

timely, effective decisions; and communicate those decisions as orders to subordinate commanders to control the course of an operation. The execution of orders on both sides of an operation alters the situation in the operational area. These changes, in turn, must be **observed, assessed, and acted upon in a continuous process**. This process can be thought of as a “decision cycle.”

g. **Synchronized C2W operations should enable a JFC to operate “inside” an adversary’s decision cycle** by allowing the JFC to process information through the C2 decision cycle faster than an adversary commander. Initiative is fundamental to success in military operations. In C2W, both C2-attack and C2-protect operations

a. **OPSEC is concerned with denying critical information about friendly forces to the adversary.** In C2W, the threat to OPSEC is ultimately the adversary commander. Denial of critical information about friendly capabilities and limitations may result in flawed command decisions that prove devastating to the adversary force. The emphasis of OPSEC as a part of an overall C2W effort should be **to deny critical information necessary for the adversary commander to accurately estimate the military situation**. The intent of OPSEC in C2W should be to force the adversary commander to make faulty decisions based upon insufficient information and/or to delay the decision making process due to a lack of information.



Since the news media potentially can be a lucrative source of information to adversaries, OPSEC planners must work closely with public affairs personnel to avoid inadvertent disclosure of critical information.

contribute to gaining and maintaining military initiative.

h. For more information on C2W, see Joint Pub 3-13.1, “Joint Doctrine for Command and Control Warfare.”

6. OPSEC and Command and Control Warfare

See Figure I-1.

b. **The inevitable presence of the news media during military operations complicates OPSEC.** As part of the global information infrastructure, the news media portrays and offers commentary on military activities on the battlefield—both preparatory to and during battle. News media portrayal of military activities prior to hostilities can **help to deter actual hostilities and/or build public support for inevitable hostilities**. By portraying the presence of US and/or

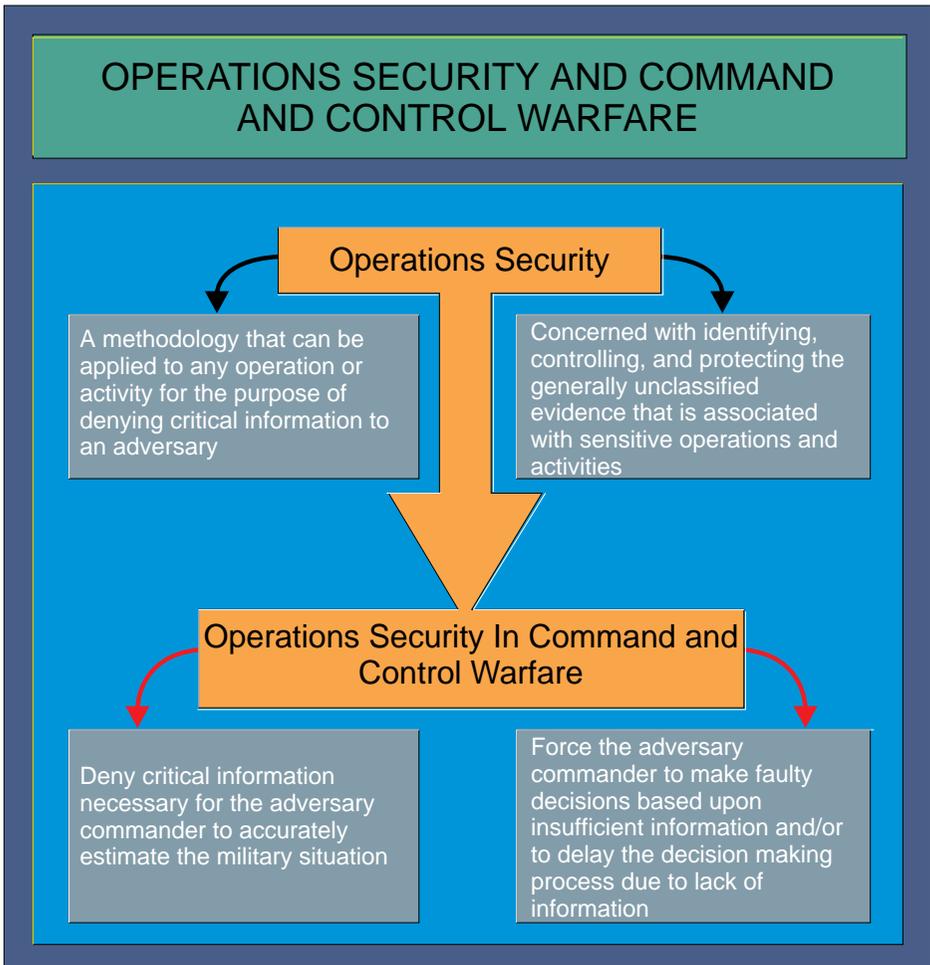


Figure I-1. Operations Security and Command and Control Warfare

multinational military forces in or en route to the operational area, **news media stories can demonstrate the readiness, commitment and resolve of the United States and its multinational partners** to commit military forces to battle if necessary to protect US and/or multinational interests, lives, or property. However, the presence of the news media in the operational area, with the capability to transmit information on a real-time basis to a worldwide audience, has the potential to be a **lucrative source of information to adversaries**. OPSEC planners must keep these considerations in mind when determining which aspects of a military operation are “critical information”

that must be denied to the adversary. OPSEC planners must work closely with military public affairs personnel to develop guidelines that can be used by both military and news media personnel to **avoid inadvertent disclosure of critical information** that could, ultimately, increase the risk to the lives of US and/or multinational military personnel.

c. **Denial of critical information to the adversary commander** contributes to uncertainty and slows the adversary’s decision cycle. Critical information can be hidden by such traditional OPSEC measures as action control, countermeasures, and counteranalysis. **Counterintelligence**

support is an integral part of successful OPSEC. PSYOP and military deception personnel also work closely with OPSEC planners to mutually support their respective efforts.

d. Critical information denied to an adversary can be replaced or refocused to support the commander's goals through military deception and/or PSYOP, if use of those elements has been approved at the

appropriate level. In C2W, **operational planners concerned with OPSEC should also coordinate with C2 planners, EW planners, and targeteers** to deny critical information to the adversary commander. The OPSEC process may also identify for attack particular adversary collection, processing, analysis, and distribution systems in order to deny the adversary commander critical information by forestalling that commander's ability to collect it.

CHAPTER II

OPSEC PLANNING

“To keep your actions and your plans secret always has been a very good thing . . . Marcus Crassus said to one who asked him when he was going to move the army: ‘Do you believe that you will be the only one not to hear the trumpet?’”

**Niccolo Machiavelli,
The Art of War, 1521**

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.

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



While planning joint operations, including those requiring highly visible deployments, OPSEC measures must be considered as early as possible to prevent adversaries from gaining valuable intelligence.

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.

*"O divine art of subtlety and secrecy!
Through you we learn to be invisible,
through you inaudible; and hence hold
the enemy's fate in our hands."*

Sun Tzu, c. 500 BC
The Art of War

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, communications security (COMSEC) monitoring, and OPSEC surveys are the primary sources for feedback information.

g. **Public affairs officers 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 as well as any interested third parties from discovering sensitive information relating to OPSEC during the post-execution phase.

3. OPSEC Planning and the Joint Operation 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, "The OPSEC Process." Joint OPSEC planning is always done in conjunction with normal joint operation planning and is a part of the overall C2W planning effort.

b. **Planning Processes.** There are **three major planning processes** for joint planning. Plans are proposed under different processes depending on the focus of a specific plan. The processes are labeled either **campaign, deliberate, or crisis action planning**, and are interrelated. They are described in Joint Pub 5-0, "Doctrine for Planning Joint Operations."

c. **The Deliberate Planning Process.** OPSEC planning relates to the Joint Operation Planning and Execution System (JOPES) deliberate planning process as shown in Figure II-1.

CHAPTER III

THE OPSEC PROCESS

"He passes through life most securely who has least reason to reproach himself with complaisance toward his enemies."

Thucydides,
History of the Peloponnesian Wars, 404 BC

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 or adaptive 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.**

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

- **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. The OPSEC Process

See Figure III-1 and Figure III-2.

a. OPSEC Action 1— Identification of Critical Information

- 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).
- **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.

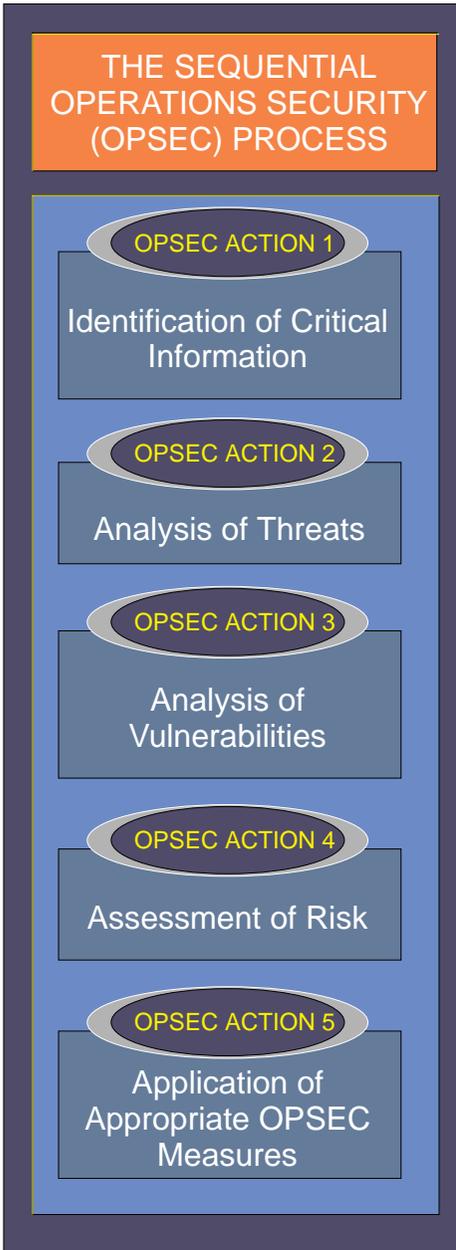


Figure III-1. The Sequential Operations Security (OPSEC) Process

- **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, “Examples of Critical Information.”

b. OPSEC Action 2—Analysis of Threats

- 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.
- **The operations planners**, working with the intelligence and counterintelligence staffs and assisted by the OPSEC program personnel, **seek answers to the following questions:**
 - Who is the adversary? (Who has the intent and capability to take action against the planned operation?)
 - What are the adversary’s goals? (What does the adversary want to accomplish?)
 - What is the adversary’s strategy for opposing the planned operation? (What actions might the adversary take?)
 - What critical information does the adversary already know about the operation? (What information is it too late to protect?)
 - What are the adversary’s intelligence collection capabilities?
- 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, “The Intelligence Threat,” discusses the general characteristics of intelligence systems.

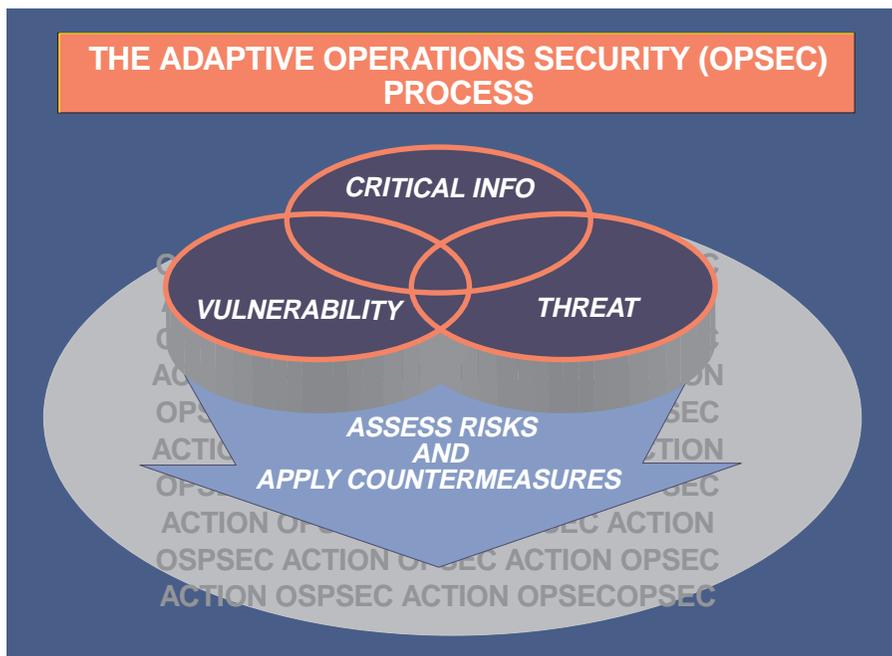


Figure III-2. The Adaptive Operations Security (OPSEC) Process

c. OPSEC Action 3 — Analysis of Vulnerabilities

“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
The Art of Modern War, 1940

- 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.
- Continuing to work with the intelligence and counterintelligence staffs, **the operations planners seek answers to the following questions:**
 - 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?
 - What indicators can the adversary actually collect?
 - 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?)
- See Appendix C, “OPSEC Indicators,” for a detailed discussion of OPSEC indicators.



When conducting joint operations, all personnel must understand the adversary's intelligence collection capabilities and take action to deny the use of those capabilities.

d. OPSEC Action 4 — Assessment of Risk

- 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.

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

- **OPSEC measures can be used to:**

- (1) Prevent the adversary from detecting an indicator;
 - (2) Provide an alternative analysis of an indicator; and/or
 - (3) Attack the adversary's collection system.

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

- **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, "Operations Security Measures," provides examples of OPSEC measures.

- **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.

- **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.

• **Typical questions that might be asked when making this analysis include the following:** (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?

• **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.

• **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, military 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**

- 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.
- 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 that 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.



A key action during the OPSEC process is to analyze potential vulnerabilities to joint forces.