Joint Publication 3-13.3

Operations Security

04 January 2012

CHAPTER II

> *"Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing."*
>
> **Frederick the Great**
> **Instructions for His Generals, 1747**

THE OPERATIONS SECURITY PROCESS

1. General

a. **OPSEC planning is based upon the OPSEC process.** This process, when used in conjunction with the joint planning process, provides the information required to write the OPSEC section of any plan or order. OPSEC planning is done in close coordination with the overall IO planning effort.

b. The OPSEC process is applicable across the range of military operations. Use of the process ensures that the resulting OPSEC countermeasures address all significant aspects of the particular situation and are balanced against operational requirements. OPSEC is a continuous process. **The OPSEC process (Figure II-1) consists of five distinct actions:** identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate OPSEC countermeasures. These OPSEC actions are applied continuously during OPSEC planning. In dynamic situations, however, individual actions may be reevaluated 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.** These are specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against 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 decision making.

2. Identify Critical Information

a. The **identification of critical information is a key part of the OPSEC process because it focuses the remainder of the OPSEC process on protecting vital information**

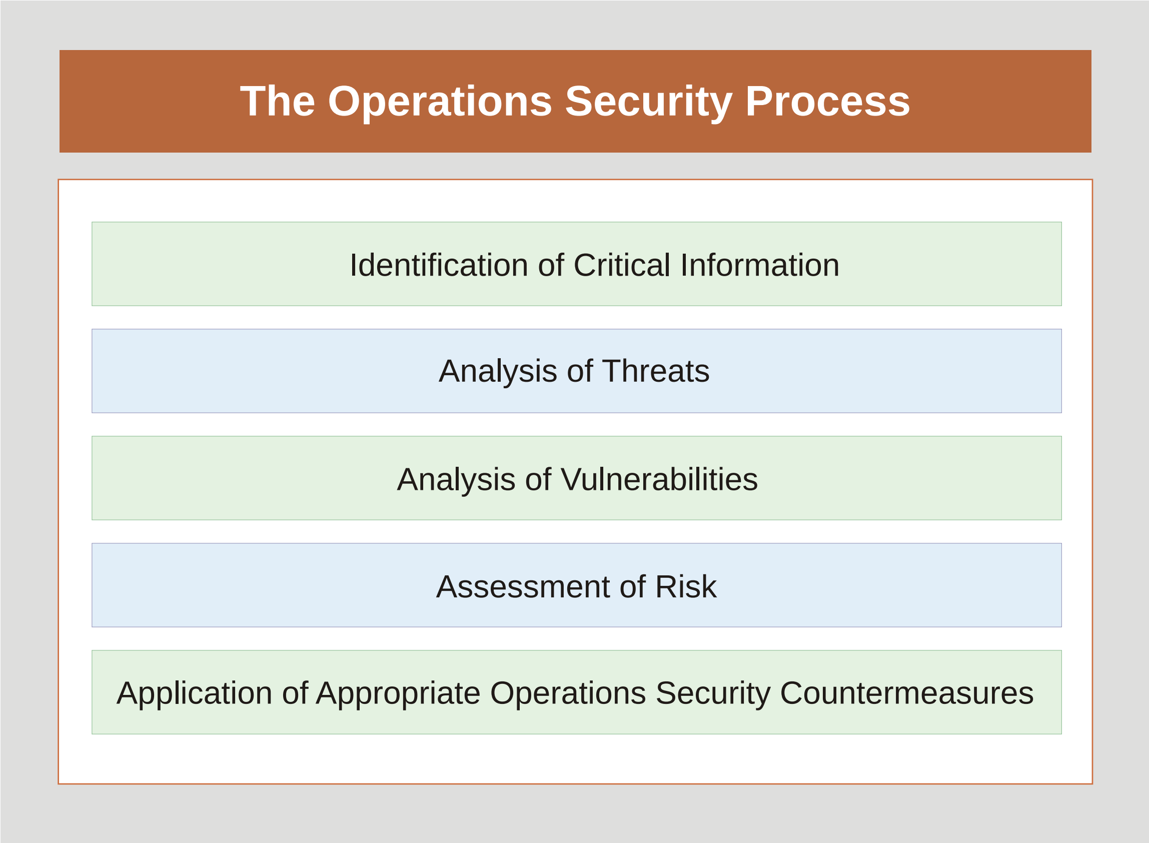
The Operations Security Process
Identification of Critical Information
Analysis of Threats
Analysis of Vulnerabilities
Assessment of Risk
Application of Appropriate Operations Security Countermeasures

Figure II-1. The Operations Security Process

rather than attempting to protect all unclassified information. Critical information answers key questions likely to be asked by adversaries about specific friendly intentions, capabilities, and activities necessary for adversaries to plan and act effectively against friendly mission accomplishment. There are many areas within an organization where elements of critical information can be obtained. Personnel from outside the organization may also handle portions of its critical information. Therefore it is important to have personnel from each staff section and component involved in the process of identifying critical information. The critical information items should be consolidated into a list known as a CIL.

b. **Critical information is listed in tab C (Operations Security) to appendix 3 (Information Operations) to annex C (Operations) of an OPLAN or OPORD.** Generic CILs (Figure II-2) can be developed beforehand to assist in identifying the specific critical information.

3. Threat Analysis

a. This action involves the research and analysis of **intelligence, CI,** and **open-source information** to identify the likely adversaries to the planned operation.

b. **The operations planners,** working with the intelligence and CI staffs and assisted by the OPSEC program manager, **seek answers to the following threat questions:**

Examples of Critical Information

Model Joint Operation Phases

Shape

Negotiating positions
Intelligence verification capabilities
Forces available
Targets
Timing

Tactics, techniques, and procedures
Logistic capabilities and constraints
Critical communication nodes
Exercise concept plans and operation plans

Deter

Intentions
Alert posture
Military capabilities
Forces assigned and in reserve
Target selection

Tactics, techniques, and procedures
Logistic capabilities and constraints
Mobilization
Purpose, targets and processing of intelligence collection

Seize the Initiative

Intentions
Military capability
Critical communication nodes
Forces assigned and in reserve

Target selection
Tactics, techniques, and procedures
Logistic capabilities and constraints

Dominate

Forces assigned and in reserve
Target selection
Tactics, techniques, and procedures

Logistic capabilities and constraints
Critical communication nodes

Stabilize

Lines of communications
Tactics, techniques, and procedures

Logistic capabilities and constraints
Critical communication nodes

Enable Civil Authority

Identity of military forces
Military support of law enforcement
Host-nation support
Capabilities

Third nation support
Lines of communications
Critical communication nodes
Tactics, techniques, and procedures

Figure II-2. Examples of Critical Information

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

(2) What are the adversary's goals? (What does the adversary want to accomplish?)

(3) What is the adversary's COA for opposing the planned operation? (What actions might the adversary take? Include the most likely COA and COA most dangerous to friendly forces and mission accomplishment.)

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

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

(6) Who are the affiliates of the adversary, and will they share information?

4. Vulnerability Analysis

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

b. Continuing to work with the intelligence personnel, the operations planners seek answers to the following vulnerability questions:

(1) 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?

All personnel must understand the adversary's capability to collect information and take operations security countermeasures to deny the use of that capability.

(2) What indicators can the adversary actually collect?

(3) 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?)

(4) Will the application of OPSEC countermeasures introduce more indicators that the adversary will be able to collect?

See Appendix A, "Operations Security Indicators," *for a detailed discussion of OPSEC indicators.*

5. Risk Assessment

a. This action has three components. First, **planners analyze the vulnerabilities** identified in the previous action and **identify possible OPSEC countermeasures** for each vulnerability. Second, the commander and staff estimate the impact to operations such as cost in time, resources, personnel or interference with other operations associated with implementing each possible OPSEC countermeasure versus the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability. Third, the commander and staff select **specific OPSEC countermeasures for execution** based upon a risk assessment done by the commander and staff.

b. OPSEC countermeasures reduce the probability of the adversary either observing indicators or exploiting vulnerabilities, being able to correctly analyze the information obtained, and being able to act on this information in a timely manner.

(1) **OPSEC countermeasures can be used** to prevent the adversary from detecting an indicator or exploiting a vulnerability, provide an alternative analysis of a vulnerability or an indicator (prevent the adversary from correctly interpreting the indicator), and/or attack the adversary's collection system.

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

(3) **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 countermeasures are those that combine the highest possible protection with the least adverse effect on operational effectiveness. Chapter III, "Operations Security Planning," provides a detailed discussion of OPSEC countermeasures.

c. **Risk assessment** requires comparing the estimated cost associated with implementing specific OPSEC countermeasure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

(1) **OPSEC countermeasures may 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 countermeasure entails risks, this step requires the commander's approval. Critical intelligence operations and sources may be compromised if OPSEC countermeasures are applied. Some operations and collection methods/sources may be too important to be compromised if the adversary detects friendly OPSEC countermeasures.

(2) Typical questions that might be asked when making this analysis include the following:

(a) What effect is likely to occur if a particular OPSEC countermeasure is implemented?

(b) What impact to mission success is likely to occur if an OPSEC countermeasure is not implemented?

(c) What impact to mission success is likely if an OPSEC countermeasure fails to be effective?

(d) What additional indicators may be collected by the adversary if an OPSEC countermeasure is implemented?

(3) **The interaction of OPSEC countermeasures should also be analyzed.** In some situations, certain OPSEC countermeasures may actually create indicators of critical information. For example, camouflaging previously unprotected facilities can indicate preparations for military action.

d. **The selection of measures must be coordinated with other capabilities of IO.** Actions such as jamming of intelligence nets or the physical destruction of critical intelligence centers can be used as OPSEC countermeasures. Conversely, MILDEC and military information support operations plans may require that OPSEC countermeasures not be applied to certain indicators in order to project a specific message to the adversary.

For more detailed discussion on risk assessment, see DOD 5205.02-M, DOD Operations Security (OPSEC) Program Manual.

6. Apply Operations Security Countermeasures

a. The command **implements the OPSEC countermeasures** selected in the risk assessment process or, in the case of planned future operations and activities, includes the measures in specific operations plans. Before OPSEC countermeasures can be selected, security objectives and critical information must be known, indicators identified, vulnerabilities assessed, and risks assessed.

A key action during the operations security process is to analyze potential vulnerabilities to joint forces. It requires identifying any operations security indicators that could reveal critical information about the operation, such as increased troop movement.

b. A general OPSEC countermeasure strategy should be to:

(1) Minimize predictability from previous operations.

(2) Determine detection indicators and protect them by elimination, control, or deception.

(3) Conceal indicators of key capabilities and potential objectives.

(4) Counter the inherent vulnerabilities in the execution of mission processes and the technologies used to support them.

c. During the execution of OPSEC countermeasures, OPSEC personnel should establish measures of effectiveness (MOEs) and measures of performance (MOPs) to assess if their OPSEC analysis is correct.

(1) MOE. **The adversary's reaction is monitored to determine the countermeasures' effectiveness and to provide feedback.** As it has been indicated above, implementing OPSEC countermeasures should not reveal additional critical information. As a corollary to that, if an OPSEC countermeasure is identified by the adversary, that, in itself, may be enough to alert the adversary that a military operation is imminent.

(2) MOP. Provides OPSEC personnel a way to determine if OPSEC countermeasures are being properly implemented.

(3) Commanders and their staffs can use feedback to adjust ongoing activities and for future OPSEC planning. Provisions for feedback must be coordinated with the command's intelligence and CI staffs to ensure requirements that support OPSEC receive the appropriate priority. In addition to intelligence sources providing feedback, OPSEC assessments can provide useful information relating to the success of OPSEC countermeasures.