INFORMATION-RELATED CAPABILITIES: OPERATIONS SECURITY

Last Updated: 28 April 2016

Operations security (OPSEC) is defined as "a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities."[1] OPSEC denies adversaries critical information and observable indicators about friendly forces and intentions. OPSEC identifies any unclassified activity or information that, when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities. A critical information list should be developed and continuously updated in peacetime as well as conflict. The critical information list helps ensure military personnel and media are aware of non-releasable information.

The information operations (IO) team enables the OPSEC planner to maintain situational awareness of friendly information and actions and to assist other air operations center planners in incorporating OPSEC considerations during the planning process. Once the OPSEC process identifies vulnerabilities, other information-related capabilities (e.g., military deception, military information support operations, electronic warfare, cyberspace operations) can be used to ensure OPSEC requirements are satisfied.

---

[1] JP 3-13.3, *Operations Security*.