



Operationalizing OPSEC

By Marc J. Romanych, Major, USA (Retired) and Robert Cordray III
1st Information Operations Command (Land)

Editorial Abstract: Dispelling myths and taking an operational perspective, 1st IOC's Marc Romanych and Robert Cordray describe the purpose of OPSEC and how it can be more effective through its integration with other IO capabilities.

Operations security (OPSEC), as a core capability of information operations (IO), is an enigma. The OPSEC process does not readily fit with staff planning processes, OPSEC's methodology is couched in non-operational terminology, and OPSEC procedures and practices are rooted in a programmatic focus that lacks relevancy to deployed forces. As a result, while joint force commanders and staffs readily accept the need for OPSEC, their understanding of OPSEC's practical contribution to the conduct of combat operations is inadequate.

The confusion begins with the purpose of OPSEC. Unfortunately, OPSEC is frequently mistaken for the control of information distribution or the protection of classified information and, therefore, is confused with security disciplines such as communications security (deny unauthorized access to telecommunications), physical security (prevent unauthorized access to equipment, installations, material, and documents), and computer security (unauthorized access and exploitation of computer systems).¹ As a result, OPSEC is now entangled with administrative security programs at the expense of protecting indicators associated with military operations. Furthermore, even in the field, OPSEC is focused more on programmatic inspections and awareness training than ongoing and planned

operations. This becomes particularly evident when trying to integrate OPSEC into information operations (IO).

While this article cannot solve OPSEC's woes, it can provide a view of OPSEC that helps IO practitioners integrate OPSEC into an information operation. This is not to discount the importance of those procedural programs that seek to limit public disclosure of information in garrison environments, but the integration of OPSEC into something larger than itself. Information operations, or better yet, joint force operations, are needed if the U.S. military is going to achieve information superiority over its adversaries. This article discusses how, from an operational perspective, OPSEC can contribute to the joint force commander's objectives.

What is OPSEC's Purpose?

"OPSEC is frequently mistaken for the control of information distribution or the protection of classified information"

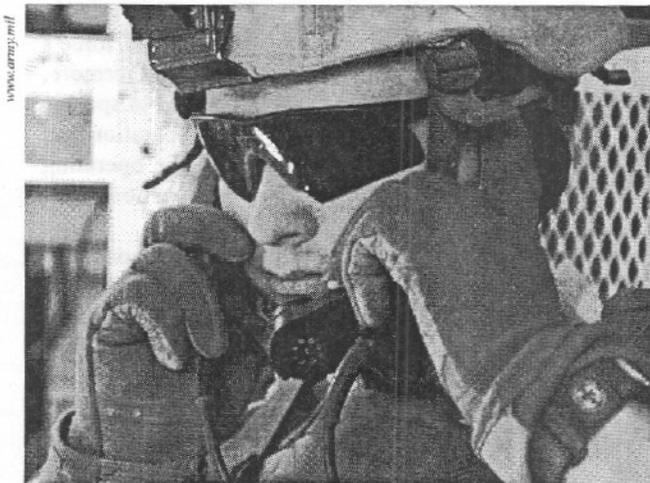
Joint doctrine defines OPSEC in terms of a methodology:

"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 that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation."²

The last part of the definition loosely describes OPSEC's purpose: "eliminate or reduce, to an acceptable level, the vulnerabilities of friendly actions to adversary exploitation." Friendly actions generate indicators (i.e., detectable actions and open source information³) which can be collected and developed into critical information (i.e., specific facts about friendly intentions, capabilities, and activities⁴). Critical information can then be used by an adversary to plan and execute its own operations.

Stated a different way, critical information is derived from the aggregation of indicators resulting from the observation or detection of friendly force activity. Thus, the broad purpose of OPSEC is to control and protect those physical indicators (i.e., actions) that can lead to loss of critical information about the friendly force.⁵



A soldier joins radio traffic in a Stryker vehicle while on patrol near Mosul, Iraq.



An Army Captain from the Civil Affairs Office of the 155th Brigade Combat Team briefs his soldiers on the route their convoy of Humvees will take to inspect construction progress of the Mishkub Policy Station near Najaf, Iraq.

Essential Secrecy

Central to the role of OPSEC is the concept of “essential secrecy.” By doctrine, essential secrecy is “the condition achieved from the denial of critical information to adversaries.”⁶ By achieving essential secrecy, military forces protect their intentions, capabilities, and activities in order to retain initiative and the element of surprise for operations. As a condition, essential secrecy is not static—it must first be developed and then maintained as the situation and mission evolves.

Essential secrecy is concerned about the content and flow of critical information. Military forces seek critical information about their opponents for the purpose of fulfilling their own information needs. To do this, they attempt to collect accurate, timely, relevant information, process it, and disseminate it for use in planning and directing operations. Conversely, if a military force is to prevent an adversary from gaining useful information it can use, then it must prevent the flow of critical information from friendly to adversary forces.

Every command and every operation has a tremendous amount of information, both classified and unclassified, that must be protected. However, as pointed out in joint doctrine, “denying all information about a friendly operation or activity is seldom cost effective or realistic.”⁷ Essential secrecy cannot be achieved

everywhere all the time and, therefore, the protection of information must be focused and prioritized to counter specific threats.

Essential secrecy, or the protection of critical information, is not the exclusive responsibility of OPSEC. It is the result of mutually supportive OPSEC and security programs. OPSEC’s role is to prevent, or at least limit, the flow of sensitive, unclassified information to adversary forces. The actual content of the information, whether classified or unclassified, is the responsibility of information security program controls and procedures.

From Essential Secrecy into Operational Objectives

While the essential secrecy is a useful framework for integrating OPSEC and other security programs, the concept must to be translated into doctrinal terminology that operationalizes OPSEC. If appropriately framed, OPSEC’s contribution will be better understood by the commander and staff, thereby increasing the likelihood it will receive command emphasis.

The basis for OPSEC’s contribution to an operation is the commander’s objectives for IO.⁸ This means that for OPSEC to be part of an information operation, at least one IO objective should address the protection or defense of friendly information. To this end, the concept of essential secrecy translates nicely into an IO objective.

IO objectives define the effects that IO seeks in the battlespace. Achieving these effects requires the synchronization of multiple disciplines. Because OPSEC is not the sole contributor to essential secrecy, an IO objective can integrate other capabilities such as deception, physical security, information security, and counterintelligence that are not habitually related to OPSEC. For example, an objective for a combat operation could be:

Deny the enemy force information about the time and place of the main attack in order to achieve surprise at the start of offensive operations.

For stability operations an objective could be:

Deny civilian populace information about basecamp force protection measures IOT prevent interference with security operations.

Converting Measures into Tasks

To execute successfully, OPSEC must clearly articulate what the joint force should do to deny the flow of information from friendly to adversary forces. Doctrine states that the OPSEC staff develops and executes OPSEC measures to address identified indicators. However, even though OPSEC measures are directive in nature, the likelihood of implementation is greatly increased if the planned measures are written as tasks.⁹ Military forces are task-centric, often defining their missions by the specified and implied tasks that they must execute. Because OPSEC measures do not follow any doctrinal format familiar to a conventional joint planner, writing measures directly into orders risks having OPSEC overlooked or ignored.

Developing OPSEC tasks is a balance between cost and resources, in terms of time, personnel, assets, or interference with operations. By doctrine, a risk management process is used to determine OPSEC priorities. While this may be useful in a programmatic setting, the best way to support the operations of joint forces is to develop tasks that support the identified IO objectives as well as protect and control the specific indicators associated with the force’s key operational tasks. Furthermore, OPSEC tasks should be tied to specific places and times in the operation and carefully adapted to fit the operating characteristics of each subordinate command or element.

Tasks turn OPSEC measures into specified actions. A useful planning format is: *task* (the specific action to be performed), *purpose* (why the task must be performed), and *method* (what means or method will execute the task). In general, for OPSEC, a task is an action that controls or protects observable activities, a purpose can be critical information requiring protection, and

a method is the OPSEC means or methods used to execute the task. An example OPSEC task that supports combat operations is:

- Task: Jam enemy ground surveillance radars
- Purpose: Conceal movement of combat elements from electronic collection

- Method: Screen jamming

An example OPSEC task to support stability operations is:

- T: Deny civilian populace access to basecamp overwatch sites
- P: Prevent line-of-sight observation of security activities
- M: Unit patrols, local police

When developing tasks, it is important to consider that although the purpose of OPSEC is a constant, its focus may change by echelon. At the tactical level, OPSEC prevents adversary detection and identification of friendly activities and operations in order to prevent the targeting of critical assets and countering of current activities and operations. Operational-level OPSEC prevents the disclosure of intentions, capabilities, and future operations (i.e. courses of action) in order to avoid the compromise of planning and operations. To a large extent, operational-level OPSEC consists of broad guidance or general measures for the entire force and new measures to counter adversary intelligence capabilities.

Conclusion

In concert with other security programs, OPSEC contributes to a force's essential secrecy, or denial of critical information to the adversary. Defining essential secrecy for an operation as an IO objective can integrate and synchronize various security disciplines and programs to achieve a single purpose for the joint force commander. Similarly, tactical tasks execute identified doctrinal OPSEC measures that turn essential secrecy into an operational advantage for the joint force commander. Clearly though, the concept of essential secrecy demands additional scrutiny to define and establish its utility to joint force IO, OPSEC, and other security disciplines.

"In concert with other security programs, OPSEC contributes to a force's essential secrecy, or denial of critical information to the adversary."

At its core, OPSEC is an approach to conducting operations. Recent experiences with fielded forces have shown OPSEC relegated to a programmatic role with limited command influence. More effort needs to be placed to get OPSEC back in its rightful place—supporting joint forces by controlling and protecting physical actions, signatures, and indicators. Although tactical and operational level OPSEC may differ in focus, their purpose remains constant—the control and protection of friendly indicators that can lead to loss of critical information about the friendly force.

Authors' biographies can be found at the end of their Feature article in this journal, entitled: "Mapping the Information Environment."

Endnotes

¹ OPSEC was not intended to replace security programs such as physical, information, and security that protect classified information. OPSEC was created to support operational effectiveness by denying openly available indicators of sensitive or classified activities, capabilities, or intentions to adversaries. JP 3-54, *Joint Doctrine for Operations Security*, states that "OPSEC is an operations function, not a security function," and that "OPSEC planning must be done by operations planners."

² Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*.

³ The complete joint definition of an OPSEC indicator is "friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information."

⁴ The complete joint definition of critical information is "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."

⁵ Arguably, the protection of open source information is the primarily the role of command security programs.

⁶ Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*. Unfortunately, the concept of essential secrecy receives minimal attention in joint doctrine.

⁷ JP 3-54, page II-2.

⁸ This is so stated in JP 3-54, page vi.

⁹ In general, there are two basic types of OPSEC measures – passive and active. Passive measures, the means and methods to protect the true status of friendly activities and operations, include the concealment and camouflage of operating patterns and other recognition factors. Active measures, the means and methods to prevent observation or surveillance, include countermeasures to defeat specific adversary intelligence collection capabilities, and deceptive activities such as demonstrations and feints to present false indicators and signatures. Categorizing OPSEC measures as either active or passive is useful for planning measures during phases of an operation when mission constraints and rules of engagement prohibit active contact or engagement of the enemy. ☺



The effectiveness of any OPSEC program ultimately rides on each member of the organization. Here, a soldier calls for air support during an exercise near Bagram, Afghanistan.