Chapter 5

COUNTERINTELLIGENCE ANALYSIS AND PRODUCTION

GENERAL

Analysis and production is the heart of intelligence. No matter what quality and quantity of information is gathered, it does absolutely no good if the information is not turned into intelligence and disseminated to the commander in time for him to use it in the decisionmaking process. The same is doubly true of CI. CI agents, interrogators, and MDCI analysts work in teams to gather information, process it into intelligence, put it into products usable at all levels, and disseminate it in time to keep our commander's decision time inside the decision time required by an adversary.

CI analysis and production is focused on three well-defined FIS activities: HUMINT, SIGINT, and IMINT. The process of countering each of these disciplines involves a threat assessment, vulnerability assessment, development of countermeasures options, countermeasures implementation, and countermeasures evaluation. These are referred to as the five-step CI process. (See Section II through Section V of Appendix B.) But they are more than that.

- While each step is a product, it is also a process. Each step can stand alone, yet each depends upon the other for validity. Once begun, the five-step CI process becomes cyclic. The cyclic process does not end, for within each step is the requirement for continuous updating of the CI database. This is necessitated by any new information reflecting change in either the FIS posture, the friendly posture, or both.
- Because FIS activities involve collection, analysis, and production and are themselves multidisciplined, efforts to counter FIS activities will likewise be multidisciplined and will require collection, analysis, and production in order to be successful. The analyst will be able to produce a truly multidisciplined product only if collection is productive.
- Collection is a single discipline function and the attendant initial analysis is likewise a single discipline. The fusion and refined analysis of individual disciplines occurs at various echelons of command, specifically the ACE at theater, corps, and division and at the Army CI Center, 902d Ml Group, Fort Meade, MD.

CI analysis is by no means exclusive to Army agencies, but is a crucial activity of DOD. CI analysis is performed at the Defense Intelligence

Agency (DIA), as well as other federal agencies such as the Central Intelligence Agency (CIA), FBI, and the National CI Center. CI analysis must be performed by highly trained, experienced, and skilled analysts using the latest technology and modern methods of planning and directing, processing, producing, and disseminating.

C-HUMINT:

HUMINT analysis focuses not only upon the FIS entity or entities operating in the area but also upon the intelligence product most likely being developed through their collection activities. The analytical effort should attempt to identify the FIS HUMINT cycle (collection, analysis, production, targeting) and FIS personalities. To produce a complete product, the MDCI analyst may need access to considerable data and require significant resources. The MDCI analyst will require collection in the areas of subversion, espionage, sabotage, terrorism, and other HUMINT supported activities. Collection of friendly data is also required to substantiate analytical findings and recommendations. Consistent with time, mission, and availability of resources, efforts must be made to provide an analytical product that identifies FIS efforts.

C-SIGINT:

SIGINT like C-HUMINT focuses upon the FIS entities which can collect on friendly forces. It also focuses on the intelligence which is most likely being collected. Also like C-HUMINT and C-IMINT, any C-SIGINT analysis effort should be fully automated (data storage, sorting, and filing). The MDCI analyst requires SIGINT data collection to support vulnerability assessment and countermeasures evaluation. Validation of vulnerabilities (data capturable by FIS SIGINT) and the effectiveness of implemented countermeasures (a before and after comparison of electromagnetic signatures and data) will be nearly impossible without active and timely collection as a prerequisite to analysis. The MDCI analyst requires a comprehensive, relational database consisting of FIS SIGINT systems, installations, methodology, and associated SIGINT cycle data. In addition, all friendly C-E systems and user unit identification must be readily available, as well as a library of countermeasures and a history of those previously implemented countermeasures and results. Ideally, the MDCI analyst should, at any given time, be able to forecast FIS SIGINT activity. However, such predictions must rely upon other CI, interrogator, SIGINT, and IMINT collection as well as access to adjacent friendly unit CI files. Information on FIS SIGINT must be readily accessible from intelligence elements higher as well as lower in echelon than the supported command.

C-IMINT:

IMINT requires the analyst to have an indepth knowledge of the supported commander's plans, intentions, and proposed AO as far in advance of commitment as possible. The analyst must have access to all available data and intelligence on FIS IMINT methodology, systems, and processing

as well as indepth information on commercial satellite systems and their availability to the foreign consumer. The analyst attempts to define the specific imagery platform deployed against US Forces and the cycle involved (time based) from time of imaging through analysis to targeting. Knowledge of FIS intelligence cycle to targeting is critical in developing countermeasures to defeat, destroy, or deceive FIS IMINT. For ground-based HUMINT oriented IMINT (video cassette recorders [VCRs], cameras, host nation curiosity, news media organizations) the CI team will be required to collect the data for the analyst. This type of information cannot be reasonably considered to exist in any current database. Traditional FIS IMINT data is readily available and should not require any CI collection effort. However, collection to support CI (overflights of friendly forces by friendly forces) during identified, critical, and IMINT vulnerable times will validate other CI findings and justify countermeasures. This "collection" will be of immense value to the analyst and the supported commander in determining what, if anything, FIS imagery has captured. It must be done within the established or accepted FIS activity cycle.

The CI analyst uses the tools and skills identified in this chapter and in FM 34-3. The intelligence analyst focuses on "how we see the opposition"; the MDCI analyst focuses on this and "how the opposition sees us." The MDCI analyst must also focus on how to counter the opposition's collection efforts. Where the intelligence analyst is a subject matter expert on the opposition, the MDCI analyst, in addition to having an indepth understanding and expertise on foreign intelligence collection capabilities, must have a good working knowledge of our own force. The CI analysis assets of the ACE must be fully integrated into the ASAS as well as the single-source C-HUMINT processor. They require access to all-source data that is applicable to CI analytical products.

The principles and techniques identified in FM 34-3 apply equally in CI analysis. This chapter focuses specifically on the application of analysis on CI matters.

CI ANALYSIS

The CI and C-HUMINT multidiscipline assets of the ACE are under the staff supervision of the G2 at theater, corps, and division levels. Theater ACE staffing is provided from the operations battalion of the theater MI brigade. Corps ACE staffing is provided from the corps MI brigade headquarters and operations battalion. Division ACE staffing is provided by personnel assigned to the headquarters company of the divisional MI battalion. In addition to CI personnel, an all-source mix of single discipline analysts is sometimes required for interpretation to produce the CI analytical products required by the commander at each echelon. CI products are also critical to the function of the G3 OPSEC and deception cells as well.

The CI mission is a diverse and all-encompassing CI analytical effort. MDCI analysts perform the following functions:

- Analyze the multidiscipline intelligence collection threat targeted against friendly forces.
- Assess opposition intelligence collection threat vulnerabilities and susceptibilities to friendly deception efforts.
- Support friendly vulnerability assessment.
- Develop, evaluate, and recommend countermeasures to the commander. These countermeasures reduce, eliminate, or take advantage of friendly force vulnerabilities.
- Support rear operations by identifying collection threats to rear area units and installations, to include low-level agents responsible for sabotage and subversion.
- Nominate targets for exploitation, neutralization, or destruction.
- Develop and maintain a comprehensive and current CI database.
- Identify information gaps in the form of intelligence requirements and provide requirements to the collection management element. This element will task collection missions to the appropriate supporting MI element or request information from higher echelons.

Specific responsibilities pertaining to analysis of FIS use of HUMINT, SIGINT, and IMINT follow:

- C-HUMINT analysis includes—
  - — Analyzing and assessing the espionage, terrorism, subversion, treason, sedition, and sabotage threats.
  - — Analyzing enemy HUMINT collection capabilities and activities, and further analyzing how those collection capabilities can affect the friendly command.
  - — Analyzing Level I threats such as enemy controlled agents or partisan collection, and Level II threats such as diversionary and sabotage operations conducted by unconventional forces.
  - — Recommending countermeasures and deception.
  - — Nominating targets for exploitation, neutralization, or elimination.

C-SIGINT analysis includes—

- Analyzing and assessing foreign SIGINT collection capabilities and activities.
- Comparing opposition collection systems capabilities against friendly targets.
- Identifying, analyzing, and assessing friendly electronic patterns and signatures.
- Analyzing friendly vulnerabilities against foreign SIGINT collection efforts.
- Recommending countermeasures and deception.
- Nominating enemy SIGINT targets for exploitation, neutralization, or destruction.

C-IMINT analysis includes—

- Analyzing and assessing adversary imagery collection capabilities and activities, to include ground, air, and space systems. Threat systems include anything from hand-held cameras to satellite platforms, or fixed or rotary-wing aircraft and unmanned aerial vehicles (UAVs). The assessment should include adversary access to commercial satellite imagery and the ability to properly analyze the imagery.
- Measuring enemy collection systems against friendly targets.
- Identifying, analyzing, and assessing friendly patterns, signatures, and vulnerabilities for subsequent development and recommendation of countermeasures and deception.
- Nominating opposition IMINT systems for exploitation, neutralization, or destruction.

Other intelligence support to CI analysis cannot be conducted without the support of all three intelligence disciplines—HUMINT, SIGINT, and IMINT. These disciplines collect critical information on adversary collection, analysis, and dissemination systems. Analysts extract information from the all-source database within the ACE to determine adversary collection capabilities and operations. These systems, coincidentally, collect a great deal of intelligence on friendly forces. This intelligence is vital in evaluating friendly profiles and thereby determining their vulnerabilities. If the situation warrants, we can task friendly collection systems to specifically collect

information on friendly forces for the MDCI analysts through the collection management team.

The CI mission mandates a wide range of functions and tasks that are accomplished in peace and at all intensities of conflict. CI operational activities perform such functions as investigations, operations, and collection. Their products are of great value to the MDCI analyst. MDCI analysts work with CI teams and the collection management team in the ACE, and maintain rapport with operational CI and interrogation personnel in the AO in order to obtain information from all echelons.

CI ANALYSIS TARGET NOMINATIONS

The G2 nominates targets that enable the commander to exploit, neutralize, or destroy the enemy. The ability to recommend target nominations to the G2 is one of the most important contributions of the CI interrogator or CI teams.

The CI team develops target nominations by using MDCI products developed in the analytical process. Target nominations are coordinated through the single-source analysis section and all-source intelligence section for inclusion on the G2's list of high-value targets (HVTs). The commander, G3, G2, and fire support coordinator comprise an informal targeting team that develops the high-payoff target (HPT) list from the list of HVTs through the wargaming process. HPTs are those that must be acquired and attacked in order to ensure success of friendly operations. Approved targets are listed in CI threat assessments and briefings, in accordance with the unit SOP. The G2 or G3 disseminates decisions concerning actions to be taken with regard to targets. For detailed information on the operations of the ACE, see FM 34-25-3. For more information on the targeting process, see FM 6-20-10.

The commander directs that HPTs be countered in three ways-exploitation, neutralization, or destruction. Targets for exploitation are monitored for their value to friendly operations. Targets for neutralization may be isolated, damaged, or otherwise rendered ineffective so they cannot interfere with the success of friendly operations. Targets for destruction are killed.

Exploited targets can assist commanders in securing their forces and operations; and identifying windows of operational risk, areas of operational risk, and windows of operational advantage. Exploited targets can be a combat multiplier. Exploitation should be used when the opposition element or resource can be manipulated, controlled, or in some other manner used to the advantage of the friendly force. This usually occurs

when the identity, capability, location, and intentions of the target are known. Key considerations in nominating targets for exploitation include—

- Friendly forces' ability to deceive, control, or manipulate the target.
- Neutralization or destruction which is not possible or practical.
- Exploitation which will benefit friendly forces.
- Benefits to the friendly force which outweigh neutralization or destruction.

Targets should be neutralized when the opposition elements or resources are known and located by the friendly force, and can be rendered ineffective. Actions taken to neutralize targets can be offensive or defensive measures which prevent the opposition from achieving its objective. Usually, destruction or elimination of these targets is neither possible nor practical.

Key considerations in nominating targets for neutralization include—

- Friendly forces' inability to destroy or eliminate the target.
- Knowledge or ability to know the target's location, identity, capability, and intentions.
- Friendly operational activities and resources targeted by the opposition.
- Ability of friendly forces to neutralize the target.

Targets which may be considered for neutralization are—

- Targets which can be effectively jammed.
- Targets which can be isolated from their objectives through the use of physical obstacles, including barriers, friendly maneuver, and entrapment.
- Known opposition collectors against which friendly force countermeasures can be implemented.

Countermeasures developed to neutralize a target are specific measures in addition to OPSEC measures. This may include moving a tactical operations center (TOC) during a known window of advantage; working with the G4 to redesignate main supply routes based on a known threat; and recommending barrier locations to engineers. Remember, nominating targets for destruction or elimination is almost always preferable to

nominating targets for neutralization or recommending actions to neutralize targets—provided destruction of the target is practical.

Destruction or elimination of targets. These targets are battalion size or smaller, which the friendly force can destroy or render combat ineffective or render intelligence collection ineffective. Usually, the identity, capability, intentions, and locations are known. Targets which may be recommended for destruction include—

- Bases of airborne reconnaissance units.
- Hostile intelligence services operatives, saboteurs, and terrorists.
- Base camps for opposition unconventional warfare forces either in friendly or opposition territory.
- Special purpose forces.
- The entire spectrum of enemy intelligence collection, analysis; and dissemination systems, including critical enemy command posts (CPs).

MP, special reaction forces, attack helicopters, field artillery, tactical air, or infantry can destroy targets. When nominating for destruction targets which are located behind friendly lines, the analyst must consider the risk to friendly forces in making the recommendation. Exact CI analysis, fully coordinated with the G3, is essential. If all the necessary information for destruction of the target with minimal risk to friendly forces is not available, it may be better to recommend neutralization of the target. Consider:

- The ability of friendly forces to destroy the target without undue risk.
- The ability to isolate, locate, and identify the target.
- The availability of friendly forces to accomplish destruction.
- The destruction is beneficial to friendly forces.
- The overall gains outweigh potential risks.

The end purpose of all analysis is to enable the friendly commander to engage and destroy the opposition. Where the opposition cannot be destroyed outright, the friendly commander must be able to exploit or neutralize them. This must be accomplished with minimal loss of friendly forces. CI analysis contributes to the accomplishment of each of these missions.

CI ANALYSIS PRODUCTS

CI analysis products convey the essence of the CI analysis to the commander and staff and higher, lower, and adjacent units. MDCI analysts prepare C-HUMINT, C-SIGINT, and C-IMINT products that become the analytical tools used to produce collective CI products. CI products also provide OPSEC or deception planners critical information required for their operations. Among these products are rear operations IPB; MDCI summaries (MDCISUMs); CI threat assessments; CI situation overlays; and CI estimates.

REAR OPERATIONS IPB:

In every operation, someone has to watch the back door. That someone is the MDCI analyst. Working in the rear CP or the combat service support CP, the MDCI analyst works through the steps of the IPB process taking a slightly different approach than his counterparts in the main CP. Specific responsibilities follow:

- MDCI analysts use maps at a scale of 1:50,000 or larger (1:25,000 scale or town plans at 1:12,500 scale are even better). This scale permits them to obtain the resolution needed to precisely locate and evaluate terrain suitable for Level I or II threats.
- MDCI analysts identify the most probable area for a small threat insertion of perhaps 6 to 10 personnel. They also identify a Level III threat. Insertion of a Level III threat in the rear area would most likely take place as a cross-forward line of own troops (FLOT) operation. Close coordination with ACE analysts ensures the inclusion of IPB products to predict this threat.
- Divisional analysts are concerned with the division rear area up to the brigade rear area.
- Corps analysts would concentrate on the corps rear area down through the division rear area.
- EAC ACE is concerned with the communications zone down through the corps rear area.
- FORSCOM J2 is responsible for CONUS rear operations IPB.

During peacetime, the MDCI analyst builds an extensive database for each potential area in which threat intelligence collectors or battalion size or smaller units might operate. He analyzes this intelligence base in detail to determine the impact of enemy, weather, and terrain on operations and

presents it in graphic form. The analysis has the added ingredient of assisting in the assessment of friendly COAs from the enemy's perspective. Graphics assist the commander in identifying targets as they enter the battle area. Because rear operations IPB targets consist of small units or threat intelligence collection resources, these targets are not as prominent as those viewed in the all-source products. However, the process still generates HVTs and HPTs. Additionally, rear operations IPB assists in determining friendly HVTs and HPTs from the enemy's perspective. These are the friendly critical nodes or clusters susceptible to enemy collection or hostile action that are deemed critical to successful operations.

Rear operations IPB and IPB threat evaluation use the same analytical technique—templating. Rear operations IPB templates are similar to IPB templates in the main battlefield area. They provide a comparative intelligence database for integrating threat intelligence collection activities and small unit operations with the weather and terrain for a specific area. This enables the MDCI analyst to graphically portray enemy intelligence collection and small unit capabilities; depict probable COAs both before and during the battle; and confirm or refute predictions.

Both rear operations IPB templates and IPB templates are dynamic and require continual review. Not only do they portray enemy intelligence elements and small unit characteristics but they also seek to graphically portray named areas of interest (NAIs). Like the IPB process, rear operations IPB develops and employs doctrinal, situational, and event templates, and matrices that focus on intelligence collection and identifying which COA an adversary will execute. These COA models are products the staff will use to portray the threat in the decisionmaking and targeting process.

MDCI analysts develop and maintain templates throughout the IPB process and provide the basis for collection and further CI analysis. The analyst's ultimate goal is the nomination of targets for exploitation, neutralization, suppression, harassment, and destruction. For more information on IPB, see FM 34-130.

MDCI SUMMARY:

The MDCISUM is a graphic portrayal of the current situation from a CI point of view. The MDCI analyst uses the MDCISUM to show known adversary collection units, as well as Levels I and II threats within the friendly area. The MDCISUM is a periodic report usually covering a 12-hour period. It shows friendly targets identified as adversary objectives during the specified timeframe as shown in Figure 5-1. The MDCI analyst includes a clear, concise legend on each MDCISUM showing the time period, map reference, and symbols identifying friendly and adversary information. As the MDCI analyst identifies a friendly critical node, element, or resource as

an adversary combat or intelligence collection target, he puts a box around it and labels it with a "T" number. The legend explains whether the "T" is—

- A combat intelligence target.
- A source and time confirmation.
- An adversary resource or element that will attack or collect against the target in the future.
- The expected timeframe for the adversary to exploit the target.

The MDCISUM incorporates rear operations IPB products and individual and specific products to the extent they are relevant to the MDCISUM reporting period. The MDCISUM might portray the following information:

- Satellite or tactical reconnaissance patterns over the friendly area.
- Sweeps by enemy side looking airborne radar (SLAR) or EA air platforms to the full extent of their maximum ranges.
- Suspected landing zones or drop zones which will be used by an enemy element in the rear area.
- Area or unit which has received unusual enemy jamming.
- Movement of an enemy mobile SIGINT site forward along with a graphic description of the direction and depth of its targeting.
- Location of an operational enemy agent or sabotage net.
- Last known location of threat special operations forces.

The MDCI analyst retains copies of the MDCISUM to provide a historical database for future use; to use the preparation of CI threat assessments; and to update the CI estimate. The MDCISUM usually accompanies the graphic intelligence summary prepared by the ACE. This allows commanders to view them simultaneously. The MDCISUM, like the graphic intelligence summary, is an extremely valuable tool. It gives the commander critical information in a concise, graphic manner.

COUNTERINTELLIGENCE THREAT ASSESSMENT:

The CI threat assessment is a four-paragraph statement which is published as often as necessary or when significant changes occur, depending on the situation and the needs of the commander. As a general rule, the CI threat assessment is disseminated by the ACE with every third or fourth MDCISUM. The CI threat assessment provides justification for CI target nominations, a primary goal of CI analysis. Essentially, the CI threat assessment provides the following to the consumer:

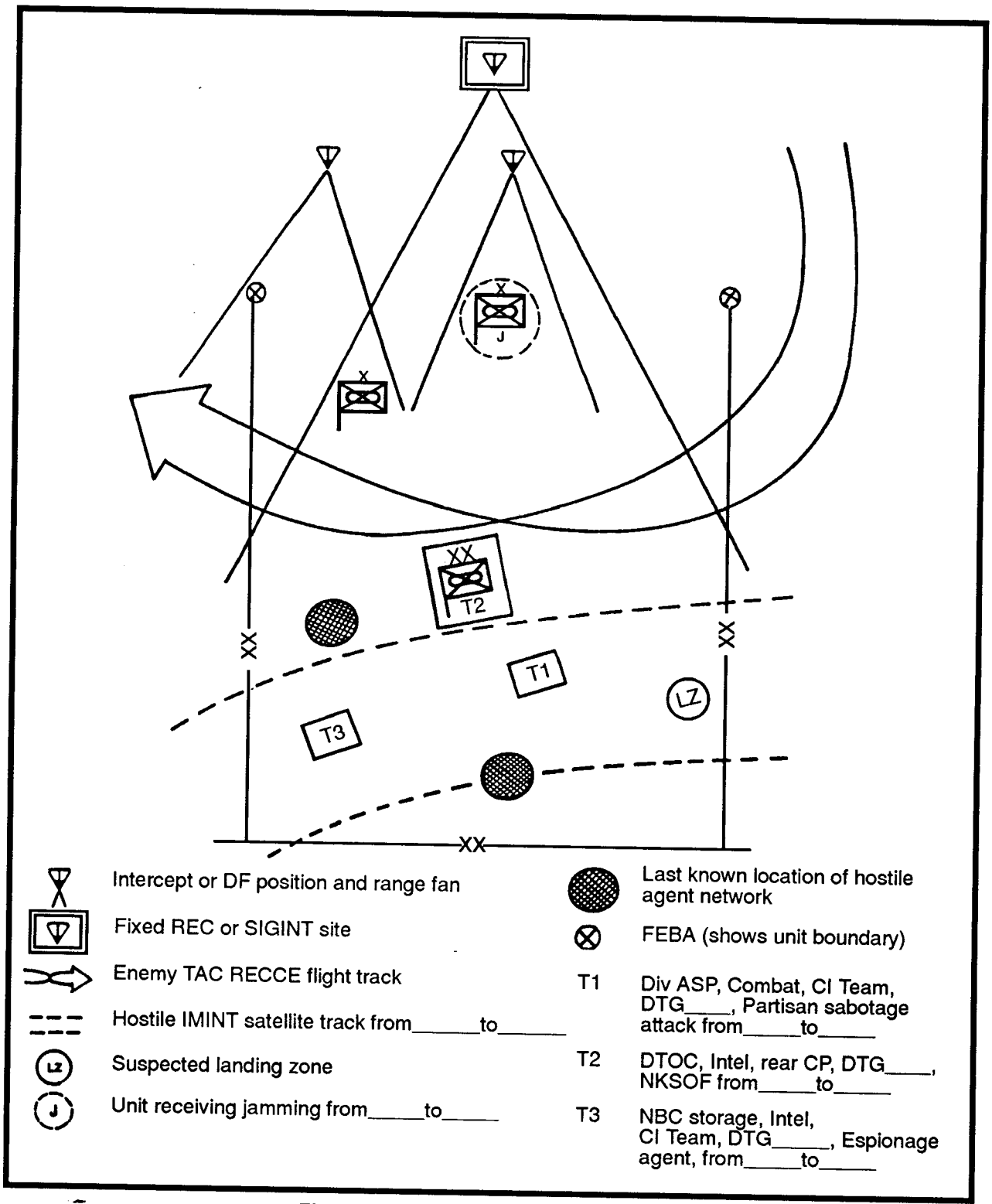

Figure 5-1. Sample graphic MDCISUM.

- A quick overview of significant activity during the reporting period.
- An assessment of the intelligence damage.
- A projected assessment of enemy activity for the next reporting period.
- Target nominations.

The CI threat assessment is a valuable means for providing peacetime assessment to commanders, activities, or operations shown in Figure 5-2. This assessment also satisfies the NATO requirement for a CI summary (ITSUM-CI).

CI SITUATION OVERLAY:

The CI situation overlay is a composite of the functional area overlay prepared by the subject matter experts assigned to perform CI analysis. The CI situation overlay incorporates the most important information from each of the other overlays. The functional area overlay serves as the "working" overlay, while the CI overlay is the master and serves as the briefing overlay. It should be ready for briefings at all times. Ordinarily, the senior MDCI analyst is responsible for maintaining the overlay; however, its preparation is a collective effort of all members of the CI team.

CI ESTIMATE:

The CI estimate is a composite study containing information from each functional area pertaining to a specified contingency area. It is a dynamic document prepared during peacetime and refined and updated continuously. The CI estimate addresses all friendly AOs with the strongest emphasis on the rear area. The rear operations IPB process is tied to the development of the CI estimate. Types of information contained in these estimates vary depending on the contingency area. They generally contain discussions on friendly deployment (including friendly critical nodes) and enemy intelligence collection capabilities and operations (such as sabotage or unconventional warfare). The following are examples of information found in an estimate:

- CONUS base.
- Major supply routes.
- Rail lines.
- Points of entry.
- Air and sea lanes.
- Air points of departure and sea points of departure.
- Staging areas.

- Maneuver areas.
- Host nation support and nature of resistance in any US AO.
- Assessment of threats to the logistic system.
- Enemy multidiscipline collection capabilities.
- Level I or II threats.

(CLASSIFICATION)

1. ENEMY ACTIVITY DURING PERIOD ___ TO ___ (LIST DTGs)

a. HUMINT: Summarize in one paragraph all known HUMINT activity during the reporting period. Compile data from HUMINT situation overlay, matrices, link diagrams, and MDCISUMs.

b. SIGINT: Summarize in one paragraph all known SIGINT activity during the reporting period. Compile data from SIGINT situation overlay, matrices, direction charts, and MDCISUMs.

c. IMINT: Summarize in one paragraph all known IMINT activity during the reporting period. Compile data from IMINT situation overlay, matrices, pattern and analysis charts, and MDCISUMs.

d. Other: Summarize all other enemy activity that is not already addressed using the same analytical tools.

2. INTELLIGENCE DAMAGE ASSESSMENT FOR THE PERIOD ___ TO ___ (LIST DTGs)

Briefly assess the intelligence damage to the friendly units for which the assessment is being prepared. Assessment is based on enemy collection activities that were traced, analyzed, and reported in MDCISUMs and were measured against the friendly force operations profile and countermeasures implemented by the friendly force. Coordination with G3 OPSEC staff element is essential in preparing this paragraph.

3. PROJECTED ENEMY ACTIVITY ASSESSMENT FOR THE PERIOD ___ TO ___ (LIST DTGs)

a. HUMINT: Using the same analytical tools identified in paragraph 1A above, plus IPB, project or assess enemy HUMINT activity for the next reporting period.

b. SIGINT: Using the same analytical tools identified in paragraph 1B above, plus IPB, project or assess enemy SIGINT activity for the next reporting period.

c. IMINT: Using the same analytical tools identified in paragraph 1C above, plus IPB, project or assess enemy IMINT activity for the next reporting period.

(CLASSIFICATION)

Figure 5-2. CI threat assessment.

(CLASSIFICATION)

d. Other: Using the same analytical tools identified in paragraph 1D above, plus IPB, project or assess all other enemy activity for the next reporting period that is not otherwise addressed in the HUMINT, SIGINT, or IMINT assessments.

4. TARGET NOMINATION

a. Exploitation: Using aforementioned information and all other analytical tools, identify any targets worthy of exploitation. Provide recommended time frames, locations, methods of exploitation, justification, and any other pertinent data.

b. Neutralization: Using aforementioned information and all other analytical tools, identify any targets worthy of neutralization. Provide recommended time frames, methods of neutralization, locations, justification, and any other pertinent data.

c. Destruction or Elimination: Using aforementioned information and all other analytical tools, identify any targets worthy of destruction or elimination. Provide recommended methods for engagement, time frames, locations, justification, and any other pertinent data.

NOTE: All target nominations must have G2 or G3 approval before dissemination or presentation to the commander or his designated representative for decision. Coordination with appropriate elements, consistent with type nomination, is essential.

(CLASSIFICATION)

Figure 5-2. CI threat assessment (continued).

These considerations necessitate complete CI analysis of the threat and an assessment of friendly critical nodes and targets. Some of these friendly targets will be identified almost out of common sense, but others will require a concerted analytical effort. In preparing the CI estimate, the team should first concentrate on identifying friendly critical nodes and targets and then examine the threat. It should then evaluate the target with respect to their relative criticality, accessibility, vulnerability, and the potential effect of their destruction. This is done for both friendly and enemy targets under the purview of the team. Figure 5-3 is an example of the CI estimate.

(CLASSIFICATION)

Headquarters
Place
Date, Time, and Zone

CI Estimate Number ___.
References: Maps, charts, or other documents.

1. **MISSION:** The restated mission determined by the commander.

2. **AREA OF OPERATIONS:** Summarizes the analysis of the AOs.

a. **Weather.**

(1) Factors. Include light data and either a weather forecast or climatic information, as appropriate. Use appendixes for graphic representation or weather factors and other details.

(2) Effect on enemy COAs. Discuss the effects of weather on possible enemy COAs (for example, sabotage, subversion, raids, air operations) in terms of mobility, concealment, and logistic sustainability. Discuss in terms of Level I or II threat, and enemy all-source intelligence collection operations.

b. **Terrain.**

(1) Existing situation. Use graphic symbols where possible especially for cover, concealment, and logistic sustainability. Use annexes for detailed information. Information covering observation, fields of fire, obstacles, key terrain, and approaches to the probable target aid in determining insurgent terrain. Also, consider graphics for critical facilities and buildings.

(2) Effect on enemy COAs. Discuss in the same manner as for effects of weather in a(2) above. Discuss in detail those areas favorable and unfavorable to the levels of threat I or II enemy all-source intelligence collection opportunities.

(3) Effect on own COAs. Discuss in the same manner as for effects of weather in a(2) above. Note the positive or detrimental effects on response forces and defensive measures.

c. **Other characteristics.** Include in subparagraphs any of the following factors or characteristics which pertain to friendly area activity (emphasis on rear area): population, ethnicity, religious makeup, literacy rate, medical considerations, economic stability, transportation, mass media, public services, and current political situation.

3. **ENEMY SITUATION:** Information on the enemy which will permit later development of enemy capabilities and vulnerabilities and refinement of these capabilities into specific COAs and their adoption.

a. **Disposition.** Reference overlays, enemy situation maps, or previously published documents. Location of potential threat forces may be difficult to pinpoint, but the greater the detail, the more thorough the analysis. Separate by level and type of threat (that is, combat Levels I and II threats) or intelligence.

b. **Composition.** Summary of the OB of conventional Levels I and II threats, intelligence collection units and elements, and the structure or organization of paramilitary and/or terrorist groups. Separate by level and type of threat.

(CLASSIFICATION)

Figure 5-3. CI estimate.

(CLASSIFICATION)

c. **Strength**. This listing assists in developing enemy capabilities and vulnerabilities. Conventional and intelligence threats are discussed as in a regular intelligence estimate. Terrorist, paramilitary, and other threats need to be assessed based on support from populace, monetary base, supplies, armament, personnel, and other pertinent considerations. Use subparagraphs to address the different threats. Separate by level and type of threat.

d. **Recent and present significant activities.** Items of information are listed to provide bases for analysis to determine relative probability of adoption of specific COAs and enemy vulnerabilities. Enemy failures to take expected actions are listed as well as positive information. Include recent all-source collection activities, terrorist actions, and other indications.

e. **Peculiarities and weaknesses.** For conventional and intelligence collection threats, discuss as in an intelligence estimate. For terrorist, paramilitary, or other unconventional threats, discuss such pertinent information as leadership (key personalities), equipment, finances, and relations with the local populace.

4. **ENEMY CAPABILITIES:** Based on all the previous information and analysis, develop and list enemy capabilities to conduct operations against the friendly area, with emphasis on the rear area. The listing provides a basis for analyzing the available information to arrive at those capabilities that the enemy can adopt as specific COAs and their relative probability of adoption. Separate items by levels and type of threat.

a. **Enumeration.** State what, when, where, in what strength, and by what method for each threat.

b. **Analysis and discussion**. Each enumerated threat is discussed in terms of indicators of adoption or rejection. The intent is to assess the likelihood of a given threat taking a given action. Consider all information previously recorded in this estimate. Some threats may not have any indicators of rejection listed due to insufficient data.

5. **POTENTIAL ENEMY TARGETS:** Based on all previous information and analysis, develop, to the extent possible, a listing of potential enemy targets. Ensure you can identify, at a minimum: target identity, capability, location or projected location, and projected intentions. Ascertain if targets can be exploited, neutralized, destroyed, or eliminated. Use subparagraphs and/or annexes as needed.

6. **CONCLUSIONS:**

a. **Effects of AOs on own COAs**. Indicate weaknesses in ability of response forces to react in defensive measures.

b. **HVT analysis based on the criticality, accessibility, recuperability, vulnerability, and effect (CARVE) format.** Such targets range from bridges to friendly units, public services, and key facilities. Complete for both friendly and enemy targets.

c. **Probable enemy COAs.** COAs are listed in order of relative probability of action. However, insufficient data may only permit the probable level of threat for a given target.

d. **Enemy vulnerabilities.** List the effects of peculiarities and weaknesses that result in vulnerabilities that are exploitable.

Annexes (as required): Annexes may include graphic analysis products which support the estimate such as link diagrams, association matrices, rear operations IPB products, or black, white, and gray lists distributed to units requiring them.

(CLASSIFICATION)

Figure 5-3. CI estimate (continued).