

electronic reconnaissance and electronic intelligence operations. There are four VMAQs (designated VMAQ-1 through VMAQ-4) assigned to MAG-14, 2d MAW, Cherry Point, NC. Each squadron has five EA-6B Prowler aircraft.

Responsibilities

EW is the responsibility of the G-3/S-3. An EWO is normally appointed who is responsible for planning, coordinating, and tasking EW operations and activities. Other responsibilities include the following:

- Coordinate with the G-2/S-2 to establish priorities between EW and signals intelligence missions.
- Coordinate with the G-6/S-6 to facilitate maximum use of the electromagnetic spectrum through electronic protection and minimizing electromagnetic interference.

The Electronic Warfare Coordination Cell/ Information Operations Cell

The electronic warfare coordination cell (EWCC) is a dedicated EW planning cell that may be established to coordinate EW activities. The IO cell may perform functions of the EWCC if one is established.

The MAGTF commander will normally plan, synchronize, coordinate, and de-conflict EW operations through the EWCC or an IO cell. Each facilitates coordination of EW operations with other fires and communications and information systems. These centers coordinate efforts by the G-2/S-2, G-3/S-3, and G-6/S-6 to eliminate conflicts between battlespace functions. The EWCC or IO cell is under staff cognizance of the G-3/S-3. Assigned personnel identify and resolve potential conflicts in planned operations. The EWCC or IO cell includes an EWO, a communications and information systems representative, and other liaison officers as needed. Liaison

could include RadBn representation, airborne electronic countermeasures officers, a Marine air control group radar officer, and other Service representatives.

MAGTF staffs will provide personnel to incorporate an EWCC or IO cell with the Marine Expeditionary Force (MEF) G-3/S-3. Personnel will also be provided for liaison teams to higher headquarters EW coordination organizations when required, such as the joint commander's electronic warfare staff (JCEWS) or JTF IO cells created by JTFs.

Electronic Warfare and the Operation Order

Tab B to Appendix 3 (IO) of Annex C (Operations) of the OPORD is the EW tab. It details specific EW tasks to be performed and specifies coordinating instructions for the control and management of EW missions.

Specific instructions for SIGINT is contained in Appendix 2 to Annex B (Intelligence). Defensive information warfare operations (IW-D) are contained in Tab G to Appendix 3 (IO) of Annex C (Operations). IA activities are contained in Appendix 1 to Annex K (Communication and Information Systems).

Operations Security

Description

OPSEC is the key to information denial. It gives the commander the capability to identify indicators that can be observed by adversary intelligence systems. These indicators could be interpreted or pieced together to derive critical information regarding friendly force dispositions, intent, and/or COAs that must be protected. The goal of OPSEC is to identify, select, and execute measures that eliminate or reduce indications and other sources of information, which may be exploited by an adversary, to an acceptable level.

Definition

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to (1) identify those actions that can be observed by adversary intelligence systems; (2) 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 (3) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

Operations Security in Support of the Offense

Although primarily associated with defensive measures, OPSEC contributes to the offense by depriving the enemy of information—slowing the enemy's decision cycle thereby providing opportunity attainment of friendly objectives.

Operations Security in Support of the Defense

The overall goal of OPSEC is denial and the establishment of essential secrecy. The key element that OPSEC protects is the commander's concept of operation. A good OPSEC plan denies information to the enemy intelligence system, reducing its ability to orient combat power against friendly operations.

The Operations Process

OPSEC planning is accomplished through the OPSEC process. The OPSEC process has the following five distinctive steps that provide a framework for the systematic identification, analysis, and protection of information necessary to maintain essential secrecy. (See JP 3-54, *Operations Security*)

- Identification of critical information.
- Analysis of threats.
- Analysis of vulnerabilities.
- Assessment of risk.
- Application of appropriate OPSEC measures.

Responsibilities

The G-3/S-3 has primary responsibility for OPSEC. Normally, an OPSEC officer is appointed and is responsible to the G-3/S-3 for OPSEC planning and oversight. In joint operations, an OPSEC working group may be established to recommend OPSEC measures, coordinate or conduct OPSEC surveys, and write the OPSEC portion of the OPORD.

Operations Security Support Agencies

Counterintelligence/Human Intelligence Teams

CI/human intelligence (HUMINT) teams perform a wide range of duties such as security briefings, countersabotage, counterespionage, and countersurveillance inspections. CI measures enhance security, aid in reducing risks to a command, and are essential in achieving operational surprise during military operations. CI can provide a significant contribution to a unit's OPSEC program. CI personnel can support a command's OPSEC program by the following:

- CI surveys.
- Physical security evaluations.
- Security inspections.
- Vacated command post inspections.
- Penetration inspections.
- Security education.

There is a CI/HUMINT company located within the intelligence battalion. (See MCWP 2-14, *Counterintelligence*)

Imagery Interpretation Platoon

These units interpret overhead imagery and explain the signature that a unit reveals to adversary imagery systems. This type of product requires coordination through the G-2/S-2 and sufficient lead-time to obtain. A comprehensive OPSEC plan would ideally incorporate friendly imagery support to assist in the maintenance and improvement of OPSEC measures.

Naval Criminal Investigative Service

The Naval Criminal Investigative Service (NCIS) operates a worldwide organization to fulfill the investigative and CI responsibilities of the Department of the Navy. Within this charter, the NCIS has exclusive jurisdiction in matters involving actual, potential or suspected espionage, sabotage, and subversion including defection. In a combat environment, this CI jurisdiction is assigned to Marine CI, assuming that NCIS assets are not locally available.

Operations Security and the Operation Order

Tab C (OPSEC) to Appendix 3 (IO) of Annex C (Operations) of the OPORD is the OPSEC tab. This tab implements the recommended COA for OPSEC. It details specific OPSEC tasks to be performed and specifies coordinating instructions for the control and management of OPSEC tasks.

Psychological Operations

Description

At the strategic level, PSYOP may take the form of political or diplomatic positions, announcements or communiques. At the operational level, PSYOP can include the distribution of leaflets, radio and television broadcasts, and other means of transmitting information that provides information intended to influence a selected group. It may be used to encourage enemy forces to defect, desert, flee, surrender or take any other action beneficial to friendly forces. At the tactical level, PSYOP include face-to-face contact and the use of loudspeakers or other means to deliver PSYOP messages. PSYOP shape attitudes and influence behavior. The mere presence of Marine Corps forces may be a PSYOP activity in itself, bringing influence on a situation through a display of purpose. PSYOP may support military deception operations.

Definition

Psychological operations are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. (JP 1-02). See also MCWP 3-40.6 (formerly FMFM 3-53), *Psychological Operations*.

Psychological Operations Integration

PSYOP is only one of the means available to influence enemy attitudes and behaviors. IO must broadly coordinate PA (the delivery of the truth), OPSEC (protection of friendly critical information), concealment and deception (creation of misleading perceptions), along with PSYOP (influencing people by conveying selected information).

Organization

The Marine Corps has no dedicated PSYOP units. If requested, external PSYOP support may be provided by the US Army's 4th Psychological Operations Group (POG).

Employment

During peacetime, PSYOP activities that support combatant commanders take the form of overt peacetime PSYOP programs. These programs are proposed by combatant commanders through the chairman of the joint chiefs of staff who, in turn, refers them to the assistant secretary of defense for special operations and low intensity conflict for review and approval. During contingencies, a PSYOP concept plan that is broad in scope is forwarded from the combatant commander to the joint staff for approval of overarching themes, objectives, and guidance, but not products. Once the concept plan is approved, a more detailed theater PSYOP plan is developed.