Appendix C

COUNTER-IMAGERY INTELLIGENCE TECHNIQUES AND PROCEDURES

C-1. **General.** The proliferation of imagery systems worldwide, especially the platforms carrying imagery systems, makes the task of the C-IMINT analyst much more complicated than ever before. Relatively inexpensive platforms that are easily transported and operated, such as unmanned aerial vehicles, are becoming available to anyone who wants to employ them. For the more sophisticated, there are other platforms either continuously circling the planet or in geosynchronous orbit, available for hire by anyone with the desire and the ability to pay the freight. An adversary need not possess the technology to build and launch such a platform. He merely buys time from the operators of the platform and obtains the products acquired during his allotted time. Like all other CI functions, C-IMINT depends on the analyst knowing the adversary and knowing ourselves. It begins long before friendly forces deploy for any operation and continues throughout the operation. It goes on even after our forces return to their home station after completion of the operation.

C-2. **Operations.** C-IMINT begins with knowledge. The MDCI analyst must have a thorough knowledge of the threat in the objective area and any threat from outside the AO that may influence our operations.

a. **Predeployment.** Prior to any operation, the MDCI analyst needs to prepare indepth. In addition to researching data on the threat and the AO, the MDCI analyst gathers information and builds a database to serve C-IMINT in the coming operation. During this phase, the MDCI analyst initiates quick reference matrices and the IMINT situation overlay.

(1) Adversary intelligence flight matrix. These matrices are concerned with other platforms used by the adversary. Tracking these collection systems continuously allows the analyst to analyze threat IMINT collection patterns.

(2) System component quick reference matrix. These matrices are concerned with adversary system's capabilities and processing times. This file is part of the database which equates to an OB file on threat IMINT systems shown in Figure C-1.

(3) IMINT situation overlays. These are the paths of adversary intelligence collection flights depicted on the friendly operations graphics. They identify areas susceptible to collection.

b. Friendly patterns. Pattern analysis is the detailed study of friendly activities to determine if a unit performs the activities in a predictable manner, thus creating a monitorable pattern of activity. These actions cue an observer to a unit's type, disposition, activity, and capability. Imagery coverage of the AO is essential for planning and for reference later during operations. Small or intermediate scale imagery covering the entire AO may be obtained from general reference files or national sources and need not be newly flown. The presence of US reconnaissance aircraft making numerous passes over territory belonging to another nation would

tip off an impending operation. Therefore, file imagery or imagery obtained by satellite may be the only reference available.

SYSTEM COMPONENT QUICK-REFERENCE MATRIX					
SYSTEM: _____		DATE: _____			
ORGANIZATION	LOCATION	CHARACTERISTICS	STRENGTH	TACTICS	REMARKS

Figure C-1. System component quick-reference matrix.

(1) Friendly IMINT is used, when available and of high enough priority, to determine friendly patterns which may be susceptible to IMINT collection. These patterns are key indicators to the enemy of specific operational activities. Patterns usually occur because of a unit's SOP and doctrine. Example patterns include—

(a) Relocating fire support units forward before an attack.

(b) Locating TOCs in the same relative position to maneuver elements and to each other.

(c) Repeating reconnaissance overflights of areas planned for ground or air attack about the same time before each operation.

(2) Information gained from imagery provides a means of checking other reports and often produces additional detailed information on a specific AI. All friendly activities thus need to be examined collaterally with imagery of a particular area. Imagery can provide confirmation of installations, lines of communications, and operational zones. SLAR, for example, can detect night movements of watercraft.

(3) Finally, in the overall evaluation, analysts synthesize the separate trends developed during analysis. Such a process identifies the possible compromise of an existing element, activity, or characteristic based on logical relationships and hypotheses developed by analysis. The pattern analysis technique is just one of many techniques designed to help evaluate friendly units for vulnerability to threat IMINT. The process is a continuous one.

(4) Analysis of a unit's movements gives significant clues to its intentions, capabilities, and objectives. By-applying this technique against our own units, analysts can identify

vulnerabilities. Movement analysis forms an important step in the identification and recommendation of countermeasures.

(a) SLAR is a primary sensor in detecting moving targets or moving target indicators (MTIs) and is usually associated with the special electronics mission aircraft and Joint STARS platform. While the sensor is primarily focused at enemy MTIs, it can be used to identify friendly movement patterns that may also be collected by the enemy.

(b) The tracks created by a unit can give excellent indication of a unit's disposition. Any time a unit moves away from hard packed roads, the danger of leaving track signatures is very high. There are certain countermeasures which should be observed to disguise or eliminate these signatures:

1 Conceal tracks by netting or other garnish.

2 Disperse turnouts near CPs.

3 Place installations and equipment near hard roads where concealment is available.

(c) Our IMINT resources can determine the effectiveness of a friendly unit's program to suppress its visual and thermal signatures, including positioning of assets. Friendly aerial reconnaissance is extremely limited and must be planned for well in advance. The following are examples of countermeasures that could be used to reduce our vulnerability to enemy IMINT:

1 Using traffic discipline when moving into and out of the installation. This may require walking some distance to a CP.

2 Driving in the tree lines when roads are not available.

3 Extending new roads beyond the CP to another termination.

4 Controlling unauthorized photographic equipment.

5 Using physical security measures to prevent optical penetration.

6 Using proper camouflage procedures.

7 Limiting the dissemination of photographs made from within the installation.

8 Avoiding the use of direction signals and other devices which provide information.

9 Concealing equipment markings.

10 Preventing detection by infrared imaging (nets, infrared generators).

11 Eliminating open-air storage of special equipment, raw materials, and telltale objects.

(d) The key to proper positioning of assets on the ground is to use natural features as much as possible. Obvious locations such as clearings may be more convenient but should be avoided at all costs. This includes night operations. Infrared and SLAR missions are particularly effective at night. Units should be well dispersed since a high concentration of tents and vehicles, even well hidden, will stand out on imagery to a trained analyst.

c. Evaluation of countermeasures. For these countermeasures to be effective, every command should develop a self-evaluation system to ensure proper employment.