between the card file system and the threat book is the added capability to include charts, graphs, and photographs. Ensure that you include a means for updating and disposing of information.

- Graphic overlays: All information concerning the threat can be plotted graphically on a map overlay. Separate overlays can be used for each hostile intelligence collection discipline, or all three can be maintained and integrated on one hostile collection overlay. If one overlay is used, different colors will be used to indicate the various threat disciplines. Overlays should contain all of the information required to perform analysis to determine friendly vulnerabilities and the risks to friendly operations. To eliminate excessive clutter, graphic overlays should be used in conjunction with one of the above mentioned methods. Overlays provide an excellent means for briefing the decision maker on your recommendations. The decision maker can visually see the threat and friendly vulnerabilities which will enable them to make better decisions.

- Automated data bases: All of the above methods can also be automated, when available or feasible, for faster processing, updating, and retrieval of information. The Army currently has the Microfix computer in its inventory. This can be maintained for the OPSEC data base. The All-Source Analysis System (ASAS) is being developed for future fielding to the division and corps levels. The system will include an OPSEC subsystem which will have the capability to perform or at least assist the analyst in most OPSEC functions.

- FM 34-60A(S): FM 34-60A(S), Counterintelligence Operations, has additional information on developing and maintaining data bases.

Identify Friendly Force Profile:

The second part of the OPSEC data base, the friendly force profile, plays just as an important role in effective OPSEC analysis as does the threat portion.

Friendly force profile: Friendly force profiles are comprehensive, detailed studies of all of a unit's characteristics. This includes the timing of actions taken by a unit as a whole and those of individual soldiers. Profiles contain all information which may be of intelligence value to potential or actual adversaries. Development of these profiles requires a joint effort between the G3/S3, the G2/S2 and other staff personnel. It is primarily the responsibility of the OPSEC Staff Element; however, the CI Analysis section assists the OPSEC Staff Element in the identification and development of these profiles. Once the unit profile has been developed, it is maintained by the OPSEC Staff Element for later use in analysis. Information to be included in a friendly force profile includes the following:

- Friendly doctrine: All of the information on how we deploy and how we fight under normal conditions. You can obtain this information by reviewing regulations, FMs, and local SOPs.

- Equipment: Obtain information on all types of equipment assigned to the unit, to include how its deployed, unique characteristics, physical appearance, and any technical information relating to its operation.

- Historical records: Chronological after-action reports on past operations to include how things were done and why.

- Past compromises or security violations: Historical information on the types of Incidents, what was compromised and the way it occurred.

- OPSEC evaluations: All information obtained as a result of performing an OPSEC evaluation service.

- Probable friendly courses of action: In order to work through the OPSEC process for an operation, it is necessary to have the probable friendly courses of action. Include the actual course of action and all of those which are being considered. This is obtained from the commander or G3 during his/her initial briefing for an operation.

- Patterns, signatures, indicators, vulnerabilities and Essential Elements of Friendly Information (EEFI) will also be included as part of the friendly force profile. We will discuss these terms at great length shortly.

Profile areas: All unit activities must be identified and included in the friendly force profile. Profiles are developed in five areas. These five areas need to be looked at overall as they pertain to unit operations and then again as the unit organizes for a specific military operation. The areas to be looked at are-

- Command posts and communications.

- Intelligence.

- Operations and maneuver.

- Logistics.

- Administrative and other support.

Unit profiles must be developed in peacetime, using all available assets, and then periodically updated and revised as needed. Updating occurs when new equipment is received, when casualties occur, and so on.

The three key components of a unit profile (See Figure 1-2) are developed from integration of all available sources of information. Definitions are as follows:

1. Patterns: Patterns are stereotyped actions which so habitually occur in a given set of circumstances that an observer can use them as cues to determine what capabilities, vulnerabilities or intentions exist. Basically, patterns are the result of the way military operations are conducted. Predictable patterns are caused by unit SOPs, staff personalities and Army doctrine. An example of a pattern established by many units and easily detected by hostile intelligence, is the practice of going on radio silence just prior to an operation. To develop your units established patterns, you must study the unit activities as determined by Army doctrine, local SOPs, commanders, and so on. You must also observe the unit in action while conducting various types of mission-related activities.

2. Signatures: Signatures are the distinctive, unique characteristics of a unit which result from that units mere presence on the battlefield or in garrison. Signatures are detected because units differ in types of equipment, sizes, emission of electromagnetic signals, deployment, and in noises and smells associated with them. Signatures fall into four general categories:

a. Imagery signatures: Imagery signatures are detected by various systems which have the capability to pick up on visible light reflections, as well as heat from objects. Generally, signatures in the imagery spectrum are pieces of equipment, personnel and other objects or activities. Theoretically, a target is detected by photography and identified by the analyst because of the five "S" formula:

- size
- shape
- shade
- shadow
- surroundings

b. Electromagnetic signatures: Electromagnetic signatures are caused by electronic radiation from communications and noncommunications emitters. In broad terms, the detection of a specific electronic signature may show the presence of an entire unit or activity in the area. This will normally cue other sensors to search the area.

c. Olfactory signatures: Olfactory signatures deal with those aspects of a military unit or activity which can be detected and possibly identified because of a peculiar odor associated with them. For example, diesel fuel smells different than regular gasoline.

d. Acoustical signatures: Acoustical signatures are the result of sounds being emitted by a unit. They are broken down into two basic types: battle noise, or those noises caused by gunfire and explosives; and sounds associated with military operations such as vehicles, equipment and installation activities.

3. Indicators: Once the analyst has developed the unit's patterns and signatures, it is time to go back and look at the gathered information contained in the profile, paying particular attention to the patterns and signatures, to identify all of those bits of information or actions which provide an indicator to the enemy. Indicators are items of information which reflect the intention or capability of a potential enemy to adopt or reject a course of action. Indicators are not abstract events. They are actual actions taken by a military unit or the direct result of military operations and activities. Identification and interpretation of specific indicators are critical tasks in intelligence operations. The friendly data base should contain a listing of generic indicators associated with your unit and all types of operations it might become involved in. This listing can then be used later to determine aspects of friendly courses of action which could compromise the mission. Generic indicators of attack and defense are located in Appendix B of this subcourse.

Critical Nodes. The development of a complete friendly force profile takes a long time. Even then it is not really complete due to the constantly changing nature of military units and activities. Therefore, it is absolutely essential that we prioritize our efforts and begin with the key elements and activities of the command. These key activities and elements are called critical nodes. So, critical nodes are the key activities and elements within a command without which the command could not operate.

Within the five areas of concentration during profile development, some of the key elements and activities we need to consider are shown below. Many of the items listed under each category are places where patterns develop and signatures exist. This list will serve as a guide to give you an idea of those things which could be indicators:

- Command posts (CP) and communications:

  a. Where are CPs in relation to other elements of the command?

  b. What does the CP look like?

  c. When does the CP move in relation to other elements of the command?

  d. Is the CP surrounded by antennas?

  e. What types of communications equipment is used and where is it located?

  f. What kind of information is passed over the communications net? What is the volume? Are there secure nets?

  g. Are there road signs which assist the enemy in locating head- quarters and CPs?

- Intelligence:

  a. Examine the frequency and areas in which ground and air elements are tasked to gather information.

b. Where are collectors deployed? What reporting and security procedures are they using?

c. How are radars used? How long are they operational before re- locating?

- Operations and maneuver:

a. Can tactical rehearsals and drills be easily observed?

b. Is special training required? Is this fact protected appropriately?

c. Are new units arriving in the operational area?

d. What actions are the same when preparing for offensive and defensive operations? Do they show intentions?

- Logistics:

a. What movements indicate the start of an operation?

b. Are special equipment or materials visible?

c. Where is prepositioning and stock piling being done and why?

d. Are shortages in specific corps and divisions suddenly corrected?

- Administrative and other support:

a. Do things change before an operation such as wake up and mess schedules, unit designators?

b. Have personnel on leave or pass been recalled?

c. Is there an increase in outgoing mail?

d. How is litter and refuse disposed of?

Now that the friendly force profile portion of your data base is completed, you have a compilation of information, and the analysis of that information, which shows you how your unit looks and acts. You are now able to see your unit as the enemy sees it. Development of the friendly force profile has always been the major OPSEC deficiency. Units fail to see the importance of developing a detailed picture of themselves. Usually they are more interested in looking at the enemy. For effective OPSEC, we need to match the friendly indicators to the threat in order to develop the best OPSEC measures.

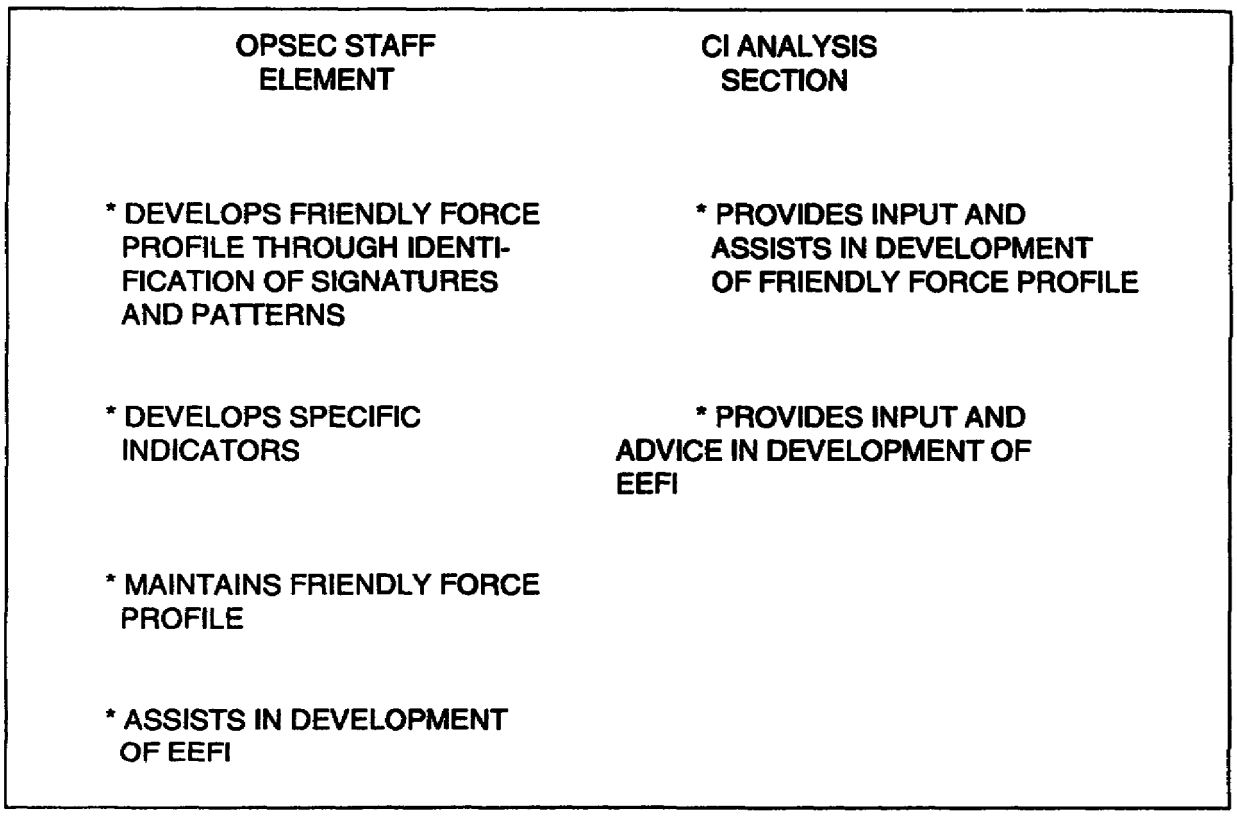


Figure 1-2. Key Ingredients.

LESSON

PRACTICE EXERCISE 2A

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. The OPSEC Planning Sequence is a _____ process encompassing all aspects of _____ and common sense.

2. The two pas of the OPSEC data base are and _____.

3. Patterns are _____ which so habitually occur in a given set of circumstances that an observer can

_____

_____

4. _____ are the distinctive, unique characteristics of a unit which result from the unit's mere presence on the battlefield or in garrison.

5. Indicators are not _____. They are _____ taken by a military unit or the direct result of _____ and _____.

6. Critical nodes are the _____ within a command without which the command could not _____.

LESSON 1

PRACTICE EXERCISE 2A

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	Systematic; security (page 1-9, para 1).
2.	Identifying the hostile intelligence collection threat; friendly force profile (pages 1-9, para 3 and 1-13, para 7).
3.	Stereotyped actions; use them as cues to determine what capabilities, vulnerabilities or intentions exist (page 1-15, para 3).
4.	Signatures (page 1-15, para 4).
5.	Abstract events; actual actions; military operations; activities (page 1-16, para 1).
6.	Key activities; operate (page 1-16, para 2).

PART 2B. OPSEC PLANNING SEQUENCE STEPS 2 AND 3

STEP 2: ISSUE OPSEC PLANNING GUIDANCE.

It is within this step of the OPSEC Planning Sequence that it becomes necessary to further analyze the friendly force profile in relation to the current friendly course of action to develop an initial listing of essential elements of friendly information (EEFI). EEFI are questions about friendly intentions and military capabilities likely to be asked by the opposing planners and decision makers in competitive circumstances. Answers to the EEFI provide key information that adversary planners and commanders need to know about friendly intentions and capabilities. At this point, the list of EEFI is nothing more than a laundry list. The list is based on the commanders concept of the operation and the friendly force profile. It contains all information which should be protected, not just those bits of information which are critical to the success of the operation. This list will be further refined during the analysis that is performed later on, so that you end up with the true EEFI for the operation. The key point to remember about EEFI is that they will prioritize and identify the profiles on which the OPSEC Planning Sequence should concentrate.

STEP 3: IDENTIFY PROTECTIVE MEASURES.

Identify Friendly Force Vulnerabilities: The CI Analysis Section, with assistance from the OPSEC Staff Element, has the primary responsibility far performing the vulnerability assessment to identify the friendly force vulnerabilities. The vulnerability assessment is performed to determine which friendly indicators are most vulnerable to hostile collection efforts.

Vulnerabilities are those profiles which disclose indicators of a unit's planning or operational procedures which, unless adequate OPSEC measures are implemented, will be detected by hostile collection resources. If collected, these vulnerabilities could compromise the commanders EEFI, thus jeopardizing the success of the planned operation or mission.

A vulnerability exists whenever the enemy has the capability to collect information on our forces (date, time, location, and type of unit or activity), and process the information in time to react in a manner which could affect the outcome of the operation or mission. During the vulnerability assessment, you will compare the friendly force profile to the hostile intelligence collection capabilities to identify unit vulnerabilities. Depending upon the current situation, you may compare the entire friendly profile to the threat, as it is done during peacetime, in garrison; or you may only compare that portion of the profile concerned with the current combat operation. No matter how much of the profile is used, the comparison is still completed. The area where the two overlap are the friendly vulnerabilities.

To break the vulnerability assessment process down a little farther, there are a number of things to look at in order to identify vulnerabilities. Normally, you will begin by comparing the date and time of an operation and the location of the hostile collector to the friendly profile or that portion of the profile relating to the operation. Eliminating those collectors that do not initially match up, you will next look at each remaining collector to determine if they can actually collect the displayed indicator. Once you have determined that you still have a vulnerability, take a look at the amount of time it takes for the enemy to process the information and react to it. Identified vulnerabilities that are essential to the success of the operation and those which must be protected will become part of the commanders EEFI. All identified vulnerabilities may not become EEFIs. It will depend upon their importance to the mission. This list of EEFI is a reduced version of the one you dealt

with during the previous step to the OPSEC Planning Sequence. This list is no longer a generic laundry list. It is very specific to the current operation. As you identify each vulnerability, lit it on the OPSEC measures worksheet, which is the exact same thing as the countermeasure worksheet located in Appendix D. When listing these vulnerabilities, the OPSEC Staff Element ranks them according to their importance to the operation and the CI Analysis Section contributes by ranking them according to susceptibility to collection (the more collectors, the higher the susceptibility).

Perform Risk Analysis and Select EEFI: Risk analysis is the act of determining the risks to operations when no OPSEC measures are applied to protect friendly vulnerabilities from enemy intelligence collection; and then comparing the costs of implementing identified OPSEC measures to their probable effectiveness. Costs are measured in terms of time, equipment, funds, and/or manpower. Determining the risks to an operation when no OPSEC measures are applied is the first task to be accomplished during risk analysis. The OPSEC Staff Element performs this task with whatever assistance is needed from the CI Analysis Section and other operations personnel.

Each ranked vulnerability on the OPSEC measures worksheet is looked at closely to determine the impact that hostile collection would have on the outcome of the operation. There are many factors which can effect the risks to an operation, but basically risks are increased when:

- Enemy force lethality increases.
- Warning time decreases.
- Number of enemy options increases.
- Number of friendly options decreases.
- Enemy's knowledge of the area increases.

On the other hand, risks are decreased when:

- Enemy force lethality decreases.
- Warning time is extended.
- Enemy has fewer options.
- Friendly options increase.
- Friendly force knowledge of area increases.

Once the risks have been identified, we begin to systematically develop OPSEC measures to protect each vulnerable friendly indicator, thereby reducing or eliminating the risk levels. Some OPSEC measures are designed to defeat more than one collector, if properly applied. The threat and vulnerable indicator will be the determining factors for choosing the best OPSEC measures.

OPSEC measures fall into three inter-related categories. These categories are:

- Countersurveillance measures: These are routine security measures which are designed and implemented to prevent hostile collection of friendly indicators to operations or activities. They are designed to protect the true status of friendly operations. Countersurveillance measures am normally listed in the unit's OPSEC and security SOPs, as well as in Army Regulations. Units use countersurveillance measures all of the time, for every operation or activity. These measures include the following:

  Camouflage.

  Noise and Light Discipline.

  Information Security.

  Physical Security.

  Personnel Security.

  Signals Security.

- Countermeasures: They are actions taken to offset a specific hostile intelligence collection operation. Countermeasures employ devices or techniques with the objective of impairing the operational effectiveness of enemy collection activities. Countermeasures fall into four basic subcategories:

  1. Destruction of the hostile collector: Once located, a hostile collector is targeted by one or more destruction means. This action must be taken swiftly to prevent further intelligence collection from taking place.

  2. Counter-HUMINT measures: Measures that am taken to deny information to the human source. Examples are:

     SAEDA training.

     Restricted areas.

     Surveillance.

  3. Signal activity or counter-SIGINT: Counter-SIGINT measures am those actions taken to counter hostile signal collectors, whether communications or noncommunications. The objective of counter-SIGINT is to ensure that all friendly use of the electromagnetic spectrum is unexploitable by the enemy. Signal security is broken down to include COMSEC and ELSEC techniques. These measures include:

Proper training of operators.

Secure voice.

Moving the emitter.

Jamming.

Transmission brevity.

4. Counter-IMINT measures: They are those measures which are implemented to deny the enemy from obtaining imagery of friendly operation. All counter-IMINT measures are designed to conceal the friendly force from enemy observation.

- Deception: Deception consists of all actions designed and taken to mislead the enemy. It may include manipulation, distortion or falsification of information to cause the enemy to act in a way prejudicial to his best interests.

Once all of the OPSEC measures which will protect each indicator have been identified, the OPSEC Staff Element and the CI Analysis Section coordinate their efforts to determine the costs involved in implementing the measures as compared to the expected benefit to be derived. Benefit is measured in terms of reduction of risk. And as stated earlier, costs are measured in time, manpower, equipment, money and even loss of effectiveness. The primary reason for doing this costs versus benefit analysis is to identify the best OPSEC measures (the cheapest and most effective). All of the information resulting from the complete risk analysis is added to the OPSEC measures worksheet. You now have in a single place, the friendly indicator, the threat, risks to the operation, OPSEC measures, and the costs and benefits associated with implementing those OPSEC measures (see Figure 1-3).

The risk analysis process will also result in the final selection of the EEFI which are critical enough to warrant the application of OPSEC measures. This selection, accomplished by the commander or the G3, will be based on those critical indicators which are vulnerable, and if detected, would result in high risks to the operation. These are true EEFI.

Recommend and Select OPSEC Measures: At this point in the sequence, the CI Analysis Section and the OPSEC Staff Element provide the decision maker, whether it be the commander or his G3, with the OPSEC estimate. This can be done orally or in writing. The estimate consists of the results of the vulnerability assessment and the risk analysis, to include identified OPSEC measures.

Once the OPSEC Staff Element and the CI Analysis Section make their recommendations of OPSEC measures, the decision maker will select the OPSEC measures to be implemented. The selection of OPSEC measures will be based on the commanders perception of the operation, the risks involved, the cost of implementing OPSEC and the likelihood of success. When going through the selection process, the decision maker has basically only two real options:

No OPSEC measure is necessary.

Apply one or more OPSEC measures.

So, the options exist to ether select and implement an OPSEC measure(s), or don't. The next three options listed here are basically OPSEC measures in themselves and therefore they are add-ons rather than real options:

Stop the activity.

Change the operation.

Implement a deception plan.

If the first option, no OPSEC measure is necessary, if chosen, then one of the following conditions should exist:

No vulnerability exists.

If detected by the enemy, the indicator would support the deception plan.

The commander is willing to accept the risks.

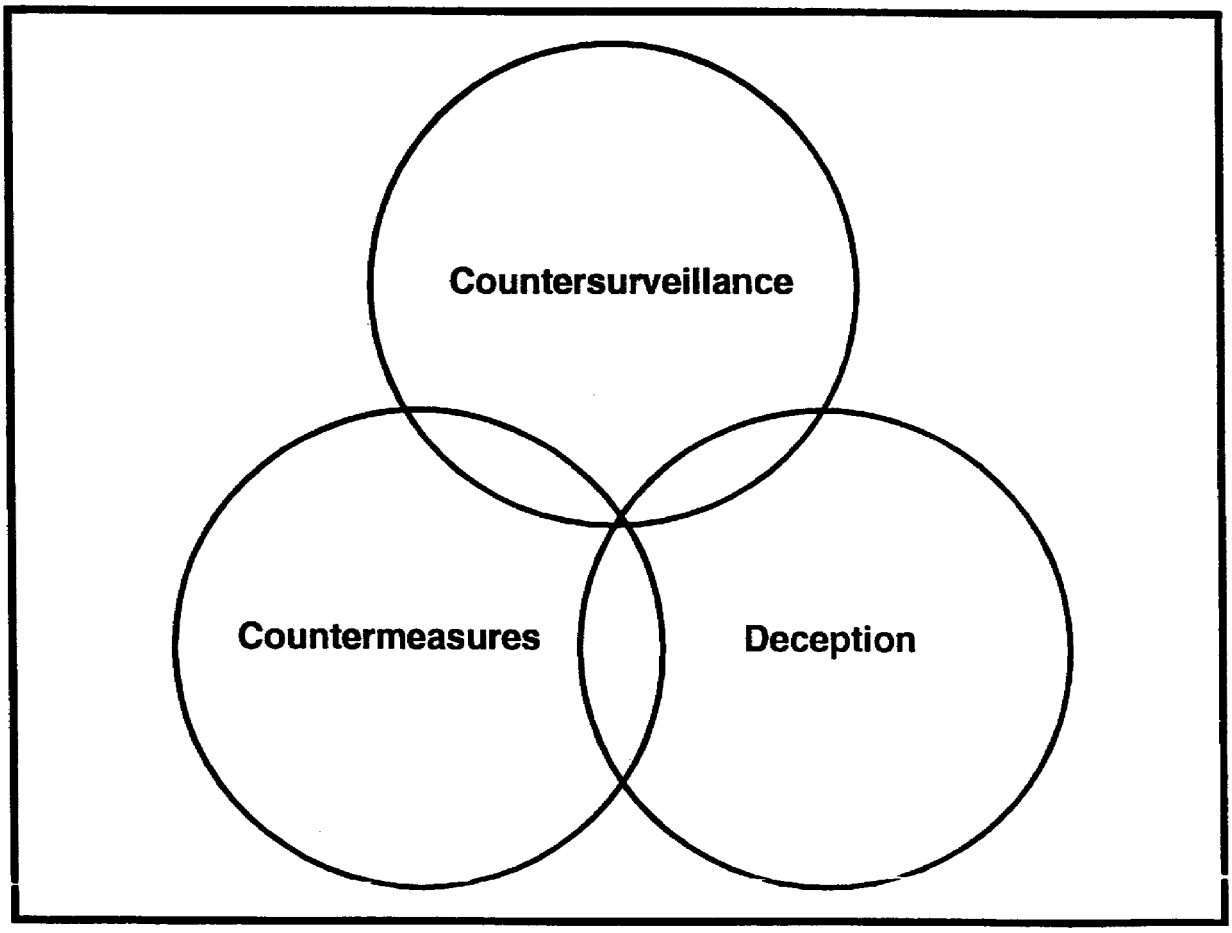


Figure 1-3. OPSEC Measures.

LESSON

PRACTICE EXERCISE 2B

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. EEFI are questions about _____. and_____likely to be asked by the opposing planners and decision makers in _____ circumstances.

2. EEFI will _____ and _____ the profiles on which the_____ should concentrate.

3. A vulnerability exists whenever the enemy has _____ _____

4. Risk analysis is the act of determining _____ when no OPSEC measures are applied to protect friendly_____ _____from enemy intelligence collection; and then _____of ineffectiveness.

5. Costs are measured in terms of _____, _____,and/or _____.

6. OPSEC measures fall into three inter-related categories. These categories are:

   a.

   b.

   c.

7. The risk analysis process will also result in the final selection of _____ which are critical enough to warrant the application of _____.

LESSON

PRACTICE EXERCISE 2B

ANSWER KEY AND FEEDBACK

Item	Current Answer and Feedback
1.	Friendly intentions; military capabilities; competitive (page 1-21, para 1).
2.	Prioritize; identify; OPSEC Planning Sequence (page 1-21, para 1).
3.	The capability to collect information on our forces (date, time, location and type of unit or activity)(page 1-21, para 4).
4.	The risks to operations; vulnerabilities; comparing the costs (page 1-22, para 2).
5.	Time, equipment, funds, and manpower (page 1-22, para 2).
6.	a. Countersurveillance measures; b. countermeasures; c. deception (pages 1-23, para 2; 1-23 para 3; and 1-24, para 2).
7.	EEFI; OPSEC measures (page 1-24, para 4).

PART 2C. OPSEC PLANNING SEQUENCE STEPS 4 THRU 7

STEP 4: PREPARE AN OPSEC ANNEX OR PLAN.

During the planning and selection process for OPSEC measures, the countermeasures worksheet is completed. The worksheet describes OPSEC measures for the force as a whole and specific OPSEC measures to be employed by the subordinate maneuver and support units. The worksheet becomes a part of the OPSEC annex to the Operations Order (OPORD).

Plans for operations, exercises, technology, or other activities to include acquisition and research programs that are of interest to foreign intelligence will be supported by the OPSEC annex or plan. A model outline of the OPSEC annex is provided in Appendix A and AR 530-1. The format and content of the OPSEC annex will be tailored to meet the specific needs of the project, activity, operation, or function concerned. It may be disseminated by any of the following means: as an annex to the OPORD, as a fragmentary order (FRAGO) or as written instructions.

Tasking for OPSEC measures implementation is accomplished through the use of the OPSEC annex or the OPSEC measures worksheet. Fragmentary orders or amendments to the initial OPSEC annex can also be used to update or change the implementation process.

STEP 5: BRIEFING PARTICIPANTS.

OPSEC measures will be executed as command directed actions and as individual responsibilities. OPSEC briefings will be provided to planners, participants, and those supporting operations, exercises, materiel acquisition and other activities. The briefings will be directed specifically at the responsibilities of the group addressed. These briefings are given not only by OPSEC officers, but also by other cognizant planners, project managers, and security and support personnel.

STEP 6: EXECUTE PROTECTIVE MEASURES AND MONITOR RESULTS.

At this point, the primary function of the OPSEC Staff Element and the CI Analysis Section is to ensure that all elements of the command are knowledgeable of the OPSEC measures to be implemented. This is accomplished using one of the methods mentioned earlier. Once each element knows what to do, the OPSEC Staff Element and the CI Analysis Section will further ensure that the OPSEC measures are implemented correctly--when and where needed.

The friendly force must establish procedures for a periodic evaluation of the overall effectiveness of the OPSEC measures that they have implemented. Unevaluated OPSEC measures can lead to a false and very dangerous sense of security. Units are lulled into believing that since they have applied OPSEC, the enemy cannot detect information concerning their operations. Therefore, they tend to let their guard down somewhat. OPSEC evaluations are nothing more than the monitoring of applied OPSEC measures to determine their effectiveness. In other words, we are looking for strengths to recognize and weaknesses to correct.

It is during this point of the Planning Sequence that all planning requirements for evaluating applied OPSEC measures will be completed. In addition to determining the scope, the OPSEC Staff Element and CI Analysis Section will also determine when the evaluation will be conducted, how it will be conducted, the kind of evaluation to be conducted, and who will conduct it. The OPSEC measures worksheet will be used to assist in identifying the scope and methods to be used.

Wartime evaluations. Evaluations conducted during hostilities are usually initiated when critical vulnerabilities and threats are identified. Trained OPSEC and unit personnel then responded to immediate taskings to resolve specific problems rather than performing generalized unit evaluations.

Peacetime evaluations: In this type of environment, it is possible to examine the entire OPSEC program of a unit. Special teams from outside-the unit are usually the best way to perform these peacetime evaluations, but it is not necessary. Outside teams increase objectivity and allow the unit's OPSEC personnel to continue to carry on their normal duties. If possible, an evaluation of the entire OPSEC program should be completed at least annually.

It is important for you, the team, and the unit personnel to realize that OPSEC evaluations are not inspections. They are designed and aimed at identifying shortfalls or problem areas with the application of OPSEC, so that those problems can be corrected. The evaluator is looking at the unit from an enemy point of view, using his/her methods of intelligence collection, to determine if the applied OPSEC measures are working as intended. They will attempt to identify friendly indicators which are supposed to be protected.

OPSEC evaluation reports, either orally or in writing, are provided to the commander, OPSEC Staff Element and the CI Analysis Section. Copies of the report are provided for inclusion in the OPSEC data base.

Recommend Adjustments to OPSEC measures: Based on the information reported by the OPSEC evaluators, adjustments are made to the OPSEC measures. The OPSEC Staff Element and CI Analysis Section will analyze the evaluation results to determine where corrective action is needed. Once identified, corrections or adjustments will be implemented as quickly as possible.

STEP 7: PROVIDE OPSEC FOLLOW-UP AND IDENTIFY LESSONS LEARNED.

The majority of lessons learned can normally be identified during the monitoring process. The others can be identified during an evaluation of the completed operation, plan or program. Lessons learned are the basis to integrate improvements into the command's overall OPSEC planning process. Improvements include briefing key participants on the success or failure of OPSEC efforts and sharing information with nonparticipants through lessons learned.

Continuous nature of OPSEC: The last step of the OPSEC Planning Sequence can lead you back up to where the selection of OPSEC measures were made. Changes identified to either the threat or friendly profile, due to the battle, necessitate going back to the OPSEC data base. This in turn requires redoing the vulnerability assessment and risk analysis. So, as you can see, the OPSEC Planning Sequence is a continuous cycle which is applied before, during and after an operation. We must protect all phases of an operation with effective OPSEC.

THINK OPSEC!

LESSON

PRACTICE EXERCISE 2C

The following items will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. A model outline of the OPSEC annex is provided in _____ and_____.

2. The OPSEC annex may be disseminated by any of these means:

   a.

   b.

   c.

3. Unevaluated OPSEC measures can lead to a _____ and very dangerous _____.

4. OPSEC evaluations are nothing more than the _____ to determine their effectiveness. In other words, we are looking for _____to recognize, and _____ to correct.

5. The _____ and the _____ will analyze the evaluation results to determine where corrective action is needed.

LESSON

PRACTICE EXERCISE 2C

ANSWER KEY AND FEEDBACK

Item	Correct Answer and Feedback
1.	AR 530-1; Appendix A (page 1-29, para 2).
2.	a. Annex to the OPORD; b. FRAGO; c. written instructions (page 1-29, para 2).
3.	False; sense of security (page 1-29, para 6).
4.	Monitoring of applied OPSEC measures; strengths; weaknesses (page 1-29, para 6).
5.	OPSEC Staff Element; CI Analysis Section (page 1-30, para 5).

APPENDIX A

OPERATIONS SECURITY (OPSEC) ANNEX FORMAT

(CLASSIFICATION)

HEADQUARTERS
UNITED STATES ARMY XXX XXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 12345-6789
XX XXX 19XX

Annex X (Operations Security) to XXX XXXXX OPLAN XXXXX XXXXX

1. ( ) References:
   a. AR 530-1, Operations Security.
   b. Reference documents needed to accomplish tasks stated herein.

2. ( ) Situation. Refer to other annexes and paragraphs in the basic plan as much as possible to avoid duplication. When publishing the OPSEC annex separately from the basic order, however, it is necessary to copy the information here in detail. That allows the OPSEC annex to be useful, stand-along document.

   a. ( ) Enemy Forces.
      (1) ( ) Current Enemy Intelligence Assessment. State the estimated enemy's assessment of friendly operations, capabilities, and intention. Specifically address any known enemy knowledge of the friendly operation covered in the basic plan.
      (2) ( ) Enemy Intelligence Capabilities. State the enemy's intelligence collection capabilities according to major categories (SIGINT, HUMINT, and so forth). Address all potential sources to include the capabilities of any non-belligerents, who may provide support to the enemy. Describe how the enemy's intelligence system works to include the time required for intelligence to reach key decision makers. Identify major analytical organizations and key personalities. Discuss unofficial intelligence organizations, if any, that support the leadership. Identify strengths and weaknesses.
   b. ( ) Friendly Forces.
      (1) Friendly Operations. Briefly describe the major actions of friendly forces during execution of the basic plan.
      (2) C2W Operations. Describe the mission and concept of operations for command and control warfare.
      (3) Critical Information. List the identified critical information. Include the critical information of higher headquarters. In phased operations, list it by phrase; information that is critical in an early phase may not require protection in later phases.
   c. ( ) Assumptions. Identify any assumptions for the OPSEC part of the plan.

3. ( ) Mission. Refer to the basic plan. Reproduce the basic plan's mission statement, if publishing the OPSEC annex separately. (There is no separate "OPSEC mission.")

(CLASSIFICATION)

(CLASSIFICATION)

4. ( ) Execution.
   a. ( ) Concept of Operations. Describe the general concept to implement OPSEC measures. Give it by phrase and major activity (maneuver, logistics, communications, and so forth), if appropriate. Address OPSEC support to other elements of command and control warfare (C^2W).
   b. ( ) Tasks. Identify specific OPSEC measures to implement. List by phrase, if appropriate. Assign responsibility for execution to subordinate elements. Add an appendix to this annex for detailed or lengthy lists.
   c. ( ) Coordinating Instructions. Identify requirements to coordinate OPSEC measures between subordinate elements. Address required coordination with public affairs. Provide guidance how to terminate OPSEC related activities of this operation. Address declassification and public release of OPSEC related information.

5. ( ) Administration and Logistics. Give special OPSEC related administrative or logistical support requirements. (List any OPSEC measures for administration or logistics in paragraph 3.)

6. ( ) Command and Control.
   a. ( ) Feedback. Describe how to monitor the effectiveness of OPSEC measures during execution. Identify specific intelligence requirements.
   b. ( ) OPSEC Surveys. Describe any OPSEC surveys in support of this operation.
   c. ( ) After Action Reports. Identify any requirements.
   d. ( ) Signal. Cover special or unusual OPSEC related communications requirements. (List all OPSEC measures concerning communications in para 3.)

NAME
General, USA
Commanding

Official:

/s/

NAME
Deputy Chief of Staff, Operations

CLASSIFIED BY:
DECLASSIFY

(CLASSIFICATION)

APPENDIX B

Possible Indicators of Attack:

Massing of mechanized elements, tanks, artillery, and logistical support.

Deployment of combat elements (mechanized, armor, antitank) in echelon.

Dispersal of tanks and self-propelled guns to forward units.

Extensive artillery preparation.

Artillery positions well forward and concentrated.

Extensive patrol activity.

Change in communication levels, call signs, and frequencies.

Location of air defense forces farther forward than normal.

Extensive resupply, reinforcement, and unit replacement activity.

Relocation of support units forward.

Possible Indicators of Defense:

Withdrawal from defensive position before becoming heavily engaged.

Successive local counterattacks with limited objectives.

Counterattacks broken off before position is restored.

Preparation of battalion and company defensive areas.

Extensive preparation of field fortifications and minefields.

Rearward movement of long-range artillery and supply echelons.

Frontages up to four times that normally assigned to units.

Destruction of bridges, communication facilities, and other military assets.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX C

OPERATIONS SECURITY

EVALUATION

CHECKLIST

THRU: TO: FROM:
UNIT: COMMANDER:
CONTENTS DISCUSSES WITH:
NAME RANK UNIT
EVALUATOR'S SIGNATURE: OVERALL RATING:

OVERALL

AREA 1. CAMOUFLAGE:

YES NO RMKS

a. Have all vehicle markings (serial numbers, unit ID) been effectively masked?

b. Have canvas tops and side curtains been removed from vehicles in accordance with prevalent weather conditions?

c. Have glass surfaces been covered with a nonreflecting material to prevent glare?

d. While parked, have vehicles been dispersed?

e. Were vehicles parked in shadows and moved when shadows shifted?

f. Was advantage of natural foliage and terrain features used in camouflaging vehicles?

g. If camouflage nets were used, were they properly hung?

h. Was advantage of natural foliage and terrain features used in camouflaging tents?

i. Was cut foliage replaced as needed?

j. Were tents properly dispersed?

k. When antennas were erected, was natural vegetation used to camouflage them? (Antennas may be erected so that the top of the antenna is concealed by foliage of trees and the trunk of the tree helps to conceal the mast.)

l. Was the visibility of the antenna reduced by regulating the height of the mast without seriously reducing or hampering communications?

m. Was the area free of trash and litter?

n. Was the number of tracks, both vehicular and personnel, kept to the minimum? Does unit have a track plan?

	OVERALL		
	YES	NO	RMKS
o. Were personal items such as wash cloths, towels, undershirts, and shorts, which would contrast with the natural surroundings, kept out of sight?			
p. Did personnel cutting foliage avoid stripping or cutting too much foliage in areas near their tents, vehicles, or positions?			
q. After digging a fighting position or other type of hole, was the freshly turned earth or berm camouflaged?			
r. Was care taken to conceal the freshly cut portions of a tree or bush when limbs or large pieces of foliage were removed?			
s. When cutting limbs from trees, was care taken to make the cut on the wooden side of the tree?			
t. Was the average distance between major items of equipment at least 30 meters?			
u. Are helicopters that are on the ground for more than 30 minutes moved into treelines and camouflaged?			
v. Are generators dispersed as much as power cables allow?			
w. Were light leaks from tents and vans present?			
x. Were steps taken to prevent light leaks from tents when flaps were opened for entry or exit?			
y. Were guides and blackout lights used when moving vehicles in or near CP areas?			
z. Were red filters used on flashlights?			
aa. Did personnel observe the principles of light discipline while smoking?			
bb. When operating radios at night, were volume and squelch turned on low?			
cc. Were personnel noises kept to the absolute minimum?			
dd. Were effective measures taken to reduce generator noise?			

AREA 2. DOCUMENT SECURITY:

PART I: The following items are checked for control of actual classified material in the field.

	OVERALL		
	YES	NO	RMKS
a. Are adequate storage facilities available to store actual classified material in the field?			
b. Is an inventory list made up on all actual classified material being held in the field?			
c. Is actual classified material being inventoried daily to ensure it has not been lost?			
d. Are adequate measures being taken to ensure that actual classified information is not being included in documents created for training purposes and that are for training only?			
e. Is the S2 maintaining a record of personnel who have actual clearances and is access to actual classified material limited to those people?			
f. Are units/sections reproducing actual classified material in the field without first clearing with higher headquarters?			
g. Are units/sections transferring actual classified material?			
h. Are all documents marked in accordance with AR 380-5 with correct classification and downgrading instructions?			
i. Are actual classified documents being properly destroyed in the field?			
j. Is a written Emergency Evacuation Plan for classified material displayed in a prominent location? And is it current with the situation?			
k. Is all classified waste treated and protected as classified material? Items to be especially careful of are carbon papers, pencil notes and typewritten ribbon.			
l. Are typewriter ribbons used to type classified material being handled as classified documents?			

PART III. Document Security for Material Classified for Training:

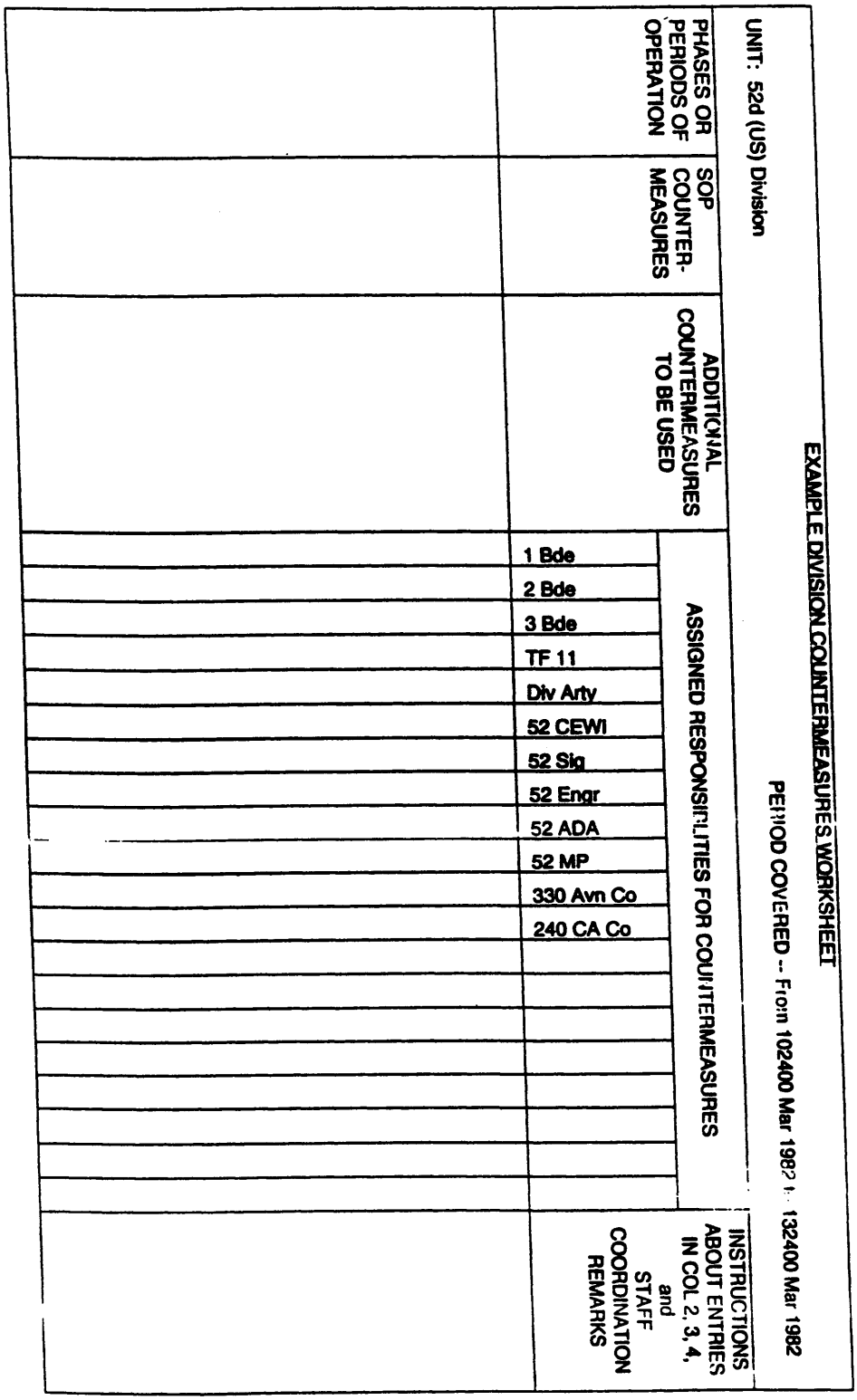
	OVERALL		
	YES	NO	RMKS
a. Are adequate storage facilities available separate from actual classified material?			
b. Is access to material classified for training purposes restricted to properly cleared individuals with a need to know?			
c. Is the S2 maintaining a roster of personnel clearances?			
d. Are clearances granted for training material clearly marked as such and are they being kept separate from actual clearances?			
e. Is reproduction of materials classified for training being controlled?			
f. Is the unit maintaining a record of all material transferred to another unit on a DA 3964 as prescribed in regulations?			

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX D

EXAMPLE

COUNTERMEASURES (OPSEC)



EXAMPLE COUNTERMEASURES WORKSHEET

UNIT: _____ PERIOD COVERED- FM _____ TO _____

FRIENDLY UNIT INDICATORS	ENEMY COLLECTION MEANS TO BE TARGETED	COUNTERMEASURES	INSTRUCTIONS OR REMARKS	UNITS RESPONSIBLE

APPENDIX E

OPSEC PLAN FORMAT

(CLASSIFICATION)

HEADQUARTERS
UNITED STATES ARMY XXX XXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 12345-6789

SUBJECT: Operations Security Plan for XXXXX XXXXX

1. ( ) References:

   a. AR 530-1. Operations Security.
   b. Reference source documents for information in this plan.
   c. Reference documents that recipients will require to accomplish tasks states in this plan.
   d. Reference may be made to other plans, annexes, SOPs, and so on.

2. ( ) General. (May be captioned as Administration).
   a. ( ) Introduction. Briefly describe the organization and its overall mission. For RDT&E related programs, the System Description translates to the mission statement. State the purpose of the OPSEC plan, applicability, and administrative responsibilities for implementation.
   b. ( ) Requirements for Essential Secrecy. State the reason the activity, program, or organization must establish and maintain the condition of essential secrecy. Clearly identify why specific information, activities, functions, and procedures must be protected from adversary collection and knowledge through the application of OPSEC.

3. ( ) Sensitive Mission Areas and Essential Elements of Friendly Information (EEFI).
   a. ( ) Sensitive Mission Areas. Identify each area, function, element, and activity that is sensitive due to any of the following:
      (1) ( ) The function is critical to the accomplishment of the organization, facility, activity mission.
      (2) ( ) The identified mission area contains, processes, develops, produces, reproduces, stores, transmits, or transfers information or data (including weapons systems related technology, or system Essential Program Information, Technologies or Systems (EPITS)) that is classified or falls within the definition of unclassified sensitive or critical information. Every effort should be made to keep OPSEC plans and EEFI unclassified. Classified portions, such as threat information, should be published/provided as separate appendixes.
      (3) ( ) It is an activity, that if known and understood by an adversary, could be exploited in a way that would disrupt or have an adverse effect on the activity or would disclose key Military Critical Technology.
   b. ( ) Essential Elements of Friendly Information (EEFI). State the current EEFI that apply to all elements of the organization, activity or program on a continuous basis, or for a specified duration of time. The specific EEFI for a particular element, group, action,

(CLASSIFICATION)

activity, and so on, should be published in appendix 1, OPSEC estimate, at paragraph 1, Essential Elements of Friendly Information. (See app 1, Sample OPSEC Estimate.)

4. ( ) The Intelligence Collection Threat.
   a. ( ) Known Threat. State the known adversary intelligence collection threat to the organization, activity, acquisition or development program. If the plan is for a specific program, project, activity or action within an organization, specify the particular collection threat that will exist during each phase of the activity or action. (Detailed collection threat should be published at paragraph 4b of appendix 1, OPSEC estimate, or as a separate appendix.
   b. ( ) OPSEC Measures. State the OPSEC measures currently in effect, and their intended goal, for each identified threat. Relate OPSEC measures by category (action control, countermeasures, and counteranalysis). Refer to appendix 2, OPSEC Measures for detailed planning guidance.

5. ( ) Concept of Implementation. State how the commander wants to use OPSEC during the planning, preparation, and execution phases of activities, exercises, tests and system development programs. (For example, describe how to use OPSEC in preparation for and during arms control treaty compliance inspections and visits by foreign inspection teams.) Describe how to coordinate the traditional security disciplines and counterintelligence support activities with the OPSEC plan. This paragraph may also include OPSEC monitoring.

6. ( ) Tasking/Responsibilities. Identify tasks by staff element, directorate, or functional area. Specify procedures (staff relationships), coordinating instructions, and specific OPSEC reporting requirements. (Do not duplicate administrative information addressed in paragraph 1a.) Assign responsibilities for the implementation of OPSEC measures identified in appendix 2, OPSEC measures.

NAME
General, USA
Commanding

Appendixes
1. Operations Security Estimate
2. Operations Security Measures

Official:

/s/

NAME
Deputy Chief of Staff, Operations

CLASSIFIED BY:
DECLASSIFY

(CLASSIFICATION)

APPENDIX F

OPERATIONS SECURITY ESTIMATE

(CLASSIFICATION)

(Operations Security Estimate) to Operations Security Plan for XXXXX XXXXX ( )

1. ( ) Essential Elements of Friendly Information (EEFI).
   a. ( ) State the EEFI as questions. (Examples of EEFI are provided in AR 530-1 Appendix C, for various types of organizations and functions.) Non-tactical organizations (such as RDT&E activities, test and evaluation activities,weapons systems test ranges, and technology development activities) state EEFI in the same manner as tactical units. The EEFI may be for an activity, phase of an operation, specific function, or other logical group.
   b. ( ) The EEFI may be a tab to this appendix or a separate document. This may be desirable when the organizational will provide the EEFI to several users. This is particularly useful during the acquisition process, which involves contractors, or when a particular program supports several other programs, projects, or activities.

2. ( ) Classification of EEFI. State whether classified or unclassified

3. ( ) Detectable Activities. Identify the activities that are or will be detectable during the conduct of the activity, action, function, and so forth. These are OPSEC indicators. List the indicators by type in this paragraph or attach as a tab to this appendix. See AR 530-1 appendix B for a discussion of the types of OPSEC indicators.

4. ( ) Adversary Threat. Cover two areas-adversary knowledge and information-gathering threat. Specific adversary threat information is normally classified and may be extensive. The threat should be stated for the Intelligence Collection Threat. Identify the threat by category and collection discipline. Refer to detailed threat information and data in other documents.
   a. ( ) Adversary Knowledge.
      (1) ( ) Describe the information about the organization, activity, or program that is known to have been available to adversary collection disciplines. For example, information about RDT&E programs is commonly available through news articles, special TV programs, PAO releases, environmental impact statements (EISs), the Congressional Record, military newspapers and magazine, service journals, scientific journals, and computer databases (Lexis/Nexis).
      (2) ( ) Identify each adversary and the specific information each knows.
   b. (U) Information-Gathering Threat. This paragraph may be a short reference to a threat document, a threat report, or a series of documents. Identify each phase, period of time, or specific event; Then identify the specific vulnerability of each to the collection disciplines.
5. (U) Monitoring. Identify the method for use within the activity to monitor the OPSEC status. Identify who, what, when, where, why and how to accomplish OPSEC monitoring.

CLASSIFIED BY:
DECLASSIFY

((CLASSIFICATION)

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX G

ACRONYMS

ACE	Analysis and Control Element
ASAS	All-Source Analysis System
ASPS	All-Source Production Section
CI	Counterintelligence
C2W	Command and Control Warfare
COMINT	Communications Intelligence
COMSEC	Communications Security
CP	Command Post
CTOC	Corps Tactical Operations Center
DTOC	Division Tactical Operations Center
EAC	Echelons Above Corps
ECB	Echelons Corps and Below
EEFI	Essential Elements of Friendly Information
ELINT	Electronic Intelligence
ELSEC	Electronic Security
EPITS	Essential Program Information, Technologies, or Systems
FISINT	Foreign Instrumentation Intelligence
FRAGO	Fragmentary Order
HoIS	Hostile Intelligence Service
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
INSCOM	Intelligence and Security Command
MASINT	Measurement and Signature Intelligence
OPORD	Operations Order
OPSEC	Operations Security
RDT&E	Research, Development, Test and Evaluation
SAEDA	Subversion and Espionage Directed Against the US Army
SIGINT	Signals Intelligence
SOI	Signal Operating Instructions
SOP	Standing Operating Procedure
SSO	Special Security Officer

*U.S. Government Printing Office: 2003—528-075/80332