JOINT PUB 3-54

CHANGE 1
15 APRIL 1994

JOINT DOCTRINE FOR OPERATIONS SECURITY



22 AUGUST 1991

OFFICE OF THE CHAIRMAN
THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20318-0001

Reply ZIP Code:
20318-0400

Joint Pub 3-54
15 April 1994

MEMORANDUM FOR: Distribution List

Subject: Change 1, Joint Pub 3-54, "Joint Doctrine for Operations Security"

1. Enclosed is Change 1 to Joint Pub 3-54. This change includes the following:

a. Eliminates unnecessary duplications with CJCSI 3212.01, "Joint Operations Security."

b. Addresses the relationship of OPSEC to command and control warfare.

c. Establishes an OPSEC planning process that supports the joint planning processes.

d. Revises the description of the OPSEC process.

e. Updates the references and the glossary.

f. Implements various administrative changes required by Joint Pub 1-01, "Joint Publication System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program."

2. This publication has been reprinted in its entirety due to the numerous pages affected. This change replaces the existing Joint Pub 3-54, 22 August 1991.

3. Recommendations for changes to this publication should be submitted to the Director for Operational Plans and Interoperability (J-7), 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000.

4. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal.

5. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

6. Additional copies of this publication can be obtained through Service publication centers.

7. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

8. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attache Office) to DIA Foreign Liaison Branch,
C-AS1, Room 1A674, Pentagon, Washington, D.C. 20301-6111.

9. The lead agent and Joint Staff doctrine sponsor for this publication is the Director, J-3.

10. This change should be distributed in accordance with the distribution list.

For the Chairman of the Joint Chiefs of Staff:

T. R. PATRICK
Colonel, USA
Secretary, Joint Staff

Enclosure

Distribution:

By Secretary, Joint Staff:

Joint Staff	OSD	NSA	CIA	DMA	USELEMNORAD
FEMA	DISA	DIA	DLA	JWFC/DD	DNA
NDU	MCCDC	JEWC	AFSC	CIO	DISA-JIEO

Additional copies may be obtained from the Secretary, Joint Staff (Documents Division).

Five copies each to: Offices of CSA, CNO, CSAF, CMC, USCG.

Twenty-five copies each to:

USACOM	USCENTCOM	USEUCOM
USPACOM	USSOUTHCOM	USSPACECOM
USSOCOM	USSTRATCOM	USTRANSCOM

Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army: US Army AG Publication Center
2800 Eastern Boulevard
Baltimore, MD 21220-2898

Air Force: Air Force Publications Distribution Center
2800 Eastern Boulevard
Baltimore, MD 21220-2896

Navy: CO, Navy Aviation Supply Office
Distribution Division (Code 03443)
5801 Tabor Avenue
Philadelphia, PA 19120-5000

Marine Corps: Marine Corps Logistics Base,
Albany, GA 31704-5000

Coast Guard: Coast Guard Headquarters, COMDT (G-REP)
2100 2nd Street, SW
Washington, D.C. 20593-0001

(INTENTIONALLY BLANK)

JOINT DOCTRINE FOR OPERATIONS SECURITY

RECORD OF CHANGES

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS
1		Apr 94	New edition reprinted in total		

In accordance with the procedures contained in Joint Pub 1-01, change recommendations to this publication will be forwarded to:

Urgent: TO: JOINT STAFF WASHINGTON DC//J-33/STOD//
INFO: JOINT STAFF WASHINGTON DC//J7-JDD//

Routine: Operational Plans and Interoperability
Directorate, J-7, JDD
7000 Joint Staff Pentagon
Washington, D.C. 20318-7000

LIST OF EFFECTIVE PAGES

The following is a list of effective pages. Use this list to verify the currency and completeness of your document. An "O" indicates a page in the original document.

PAGE	CHANGE
1 thru 4	1
i thru vi	1
I-1 thru I-4	1
II-1 thru II-4	1
III-1 thru III-6	1
A-1 thru A-4	1
B-1 thru B-6	1
C-1 thru C-12	1
D-1 thru D-4	1
E-1 thru E-4	1
E-A-1 thru E-A-4	1
E-A-A-1 thru E-A-A-2	1
E-A-B-1 thru E-A-B-2	1
E-A-C-1 thru E-A-C-2	1
E-A-D-1 thru E-A-D-2	1
E-A-E-1 thru E-A-E-2	1
E-A-F-1 thru E-A-F-2	1
E-B-1 thru E-B-6	1
E-C-1 thru E-C-4	1
E-C-A-1 thru E-C-A-2	1
F-1 thru F-2	1
G-1 thru G-4	1
GL-1 thru GL-4	1

Deleted Pages:

JOINT DOCTRINE FOR OPERATIONS SECURITY

PREFACE

1. Purpose. This publication sets forth doctrine and selected tactics, techniques, and procedures for operations security to govern the joint activities and performance of the Armed Forces of the United States in joint operations as well as the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine and selected tactics, techniques, and procedures for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander (JFC) from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

2. Application

a. Doctrine and selected tactics, techniques, and procedures and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. In applying the doctrine and selected tactics, techniques, and procedures set forth in this publication, care must be taken to distinguish between distinct but related responsibilities in the two channels of authority to forces assigned to combatant commands. The Military Departments and Services recruit, organize, train, equip, and provide forces for assignment to combatant commands and administer and support these forces. This authority is, by law, subject to the provisions of title 10, United States Code, chapter 6, which is the section that details the authority of combatant commanders. These commanders exercise combatant command (command authority) over their assigned forces. Service component commanders are subject to the orders of combatant commanders and,

subject to the combatant commander's direction, are also responsible to the Military Departments and Services in the exercise of their administrative and support responsibilities.

c. This publication is authoritative but not directive. Commanders will exercise judgment in applying the procedures herein to accomplish their missions. This doctrine and selected tactics, techniques, and procedures should be followed, except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

3. Scope. This publication describes the use of OPSEC in the planning, preparation, and execution of joint operations. Additionally, it provides the procedures for the conduct of OPSEC surveys.

4. Basis. This publication is published in accordance with CJCS Instruction 3213.01, "Joint Operations Security."

TABLE OF CONTENTS

CHAPTER
PAGE

I GENERAL I-1

Policy. I-1
Definition. I-1
Characteristics of OPSEC. I-1
OPSEC Survey. I-2
OPSEC and Command and Control Warfare I-2
OPSEC and Public Affairs. I-3

II OPSEC PLANNING. II-1

General II-1
OPSEC Planning Factors. II-1
OPSEC Planning and the Joint Planning Processes II-2

III THE OPSEC PROCESS III-1

General III-1
The OPSEC Process III-2

APPENDIX

A Examples of Critical Information A-1
B The Intelligence Threat. B-1
C OPSEC Indicators C-1
D Operations Security Measures D-1
E Procedures for OPSEC Surveys E-1

ANNEX

A OPSEC Survey Planning Phase E-A-1

TAB

A Composite OPSEC Profile for Combat Operations. E-A-A-1
B Functional Outline and Profile Guideline for Intelligence Collection Operations E-A-B-1
C Functional Outline and Profile Guideline for Logistics E-A-C-1
D Functional Outline and Profile Guideline for Communications. E-A-D-1

E Functional Outline and Profile Guideline for Operations. E-A-E-1
F Functional Outline and Profile Guideline for Administration and Support E-A-F-1

B Field Survey Phase. E-B-1
C Analysis and Reporting Phase. E-C-1

TAB

Suggested Format for Final OPSEC Survey Report. E-C-A-1

F References F-1
G Users Evaluation Report. G-1

Glossary

Part I--Abbreviations and Acronyms GL-1
Part II--Terms and Definitions GL-3

FIGURE

B-1 The Intelligence Cycle. B-1
E-1 Sample Composite OPSEC Profile for Combat Operations. . . .E-A-A-2

CHAPTER I

GENERAL

1. Policy. Policy for joint OPSEC is established by CJCS Instruction 3213.01. Reference should be made to that document for information concerning responsibilities relating to joint OPSEC and for requirements for establishing joint OPSEC programs.

2. Definition. OPSEC 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 adversary 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.

3. Characteristics of OPSEC

a. OPSEC’s most important characteristic is that it is a process. OPSEC is not a collection of specific rules and instructions that can be applied to every operation. It is a methodology that can be applied to any operation or activity for the purpose of denying critical information to an adversary.

b. Unlike security programs that seek to protect classified information, OPSEC is concerned with identifying, controlling, and protecting the generally unclassified evidence that is associated with sensitive operations and activities. OPSEC and security programs must be closely coordinated to ensure that all aspects of sensitive operations are protected.

c. OPSEC acknowledges that commanders must be prepared to assume some degree of risk when choosing whether or not to execute OPSEC measures. OPSEC measures will, in most cases, entail the expenditure of resources. In choosing to execute particular OPSEC measures,

commanders must decide that the assumed gain in secrecy outweighs the costs in resources. If commanders decide not to execute certain measures because the costs outweigh the gain, then they are assuming risks. The OPSEC process requires that decisionmakers directly address how much risk they are willing to assume.

4. OPSEC Survey. An OPSEC survey is an intensive application of the OPSEC process to an existing operation or activity by a multi-disciplined team of experts. Surveys are essential for identifying requirements for additional measures and for making necessary changes in existing measures. Appendix E describes the procedures for conducting OPSEC surveys.

5. OPSEC and Command and Control Warfare

a. Command and control warfare (C2W) is the military strategy that seeks to deny the adversary the effective use of its command and control (C2) capabilities while at the same time protecting friendly C2 capabilities. C2W integrates the use of OPSEC, military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction.

b. OPSEC's primary role in C2W is denying adversaries the critical information concerning friendly intentions and capabilities that they need for effective decisionmaking. Deprived of the foreknowledge of US actions, adversary leaders cannot, with any degree of certainty, make the decisions that would enable their forces to effectively counter the actions of US forces.

c. OPSEC's other role in C2W is providing support to the other C2W elements. It hides the real, while deception portrays the false. It protects physical destruction assets from discovery and attack. It helps in preventing adversaries from finding out the technical characteristics of friendly EW equipment. OPSEC can be used to protect sensitive PSYOP activities.

d. In turn, the other elements of C2W can be employed in support of OPSEC. Deception and PSYOP can be used to provide plausible cover stories for activities that cannot be hidden from adversary observation. Physical destruction assets can be used to attack and reduce the adversary's intelligence collection capabilities. EW

can prevent or disrupt the flow of information within the adversary’s intelligence system.

6. OPSEC and Public Affairs. Planning and executing OPSEC measures require close coordination with public affairs officers (PAOs). As appropriate, but particularly during military operations other than war, OPSEC program personnel and operational planners should consult with PAOs to anticipate and plan for the potential impact of media activities in the area of operations.

(INTENTIONALLY BLANK)

CHAPTER II

OPSEC PLANNING

1. General

a. In order to prevent adversaries (or potential adversaries) from gaining valuable intelligence about friendly operations, joint forces must plan and execute OPSEC measures. To be effective, OPSEC measures must be considered as early as possible during mission planning and then be appropriately revised to keep pace with any changes in current operations and adversarial threats.

b. Joint OPSEC planning and execution occur as part of the command's or organization's C2W effort. The commander's objectives for C2W are the basis for OPSEC planning. In addition to directly supporting the accomplishment of the commander's objectives, the use of OPSEC measures in support of the other components of C2W must also be considered during OPSEC planning. Those operational planners responsible for OPSEC must work in close coordination with the deception, EW, PSYOP, and physical destruction planners.

2. OPSEC Planning Factors. The following factors must be considered when conducting OPSEC planning:

a. The commander plays the critical role. OPSEC planning guidance must be provided as part of the commander's C2W planning guidance to ensure that OPSEC is considered during the development of friendly courses of action (COAs).

b. OPSEC is an operational function, not a security function. OPSEC planning must be done by the operations planners. They are assisted by the organization's OPSEC program personnel and appropriate planners from other staff elements. Intelligence support is particularly important in determining the threat to friendly operations and in assessing friendly vulnerabilities.

c. Planning must focus on identifying and protecting critical information. Denying all information about a friendly operation or activity is seldom cost effective or realistic.

d. The ultimate goal of OPSEC is increased mission effectiveness. By preventing an adversary from determining friendly intentions or capabilities, OPSEC reduces losses to friendly units and increases the likelihood of mission success.

e. OPSEC should be one of the factors considered during the development and selection of friendly COAs. COAs will differ in terms of how many OPSEC indicators will be created and how easily those indicators can be managed by OPSEC measures. Depending upon how important maintaining secrecy is to mission success, OPSEC considerations may be a factor in selecting a COA.

f. OPSEC planning is a continuous process. During the execution phase of an operation, feedback on the success or failure of OPSEC measures is evaluated and the OPSEC plan is modified accordingly. Friendly intelligence and counterintelligence organizations, COMSEC monitoring, and OPSEC surveys are the primary sources for feedback information.

g. PAOs should participate in OPSEC planning to provide their assessments on the possible effects of media coverage and for the coordination of OPSEC measures to minimize those effects.

h. The termination of OPSEC measures must be addressed in the OPSEC plan to prevent future adversaries from developing countermeasures to successful OPSEC measures. In some situations, it may be necessary for the OPSEC plan to provide guidance on how to prevent the target of the OPSEC operation, and any interested third parties, from discovering sensitive information relating to OPSEC during the postexecution phase.

3. OPSEC Planning and the Joint Planning Processes

a. Joint OPSEC Planning. OPSEC planning in support of joint operations is accomplished through the application of the OPSEC process. The five actions that compose the OPSEC process are described in detail in Chapter III. Joint OPSEC planning is always done in conjunction with normal operational planning and as part of the overall C2W planning effort.

b. Planning Processes. There are three major planning processes for joint planning. In the Joint Operation

Planning and Execution System (JOPES), there are the deliberate and crisis action processes. They are described in Joint Pub 5-03.1. For campaign planning, there is the campaign planning process. It is described in Joint Pub 5-0.

c. The Deliberate Planning Process. OPSEC planning relates to the JOPES deliberate planning process in the following manner:

Phase I--Initiation
Phase II--Concept Development
  Step 1--Mission Analysis
  Step 2--Planning Guidance
    OPSEC Action 1--Identification of Critical Information
  Step 3--Staff Estimates
    OPSEC Action 2--Analysis of Threats
    OPSEC Action 3--Analysis of Vulnerabilities
  Step 4--Commander's Estimate
    OPSEC Action 4--Assessment of Risks
  Step 5--Commander's Concept
  Step 6--CJCS Concept Review
Phase III--Plan Development
Phase IV--Plan Review
Phase V--Supporting Plans

OPSEC Action 5--Application of Appropriate OPSEC Measures (Except for those measures intended to protect the plan prior to its being implemented, this part of the OPSEC process relates to the execution of operations orders.)

d. The Crisis Action Planning Process. OPSEC planning relates to the JOPES crisis action planning process in the following manner:

Phase I--Situation Development
Phase II--Crisis Assessment
Phase III--Course of Action Development
  OPSEC Action 1--Identification of Critical Information
  OPSEC Action 2--Analysis of Threats
  OPSEC Action 3--Analysis of Vulnerabilities
  OPSEC Action 4--Assessment of Risks
Phase IV--Course of Action Selection
Phase V--Execution Planning

Phase VI--Execution
OPSEC Action 5--Application of Appropriate OPSEC Measures

e. The Campaign Planning Process

(1) A campaign plan is the combatant commander's vision of how operations will be arranged in time and space to attain the strategic objectives assigned by National Command Authorities (NCA). They translate strategic concepts into unified plans for military action by specifying how operations, logistics, and time will be used to attain theater strategic objectives.

(2) Campaign plans are normally not created until the Execution Planning Phase (Phase V) of crisis action planning. The campaign planning process, however, begins during crisis action planning when the supported commander develops the COA recommendation for the NCA (Phase III). After the NCA approve the COA (Phase IV), the supported commander provides specific guidance to the staff. That COA becomes the basis for the development of an operations order (Phase V). OPSEC planning is done the same as in crisis action planning:

Phase I--Situation Development
Phase II--Crisis Assessment
Phase III--Course of Action Development
OPSEC Action 1--Identification of Critical Information
OPSEC Action 2--Analysis of Threats
OPSEC Action 3--Analysis of Vulnerabilities
OPSEC Action 4--Assessment of Risks
Phase IV--Course of Action Selection
Phase V--Execution Planning
Phase VI--Execution
OPSEC Action 5--Application of Appropriate OPSEC Measures

f. OPSEC Plans Format. OPSEC plans are prepared as part of all joint operations plans and orders. The format is found in Joint Pub 5-03.2, JOPES Volume II.

CHAPTER III

THE OPSEC PROCESS

1. General

a. OPSEC planning is accomplished through the use of the OPSEC process. This process, when used in conjunction with the joint planning processes, provides the information required to write the OPSEC section of any plan or order. OPSEC planning is done in close coordination with the overall C2W planning effort and with the planning of the other C2W components.

b. The OPSEC process consists of five distinct actions. These actions are applied in a sequential manner during OPSEC planning. In dynamic situations, however, individual actions may be revisited at any time. New information about the adversary's intelligence collection capabilities, for instance, would require a new analysis of threats.

c. An understanding of the following terms is required before the process can be explained:

(1) Critical Information: Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

(2) OPSEC Indicators: Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

(3) OPSEC Vulnerability: A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decisionmaking.

2. The OPSEC Process

a. OPSEC Action 1--Identification of Critical Information

(1) While assessing and comparing friendly versus adversary capabilities during the planning process for a specific operation or activity, the commander and staff seek to identify the questions that they believe the adversary will ask about friendly intentions, capabilities, and activities. These questions are the essential elements of friendly information (EEFI). In an operation plan or order, the EEFI are listed in Appendix 3 (Counterintelligence) to Annex B (Intelligence).

(2) Critical information is a subset of EEFI. It is only that information that is vitally needed by an adversary. The identification of critical information is important in that it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all classified or sensitive information.

(3) Critical information is listed in the OPSEC portion of an operation plan or order. Some general categories of critical information are provided in Appendix A.

b. OPSEC Action 2--Analysis of Threats

(1) This action involves the research and analysis of intelligence information, counterintelligence, reports, and open source information to identify who the likely adversaries are to the planned operation.

(2) The operations planners, working with the intelligence and counterintelligence staffs and assisted by the OPSEC program personnel, seek answers to the following questions:

(a) Who is the adversary? (Who has the intent and capability to take action against the planned operation?)

(b) What are the adversary’s goals? (What does the adversary want to accomplish?)

(c) What is the adversary's strategy for opposing the planned operation? (What actions might the adversary take?)

(d) What critical information does the adversary already know about the operation? (What information is it too late to protect?)

(e) What are the adversary's intelligence collection capabilities?

(3) Detailed information about the adversary's intelligence collection capabilities can be obtained from the command's counterintelligence and intelligence organizations. In addition to knowing about the adversary's capabilities, it is important to understand how the intelligence system processes the information that it gathers. Appendix B discusses the general characteristics of intelligence systems.

c. OPSEC Action 3--Analysis of Vulnerabilities

(1) The purpose of this action is to identify an operation's or activity's OPSEC vulnerabilities. It requires examining each aspect of the planned operation to identify any OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. A vulnerability exists when the adversary is capable of collecting an OPSEC indicator, correctly analyzing it, and then taking timely action.

(2) Continuing to work with the intelligence and counterintelligence staffs, the operations planners seek answers to the following questions:

(a) What indicators (friendly actions and open source information) of critical information not known to the adversary will be created by the friendly activities that will result from the planned operation?

(b) What indicators can the adversary actually collect?

(c) What indicators will the adversary be able to use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?)

(3) See Appendix C for a detailed discussion of OPSEC indicators.

d. OPSEC Action 4--Assessment of Risk

(1) This action has two components. First, planners analyze the OPSEC vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Second, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff.

(2) OPSEC measures reduce the probability of the adversary either collecting the indicators or being able to correctly analyze their meaning.

(a) OPSEC measures can be used to:

1. Prevent the adversary from detecting an indicator.

2. Provide an alternative analysis of an indicator.

3. Attack the adversary’s collection system.

(b) OPSEC measures include, among other actions, cover, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against the adversary’s intelligence system.

(c) More than one possible measure may be identified for each vulnerability. Conversely, a single measure may be used for more than one vulnerability. The most desirable OPSEC measures are those that combine the highest possible protection with the least effect on operational effectiveness.

Appendix D provides examples of OPSEC measures.

(3) Risk assessment requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

(a) OPSEC measures usually entail some cost in time, resources, personnel, or interference with normal operations. If the cost to mission effectiveness exceeds the harm that an adversary could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires command involvement.

(b) Typical questions that might be asked when making this analysis include:

1. What risk to effectiveness is likely to occur if a particular OPSEC measure is implemented?

2. What risk to mission success is likely to occur if an OPSEC measure is not implemented?

3. What risk to mission success is likely if an OPSEC measure fails to be effective?

(c) The interaction of OPSEC measures must be analyzed. In some situations, certain OPSEC measures may actually create indicators of critical information. For example, the camouflaging of previously unprotected facilities could be an indicator of preparations for military action.

(4) The selection of measures must be coordinated with the other components of C2W. Actions such as jamming of intelligence nets or the physical destruction of critical intelligence centers can be used as OPSEC measures. Conversely, deception and

PSYOP plans may require that OPSEC measures not be applied to certain indicators in order to project a specific message to the adversary.

e. OPSEC Action 5--Application of Appropriate OPSEC Measures

(1) In this step, the command implements the OPSEC measures selected in Step 4 or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

(2) During the execution of OPSEC measures, the reaction of adversaries to the measures is monitored to determine their effectiveness and to provide feedback. Planners use that feedback to adjust ongoing activities and for future OPSEC planning. Provisions for feedback must be coordinated with the command's intelligence and counterintelligence staffs to ensure the requirements to support OPSEC receive the appropriate priority. In addition to intelligence sources providing feedback, OPSEC surveys can provide useful information relating to the success of OPSEC measures.

APPENDIX A

EXAMPLES OF CRITICAL INFORMATION

This appendix provides general examples of critical information. Several generic military activities with some of their associated critical information are listed. These are only a few of the many types of military activities and their associated critical information.

a. Diplomatic Negotiations

(1) Military capabilities (pretreaty and posttreaty)

(2) Intelligence verification capabilities

(3) Minimum negotiating positions

b. Politico-Military Crisis Management

(1) Target selection

(2) Timing considerations

(3) Logistic capabilities and limitations

(4) Alert posture

c. Military Intervention

(1) Intentions

(2) Military capabilities

(3) Forces assigned and in reserve

(4) Targets

(5) Timing

(6) Logistic capabilities and constraints

(7) Limitations

(8) Third-nation support arrangements

d. Counterterrorism

(1) Forces

(2) Targets

(3) Timing

(4) Staging locations

(5) Tactics

(6) Ingress and egress methods

(7) Logistic capabilities and constraints

e. Open Hostilities

(1) Force composition and disposition

(2) Attrition and reinforcement

(3) Targets

(4) Timing

(5) Logistic constraints

(6) Location of critical C2 nodes

f. Mobilization

(1) Intent to mobilize before public announcement

(2) Impact on military industrial base

(3) Impact on civil economy

(4) Transportation capabilities and limitations

g. Intelligence, Reconnaissance, and Surveillance

(1) Purpose of collection

(2) Targets of collection

(3) Timing

(4) Capabilities of collection assets

(5) Processing capabilities

(6) Unit requesting collection

h. Peacetime Weapons and Other Military Movements

(1) Fact of movement

(2) Periodicity of movements

(3) Origin and destination of equipment being moved

(4) Capabilities and limitations of equipment being moved

(5) Extent of inventory of equipment being moved

i. Command Post or Field Training Exercises

(1) Participating units

(2) OPLAN, CONPLANs, or other contingencies that are being exercised

(3) Command relationships

(4) C3 connections and weaknesses

(5) Logistic capabilities and limitations

j. Noncombatant Evacuation Operations (Nonpermissive Environment)

(1) Targets

(2) Forces

(3) Logistic constraints

(4) Safe havens

(5) Routes

(6) Timing

k. Counternarcotics Operations

(1) Identity of military forces

(2) Drug Law Enforcement Agency (DLEA) involvement

(3) Military support to DLEAs

(4) Host nation cooperation

(5) Capabilities

(6) Timing

(7) Tactics

(8) Logistic capabilities and constraints

APPENDIX B

THE INTELLIGENCE THREAT

1. Introduction. Adversaries and potential adversaries collect and analyze information about US military operations in order to determine current capabilities and future intentions. To perform this function, most adversaries have created intelligence organizations and systems. The capabilities and levels of sophistication of these threats differ greatly, but they all share certain core characteristics. The most important of these are how intelligence is developed and how it is collected. This appendix will describe those characteristics.

2. The Intelligence Cycle. All intelligence systems follow a process. This process begins with a consumer (a commander or decisionmaker) requesting answers to certain questions and ends with the intelligence system providing those answers. Figure B-1 illustrates a typical intelligence cycle (in this case, the intelligence cycle described in Joint Pub 2-0). Understanding the concept of the intelligence cycle is basic to understanding the total adversary intelligence threat to friendly operations in general and to the specific threat to the critical information that OPSEC seeks to protect.

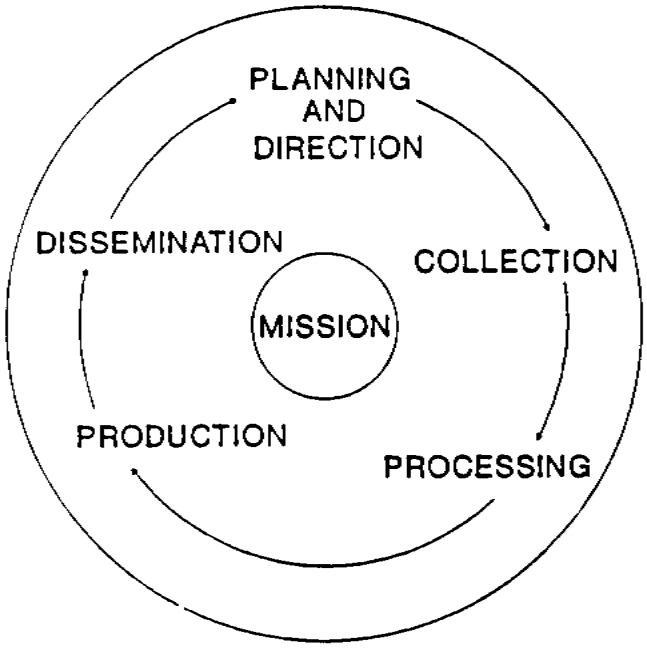


Figure B-1. The Intelligence Cycle

Figure B-1. The Intelligence Cycle

a. Planning and Direction

(1) Decisionmakers task their intelligence systems to collect and assess information about their adversaries and potential adversaries. These information requirements are the basis for intelligence collection, evaluation, and reporting.

(2) These information requirements will normally include any information that would allow the decisionmaker to better understand an adversary's goals, intentions, current capabilities, strengths, and weaknesses. At the operational and strategic levels of war, decisionmakers will want to know what their adversary counterparts think; how they make their decisions; and their social, cultural, economic, and political beliefs and habits.

(3) Intelligence specialists take the decisionmaker's information requirements and turn them into specific intelligence taskings.

b. Collection

(1) After determining the taskings, the intelligence system will evaluate the currency and amount of information already at hand. If more or newer information is needed, collection requirements will be submitted to the appropriate collection resources.

(2) Information may be collected either overtly or clandestinely.

(a) Overt collection may include such activities by military attaches assigned to embassies and the review of available open-source information.

(b) Clandestine collection acquires information while concealing the collection effort and consists of espionage and technical means such as signals and imagery intelligence.

c. Processing. Collected information must be processed into a form that is suitable for the production of intelligence. For example, imagery film must be

developed and signals must be processed before they can be evaluated, analyzed, and interpreted for significance.

d. Production

(1) The still raw intelligence is evaluated for accuracy, reliability, and credibility. It is compared for consistency with known data and examined for meaningful associations by analyzing it against its historical background. It is combined with other information. The information is analyzed, interpreted, and prepared for presentation to the consumer. There are numerous types of intelligence products ranging from informal briefings to multivolume written studies.

(2) Generally, every product attempts to address the questions, What is the adversary doing now and what is it going to do next? In many cases, because of inadequate collection or insufficient time for processing and analysis, intelligence analysts will not be able to provide unambiguous answers to those questions. This phase of the intelligence cycle is still more art than science.

e. Dissemination. In this step, the product is delivered to the consumer. There are as many forms of delivery as there are products and consumers. Automated means are becoming increasingly important in many intelligence systems.

3. Intelligence Sources

a. Human Intelligence (HUMINT). HUMINT uses people to gain information that is often inaccessible by other collection means. Although it is the oldest and most basic form of intelligence collection, HUMINT remains significant because it is often the only source with direct access to the opponent’s plans and intentions. Clandestine HUMINT collection is done in a fashion that maintains the secrecy of the collection operation.

b. Imagery Intelligence (IMINT)

(1) IMINT is derived from visual photography, infrared sensors, lasers, electro-optics, and radar sensors. IMINT systems can operate from land, sea,

air, and/or space platforms. Imagery equipment is being improved constantly and combinations of sensors are being used to enhance the quality and timeliness of the intelligence product.

(2) An increasing number of countries are starting to use photoreconnaissance satellites. In addition to being a major strategic collection capability, they are becoming an increasingly important operational and tactical capability. The traditional airborne IMINT platforms remain an important capability for those countries without access to satellite imagery.

c. Signals Intelligence (SIGINT). SIGINT is derived from communication (COMINT), electronics (ELINT), and foreign instrumentation signals (FISINT).

(1) COMINT is information derived from the study of intercepted electromagnetic communications. Prime COMINT sources include clear voice (nonencrypted) telephone and radio communications and unencrypted computer-to-computer data communications.

(2) ELINT is technical or geo-location intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Radars are the primary ELINT source.

(3) FISINT is derived from the intercept and analysis of electronically transmitted data containing measured parameters of performance, such as a ballistic missile’s performance during a test flight.

d. Measurement and Signature Intelligence (MASINT). MASINT is scientific and technical intelligence obtained by the quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, etc.) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same. MASINT includes other intelligence sources such as acoustical intelligence (ACINT), laser intelligence (LASINT), and nuclear intelligence (NUCINT).

e. Open Source Intelligence (OSINT). OSINT is information of intelligence value that is available to the general public. OSINT is available from such sources as the news media, public affairs announcements, unclassified government documents and publications, public hearings, and contracts and contract-related material.

f. Technical Intelligence (TECHINT). TECHINT is derived from the exploitation of foreign material and equipment. It results from the analysis of captured or otherwise obtained foreign equipment.

(INTENTIONALLY BLANK)

APPENDIX C

OPSEC INDICATORS

1. OPSEC Indicators. OPSEC indicators are those friendly actions and open sources of information that adversary intelligence systems can potentially detect or obtain and then interpret to derive friendly critical information.

2. Basic OPSEC Indicator Characteristics. An indicator's characteristics are those elements of an action or piece of information that make it potentially useful to an adversary. There are five major characteristics.

a. Signature

(1) A signature is the characteristic of an indicator that makes it identifiable or causes it to stand out. Key signature properties are uniqueness and stability. Uncommon or unique features reduce the ambiguity of an indicator and minimize the number of other indicators that must be observed to confirm a single indicator's significance.

(2) An indicator's signature stability, implying constant or stereotyped behavior, can allow an adversary to anticipate future actions. Varying the pattern of behavior decreases the signature's stability and thus increases the ambiguity of the adversary's observations.

(3) Procedural features are an important part of any indicator signature and may provide the greatest value to an adversary. They identify how, when, and where the indicator occurs and what part it plays in the overall scheme of operations and activities.

b. Associations

(1) Association is the relationship of an indicator to other information or activities. It is an important key to an adversary's interpretation of ongoing activity. Intelligence analysts continuously compare their current observations with what has been seen in the past in an effort to identify possible relationships.

(2) For example, a distinctive piece of ground-support equipment known to be used for servicing strategic bombers might be observed at a tactical fighter base. An intelligence analyst could conclude that a strategic bomber presence has been or will be established there. The analyst will then look for other indicators associated with bombers to verify that conclusion.

(3) Another key association deals with continuity of actions, objects, or other indicators that may register as patterns to the observer or analyst. Such continuity may not be the result of planned procedures but may result instead from repetitive practices or sequencing to accomplish a goal.

(4) If, for example, the intensive generation of aircraft sorties is always preceded by a maintenance standdown to increase aircraft readiness, detecting and observing the standdown may allow the adversary analyst or observer to predict the subsequent launch activity. Moreover, based on past patterns of the length of such standdowns, the analyst may be able to judge the scope of the sortie generation.

(5) Another type of association that is useful to intelligence analysts is organizational patterns. Military units, for example, are often symmetrically organized. Thus, when some components are detected, others that are not readily apparent can be assumed to exist.

(6) For example, an intelligence analyst knows that a particular army's infantry battalions are organized with three infantry companies, a headquarters company, and a weapons company. If only the headquarters company and one infantry company are currently being detected, the presence of the other known battalion components will be strongly suspected. Thus, in some situations, a pattern taken as a whole can be treated as a single indicator, simplifying the intelligence problem.

c. Profiles

(1) Each functional activity generates its own set of more-or-less unique signatures and associations. The sum of these signatures and associations is the

activity's profile. An activity's profile is usually unique. Given enough data, intelligence analysts can determine the profile of any activity. Most intelligence organizations seek to identify and record the profiles of their adversary's military activities.

(2) The profile of an aircraft deployment, for example, may be unique to the aircraft type or mission. This profile, in turn, has several subprofiles for the functional activities needed to deploy the particular mission aircraft (e.g., fuels, avionics, munitions, communications, air traffic control, supply, personnel, and transportation).

(3) The observation of a unique profile may sometimes be the only key that an intelligence analyst needs to determine what type of operation is occurring, thus minimizing the need to look harder for additional clues. Such unique profiles cut the time needed to make accurate intelligence estimates. As a result, profiles are the analytical tools.

d. Contrasts

(1) Contrasts are any differences that are observed between an activity's standard profile and its most recent or current actions. Contrasts are the most reliable means of detection because they depend on differences to established profiles. They also are simpler to use because they need only to be recognized, not understood.

(2) Deviations from normal profiles will normally attract the interest of intelligence analysts. They will want to know why there is a change and attempt to determine if the change means anything significant.

(3) In the previous example of the distinctive bomber-associated ground support equipment at a fighter base, the intelligence observer might ask the following questions:

(a) Have bombers been deployed at fighter bases before? At this particular fighter base? At several fighter bases simultaneously?

(b) If there have been previous bomber deployments, were they routine or did they occur during some period of crisis?

(c) If previous deployments have been made to this base or other fighter bases, how many bomber aircraft were deployed?

(d) What actions occurred while the bombers were deployed at the fighter bases?

(e) What is happening at other fighter and bomber bases? Is this an isolated incident or one of many changes to normal activity patterns?

(4) Although the detection of a single contrast may not provide intelligence analysts with a total understanding of what is happening, it may result in increased intelligence collection efforts against an activity.

e. Exposure

(1) Exposure refers to when and for how long an indicator is observed. The duration, repetition, and timing of an indicator's exposure can affect its relative importance and meaning. Limiting the duration and repetition of exposure reduces the amount of detail that can be observed and the associations that can be formed.

(2) An indicator (object or action) that appears over a long period of time will be assimilated into an overall profile and assigned a meaning. An indicator that appears for a short time and does not appear again may, if it has a high interest value, persist in the adversary intelligence data base or, if there is little or no interest, fade into the background of insignificant anomalies. An indicator that appears repeatedly will be studied carefully as a contrast to normal profiles.

(3) Because of a short exposure time, the observer or analyst may not detect key characteristics of the

indicator the first time it is seen, but he can formulate questions and focus collection assets to provide answers if the indicator is observed again.

(4) Repetition of the indicator in relationship to an operation, activity, or exercise will add it to the profile even if the purpose of the indicator is not understood by the adversary. Indicators limited to a single isolated exposure are difficult to detect and evaluate.

3. Examples of Indicators. The following paragraphs provide examples of indicators that are associated with selected military activities and information. This short list only scratches the surface of the almost infinite sources of indicators associated with the wide range of US military operations and activities that could be exploited by an adversary. This list is designed primarily to stimulate thinking about what kinds of actions can convey indicators that betray critical information for specific friendly operations or activities.

a. Indicators of General Military Force Capabilities

(1) The presence of unusual type units for a given location, area, base, etc.

(2) Friendly reactions to adversary exercises or actual hostile actions.

(3) Actions, information, or material associating Reserve components with specific commands or units (e.g., mobilization and assignment of Reserve personnel to units).

(4) Actions, information, or material indicating the levels of unit manning as well as the state of training and experience of personnel assigned.

(5) Actions, information, or material revealing spare parts availability for equipment or systems.

(6) Actions, information, or material indicating equipment or system reliability (e.g., visits of technical representatives or special repair teams).

(7) Movement of aircraft, ships, and ground units in response to friendly sensor detections of hostile units.

(8) Actions, information, or material revealing tactics, techniques, and procedures employed in different types of training exercises or during equipment or system operational tests and evaluations.

(9) Stereotyped patterns in performing the organizational mission that reveal the sequence of specific actions or when they are accomplished.

b. Indicators of General C2 Capabilities

(1) Actions, information, or material providing insight into the volume of orders and reports needed to accomplish tasks.

(2) Actions, information, or material showing unit subordination for deployment, mission, task, etc.

(3) Association of particular commanders with patterns of behavior under stress or in varying tactical situations.

(4) Information revealing problems of coordination between the commander’s staff elements.

(5) In exercises or operations, indications of the period between the occurrence of a need to act or react and the action taking place, of consultations that occur with higher commands, and of the types of actions initiated.

(6) Unusual actions with no apparent direction reflected in communications.

c. General Indicators from Communications Usage

(1) Alert and maintenance personnel using handheld radios or testing aircraft or vehicle radios.

(2) Establishing new communications nets. These might reveal entities that have intrinsic significance for the operation or activity being planned or executed. Without conditioning to

desensitize adversaries, the sudden appearance of new communications nets could prompt them to implement additional intelligence collection to discern friendly activity more accurately.

(3) Suddenly increasing traffic volume or, conversely, instituting radio silence when close to the time of starting an operation, exercise, or test. Without conditioning, unusual surges or periods of silence may catch adversaries' attention and, at a minimum, prompt them to focus their intelligence collection efforts.

(4) Using static call signs for particular units or functions and unchanged or infrequently changed radio frequencies. This usage also allows adversaries to monitor friendly activity more easily and add to their intelligence data base for building an accurate appreciation of friendly activity.

(5) Using stereotyped message characteristics that indicate particular types of activity that allow adversaries to monitor friendly activity more easily.

(6) Requiring check-in and checkout with multiple control stations before, during, and after a mission (usually connected with air operations).

d. Sources of Possible Indicators for Equipment and System Capabilities

(1) Unencrypted emissions during tests and exercises.

(2) Public media, particularly technical journals.

(3) Budget data that provide insight into the objectives and scope of a system R&D effort or the sustainability of a fielded system.

(4) The equipment or system hardware itself.

(5) Information on test and exercise schedules that allows adversaries to better plan the use of their intelligence collection assets.

(6) Deployment of unique units, targets, and sensor systems to support tests associated with particular equipment or systems.

(7) Unusual or visible security imposed on particular development efforts that highlight their significance.

(8) Information indicating special manning for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract.

(9) Notices to mariners and airmen that might highlight test areas.

(10) Stereotyped use of location, procedures, and sequences of actions when preparing for and executing test activity for specific types of equipment or systems.

(11) Use of advertisements indicating that a company has a contract on a classified system or component of a system, possesses technology of military significance, or has applied particular principles of physics and specific technologies to sensors and the guidance components of weapons.

e. Indicators of Preparations for Operations or Activities. Many indicators may reveal data during the preparatory, as compared to the execution, phase of operations or activities. Many deal with logistic activity. Examples include:

(1) Provisioning of special supplies for participating elements.

(2) Requisitioning unusual volumes of supply items to be filled by a particular date.

(3) Increasing pre-positioning of ammunition, fuels, weapon stocks, and other classes of supply.

(4) Embarking special units, installing special capabilities, and preparing unit equipment with special paint schemes.

(5) Procuring large or unusual numbers of maps and charts for specific locations.

(6) Making medical arrangements, mobilizing medical personnel, stockpiling pharmaceuticals and blood, and marshaling medical equipment.

(7) Focusing friendly intelligence and reconnaissance assets against a particular area of interest.

(8) Requisitioning or assigning increased number of linguists of a particular language or group of languages from a particular region.

(9) Initiating and maintaining unusual liaison with foreign nations for support.

(10) Providing increased or tailored personnel training.

(11) Holding rehearsals to test concepts of operation.

(12) Increasing the number of trips and conferences for senior officials and staff members.

(13) Sending notices to airmen and mariners and making airspace reservations.

(14) Arranging for tugs and pilots.

(15) Requiring personnel on leave or liberty to return to their duty locations.

(16) Having unusual off-limits restrictions.

(17) Preparing units for combat operations through equipment checks as well as operational standdowns to achieve a required readiness level for equipment and personnel.

(18) Making billeting and transportation arrangements for particular personnel or units.

(19) Taking large-scale action to change mail addresses or arrange for mail forwarding.

(20) Posting such things as supply delivery, personnel arrival, transportation, or ordnance loading schedules in a routine manner where personnel without a need-to-know will have access.

(21) Storing boxes or equipment labeled with the name of an operation or activity or with a clear unit designation outside a controlled area.

(22) Employing uncleared personnel to handle materiel used only in particular types of operations or activities.

(23) Providing unique or highly visible physical security arrangements for loading or guarding special munitions or equipment.

(24) Requesting unusual or increased meteorological, oceanographic, or ice information for a specific area.

(25) Setting up a wide-area network (WAN) over commercial lines.

f. Sources of Indicators During the Execution Phase

(1) Unit and equipment departures from normal bases.

(2) Adversary radar, sonar, or visual detections of friendly units.

(3) Friendly unit identifications through COMSEC violation, physical observation of unit symbology, etc.

(4) Force composition and tracks or routes of advance that can be provided by emissions from units or equipment and systems that provide identifying data.

(5) Stereotyped procedures; static and standard ways of composing, disposing, and controlling strike or defensive elements against particular threats; and predictable reactions to enemy actions.

(6) Alert of civilians in areas of operations.

(7) Trash and garbage dumped by units or from ships at sea that might provide unit identifying data.

(8) Transportation of spare parts or personnel to deploying or deployed units or via commercial aircraft or ship.

(9) Changes in oceanography high frequency facsimile transmissions.

(10) Changes in the activity over WAN.

g. Indicators of Postengagement Residual Capabilities

(1) Repair and maintenance facilities schedules.

(2) Urgent calls for maintenance personnel.

(3) Movement of supporting resources.

(4) Medical activity.

(5) Unusual resupply and provisioning of an activity.

(6) Assignment of new units from other areas.

(7) Search and rescue activity.

(8) Personnel orders.

(9) Discussion of repair and maintenance requirements in unsecure areas.

(10) Termination or modification of procedures for reporting of unclassified meteorological, oceanographic, or ice information.

(INTENTIONALLY BLANK)

APPENDIX D

OPERATIONS SECURITY MEASURES

The following OPSEC measures are offered as a guide only. Development of specific OPSEC measures is as varied as the specific vulnerabilities they are designed to offset.

a. Operational and Logistic Measures

(1) Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations or activities in terms of time, place, event sequencing, formations, and C2 arrangements.

(2) Employ force dispositions and C2 control arrangements that conceal the location, identity, and command relationships of major units.

(3) Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.

(4) Transport supplies and personnel to combat units in a way that conceals the location and identity of the combat units.

(5) Operate aircraft at low altitude to avoid radar detection.

(6) Operate to minimize the reflective surfaces that units or weapon systems present to radars and sonars.

(7) Use darkness to mask deployments or force generation.

(8) Approach an objective "out of the sun" to prevent detection.

b. Technical Measures

(1) Use radio communications emission control, low-probability-of-intercept techniques and systems, traffic flow security, padding, flashing light or flag hoist, UHF relay via aircraft, burst transmission technologies, secure phones, landline,

and couriers. Limit use of HF radios and directional SHF transponders.

(2) Control radar emission, operate at reduced power, operate radars common to many units, assign radar guard to units detached from formations or to air early warning aircraft, and use anechoic coatings.

(3) Mask emissions or forces from radar or visual detection by use of terrain (such as mountains and islands).

(4) Maintain sound silence or operate at reduced power, proceed at slow speeds, turn off selected equipment, and use anechoic coatings.

(5) Use screen jamming, camouflage, smoke, background noise, added sources of heat or light, paint, or weather.

c. Administrative Measures

(1) Avoid bulletin board, plan of the day, or planning schedule notices that reveal when events will occur.

(2) Conceal budgetary transactions, supply requests and actions, and arrangements for services that reveal preparations for activity.

(3) Conceal the issuance of orders, the movement of specially qualified personnel to units, and the installation of special capabilities.

(4) Control trash and garbage dumping or other housekeeping functions to conceal the locations and identities of units.

(5) Follow normal leave and liberty policies to the maximum extent possible before an operation starts in order to preserve a sense of normalcy.

(6) Ensure that personnel discretely prepare for their families' welfare in their absence and that their families are sensitized to their potential abrupt departure.

d. Military Deception In Support of OPSEC

(1) Deception can be an effective OPSEC measure, provided that prior coordination is accomplished when actions will affect other commanders. Military deception can be used to:

(a) Cause adversary intelligence to fail to target friendly activity; collect against targeted tests, operations, exercises, or other activities; or determine through analysis vital capabilities and characteristics of systems and vital aspects of policies, procedures, doctrine, and tactics.

(b) Create confusion about, or multiple interpretations of, vital information obtainable from open sources.

(c) Cause a loss of interest by foreign and random observers in test, operation, exercise, or other activity.

(d) Convey inaccurate locating and targeting information to opposing forces.

(2) In accordance with CJCSI 3211.01A, commanders are authorized to conduct military deception:

(a) To support OPSEC during the preparation and execution phases of normal operations, provided that prior coordination is accomplished for actions that will affect other commanders.

(b) When the commander’s forces are engaged or are subject to imminent attack.

e. Command and Control Warfare. During hostilities, use physical destruction and electronic attack against the adversary’s ability to collect and process information. C2W actions that can be used in support of OPSEC includes strikes against an adversary’s satellites, SIGINT sites, radars, fixed sonar installations, reconnaissance aircraft, and ships.

(INTENTIONALLY BLANK)

APPENDIX E

PROCEDURES FOR OPSEC SURVEYS

1. General

a. The purpose of an OPSEC survey is to thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists.

b. Ideally, the operation or activity being surveyed will be using OPSEC measures to protect its critical information. The OPSEC survey is used as a check on how effective the measures are. The survey will determine if the critical information identified during the OPSEC planning process is being protected.

c. A survey cannot be conducted until after an operation or activity has at least identified its critical information. Without a basis of identified critical information, there can be no specific determination that actual OPSEC vulnerabilities exist.

2. Uniqueness

a. Each OPSEC survey is unique. Surveys differ in the nature of the information requiring protection, the adversary collection capability, and the environment of the activity to be surveyed.

b. In combat, a survey’s emphasis must be on identifying operational indicators that signal friendly intentions, capabilities, and/or limitations and that will permit the adversary to counter friendly operations or reduce their effectiveness.

c. In peacetime, surveys generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit tests, practice alerts, and major exercises, are of great interest to a potential adversary because they provide insight into friendly readiness, plans, crisis procedures, and C2 capabilities that enhance that adversary’s long-range planning.

3. OPSEC Surveys versus Security Inspections

a. OPSEC surveys are different from security evaluations or inspections. A survey attempts to produce an adversary's view of the operation or activity being surveyed. A security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations.

b. Surveys are always planned and conducted by the organization responsible for the operation or activity that is to be surveyed. Inspections may be conducted without warning by outside organizations.

c. OPSEC surveys are not a check on the effectiveness of an organization's security programs or its adherence to security directives. In fact, survey teams will be seeking to determine if any security measures are creating OPSEC indicators.

d. Surveys are not punitive inspections, and no grades or evaluations are awarded as a result of them. Surveys are not designed to inspect individuals but are employed to evaluate operations and systems used to accomplish missions.

e. To obtain accurate information, a survey team must depend on positive cooperation and assistance from the organizations participating in the operation or activity being surveyed. If team members must question individuals, observe activities, and otherwise gather data during the course of the survey, they will inevitably appear as inspectors, unless this nonpunitive objective is made clear.

f. Although reports are not provided to the surveyed unit's higher headquarters, OPSEC survey teams may forward to senior officials the lessons learned on a nonattribution basis. The senior officials responsible for the operation or activity then decide to further disseminate the survey's lessons learned.

4. Types of Surveys. There are two basic kinds of OPSEC surveys: command and formal.

a. A command survey is performed using only command personnel and concentrates on events within the particular command.

b. A formal survey requires a survey team composed of members from inside and outside the command and will normally cross command lines (after prior coordination) to survey supporting and related operations and activities. Formal surveys are initiated by a letter or message stating the subject of the survey, naming the team leader and members, and indicating when the survey will be conducted. Commands, activities, and locations to be visited may also be listed, with the notation that the team may visit additional locations if required during the field portion of the survey.

c. Both types of surveys follow the same basic sequence and procedures that are established in the annexes to this appendix.

5. Survey Execution

a. Careful prior planning, thorough data collection, and thoughtful analysis of the results are the key phases of an effective OPSEC survey.

b. The following annexes describe the three phases of an OPSEC survey.

(INTENTIONALLY BLANK)

ANNEX A TO APPENDIX E

OPSEC SURVEY PLANNING PHASE

Preparations for an OPSEC survey must begin well in advance of the field survey phase. The required lead time will depend on the nature and complexity of the operation and activities to be surveyed (combat operations, peacetime operational activity, etc.). Sufficient time must be allotted in the planning phase for a thorough review of pertinent documentation, for formal and informal coordination and discussions, and for the careful preparation of functional outlines. The following actions normally make up the planning phase.

a. Determine the Scope of the Survey. The scope of the survey should be defined at the start of the planning phase and be limited to manageable proportions. Limitations will be imposed by geography, time, units to be observed, funding, and other practical matters.

b. Select Team Members

(1) Regardless of the survey's external or internal focus, the team should contain multidisciplined expertise. Survey team members should be selected for their analytical, observational, and problem solving abilities.

(2) Since surveys are normally oriented to operations, the senior member should be selected from the operations (or equivalent) staff of the commander responsible for conducting the survey.

(3) Typical team members would represent the functional areas of intelligence, security, communications, logistics, plans, and administration. When appropriate, specialists from other functional areas, such as transportation and public affairs, will participate.

(4) When communications monitoring is planned as part of the survey, the monitoring group's leader should be designated as a member of the OPSEC survey team. Team members must be brought together early in the planning phase to ensure timely, thorough accomplishment of the tasks outlined below.

c. Become Familiar with Survey Procedures. Designating team members with survey experience is advantageous, but is often not possible. In such cases, team members will require familiarization with survey procedures.

d. Determine the Adversary Intelligence Threat. The adversary threat to the activities to be surveyed must be evaluated carefully and realistically. An all-source threat assessment should comprehensively address the adversary intelligence capability, taking into account not only the adversary's collection capabilities (see Appendix B) but also the adversary's ability to exploit the collection results in a timely manner.

e. Understand the Operation or Activity to be Surveyed. The team members' thorough understanding of the operation or activity to be surveyed is crucial to ensuring the success of subsequent phases of the survey. Team members should become familiar with the operation plans, orders, standard operating procedures, or other directives bearing on the surveyed operation or activity. This initial review familiarizes team members with the mission and concept of operation and identifies most of the organizations participating in the surveyed activity (others may be identified as the survey progresses).

f. Conduct Empirical Studies

(1) Empirical studies simulate aspects of the adversary intelligence threat and support vulnerability findings. These studies also help the survey team identify vulnerabilities that cannot be determined through interviews and observation. The results of these studies are useful to the survey team during the field or analytic phase of the survey.

(2) An example of an empirical study is signals monitoring. Computer modeling or other laboratory simulations of the enemy threat may also be useful to the survey team. These studies are usually performed by organizations external to the one sponsoring the OPSEC survey team. Arrangements for their use should be made as far in advance of the survey as possible.

g. Develop a Functional Outline

(1) A basic OPSEC survey technique involves the construction of a chronology of events that are expected to occur in the surveyed operation or activity. Events are assembled sequentially, thus creating a timeline that describes in detail the activities or plans of an operation or activity.

(2) Chronologies should first be constructed for each separate functional area, such as operations, communications, logistics, or administration. This functional approach aids the team members in defining their separate areas of inquiry during the field or data collection phase of the survey. Later, the functional outlines can be correlated with each other to build an integrated chronology of the entire operation or activity (see Composite OPSEC Profile, Tab A).

(3) After the chronology is assembled, vulnerabilities can be identified in light of the known or projected threat.

(4) During the initial review of operation plans, orders, and procedures, individual team members can begin to develop functionally oriented outlines for their areas of interest. Initially, the outlines will be skeletal projections, in a narrative, table, or graph format, of what is expected to occur in the chronology for a particular functional area (see Tabs B through F).

(5) Such projections can serve as planning aids for the subsequent field survey phase. For example, units and facilities associated with each of the events can be identified and geographically grouped to aid in planning the travel itinerary of team members during the field survey. Collectively, the initial functional outlines provide a basis for planning the field survey phase and constitute a basis for observation and interviews.

(6) During the field survey phase, team members will acquire additional information through observation, interviews, and other data-collection techniques, enabling further development and refinement of the functional outlines.

(7) Collectively, the outlines project a time-phased picture of the events associated with the planning, preparation, execution, and conclusion of the operation or activity. The outlines also provide an analytic basis for identifying events and activities that are vulnerable to adversary exploitation.

h. Determine Preliminary Friendly Vulnerabilities. After the adversary intelligence threat and the OPSEC indicators are determined, a subjective evaluation must be made of the potential friendly vulnerabilities. A vulnerability (e.g., a detectable, exploitable event) may or may not carry a security classification at the time of its identification, but such preliminary vulnerabilities must be protected from disclosure by administrative or security controls. These preliminary friendly vulnerabilities will be refined in later stages of the OPSEC survey.

i. Announce the Survey

(1) After team members are selected and are familiar with the operation or activity to be surveyed, the organization conducting the survey should inform its subordinate and supporting organizations that a survey will be conducted so that preparations can be made to support the team during the field survey phase.

(2) The following information should be included:

(a) Survey purpose and scope.

(b) List of team members and their clearances.

(c) List of required briefings and orientations.

(d) Timeframe involved.

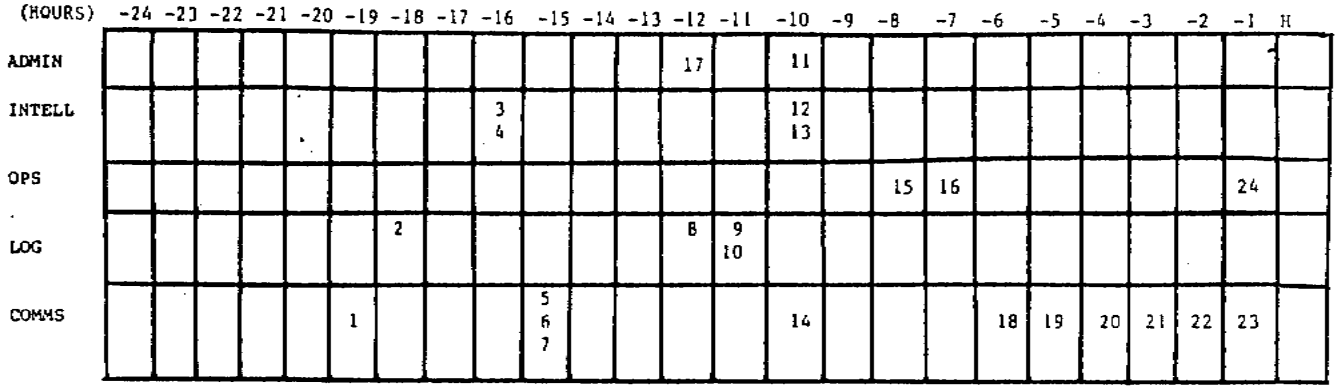
(e) Administrative support requirements.

(f) SIGSEC monitoring support requirements (if needed).

TAB A TO ANNEX A TO APPENDIX E
COMPOSITE OPSEC PROFILE FOR COMBAT OPERATIONS

Figure E-1 provides a sample composite OPSEC profile for combat operations. As illustrated by this sample, a profile can be constructed to display the event-time-agency data of significant information collected during an OPSEC survey. OPSEC survey personnel should use a composite OPSEC profile or similar tool to assist in identifying unit or mission OPSEC indicators.

COMPOSITE OPSEC PROFILE: BRIGADE COMBAT ASSAULT



1. 1100: Warning order over unsecure telephone at TF HQ.
2. 1233: AF supply order 1500 x 500 lb bombs.
3. 1310: S2 order for 100 x 1:12,500 maps of objective area
4. 1320: Recon flight over forest clearings in objective area.
5. 1405: Artillery net activated; warning to move tubes.
6. 1406: Brigade maintenance net unusually active.
7. 1430: Dustoff net disclosed establishment of field aid station.
8. 1705: 12 x sling-loaded CH-47s arrived at Brigade rear.
9. 1800: 3 x C-123s offloading wooden crates (probably artillery rounds).
10. 1850: 5 x C-123s offloading fuel doughnuts.
11. 1930: Two troops of 1-9th Air Cav released to rear on personal business "in time to return for the operation."
12. 1940: Sniffer flight in objective area.
13. 1944: ARDF flight observed in objective area.
14. 1921: LRRP radio DF'd in objective area.
15. 2100: Pathfinders assemble outside Brigade briefing tent.
16. 2230: Artillery firing H&I in objective area for first time.
17. 2315: Chaplain holding services near forward positions.
18. 2340: New frequency/call sign heard.
19. 0030: New NCS policies chatters for first time.
20. 0130: More new frequencies/call signs; many comms checks.
21. 0230: Only active stations in Brigade rear.
22. 0330: Near complete radio silence.
23. 0430: Complete radio silence.
24. 0455: Many flares.

Figure E-1. Sample Composite OPSEC Profile for Combat Operations

TAB B TO ANNEX A TO APPENDIX E

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR
INTELLIGENCE COLLECTION OPERATIONS

The completed profile reflects a picture of the intelligence collection effort. Intelligence collection is normally one of the first functional areas to present indicators of an impending operation or activity.

a. Planned Event Sequence. See intelligence collection plan prepared by intelligence staff element.

b. Actual Event Sequence. Observe events in the operation center.

c. Analysis. Determine any OPSEC vulnerabilities. If vulnerabilities exist, determine whether they exist because of an error or because they are the result of normal procedures.

d. Examples of Typical Indicators

(1) Appearance of specialized intelligence collection equipment in a particular area.

(2) Increased traffic on intelligence communications nets.

(3) Increased manning levels and/or work hours in intelligence facilities.

(4) Increased research activity by known intelligence activities and personnel in libraries and electronic data bases.

(5) Increased activity of friendly agent nets.

(6) Increased levels of activity by airborne intelligence systems.

(7) Alterations in the orbits of intelligence satellites.

(8) Interviews with nongovernmental subject matter experts conducted by intelligence personnel.

(9) Requests for maps and other topographic material.

TAB C TO ANNEX A TO APPENDIX E

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR LOGISTICS

The completed logistic profile presents a picture of logistic activities conducted in preparation for an impending operation. As in the administration function, the long lead time for some preparations gives early warning of forthcoming operations if events are compromised.

a. Planned Event Sequence. See logistic annex to OPLAN.

b. Actual Event Sequence. Observation, interviews.

c. Analysis. As in other functional areas.

d. Examples of Typical Indicators

(1) Special equipment issue.

(2) Pre-positioning of equipment and supplies.

(3) Increased weapons and vehicle maintenance.

(4) POL stockpiling.

(5) Upgrading lines of communication.

(6) Ammunition stockpiling.

(7) Delivery of special munitions and uncommon munitions (discloses possible nature of operation).

(8) Arrival of new logistic units and personnel.

(9) Increased requisition of supplies.

(10) Increased traffic on logistics communications nets.

(11) Changes in normal delivery patterns.

(INTENTIONALLY BLANK)

TAB D TO ANNEX A TO APPENDIX E

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR COMMUNICATIONS

In addition to presenting a picture of its own functional area, friendly communications also reflect all other functional areas. Communications surveillance and communications logs for all functional nets are important tools in evaluating this functional area as well as other functions involved.

a. Planned Event Sequence. OPLAN, OPORD, SOI, or SSI.

b. Actual Event Sequence. Communications monitoring and communications logs.

c. Analysis. As in other functional areas.

d. Examples of Typical Indicators

(1) Increased radio, teletype, and telephone traffic.

(2) Increased communications checks.

(3) Appearance of new stations in net.

(4) New frequency and call-sign assignments.

(5) New codes and authenticators.

(6) Radio silence.

(7) Changing callup patterns.

(8) Use of maintenance frequencies to test equipment.

(9) Communications CPXs.

(10) Appearance of different cryptographic equipment and materials.

(INTENTIONALLY BLANK)

TAB E TO ANNEX A TO APPENDIX E

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE FOR OPERATIONS

The completed profile of operational activities reflects events associated with tactical combat units as they prepare for an operation.

a. Planned Event Sequence. OPLAN, OPORD, SOP.

b. Actual Event Sequence. Observations, reports, messages, interviews.

c. Analysis. As in other functional areas.

d. Examples of Typical Indicators

(1) Rehearsals and drills.

(2) Special-tactics refresher training.

(3) Appearance of special-purpose units (bridge companies, forward air controllers, pathfinders, mobile weather units, etc.).

(4) Pre-positioning of artillery and aviation units.

(5) Artillery registration in new objective area.

(6) Complete cessation of activity in area in which reconnaissance activity previously took place.

(7) Appearance of new attached units.

(8) Issuance of new equipment.

(9) Changes in major unit leadership.

(10) Repositioning of maneuver units.

(INTENTIONALLY BLANK)

TAB F TO ANNEX A TO APPENDIX E

FUNCTIONAL OUTLINE AND PROFILE GUIDELINE
FOR ADMINISTRATION AND SUPPORT

The completed profile of administrative and support events shows activities taking place before the operation, thereby giving advance warning.

a. Planned Event Sequence. Derive from unit SOPs and administrative orders.

b. Actual Event Schedule. Observations and interviews.

c. Analysis. As in other functional areas.

d. Examples of Typical Indicators

(1) Release of groups of personnel or complete units for personal affairs.

(2) Runs on exchanges for personal articles, cleaning, etc.

(3) Changes to wake-up and mess schedules.

(4) Changes to mailing addresses.

(5) New unit designators on mail.

(6) Emergency personnel requisitions and fills for critical skills.

(7) Medical supply stockpiling.

(8) Emergency recall of personnel on pass and leave.

(INTENTIONALLY BLANK)

ANNEX B TO APPENDIX E

FIELD SURVEY PHASE

As noted previously, data collection begins in the planning phase with a review of associated documentation. During the field survey phase, interviews with personnel directly involved in the operation, together with observations and document collection, are the primary means of data collection. The following actions are normally accomplished during the field survey phase:

a. Command Briefing on Operation to be Surveyed. This briefing is presented to the OPSEC survey team by the command directing the forces or assets involved in the operation or activity being surveyed. The purpose of the briefing is to provide the survey team with an overview of the operation from the command's point of view. Team members should use this opportunity to clarify remaining questions about the information developed in the planning phase.

b. OPSEC Survey Team Briefing. This briefing is presented by the chief of the survey team to the commander and principal staff officers of the surveyed organization. The briefing may be either a formal presentation or an informal discussion. The objective is to inform the commander and the staff of how the survey will be conducted. The briefing should include a summary of the hostile threat and the vulnerability assessment developed during the planning phase. The staff should be asked to comment on the validity of this assessment. Results of previous OPSEC surveys of similar activities may be summarized.

c. Data Collection and Functional Outline Refinement

(1) Data Collection

(a) During the field survey phase, data are collected through observation of activities, document collection, and personnel interviews. Data may also be acquired through concurrent ongoing empirical data collection such as SIGSEC monitoring.

(b) Team members must be alert to differences between what they have read, what they have assumed to be the situation, what they have been told in the command briefing, and what they observe and are told by personnel participating in the operation. Conflicting data are to be expected.

(c) While observations can verify the occurrence, sequence, and exact timing of events, much essential information must be gathered from interviews.

1. Functional outlines should be reviewed before and after interviews to ensure that all pertinent points are covered. Specifics on how, when, and where people accomplish their tasks, and how these tasks relate to the planned and observed sequence of events, are recorded in order to document activities in a logical sequence.

2. Team members should assure interviewees that all sources of information will be protected by a nonattribution policy.

3. Interviews are best conducted by two team members.

4. Facts to be recorded during or soon after The interview normally include:

a. Identification and purpose of the interview.

b. Description of the positions occupied by the persons being interviewed.

c. Details of exactly what tasks the individuals perform and how, when, and where they perform them with a view toward determining what information they receive, handle, or generate, and what they do with it.

d. Whether the individuals' actions reflect an awareness of a hostile intelligence collection threat.

(2) Functional Outline Refinement

(a) As indicated earlier, each team member should have a basic functional outline to direct data collection efforts at the beginning of the field survey phase. The basic outline will be modified during this phase to reflect new information obtained by observation and interview and will ultimately become a profile of actual events.

(b) Each team member should be familiar with the outlines used by the other members of the survey team and should be alert for information that might affect them. An interview in the communications area, for example, might disclose information that would result in a change to the outline being developed for operations; or an observation in one geographic location could affect an outline being followed up in another. Also, to permit followup elsewhere, all outlines should try to reflect the information generated and the flow at each location where data are collected.

(c) As data are accumulated through observation and interviews, incorporation of such data into the basic functional outline changes the original list of projected events into a profile of actual events. The functional outline then becomes a chronological record of what actually was done, where, who did it, and how and why it was done. The outline should also reflect an assessment of the vulnerability of each event to the known or suspected hostile intelligence threat.

(d) Tentative findings will begin to emerge as data collection proceeds and information is reviewed and compared. The findings should be confirmed and fully documented as quickly as possible.

(e) If a finding is considered to have serious mission impact, it should be made known to the commander responsible for the operation in order to permit early corrective actions.

(f) Development of findings during the field survey phase ensures access to supporting data and precludes the need to reconstruct evidence after the team has left the scene. Following this procedure, the basic findings and supporting data of the final survey report will be well developed before the end of the field survey phase. Final development and production of the survey report can then proceed immediately upon the team's return to home station.

d. Team Employment

(1) The complexity, size, and duration of the surveyed operation or activity will determine the general employment of the survey team. Tentative locations for data collection, developed during the planning phase, provide initial indications of how and where to employ the team.

(2) It is rarely possible, however, to plan employment in detail before the field survey phase. A limited, short duration operation with few participating elements may permit concentrating the team in one, or a very few, locations. Larger and longer operations may require complete dispersal of the team, movement of the entire team from one location to another, or both, over a substantial period of time. The most reliable guideline for the team chief in determining how to employ the team is to reassemble it daily to assess progress, compare data, and coordinate the direction of the survey.

(3) The duration of the field survey phase is established during the planning phase and depends on how rapidly data are collected. Many surveys have required 30 days or more in the field. Less comprehensive ones might require a week or 10 days. The proximity of data collection locations to each other, number of such locations, transportation

availability, and degree of difficulty experienced in resolving conflicting data are some of the factors affecting duration of the field survey phase.

e. OPSEC Survey Team Exit Briefing

(1) An exit briefing should be presented to the commander before the team leaves a command, regardless of previous reports or tentative findings. Like the entrance briefing, the exit briefing can be an informal discussion with the commander or a formal briefing for the commander and the staff.

(2) The tentative nature of survey findings should be emphasized. Even those that appear to be firm may be altered by the final data review as the survey report is prepared. Because preparation of the written report may take some time, the exit briefing can serve as an interim basis for further consideration and possible action by the commander.

(3) The distribution of the final written report should be clearly stated during the exit briefing. Normally, the report will be provided directly to the commander. Some commands have found it useful to forward an interim report to the surveyed commander for comments before proceeding with the final version.

(INTENTIONALLY BLANK)

ANNEX C TO APPENDIX E

ANALYSIS AND REPORTING PHASE

During this phase, the OPSEC team correlates the data acquired by individual members with information from any empirical studies conducted in conjunction with the survey.

a. Correlation of Data

(1) Correlation of Functional Outlines. When the separate chronology outlines for each functional area are correlated, the chronology of events for the operation or activity as a whole will emerge. During the field survey or analytic phases, conflicts of data must be clarified.

(2) Functional Outlines. The purpose of constructing the functional outlines is to describe the time-phased unfolding of the operation or activity; to depict the manner in which separate commands, organizations, and activities interact and perform their roles in the operation or activity; and to trace the flow of information through electrical and nonelectrical communications media from its origin to its ultimate recipients. It is important that the team members present the information in a manner that facilitates analysis. The net result of the correlation will be a portrayal of the entire operation or activity.

(3) Correlation of Empirical Data. In addition to correlating data acquired from the observations of individual team members, the survey team may also use relevant, empirically derived data to refine individual functional outlines. More importantly, these data can also verify vulnerabilities that would otherwise be exceedingly speculative or tenuous. Empirical data are extremely important to a comprehensive survey.

b. Identification of Vulnerabilities

(1) The correlation and analysis of data help the team to refine the previously identified preliminary vulnerabilities or isolate new ones. This analysis is accomplished in a manner similar to the way

adversaries would process information through their intelligence systems.

(2) Indicators that are potentially observable are identified as vulnerabilities. Vulnerabilities point out situations that an adversary may be able to exploit. The key factors of a vulnerability are observable indicators and an intelligence collection threat to those indicators.

(3) The degree of risk to the friendly mission depends on the adversary's ability to react to the situation in sufficient time to degrade friendly mission or task effectiveness.

c. OPSEC Survey Report. The report of the OPSEC survey is addressed to the commander of the surveyed operation or activity. Lengthy reports (more than 15 pages) should be accompanied by an executive summary.

(1) There is no special format for OPSEC survey reports; a suggested format is at the Tab. Whatever the format, the report should provide a discussion of identified critical information, indicators, adversaries and their intelligence capabilities, OPSEC vulnerabilities, risk analysis, and recommended OPSEC measures to eliminate or reduce the vulnerabilities. Although some vulnerabilities may be virtually impossible to eliminate or reduce, they should be included in the report to enable commanders to assess their operation or activity more realistically.

(2) Each report should contain a threat statement. Its length and classification need only be adequate to substantiate the vulnerabilities (or actual sources of adversary information) described in the report. The statement may be included in the main body of the report or as an annex to it. Portions of the threat that apply to a particular vulnerability finding may be concisely stated as substantiation in a paragraph preceding or following the explanation of the observation. If the threat statement is so classified that it will impede the desired distribution and handling, the statement, or parts of it, should be affixed as an annex that can be included only in copies of the survey report provided to appropriately cleared recipients.

(3) The section that delineates vulnerabilities can be presented in a sequence that correlates with their significance, in an order that coincides with their appearance in the chronological unfolding of the surveyed operation or activity, or grouped together according to functional area (logistics, communications, personnel, etc.). A particular vulnerability can be introduced by a headline followed by an adequate description of the finding and accompanied by identification of that portion of the operation or activity that includes the vulnerability. As stated earlier, a vulnerability observation may also include relevant threat references.

(4) If possible, OPSEC teams should include recommendations for corrective actions in the report. However, the team is not compelled to accompany each vulnerability finding with a recommendation. In some situations, the team may not be qualified to devise the corrective action; in others, it may not have an appreciation of the limitations in resources and options of a particular command. It may sometimes be more effective for the team to present the recommendation informally rather than including it in the survey report. Recommendations of the OPSEC team may be particularly valuable in situations in which a vulnerability crosses command lines. Ultimately, commanders or the responsible officials must assess the effect of possible adversary exploitation of vulnerabilities on the effectiveness of their operation or activity. They must then decide between implementing corrective actions or accepting the risk posed by the vulnerability.

(5) Appendixes and annexes to OPSEC survey reports may be added to support the vulnerability findings and conclusions. Sections, such as a threat annex, may include empirical studies (or parts of them). Maps, diagrams, and other illustrative materials are some ways to substantiate OPSEC vulnerabilities.

(6) The report may end with a conclusion or summary of the survey and its findings. The summary should not include judgments about compliance with standing

security practices of the organizations. Such judgments are the purview of security disciplines.

(7) Distribution of the survey team's report should be limited to the principal commands responsible for the surveyed operation or activity. After the commands have had time to assess the report and take corrective actions, they can consider additional distribution. Abstracts from the report may be provided for lessons-learned documents or data bases on a nonattribution basis.

(8) Because they contain vulnerability information, OPSEC survey reports must be controlled from release to unauthorized persons or agencies. Affected portions of the report must be controlled in accordance with applicable security classification guides. For those portions of the report not controlled by security classification guides, administrative control of the release of survey report information must be considered. Likewise, the notes, interviews, raw data, etc., used to build a survey report must be subject to the same controls as the finished report.

TAB TO ANNEX C TO APPENDIX E

SUGGESTED FORMAT FOR FINAL OPSEC SURVEY REPORT

1. Overview

a. Background. Address the purpose and scope of the survey as well as the results of the threat and vulnerability assessments.

b. Conduct of Survey. Brief discussion of methodology, team composition, major commands visited, and timeframe of survey.

c. Critical Information

d. Threat

2. Summary of Significant Findings

3. Analysis, Conclusions, and Findings. This is the body of the report. Discussions and findings may be listed chronologically, by command, or chronologically within commands.

4. Suggested Format for Each Finding

a. Observation

b. Analysis and discussion

c. Conclusion or recommendation

(INTENTIONALLY BLANK)

APPENDIX F

REFERENCES

1. DOD Directive 5205.2, 7 July 1983, "DOD Operations Security Program"

2. CJCS MOP 6, 3 March 1993, "Electronic Warfare"

3. CJCS MOP 30, 8 March 1993, "Command and Control Warfare"

4. CJCSI 3211.01, 1 June 1993, "Joint Military Deception"

5. CJCSI 3213.01, 28 May 1993, "Joint Operations Security"

6. Joint Pub 1, 11 November 1991, "Joint Warfare for the US Armed Forces"

7. Joint Pub 1-02, 1 December 1989, "Department of Defense Dictionary of Military and Related Terms"

8. Joint Pub 1-01, 30 July 1992 (Change 1, 14 September 1993), "Joint Publication System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program"

9. Joint Pub 2-0, 12 October 1993, "Joint Doctrine for Intelligence Support to Operations"

10. Joint Pub 3-0, 9 September 1993, "Doctrine for Joint Operations"

11. Joint Pub 3-51, 30 June 1991, "Electronic Warfare in Joint Military Operations"

12. Joint Pub 3-53, 30 July 1993, "Joint Psychological Operations Doctrine"

13. Joint Pub 3-58, (Draft), "Joint Doctrine for Military Deception"

14. Joint Pub 5-03.01, 4 August 1993, "Joint Operation Planning and Execution System, Volume I (Planning Policies and Procedures)"

15. Joint Pub 5-03.02, 10 March 1992, "Joint Operation Planning and Execution System, Volume II (Planning and Execution Formats and Guidance)"

(INTENTIONALLY BLANK)

APPENDIX G
USERS EVALUATION REPORT
ON JOINT PUB 3-54

1. Users in the field are highly encouraged to directly submit comments on this pub by removing this page and sending it to JWFC/DD. Please fill out the following: users' POC, unit address, and phone (DSN) number.

_____
_____

2. Content

a. Does the pub provide a conceptual framework for the topic?

_____
_____

b. Is the information provided accurate? What needs to be updated?

_____
_____

c. Is the information provided useful? If not, how can it be improved? _____
_____

d. Is this pub consistent with other joint pubs?

_____
_____

e. Can this pub be better organized for the best understanding of the doctrine and/or JTTP? How?

_____
_____

3. Writing and Appearance

a. Where does the pub need some revision to make the writing clear and concise? What words would you use?

_____
_____

b. Are the charts and figures clear and understandable? How would you revise them? _____
_____

4. Recommended urgent change(s) (if any). _____
_____

5. Other _____

_____

6. Please fold and mail comments to the Joint Warfighting Center/Doctrine Division (additional pages may be attached if desired) or FAX to DSN 564-3990 or COMM (804) 444-3990.

(FOLD)

FROM:

JOINT WARFIGHTING CENTER/DOCTRINE DIVISION
BLDG R-52
1283 CV TOWWAY STE 100
NORFOLK, VA 23511-2491

(FOLD)

APPENDIX G
USERS EVALUATION REPORT
ON JOINT PUB 3-54

1. Users in the field are highly encouraged to directly submit comments on this pub by removing this page and sending it to JWFC/DD. Please fill out the following: users' POC, unit address, and phone (DSN) number.

_____
_____

2. Content

a. Does the pub provide a conceptual framework for the topic?

_____
_____

b. Is the information provided accurate? What needs to be updated?

_____
_____

c. Is the information provided useful? If not, how can it be improved? _____
_____

d. Is this pub consistent with other joint pubs?

_____
_____

e. Can this pub be better organized for the best understanding of the doctrine and/or JTTP? How?

_____
_____

3. Writing and Appearance

a. Where does the pub need some revision to make the writing clear and concise? What words would you use?

_____
_____

b. Are the charts and figures clear and understandable? How would you revise them? _____
_____

4. Recommended urgent change(s) (if any). _____
_____

5. Other _____
_____

6. Please fold and mail comments to the Joint Warfighting Center/Doctrine Division (additional pages may be attached if desired) or FAX to DSN 564-3990 or COMM (804) 444-3990.

(FOLD)

FROM:

JOINT WARFIGHTING CENTER/DOCTRINE DIVISION
BLDG R-52
1283 CV TOWWAY STE 100
NORFOLK, VA 23511-2491

(FOLD)

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

AF	Air Force
ARDF	aerial radio direction finding
C2	command and control
C2W	command and control warfare
C3	command, control, and communications
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	CJCS instruction
COA	course of action
COMINT	communications intelligence
COMSEC	communications security
CONPLAN	operation plan in concept format
CPX	command post exercise
DF	direction finding
DOD	Department of Defense
EA	electronic attack
EEI	essential elements of information
EEFI	essential elements of friendly information
ELINT	electronics intelligence
EP	electronic protection
ES	electronic support
EW	electronic warfare
FISINT	foreign instrumentation signals intelligence
HF	high frequency
H&I	harassing and interdicting
HQ	headquarters
HUMINT	human intelligence
IMINT	imagery intelligence
JOPES	Joint Operation Planning and Execution System
JULLS	Joint Universal Lessons Learned System
LRRP	long-range reconnaissance patrol
MASINT	measurement and signature intelligence
MOP	memorandum of policy

NCS	net control station
OPLAN	operation plan in complete format
OPORD	operation order
OPSEC	operations security
POL	petroleum, oil, and lubrication
PSYOP	psychological operations
SHF	superhigh frequency
SIGINT	signals intelligence
SIGSEC	signals security
SOI	signal operation instructions
S2	battalion or brigade intelligence officer
SOP	standard operating procedure
SSI	standing signal instruction
TF	task force
UHF	ultrahigh frequency

PART II--TERMS AND DEFINITIONS

command and control warfare. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities while protecting friendly command and control against such actions. Command and control warfare applies across the operational continuum and all levels of conflict. Also called C2W. Command and control warfare is both offensive and defensive:

(1) counter command and control. To prevent effective command and control of adversary forces by denying information to, influencing, degrading or destroying the adversary command and control system.

(2) command and control protection. To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade or destroy the friendly command and control system. (Joint Pub 1-02)

critical information. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (Joint Pub 1-02)

essential elements of friendly information. Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. (Joint Pub 1-02)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to 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. Also called OPSEC. (Joint Pub 1-02)

operations security indicators. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (Joint Pub 1-02)

operations security measures. Methods and means to gain and maintain essential secrecy about critical information. The following categories apply:

a. action control. The objective is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake; decide whether or not to execute actions; and determine the "who," "when," "where," and "how" for actions necessary to accomplish tasks.

b. countermeasures. The objective is to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering and processing capabilities.

c. counteranalysis. The objective is to prevent accurate interpretations of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers. (Joint Pub 1-02)

operations security vulnerability. A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decisionmaking. (Joint Pub 1-02)