Appendix B

COUNTER-SIGNALS INTELLIGENCE TECHNIQUES AND PROCEDURES

GENERAL

One of the most self-destructive aspects of any operation is complacency. We know we are the best and we are equipped and trained to employ the finest equipment available. Our problem is improper use of the resources given to us, thus providing our adversaries with the opportunity to maximize the effect of their often inferior equipment and techniques to support their actions against us. Overcoming complacency is part of the analyst's task in C-SIGINT. Knowing and understanding the adversary and his equipment, as well as the capabilities and limitations of our personnel and equipment, is the first step in countering hostile efforts.

CONTENTS

This appendix provides the MDCI analyst with detailed, step by step procedures necessary to initiate a C-SIGINT support program or to fine-tune an existing one. This appendix also contains analytical techniques and procedures which include—

- Database.
- Threat Assessment.
- Vulnerability Assessment.
- Countermeasures Options Development.
- Countermeasures Evaluation.

It provides indepth coverage of the five-step C-SIGINT process—threat assessment, vulnerability assessment, countermeasures options development, countermeasures implementation, and countermeasures evaluation discussed in detail in Section II through Section V. Although you can apply the C-SIGINT process manually, automation is the standard tool for database manipulation and production of C-SIGINT. The All-Source Analysis System (ASAS) and compatible systems such as the Theater Rapid Response Intelligence Package (TRRIP) are the tools that make the national intelligence community become an intelligence asset responsive to the warfighter's requirements.

Section I

DATABASE

TO

Appendix B

COUNTER-SIGNALS INTELLIGENCE TECHNIQUES AND PROCEDURES

B-I-1. **General.** The MDCI analyst must establish a complete and accurate database before the C-SIGINT process can begin. Section I details the creation of the database necessary to support C-SIGINT. With an effective database, the analyst streamlines the entire five-step C-SIGINT process. The C-SIGINT portion of the CI database, hereafter referred to as the C-SIGINT database, organizes C-E information. The MDCI analyst implements the C-SIGINT database by automated procedures for ease in manipulating and maintaining information. He organizes the database to limit duplication of data and to assure the accuracy, quality, completeness, and integrity of the data.

B-I-2. **Development.**

a. The MDCI analyst develops the database during the planning phase of an operation, before deployments begin. He conducts electronic preparation of the battlefield (EPB) for the command's AI. EPB is the systematic approach to determine, through SIGINT and electronic warfare support (ES), the echelons and disposition of the threat through the electromagnetic structure of the target. The MDCI analyst employs a five-step process in EPB.

(1) Identification of expected electronic signatures.

(2) Evaluation of the current electronic environment.

(3) Comparison of expected situation with current situation.

(4) Preparation of SIGINT/EW templates.

(5) Integration of SIGINT/EW templates with all-source intelligence.

b. For C-SIGINT purposes, the MDCI analyst employs EPB to identify echelons and disposition of friendly forces through the electromagnetic structure. The purpose of EPB in C-SIGINT analysis is to build the database in order to determine and analyze vulnerabilities to threat SIGINT and to reduce or eliminate those vulnerabilities. To perform EPB, MDCI analysts must determine-friendly communications and noncommunications signatures which may be

vulnerable to threat collection or EA. Upon deployment, MDCI analysts continuously update the database with information which could influence the development of countermeasures.

c. The MDCI analyst compiles the data for each step in the C-SIGINT process. Sources of the data include—

(1) Current messages, reports, plans, and orders.

(2) Interviews specific to a command.

(3) Army regulations and technical manuals.

(4) Reviews of tables of distribution and allowances (TDA) and tables of organization and equipment (TOEs).

d. No matter what storage means is used, the MDCI analyst organizes, manipulates, and maintains the data for immediate and subsequent use and review. Since the data are not useful without modification for analysis, the formats supporting analytic techniques, methods, and measurement are essential. Like the data, the formats must be easily accessible and complete. The database includes analytic support templates, maps, and formats.

B-I-3. **Content.**

a. Information in the database should include most OB factors and other pertinent information such as—

(1) Composition.

(2) Disposition.

(3) Strength.

(4) Tactics.

(5) Training status.

(6) C-E emitters or threat collectors.

(7) EPB templates.

(8) Situation overlays.

(9) Intelligence summaries.

(10) Intelligence estimates.

b. The MDCI analyst needs to crosswalk the C-SIGINT database with the rest of the CI database to ensure accuracy and currency of overall CI information. Because there are many databases to draw information from, the analyst can save considerable time and effort by being tied into the appropriate databases, and not redoing the work all over again. Analysts constantly review and update the database by analysis and provide reports to the commander.

B-I-4. **Organization.**

a. The C-SIGINT database is organized to ease access to data. There are three rules for database organization and storage:

(1) Store like data together if primarily used in a particular task or step.

(2) Store data when first created, if they are shared or administrative data.

(3) Store administrative and reference data separately from task support data.

b. For data used in multiple steps or tasks or routinely updated, reference a data version. For example, analysts review the commander's operations plans (OPLANs) in the vulnerability assessment, and again in the countermeasure effectiveness evaluation. The second use of the OPLANs should reference the initial use and date in the vulnerability assessment. In addition to the shared resources of the CI database, the analyst maintains a note file for reminders, working aids, high priority items, procedures, and interpretations.

B-I-5. **Collection.**

a. To be an effective tool, the database requires full time dedicated personnel to maintain it. This ensures complete familiarity with friendly and threat systems, and the ability to compare threat to friendly data in a timely manner. Analysts seek the collection of data on two levels.

(1) The first collection level, the technical data file, is a listing of the technical characteristics for the friendly command's emitters and the threat SIGINT/EW equipment. Sources for friendly technical information include the command's C-E officer, technical manuals, technical bulletins, system operators, and maintenance personnel. Analysts request information on threat systems, such as communications intelligence (COMINT) and electronic intelligence (ELINT) receivers and direction finding (DF) equipment and jammers, through the collection management element.

(2) The second collection level is how the unit uses its specific equipment. The systems use file identifies how the friendly unit uses its emitters and how the threat uses its SIGINT/EW resources.

b. Whereto begin and how to progress in the collection of data are simplified by establishing a prioritized database collection list. This list is based on how the threat might prioritize their SIGINT/EW targeting. Although adversary target priorities depend on the command level and may be altered as the tactical situation develops, they generally are—

(1) Artillery, rocket, and air force units that possess nuclear projectiles or missiles and their associated control systems.

(2) CPs, observation posts, communications centers (includes automated data processing), and radar stations.

(3) Field artillery, tactical air forces, and air defense units limited to conventional firepower.

(4) Reserve forces and logistic centers.

(5) Point targets that may jeopardize advancing threat forces.

c. The collection of friendly force information for technical data files requires research on all types of emitters. This must include more than just frequency modulation (FM) voice radios and ground surveillance radars. The various C-E emitters and ancillary equipment include but are not limited to the following:

(1) Single sideband voice radios.

(2) Facsimile.

(3) Multichannel transmitters.

(4) Antennas.

(5) Retransmission systems.

(6) Tactical satellite communications systems.

(7) Automatic data processing transmission lines.

(8) Radio and wire integration.

(9) COMSEC machine encryption systems.

(10) Fiber-optic cable systems.

(11) Telephone wire systems.

(12) Countermortar radar.

(13) Air defense artillery target tracking radar.

(14) Air defense artillery target acquisition radar.

(15) Aviation guidance beacon systems.

(16) Aviation identification, friend or foe (IFF).

(17) Aviation ground control approach radars.

(18) Balloon-launched weather data radiosondes.

(19) EW jamming equipment.

(20) Cellular phones.

B-I-6. **Construction.** Analysis employing any means other than automated data processing systems is a waste of time and effort. The analyst can revert to stubby pencil mode in an emergency but it is only a temporary fix until automated data processing (ADP) is back on line. No longer is it necessary for the MDCI analyst to build a database from scratch. Adversary COMINT and ELINT information are already in a database, organized for use, and available. The analyst needs only to extract pertinent adversary information from the database to cover the friendly AO and AI. He then puts this information into a working file for his use. The analyst can add to, delete from, and manipulate the information in his file without affecting the database he drew information from. Once the analyst has extracted and copied the data needed, he creates a working file of friendly emitters for his use. The analyst now has two working files that are the basis for future analysis. The analyst begins working the data, performing the analysis to satisfy the commander's needs.

B-I-7. **Use.** The MDCI analyst is responsible for the control (security and access), use, and development of reports from the database.

a. Access to the C-SIGINT data is based on the "need to know."

b. Reports are correlated data from the CI database. The database contains working aids to help the analyst present information. Automated databases provide considerable flexibility in structuring reports. Manual databases have less flexibility and require considerable time and attention to detail unrelated to the analytic process.

B-I-8. **Maintaining the Database.** Several areas are particularly important for the MDCI analyst who must maintain the SIGINT database.

a. The first is timely review and update of the data. The analyst must update the database regularly with the most recent, valid information available, including the results of each analysis.

b. The second area of importance is data integrity. This includes maintaining the most current version of information, ensuring proper and valid data are available, and fulfilling priorities and administrative requirements.

c. Finally, the MDCI analyst must ensure the database contents support the CI analysis process. Should requirements, policies, or procedures change, the analyst should review and modify the database.

Section II

THREAT ASSESSMENT

TO

Appendix B

COUNTER-SIGNALS INTELLIGENCE TECHNIQUES AND PROCEDURES

B-II-1. **General.** One of the key words in the definition of intelligence is enemy. We must know our adversary as well or better than we know ourselves. We need to know and understand the capabilities and limitations of the threat arrayed against us and how the threat can influence our operations and mission. Section II, the first step in the C-SIGINT process, provides extensive information on determining foreign technical and operational capabilities and intentions to detect, exploit, impair, or subvert the friendly C-E environment.

a. Threat assessment is the key in planning C-SIGINT operations. The subsequent steps are necessary only when a defined threat exists.

b. Threat assessment is a continuous activity. It takes place throughout the conflict spectrum. A specific threat assessment is required to support a specific operation or activity.

c. The MDCI analyst gathers and analyzes information. He interacts with staff elements and higher, lower, and adjacent units to obtain the necessary data and access to supportive databases. Command support and direction are essential to success in the threat assessment process.

d. The major information sources available to the MDCI analyst include—

(1) Validated finished intelligence products.

(2) Theater and national level SIGINT threat database.

(3) Previous tasking.

(4) Analyst experience.

(5) The CI database.

e. MDCI analysts must continue to refine this list and identify other sources of information that may be available for their particular AO.

B-II-2. **Procedures.** There are six tasks associated with threat assessment. These tasks are presented in Figure B-II-1.

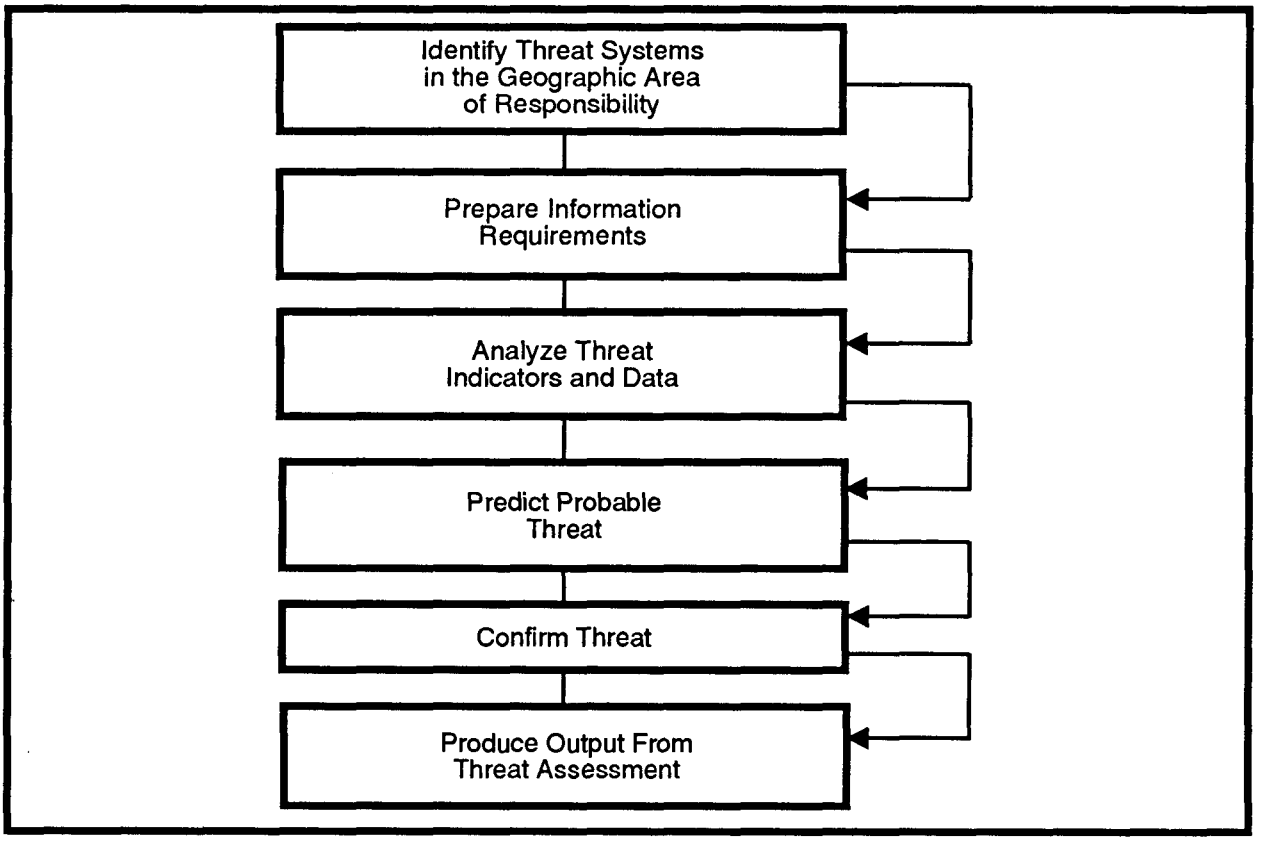

Figure B-II-1. Threat assessment process.

a. Identify threat systems in the geographic area of responsibility. This task provides the initial focus for the remaining threat assessment tasks. The primary objective of this task is to determine the specific threat faced by the supported commander. The MDCI analyst collects the required data to properly identify the threat. Additionally, the MDCI analyst must coordinate and request assistance from the collection management element. The procedures for identifying the threat systems follow:

(1) Identify the generic threat. The MDCI analyst enters the CI database and retrieves the most recent appropriate threat assessment. Analysts then review this data to determine what threat systems were known to be in their AO on the date of the assessment. Next, the analyst examines finished intelligence products published by national level agencies to obtain technical and operational data on the threat system. Some of the intelligence products include—

(a) ES and EA capability studies.

(b) Hostile intelligence threat to the Army publications.

(c) SIGINT threat by country.

(d) SIGINT support to combat operations.

(2) Create the doctrinal template. The doctrinal template is a graphic display of threat's systems deployment when not constrained by weather and terrain. The analyst should review the database for existing templates before constructing a new one.

(3) Collect data. Data collection is required when the analyst receives tasking for a specific unit or operation. The analyst must collect additional data to identify the threat to a particular unit or AO.

(4) Create the SIGINT situation overlay. The analyst reviews the collected data to determine—

(a) Technical and operational capabilities.

(b) Typical modes of operation.

(c) Current deployment.

(d) Probable tasking.

(e) Activities of the collectors of interest.

(5) Enter data. The analyst enters this data on the situation overlay.

(6) Summarize the data and identify the threat system. The MDCI analyst reviews the SIGINT situation overlay for patterns, electronic configurations, and threat command, control, and communications (C^3). The ACE has identified this information, which could help the analyst identify specific systems. A common approach is to pose and answer questions, such as—

(a) Is the threat system part of a larger system?

(b) What are the threat system's capabilities?

(c) How is the threat system doctrinally used?

(d) How does the threat system obtain information?

(e) How many collection systems were located?

(7) Request information. In some instances, sufficient information may not be available in the unit to make an accurate determination. For example, the type of equipment may be known but the technical characteristics of the system may not be available from local sources. If additional information is required, the MDCI analyst compiles the information needed and requests additional information from outside the unit.

b. Prepare information requirements.

(1) The MDCI analyst fills information shortfalls by requesting information from sources external to the unit. These external information sources are adjacent or higher echelons and national level assets. Each echelon satisfies a request with available data or organic assets, if possible. Requirements exceeding their organic capabilities are consolidated and forwarded to the next higher echelon as a request for information.

(2) Once a request reaches corps, the highest tactical echelon, the corps ACE provides the information or passes the request to the theater Ml brigade if it is beyond the capability of corps systems. This task requires the MDCI analyst to initiate a standard collection asset request format (SCARF) shown in Figure B-II-2 requesting information from higher or adjacent headquarters.

1. Request Number: 2. Originator priority: 3. Activity and target type (area emitter, size, point or area, unit): 4. BE number, ELINT notation, or case: 5. Location (if known, last known):
6. Duration: a. Start date and time: b. Frequency: c. Stop date and time: d. Latest acceptable date and time for information utility:
7. Location accuracy: a. Required: b. Acceptable:
8. PIR and IR: 9. Justification: 10. Remarks (to include disciplines and collectors recommended):

Figure B-II-2. Sample standard collection asset request format (SCARF).

(3) The SCARF is prepared in accordance with local SOP and the Joint Tactical Exploitation of National Systems (J-TENS) manual. At ECB units, this request is sent by a request for intelligence information (RII) using the US message text format (USMTF). The USMTF user's handbook provides instructions on preparing messages. The analyst forwards the request to the appropriate collection management section for action.

c. Analyze threat indicators and data.

(1) The MDCI analyst reviews, organizes, and evaluates key information components of the collected information. He evaluates the data looking for trends and patterns of the threat

system that will provide an estimate of capabilities and intentions. He focuses on each component of the collected information to determine if it reveals a tendency of the threat system to act or react in a particular manner. Additionally, the analyst evaluates the information for trends or characteristics that will aid in the ID and evaluation of the capabilities and intentions of the threat system. Additional support may be required from other staff elements.

(2) The procedures for analyzing threat indicators and data are to—

(a) Compile and organize data. First, the analyst compiles and organizes the data that has been collected. He updates the database with new information and organizes the data into collector categories.

(b) Review data. The analyst reviews the collected data to determine the ability of the threat systems to collect against a specific target.

(c) Determine intentions. To determine the intentions of the threat system, the MDCI analyst poses the following questions and enters this information in the database:

1 What area will the threat system target?

2 When will the targeting take place?

3 Why is the targeting taking place?

4 How will the threat system attempt to collect against the target?

5 How has the threat system been used in the past?

6 What does threat doctrine suggest about probable threat?

7 Does the threat system have a distinctive signature?

(3) Doctrinal templates are extracted from the database and compared to the SIGINT situation overlay. The analyst lists similarities between current and doctrinal deployments and selects the doctrinal template that has the greatest similarity to the current situation.

d. Predict probable threat.

(1) The MDCI analyst identifies the probable threat. He reviews all the information that has been collected and applies this information to the geographic AI and the capabilities and intentions of the threat system.

(2) The procedures for predicting the probable threat follow:

(a) Determine probable location. Use the SIGINT situation overlay and doctrinal templates to determine the location of the collectors. Overlay the doctrinal template over the situation overlay.

(b) Analyze terrain and weather effects. Integrate the terrain and weather data with the doctrinal template and the SIGINT situation overlay and create a situation template for the current environment. Terrain and weather conditions affect a threat system's ability to operate according to their doctrine. For example, a radio DF site must have a clear line of sight (LOS) on the emission of the target in order to gain an accurate bearing. Mountains, dense foliage, and water distort electronic emissions and impair a collector's ability to target. FM 34-130 provides information for military terrain and weather analysis.

(c) Update the SIGINT situation overlay. Place the symbols for the collectors on the doctrinal template that have not been confirmed on the SIGINT situation overlay as proposed locations.

e. Confirm threat. The MDCI analyst attempts to verify threat predictions. The procedures for confirming the threat follow:

(1) Validate existing data. Review current intelligence reports and assessments to determine if the information received from the original SCARF request and other information sources used in the assessment are valid. If there are indications that the capabilities or intentions of the threat system have changed, additional information may be required. This is determined by looking for information that could indicate a change in a collector's ability to collect against the command. For example, additional antennas have been added to the collector, or the collector has moved to provide for better targeting are indicators of a change in collection capabilities.

(2) Request additional information. If additional information is required, request this information by preparing a SCARF or request for information and forward it to the collection management section.

(3) Evaluate new information. If new information on the collector's intentions or capabilities is received, review this information to determine its impact on the original assessment, and update the situation overlay. If intentions and capabilities of the collector change, reevaluate the original threat prediction by following the tasks identified in previous sections.

f. Produce output from threat assessment. The MDCI analyst can present the threat assessment in briefings or reports. Portions of the threat assessment are included and presented in CI products.

Section III

VULNERABILITY ASSESSMENT

TO

Appendix B

COUNTER-SIGNALS INTELLIGENCE TECHNIQUES AND PROCEDURES

B-III-1. **General.** After examining our adversary's equipment, capabilities, and limitations, we now must examine our own unit to see how our adversary can affect us. Section III, the second step in the C-SIGINT process, details specific areas where a threat effort can be most damaging to the friendly force.

a. The vulnerabilities are ranked according to the severity of their impact on the success of the friendly operation. The vulnerability assessment—

(1) Examines the command's technical and operational C-E characteristics.

(2) Collects and analyzes data to identify vulnerabilities.

(3) Evaluates vulnerabilities in the context of the assessed threat.

The MDCI analyst performs the primary data gathering and analysis required. Assistance by and coordination with the appropriate staff elements (intelligence, operations) is key to this process.

b. Data gathering requires access to command personnel and to local databases. Data sources include—

(1) Technical data on C-E inventories.

(2) Doctrinal and SOP information.

(3) Output from the threat assessment step.

(4) Command operational data.

(5) Essential elements of friendly information (EEFI).

(6) PIR and IR.

c. The database of friendly technical data is used throughout the vulnerability assessment process for key equipment information, mission data, and other supporting information.

d. Vulnerability assessment is comprised of ten tasks. The first three tasks are ongoing determinations of general susceptibilities. The next six are specific to the commander's guidance and involve determinations of specific vulnerabilities. The final task is the output. Vulnerability assessment tasks are shown in Figure B-III-1.

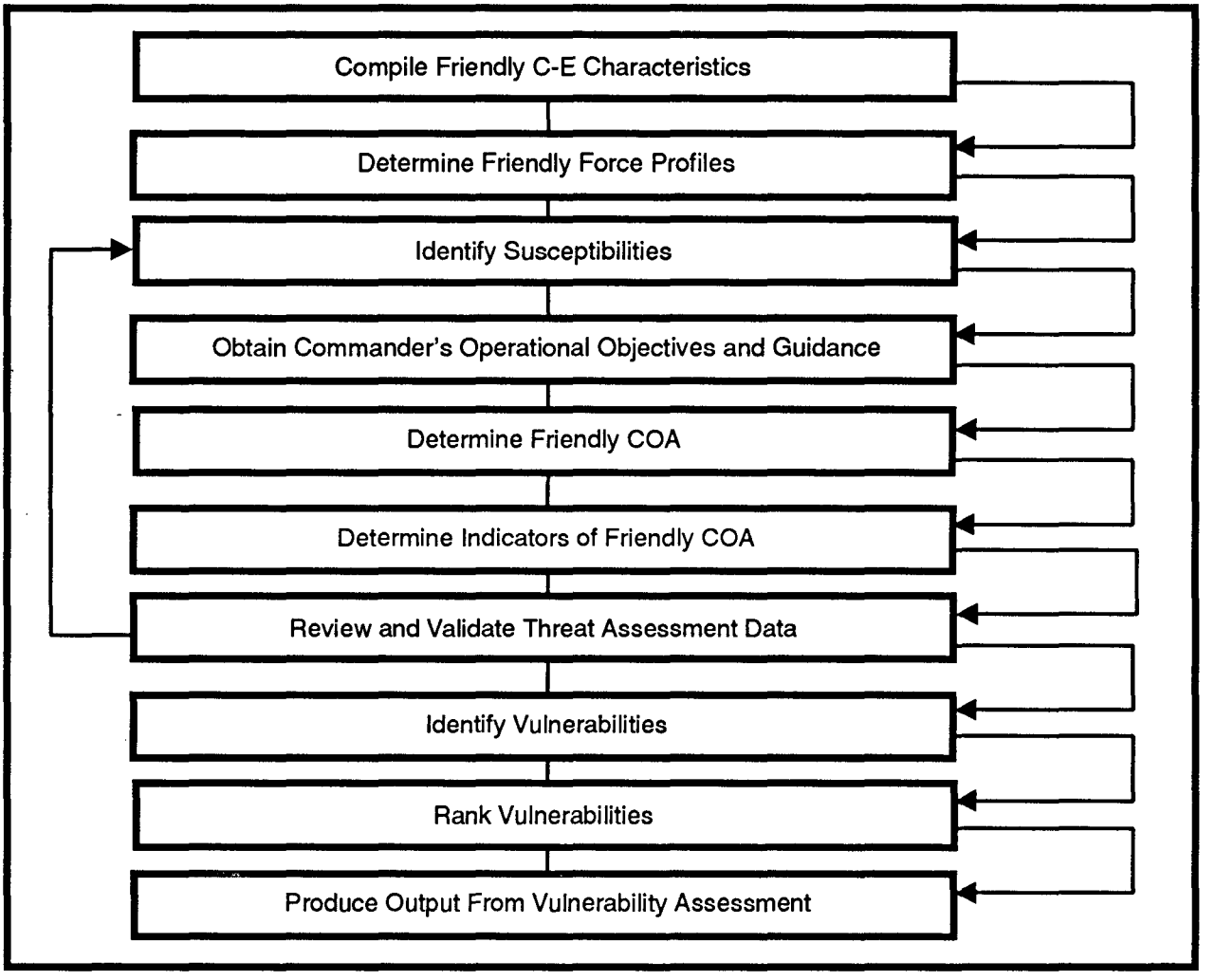

Figure B-III-1. Vulnerability assessment tasks.

B-III-2. **Compile Friendly C-E Characteristics.**

a. The MDCI analyst compiles friendly C-E characteristics. He collects and organizes unit C-E data and equipment characteristics for analysis. This analysis provides a baseline for analyzing friendly C-E equipment and operational susceptibilities to threat operations. The

compilation of C-E characteristics is an ongoing process. Assistance from the command's C-E officer, property book officer, maintenance personnel, or system operators may be necessary.

b. The C-E data are a baseline for identifying friendly susceptibilities. A unit's equipment, personnel, and associated characteristics must be identified before the pattern and signature analysis can proceed. The MDCI analyst uses available databases to extract the TOE, modification table of organization and equipment (MTOE), and TDA data on friendly equipment characteristics.

c. The procedures for compiling friendly C-E characteristics follow:

(1) Gather data on friendly C-E characteristics. Gather C-E data and characteristics of the equipment. Identify the following types of C-E data:

(a) TOE, MTOE, TDA, and technical data for all C-E equipment in a unit.

(b) References describing the unit and its equipment configuration.

(c) Current maintenance levels and normal status of the equipment.

(d) Personnel status, including current training levels of personnel in the unit.

(e) Equipment performance capabilities and operational capabilities in all weather conditions, at night, over particular terrain, and toward the end of equipment maintenance schedules.

(f) Equipment supply requirements.

(g) Special combat support requirements.

(2) Organize C-E data. The MDCI analyst organizes the information into a format useful for signature analysis. The data are organized by type of unit (if the support is multiunit), type of emitter, frequency range, number and type of vehicles or weapons which emit or carry emitters and the type of cluster. The electromagnetic overlay shown in Figure B-III-2 graphically depicts the friendly C-E equipment laydown on the battlefield.

B-III-3. **Determine Friendly Force Profiles.**

a. This task includes the analysis of signatures and patterns of the C-E equipment and a summary statement of the unit's C-E profile. A profile consists of the elements and standard actions, equipment, and details of a unit, the sum of signatures and patterns.

SIGNATURES + PATTERNS = PROFILE

b. Procedures for determining the friendly force's profile follow:

(1) Analyze friendly force signatures. The MDCI analyst—

(a) Extracts organic equipment characteristics for the operation.

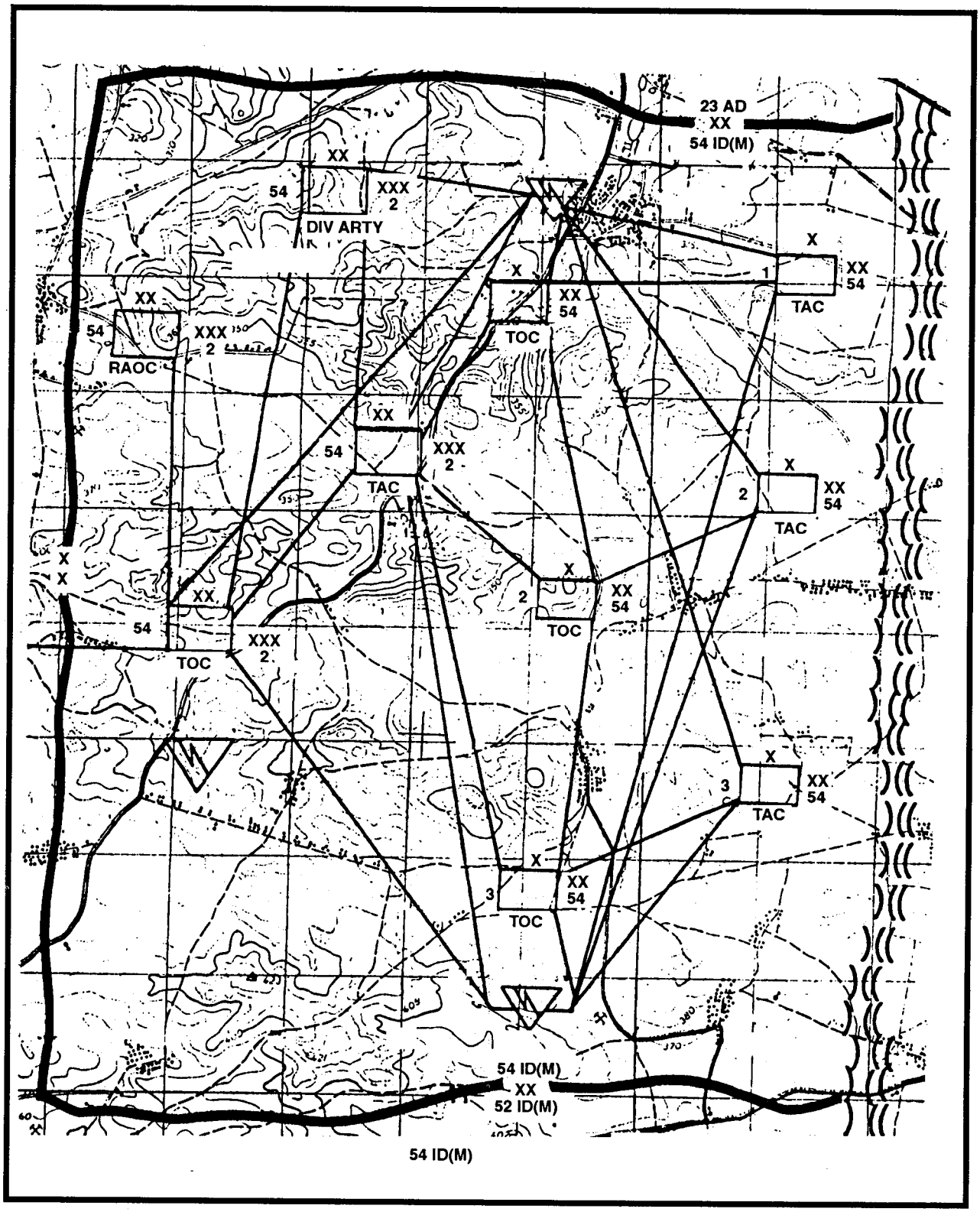

Figure B-III-2. Electromagnetic overlay.

(b) Determines environmental effects.

(c) Determines C-E characteristics for each friendly COA.

(d) Determines C-E equipment employment.

(e) Compares planned use with technical parameters.

(f) Determines if further evaluation is required.

(g) Performs tests with support from unit or higher echelon assets.

(h) Evaluates the information collected above.

(i) Diagrams physical and electronic signatures as shown in Figure B-III-3.

(j) Updates the CI database.

Physical Signature: Additional vehicles camouflaged in the woods.

4 x M35A2
1 x M104

Electronic Signature:

AN/VRC-46 Div Cmd Net
AN/GRC-106 DTOC SSB Net
AN/GRC-142 Div Ops Intel RATT Net
AN/TRC-145 MC to DIVARTY, DTAC CP, DISCOM
AN/MRC-108B USAF Air Nets

Figure B-III-3. Physical and electronic signatures.

(2) Perform friendly pattern analysis. Identify standard practices, common uses of a unit's C-E equipment, and operational patterns by—

(a) Reviewing the database to obtain information that might provide the threat with critical data regarding unit type, disposition, activities, or capabilities.

(b) Extracting from the OPLAN and operations order (OPORD) particular means of communication, operational characteristics, and key and secondary nodes for communications support.

(c) Identifying specific patterns associated with types of operations.

(3) Correlate patterns and signature. In this subtask, compile the information from the signature and pattern analysis, which creates the profile. The analyst—

(a) Lists the signature and pattern data for particular types of C-E equipment.

(b) Matches signature with patterns to form the profile.

(c) Organizes data into types of C-E operations.

(d) Correlates signature and pattern data with past profiles to produce the current profile shown in Figure B-III-4.

(4) Produce unit profile. Patterns and signatures can change as commanders, staff, and operators change. Profile development must be an ongoing effort. To produce the unit profile, use the OPORD to obtain the past task organization and then select the areas of concern to that organization, that is, C^2 and maneuver.

B-III-4. **Identify Susceptibilities.**

a. The analyst determines how the profiles would appear to threat systems and which equipment or operations are susceptible. A susceptibility is defined as the degree to which a device, equipment, or weapon system is open to effective attack due to one or more inherent weaknesses. Any susceptibilities are potential vulnerabilities.

b. Information sources are of the following types:

(1) Current friendly C-E profile.

(2) Historical profiles to compare with current profile.

(3) Knowledge and experience from other analysts.

c. The procedures for identifying susceptibilities follow:

(1) Identify weaknesses:

(a) Review current profile and identify unique equipment or characteristics that the threat may use to determine intentions.

(b) Review the CI database and compare historical profiles with current profile, noting correlations and deviations.

(c) Plot friendly weaknesses to threat operations on the electronic order of battle (EOB) overlay shown in Figure B-III-5.

(2) Categorize susceptibilities. Categorize susceptibilities to allow more specific analysis by equipment type, organization, and use. Do this—

(a) By type (for example, equipment, operations, or both).

(b) By activity (for example, logistic, C^3, intelligence, operations, and administrative support).

(c) According to resource requirements.

(d) According to the length of time the susceptibility has existed.

(e) According to scope (number of units or equipment types).

COMMAND AND CONTROL		
Physical Signatures - Types of vehicles - Number of vehicles - Distances to adjacent and higher echelon corps and HQ	**Electronic Signatures** - Types of emitters - Frequency range - Signature type and range - Emitter fingerprints	**Pattern Data** - Timing of movement - Mode of movement - Collocated or nearby units - Frequency of redeployments - Radio and radar net employment
OPERATIONS AND MANEUVER		
Physical Signatures - Types of vehicles - Number of vehicles - Distances to adjacent and higher echelon support elements - Types of weapon systems	**Electronic Signatures** - Types of emitters - Frequency range - Signature type and range - Emitter fingerprints	**Pattern Data** - Timing of reconnaissance - Mode of reconnaissance - Timing of movement - Type of movement - Mode of movement - Units involved - Mode and source of supply

Figure B-III-4. Friendly unit profile.

B-III-5. **Obtain Commander's Operational Objectives and Guidance.**

a. The commander states his operational objectives for missions in OPLANs and OPORDs. The analyst uses this information to plan the most effective support for the commander and to identify the commander's preferences for types of operations. The commander's operational concept and EEFI shown in Figure B-III-6 are essential to the analysis of friendly COAs.

EOB overlay (EM equipment located at enemy units, normally placed next to the symbol).

a.	b.	c.	d.		e.
R-104M	R-123	R-126	R-104M	R-123	R-130
R-130	R-107	R-107	R-130	R-401/405	R-107
R-107			R-107	R/TE	R-123
R-123					R-401/405

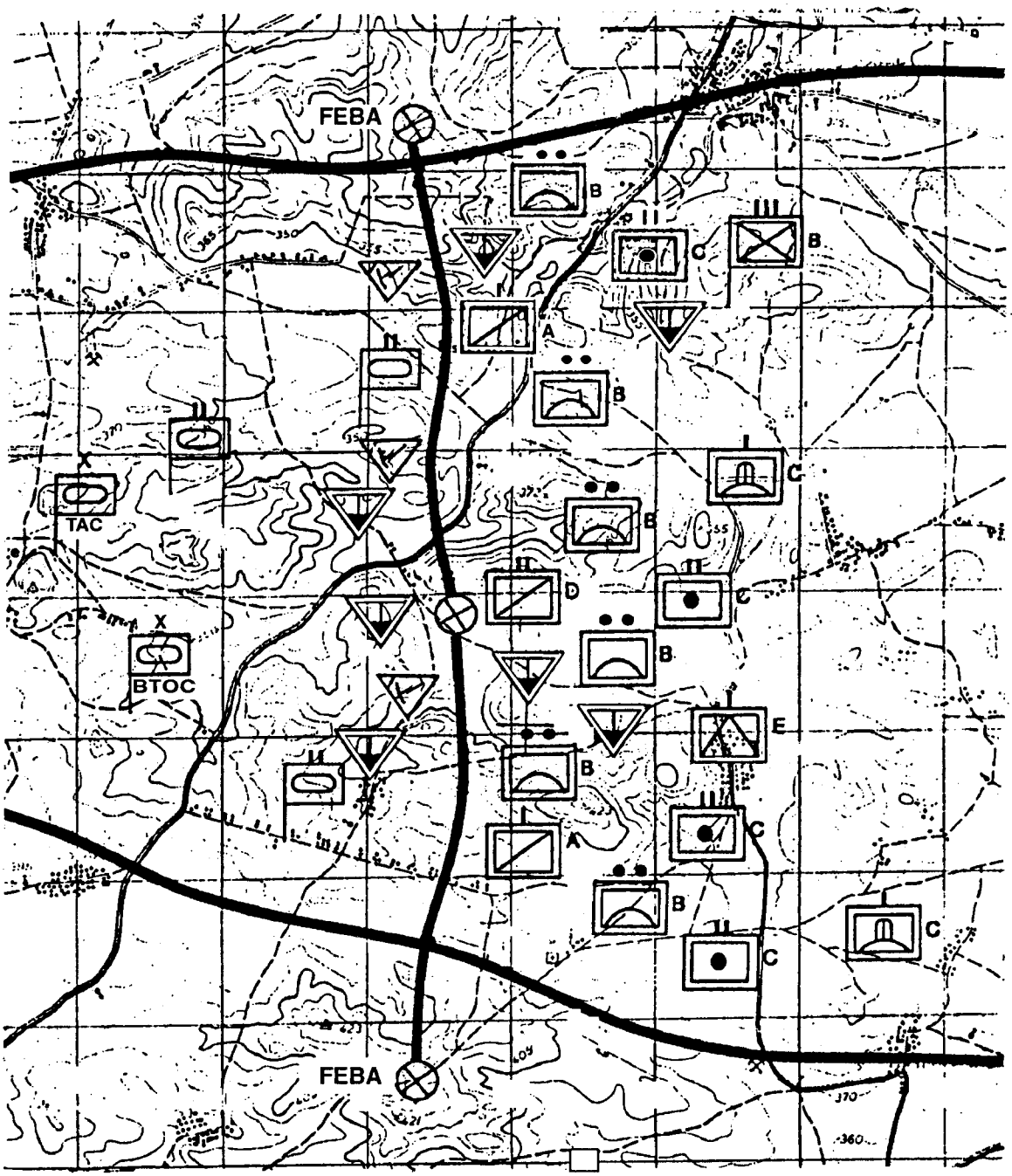

Figure B-III-5. Electronic order of battle overlay.

b. This information enables the analyst to evaluate indicators of friendly COA in the context of what the commander considers essential to the success of the operation. Setting priorities for the vulnerabilities depends on the commander's operational concept. The primary information sources are—

(1) Concept of operation.

(2) OPORDs.

(3) OPLANs.

(4) EEFI.

Essential Elements of Friendly Information Statement

FRIENDLY SUPPORTED UNIT: 5th Inf Div

1. SUBORDINATE ELEMENT: HQ
2. LOCATION: 32U NB51452035
3. OPERATIONAL OBJECTIVE:

   Defend to PL Gray, counterattack at 300001Z Oct 96
4. EEFI:
   a. SIGNIFICANT COMPROMISE:
      (1) Time of counterattack.
      (2) Identification and location of HQ elements brigade and higher.
      (3) Identification of attached units.
      (4) Loss of C^3.
   b. INSIGNIFICANT COMPROMISE: Identification of 5th Inf Div.

Figure B-III-6. Sample format for essential elements of friendly information.

B-III-6. **Determine Friendly COA.**

a. Based on the general description of the commander's objectives, the operations element plans locations and events. The analyst produces an overlay of the friendly force profile integrated with the commander's objectives.

b. The procedures for determining friendly COA follow:

(1) Identify COA. For each applicable level of command, identify friendly COA. At division level, for-example, COA would include the following minimum information:

(a) Summary of operations.

(b) Corps and EAC support.

(2) Compare COA to specific EEFI. Review the COA for events or actions that could compromise the unit's mission by disclosing key EEFI. The review is summarized in an events list that describes a particular mission, COA, or event which may compromise the EEFI or the friendly intentions.

B-III-7. **Determine Indicators of Friendly COA.**

a. Indicators of friendly COA shown in Figure B-III-7 are those events and activities which, if known by the threat, would compromise a friendly COA.

b. The procedures for determining indicators of friendly COA follow:

(1) Identify the commander's preferences and perceptions about C-SIGINT operations. Seek information about the commander's style from sources such as previous concepts, plans, and orders, or interviews with subordinate commanders and staff officers.

(2) Integrate friendly profiles and COA. In the event planned location or movement data are not available, retrieve friendly operational overlays shown in Figure B-III-8 from the database. The overlays help identify friendly historical positions for the new COA. Figure B-III-9 depicts an example of an integration of a friendly force profile and COA. Integrate the friendly profile and COA by—

(a) Noting current position and expected COA.

(b) Identifying key C-E capabilities associated with the COA (for example, radio nets, types of radios, radar, teletypewriters).

(c) Noting past C-E operational patterns.

(d) Plotting critical C-E nodes, paths, or circuits.

(3) Determine standard C-E procedures for types of operations:

(a) Begin by using the commander's objectives to identify key operational constraints, that is, nodes, paths, chokepoints, and standard C-E procedures followed during a particular COA. New or critical data, not previously included in the friendly profile and COA integration, are then added to the situation overlay.

(b) Also consider constraints and procedures while determining indicators. Document these as factors associated with those indicators in a format as in Figure B-III-7. After completing the review of existing data as obtained from the commander's objectives, determine what additional information is required.

INDICATORS OF FRIENDLY COAs			Version: OPORD 10-96 Date : 10 Oct 96 Analyst: SSG L. Morrow	
Course of Action	Indicator Number			
	1 C-E Equipment	2 C-E Nets	3 Vehicle Movements	4
Defend to PL Gray	AN/TRC-145 AN/VRC-46 AN/GRC-142	Div MC Div Cmd Div Intel	Small vehicle movement around DTOC	
	FACTORS	FACTORS	FACTORS	FACTORS
	LOS required	LOS to brigade and DIVARTY	None	
Counterattack	AN/TRC-145 AN/MRC-108B	Div MC USAF	Pack up of vehicle USAF comm increase may be a tip off	
	FACTORS	FACTORS	FACTORS	FACTORS
	LOS required	LOS to brigade and DIVARTY	Must be in range for C^3	

Figure B-III-7. Indicators of friendly COA.

(4) Determine impact of weather and terrain. As the situation changes, the significance of particular nodes or paths may shift or additional nodes may become critical. Consider the following in determining the impact:

(a) Inclement weather.

(b) Night activity.

(c) Terrain masking.

(d) Poor C-E equipment maintenance.

(e) Meaconing, intrusion, jamming, and interference (MIJI).

(5) Set priorities. Once the type of operation is determined, set priorities for the events, movements, and nodes by their overall importance to the operation.

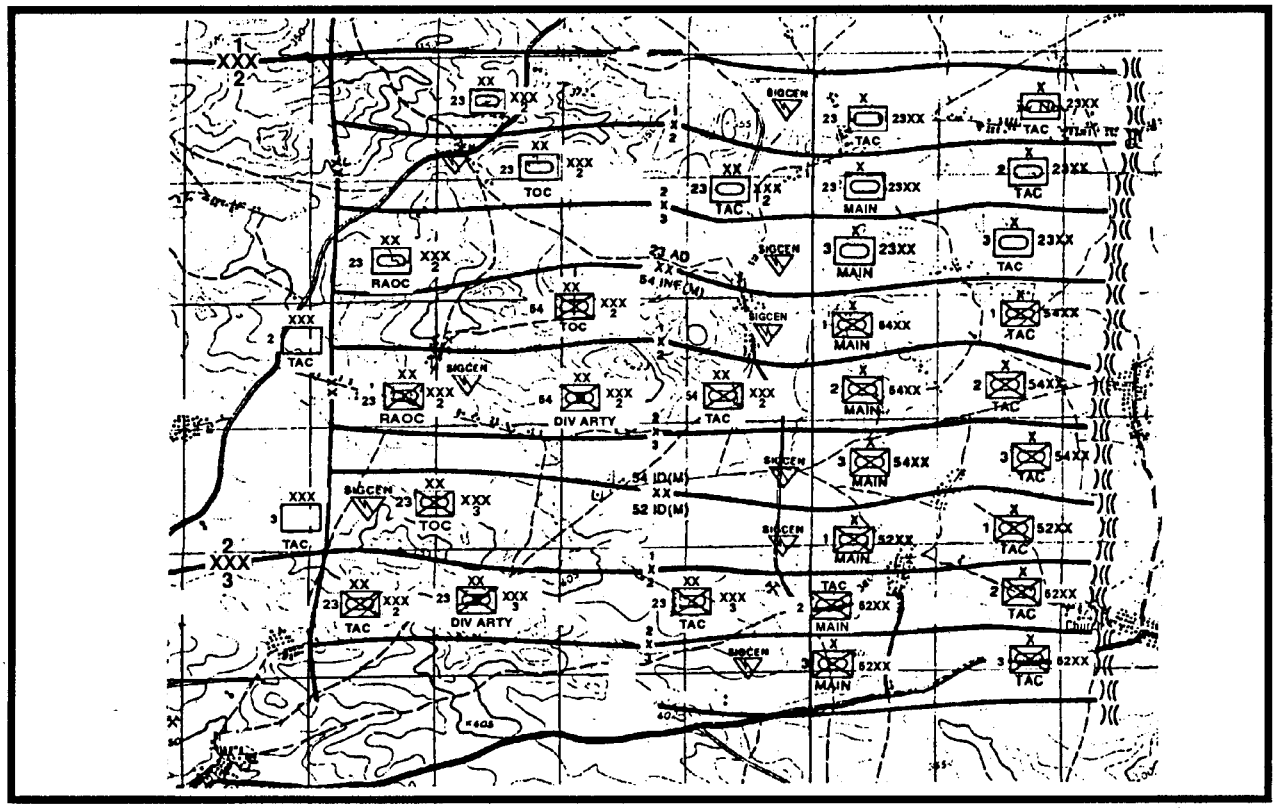

Figure B-III-8. Friendly operational overlay.

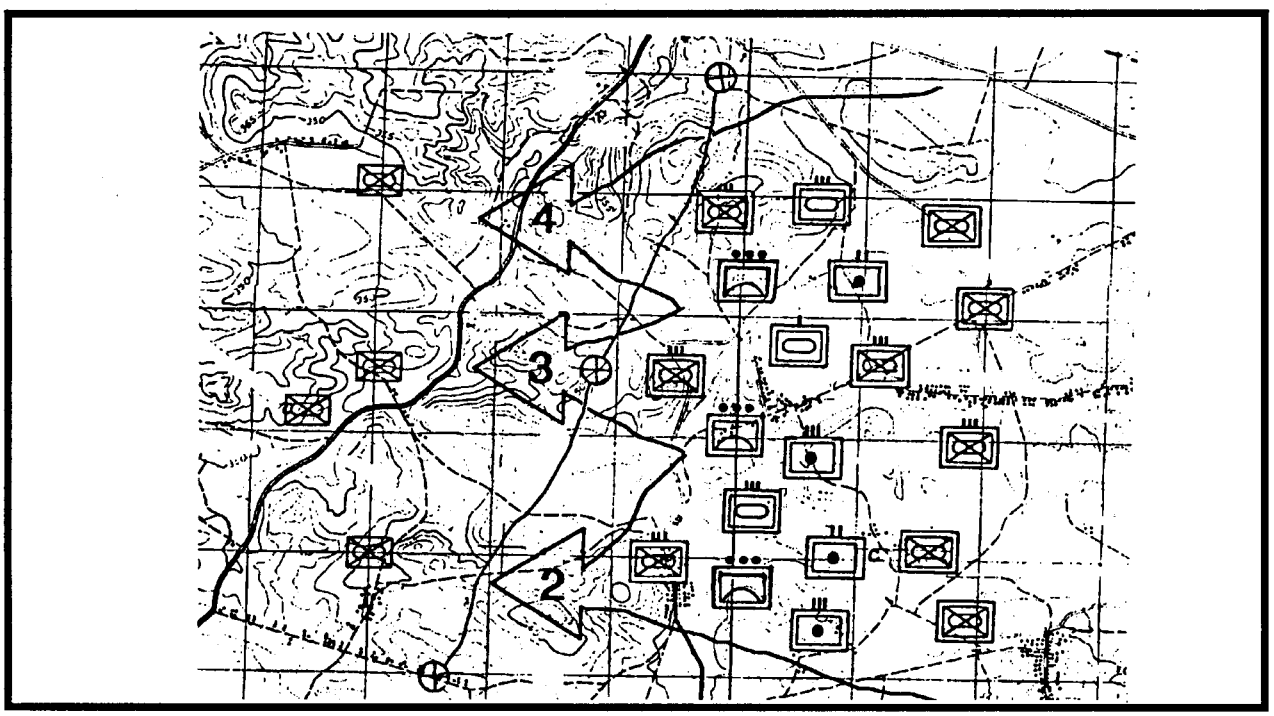

Figure B-III-9. Friendly profile and course of action integration.

(6) Identify critical C-E nodes—

(a) Using the C-E constraints and procedures identified from the information provided by the commander, together with data obtained from previous tasks, determine key indicators of friendly operations. For each COA, extract those preparations, activities, or operations that could tip off the threat to the particular COA.

(b) Using a format shown in Figure B-III-8, list the indicators associated with a COA. Any special factors such as operational constraints, optimum weather conditions, or terrain requirements associated with an indicator should be described accordingly.

B-III-8. **Review and Validate Threat Assessment Data.**

a. Threat assessment data are further refined in order to proceed with the remainder of the vulnerability assessment. The analyst organizes threat data in a format comparable to the friendly forces data. Missing data is identified and requested. The C-SIGINT analyst performs the review and validation of threat data with considerable exchanges of information with other analysts.

b. The procedures for reviewing and validating threat assessment data follow:

(1) Summarize and reorganize threat assessment data.

(a) Compile recent threat assessment information.

(b) Identify information shortfalls.

(c) Coordinate with the collection management section to initiate requests for information.

(2) Extract relevant data for vulnerability assessment.

(a) Extract areas of threat operations most critical to the supported command.

(b) Document threat capabilities and intentions.

(c) Store data for later application.

B-III-9. **Identify Vulnerabilities.**

a. The analyst compares the intelligence collection threat with the friendly unit susceptibilities to determine the vulnerabilities. Once the vulnerabilities have been identified, the analyst can rank them.

b. The procedures for identifying vulnerabilities follow:

(1) Compare current threat to friendly C-E susceptibilities.

(a) Review indicators of friendly COA.

(b) Use the products developed earlier in the C-SIGINT process to determine where threat capabilities and intentions are directed against susceptible friendly operations.

(c) Determine the probability of threat activity against a friendly C-E operation. Use various statistical and analytical tools. (See the reference list in Technical Bulletin 380-6-1-4.)

(2) Determine which susceptibilities are vulnerabilities.

(a) Designate as vulnerabilities those C-E susceptibilities which are targetable by a specific threat collector.

(b) List (and maintain separately) nontargetable indicators.

(c) Match indicators with threat systems and document specific event characteristics if known; for example, time and location of vulnerabilities.

B-III-10. **Rank Vulnerabilities.**

a. The C-SIGINT analyst ranks the vulnerabilities by analyzing them in view of the indicators of friendly COA and EEFI. The ranking is based on criteria estimating the uniqueness, degree of susceptibility, and importance of the vulnerability. The analyst designates the vulnerability as either critical, significant, or important to the success of the overall operation.

b. The procedures for ranking vulnerabilities follow:

(1) Establish criteria for measuring the vulnerability. Develop a means for judging whether each identified vulnerability is critical, significant, or important to the success of the operation. These final ratings are attained by evaluating each vulnerability against criteria which address how critical they are to the success or failure of the operation. Uniqueness, importance, and susceptibility to threat are three criteria which measure vulnerability and criticality, and permit an accurate ranking of them. They are defined as follows:

(a) Uniqueness—the extent to which a vulnerability can be readily associated with a COA.

(b) Importance—a measure of how critical the vulnerability is to the success of the operation.

(c) Susceptibility to threat—a measure of the number and variety of threats placed against the indicator.

(2) Compare vulnerabilities to criteria:

(a) Combine the criteria and vulnerabilities in a matrix format shown in Figure B-III-10. For each vulnerability, conduct a review against the established criteria. The analysts have in their possession the commander's objectives, prioritized EEFI, and ranking criteria, and can evaluate the vulnerabilities using these data. Vulnerabilities are first rated according to each of the criteria. The horizontal axis of the matrix lists the criteria of uniqueness, importance, and susceptibility.

Vulnerability	EEFI	CRITERIA			Overall Numerical Rating
		Uniqueness	Importance	Susceptibility	
Multichannel at DTOC vulnerable to intercept and DF	4(a)2	5	5	4	14
Multichannel at DTOC vulnerable to jamming	4(a)4	3	2	3	8

CRITERIA RATING VALUES	OVERALL RATING VALUES
0-2 = Low 3 = Medium 4-5 = High	0-4 = Unimportant 5-8 = Important 9-11 = Significant 12-15 = Critical

Figure B-III-10. Vulnerability matrix format.

(b) List the vulnerabilities on the vertical axis. The degree of satisfaction of a criterion is expressed numerically on a scale of 0 to 5 with 5 being the highest rating. If a vulnerability is highly unique, that is, pertaining to very specialized and infrequently exhibited indicators, it would be assigned a high rating. If the vulnerability is such that it is exhibited in many COA, in many operations, its uniqueness rating would be low (0 to 2).

1 If a vulnerability is highly important, that is, involving disclosure of a critical EEFI, its rating would be high. An EEFI lower-on the commander's list of priorities would receive a lower rating. If the vulnerability is highly susceptible, that is, targeted by numerous threat systems of several types, its rating for susceptibility wouid be high.

2 If a single threat system of limited capability is targeting the vulnerability, the rating would be low. The overall ratings are determined by adding the values of the three criteria and placing it under the overall number rating.

(3) Develop ranking.

(a) Once an overall rating is established for each vulnerability, develop a prioritized ranking. Vulnerabilities fall into the broader categories of critical, significant and important, based on the criticality level of criteria satisfied. Vulnerabilities receiving overall ratings between 5 and 8 are considered important; those between 9 and 11 are significant; and those falling between 12 and 15 would be critical.

(b) Enter the list of ranked vulnerabilities in the database. h is retained in hard copy for dissemination, and applied in the countermeasures options development in step three of the C-SIGINT process.

B-III-11. **Produce Output From Vulnerability Assessment.** The MDCI analyst presents the vulnerability assessment format shown in Figure B-III-11 as a briefing or a report.

Friendly Supported Unit: 5th Inf Div

1. Situations:

   a. Friendly:

      (1) Mission: Defend to PL Gray, counterattack at 300001Z Oct 96.

      (2) Profile statement: See Annex B.

      (3) Indicators of COAs: Multichannel at DTOC.

      (4) Essential elements of friendly information:

         (a) Identification and location of DTOC.

         (b) Loss of C^3 via multichannel.

   b. Enemy:

      (1) Intentions: See Annex A.

      (2) Disposition: See Annex S.

      (3) Capabilities: See Annex B.

      (4) Probability of intercept: 90 percent.

Figure B-III-11. Vulnerability assessment format.

2. Prioritized vulnerabilities requiring protection:

   a. Identification of Division Headquarters Element (critical).

   b. Loss of C^3 via multichannel due to jamming (important).

3. Vulnerabilities unable to protect: Loss of C^3 via multichannel due to jamming.

Figure B-III-11. Vulnerability assessment format (continued).

Section IV

COUNTERMEASURES OPTIONS DEVELOPMENT

TO

Appendix B

COUNTER-SIGNALS INTELLIGENCE TECHNIQUES AND PROCEDURES

B-IV-1. **General.** Thus far, our analysis has covered the adversary and our own vulnerabilities. Now its time to look at our countermeasure options. We need to examine how we can counter the threat's efforts, analyze the risks involved, and present our findings to the commander. Section IV, the third step in the C-SIGINT process, reviews C-E vulnerabilities and identifies, analyzes, prioritizes, and recommends specific options for controlling, eliminating, or exploiting the vulnerabilities.

a. Countermeasures are required to prevent the exploitation of friendly force vulnerabilities by threat systems. The MDCI analyst collects the data and analyzes it to determine possible countermeasures. Many sources are available to the analyst to determine the characteristics of the countermeasures required to achieve the commander's objective.

b. Countermeasures options require the completion of the six tasks shown in Figure B-IV-1.

B-IV-2. **Identify Countermeasures Options.**

a. This task is designed to overcome or limit vulnerabilities to the assessed threat.

b. The procedures for identifying countermeasures options follow:

(1) Collect data.

(a) Review the vulnerability assessment and list the identified vulnerabilities on the countermeasures options worksheet shown in Figure B-IV-2.

(b) Extract data on previously used countermeasures for the vulnerabilities and enter the countermeasures options on the countermeasures options worksheet.

(c) Review current situation for data that would further identify countermeasures options. For example, one commander will enforce strict emission controls to suppress electromagnetic signatures, while another may require continuous and extensive communication.

(d) List these data on the countermeasures options worksheet.

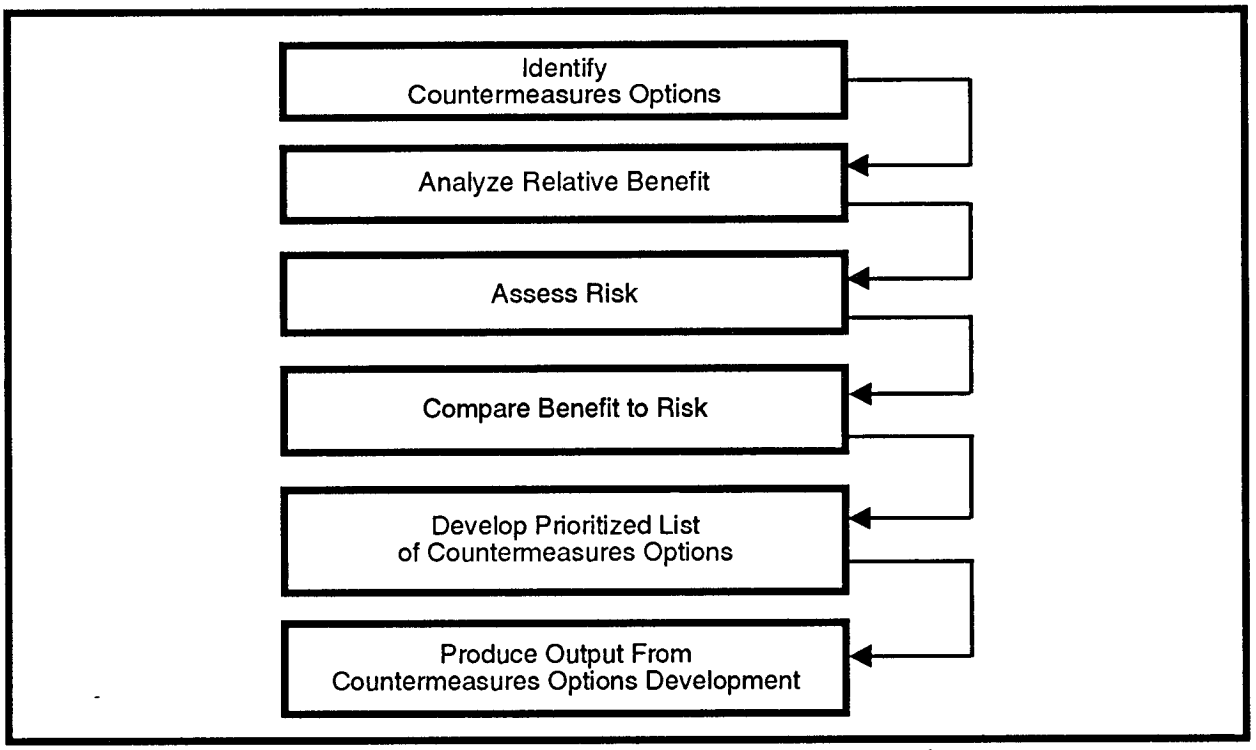

Figure B-IV-1. Development of countermeasures options.

VULNERABILITIES:	COUNTERMEASURES OPTIONS:
Multichannel vulnerable to intercept and DF	Remote equipment
Multichannel vulnerable to jamming	Use destruction
	Place equipment at another echelon
	Use other equipment
	Use deception

Figure B-IV-2. Countermeasure option worksheet.

(2) Identify countermeasures options for each vulnerability. Use the countermeasures option worksheet.

(a) Prepare a vulnerability to countermeasures matrix shown in Figure B-IV-3.

(b) List the identified vulnerabilities in the vertical column and the countermeasures options in the horizontal column.

Countermeasures options / Vulnerability	Remote equipment	Use destruction	Place equipment at another echelon	Use other equipment	Use deception
Multichannel vulnerable to intercept	X	X	X		X
Multichannel vulnerable to jamming		X		X	X

Figure B-IV-3. Vulnerability to countermeasures matrix.

(c) Match a vulnerability to a countermeasure. This match is determined by using the identified data sources.

(d) Check the block that identifies the appropriate countermeasures to the vulnerability.

c. This matrix provides the analyst the countermeasures to be used for a particular vulnerability.

B-IV-3. **Analyze Relative Benefit.**

a. This analysis provides the resource requirements for each countermeasure. The MDCI analyst, in coordination with other staff elements, performs this task.

b. The procedures for analyzing relative benefits of a countermeasure follow:

(1) Identify preferred implementation of the countermeasure. From the identified data sources, collect data on the preferred countermeasure implementation procedures for each of the countermeasures. Identify the tasks associated with the countermeasure, and gather information about the operational requirements. The following questions will help in gathering this data:

(a) What are the proper start-up procedures for the countermeasure?

(b) What software is associated with the countermeasure?

(c) What steps are involved in operating the countermeasure?

(d) What are the terrain requirements for the countermeasure?

(e) What support services are required?

(2) Identify resource requirements. In determining relative benefit, collect data on the resource requirements and command availability of the countermeasure. For example,

hardware or personnel required for implementation of the countermeasure is gleaned from the TOE. operator manuals, technical manuals, and other analyst's experience. Additionally, gather information of past experience documented in the CI database and the countermeasures database. The following questions will help in gathering this information:

(a) How many specialists are required?

(b) How many support personnel are required?

(c) What MOS is required?

(d) What are the hardware configurations?

(e) Does the countermeasure require specialized training?

(3) Develop relative benefit table. Upon completion of the data gathering process, enter information on the relative benefit table shown in Figure B-IV-4.

Vulnerability: Multichannel Vulnerable to Interception				
Countermeasures	**Resources**	**Expected Results**	**Impact on Operations**	**Shortfalls**
Remote multi-channel	Personnel Fuel Vehicles Time Wire for remote Remote equipment	Enemy will think the division is something other than a division	Will take time to set up the remote site Wire has to be guarded for security reasons	Wire comm needs high maintenance. May have to replace wire Wire needs to be guarded
Use destruction	Personnel Fire support Ammunition	Complete destruction of threat SIGINT and DF sites	None	Rounds may not be on target SIGINT and DF sites may be moved
Place multichannel at another echelon	Personnel Time Vehicles Fuel Food	Make the threat think the other echelon is the division	SIGINT and DF may not think the division did move.	Fired upon before reaching new location New location may not have trained personnel for multichannel equipment
Use deception	Vehicles Deception equipment Trained personnel Time Fuel	Make the threat think we are doing something we are not	Takes a lot of time to plan and implement	Failure to coordinate Equipment may not be available Plan may not work

Figure B-IV-4. Relative benefit table.

(4) Evaluate shortfalls. Evaluate the shortfalls of each of the countermeasures listed and identify alternatives. In the development of shortfalls and alternatives, evaluate the following:

(a) Is the threat vulnerable?

(b) Will the countermeasure reduce or eliminate the vulnerability?

(c) Is deception an effective countermeasure?

(d) Is the countermeasure being developed for training or future use?

(e) Does the countermeasure complement other OPSEC measures?

B-IV-4. **Assess Risk.**

a. Risk assessment can predict the element of risk to operations when countermeasures are not applied or do not successfully protect friendly vulnerabilities from the threat.

b. The MDCI analyst develops the risk assessment matrix shown in Figure B-IV-5. The procedures for developing a risk assessment matrix follow:

Vulnerability: Multichannel Vulnerable to Intercept					
1 CM Option	**2 EEFI**	**3 Vulnerability**	**4 CM Success**	**5 Risk Factor**	**6 Risk**
Remote equipment	4(a)2	5	5	0	Low
Use destruction	4(a)2	5	5	0	Low
Place equipment at another echelon	4(a)2	5	3	2	Medium
Use deception	4(a)2	5	0	5	High

Figure B-IV-5. Risk assessment matrix.

(1) Place a value on the vulnerability and past success of the countermeasure as they apply to specific EEFI. To determine the values, make a judgment based on available information. Use the following scale:

VULNERABILITY	PAST SUCCESS OF COUNTERMEASURE
5 = CRITICAL	5 = HIGH
3 = SIGNIFICANT	3 = MEDIUM
1 = IMPORTANT	1 = MARGINAL
0 = UNIMPORTANT	0 = FAILURE

(2) Fill out the blocks on the matrix as follows:

(a) Block l: List countermeasures options from countermeasures option list.

(b) Block 2: List specific EEFI.

(c) Block 3: Place a value on the vulnerability of EEFI (5,2,1,0).

(d) Block 4: Place a value on the past success of the countermeasure.

(e) Block 5: Place the numerical risk factor, the following algorithm should be applied:

VULNERABILITY - PAST SUCCESS = RISK FACTOR.

(f) Block 6: Annotate the element of risk in Block 6; determine the element of risk by applying the risk factor in Block 5 to the following scale:

4-5 = High Risk 2-3 = Medium Risk

B-IV-5. **Compare Benefit to Risk.**

a. Having completed the assessment of the risk associated with each countermeasure, the MDCI analyst compares the benefit to the risk for each countermeasure.

b. The procedures for comparing the benefit to the risk follow:

(1) Evaluate benefit.

(a) Using Figure B-IV-4, compare the expected result from the countermeasure implementation with its impact on operations and resource requirements. For example, if the expected results for implementation of the countermeasure are considered high, the impact on operation low, and few resources are required, the expected relative benefit will be high.

(b) Conversely, if the expected result is low, the impact on operations is high, and the countermeasure requires large resources, the relative benefit should be considered low. A value of Low, Medium, or High is then placed on the benefit to risk form shown in Figure B-IV-6.

(2) Evaluate risk. Review Figure B-IV-5. Extract the risk assessment from Block 5, and enter the value in Figure B-IV-6. This completed form provides the risk associated with the relative benefit of each countermeasure.

COUNTERMEASURES OPTION	BENEFIT	RISK
Remote equipment	Medium	Low
Use destruction	High	Low
Place equipment at another echelon	Low	Medium
Use deception	Medium	High

Figure B-IV-6. Benefit to risk form.

B-IV-6. **Develop Prioritized List of Countermeasures Options.**

a. This list provides the commander and staff with recommended countermeasures options for identified vulnerabilities.

b. The procedures for developing a list of prioritized countermeasures options follow:

(1) Prepare countermeasures effectiveness.

(a) Using the Benefit column (Figure B-IV-6), list all countermeasures options in order from the most to the least effective on the countermeasures effectiveness to costliness worksheet shown in Figure B-IV-7. For example, if destruction, remoting, deception, or moving the equipment to another echelon were your options, your effectiveness column would look like

1 Use destruction.

2 Remote equipment.

3 Use deception.

4 Place equipment at another echelon.

(b) The number in front of the countermeasure is now the effectiveness value of that countermeasure.

(2) Prepare countermeasures costliness.

(a) Using the Risk column in Figure B-IV-6, list all countermeasures options in order from the least to the most costly in the Costliness column (Figure B-IV-7). For example, using the same countermeasures options used in b(1) above, your costliness column would look like the following:

1 Remote equipment.

2 Use destruction.

3 Place equipment at another echelon.

4 Use deception.

EFFECTIVENESS	COSTLINESS	CM RATING AND PRIORITY
1. Use destruction.	1. Remote equipment.	1. Use destruction.
2. Remote equipment.	2. Use destruction.	2. Remote equipment.
3. Use deception.	3. Place equipment at another echelon.	3. Use deception.
4. Place equipment at another echelon.	4. Use deception.	4. Place equipment at another echelon.

Figure B-IV-7. Effectiveness to costliness worksheet.

(b) The number in front of the countermeasure is now the costliness value of that countermeasure.

(3) Prepare countermeasure priority list.

(a) Using Figure B-IV-7, add the number from the Effectiveness column to the number in the Costliness column. Determine the countermeasures which are the most effective and the least costly, and produce a prioritized list of countermeasures. The lower the rating the higher the priority the countermeasure has. When there is a tie, the countermeasure that has the higher effectiveness rating is given the higher priority. For example, using the information in paragraph B-IV-6(1) and (2), the countermeasure rating column would look like the following:

1 Use destruction. 3.

2 Remote equipments. 5.

3 Use deception. 5.

4 Change echelon. 7.

(b) Using this example, the countermeasure prioritized list looks like that in Figure B-IV-7.

B-IV-7. **Produce Output From Countermeasure Options Development.** The countermeasures option process is complete when the analyst reviews and recommends the countermeasures options to the operations element.

Section V

COUNTERMEASURES EVALUATION

TO

Appendix B

COUNTER-SIGNALS INTELLIGENCE TECHNIQUES AND PROCEDURES

B-V-1. **General.** Commanders determine which countermeasures are to be applied. Once applied, it is the MDCI analyst's job to evaluate the countermeasure's effect. Section V, the last step in the C-SIGINT process, determines how well the applied countermeasures worked and their impact on the operation.

a. Lessons learned provide feedback to the commander and serve as information for other commands considering similar countermeasures options. Countermeasures evaluation is the review, analysis, and evaluation of countermeasures to determine their effectiveness. The evaluation includes five major types:

(1) C-SIGINT database.

(2) Intelligence data.

(3) Interviews.

(4) Reviews of messages, reports, and other operational documentation.

(5) Reviews of actual profiles during the operation.

b. The specific tasks in the countermeasures evaluation format are shown in Figure B-V-1.

B-V-2. **Validate Commander's Guidance.**

a. Since countermeasures are planned in accordance with the commander's guidance, operational deviations from the commander's guidance may affect their effectiveness, even though the countermeasures are performed as planned. The first task validates the commander's guidance. To ensure the proper baseline is applied in evaluating the countermeasure, the MDCI analyst reviews the commander's guidance for changes or misunderstandings.

b. The procedures for validating the commander's guidance follow:

(1) Review the commander's guidance and EEFI. Retrieve the commander's guidance and objectives collected and stored during the vulnerability assessment. The EEFI statement

and friendly COAs developed during the vulnerability assessment are also important sources. Review the OPLAN, OPORD, and EEFI; add information or reports unavailable during or produced after the vulnerability assessment; and update the statement of the commander's operational concept generated during the vulnerability assessment.

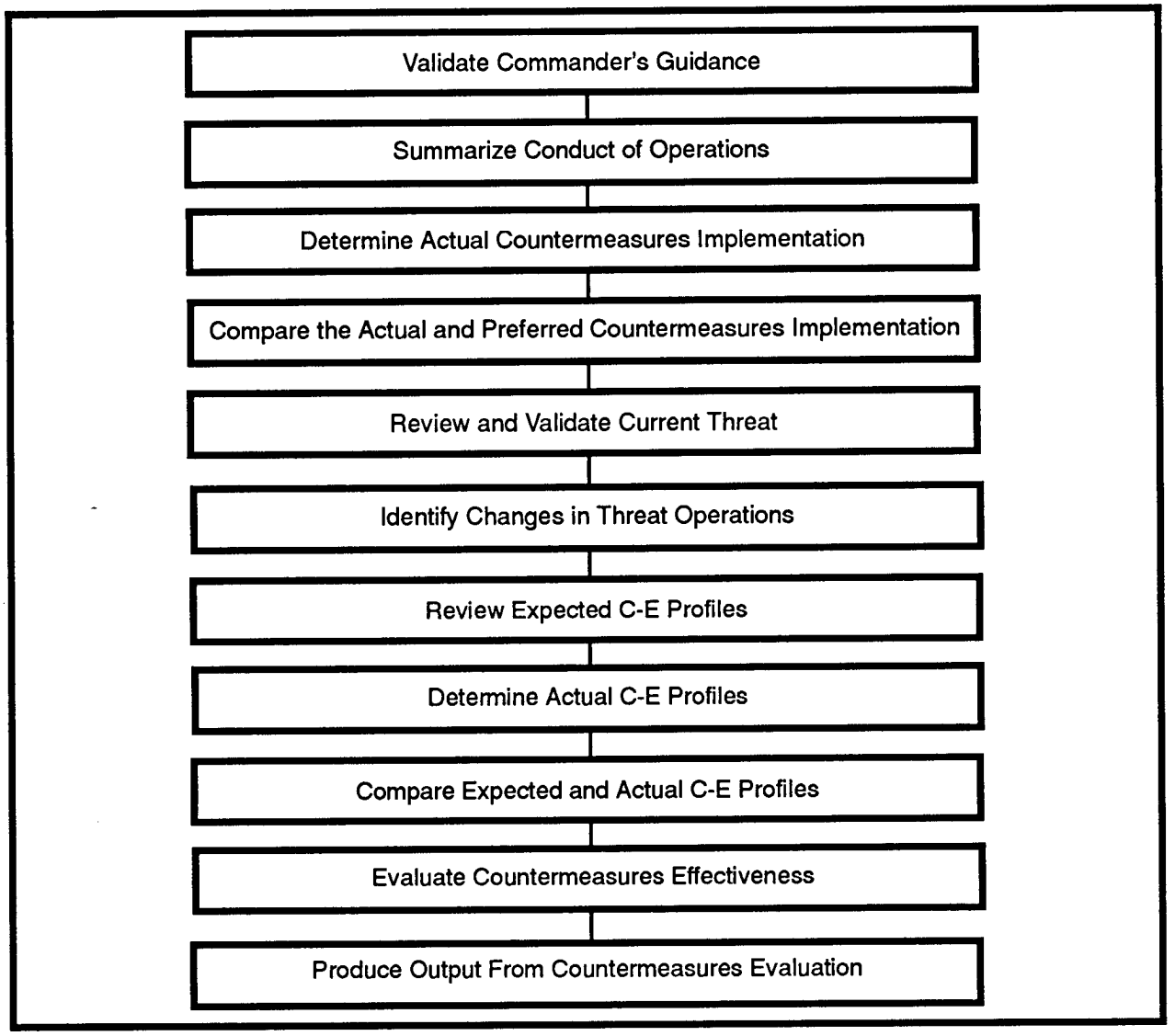

Figure B-V-1. Countermeasures evaluation format.

(2) Verify guidance and EEFI. Present the updated summary of the commander's operational concept to the operations staff. They review the summary, and note any misinterpretations or information gaps. The analyst reviews the operations staff's comments and completes the final verified statement of the commander's guidance and EEFI.

B-V-3. **Summarize Conduct of Operations.**

a. During this task the analyst compares how well actual operations matched planned operations. If the countermeasure is specific to an operation, the summary occurs upon completion of the operation. If the countermeasure is part of normal peacetime operations, the summary occurs at regular intervals. The MDCI analyst directs the evaluation. The analyst coordinates with the appropriate staff elements and talks to participants in the operation.

b. The procedures for summarizing the conduct of operations follow:

(1) Determine major activities. Use the commander's operational concept identified in paragraph B-V-2b(2) and the commander's guidance to identify the major activities required to conduct operations. Seek answers to the following questions:

(a) What type of task is it: (C^2 support)?

(b) Who was responsible (officer, NCO)?

(c) Who performed each of the tasks?

(d) What equipment was used in implementing the task in supporting the operation?

(e) What other units were involved?

(f) What supply channels were used?

(g) Was the task part of normal or special operations?

(h) Was the situation hostile or peaceful?

(2) Identify sources and collect data:

(a) Review the data requirements and identify the probable sources of data. Most frequently, the first source of information is written reports, memorandums, or journals of an operation.

(b) Develop a data collection format using the characteristics as key for describing the operation shown in Figure B-V-2.

(c) Identify personnel or units best suited to gather the data, and request they be tasked to collect data.

(d) Use organic resources to collect data not coming from tasked sources.

(e) List shortfalls in meeting the data requirements as gaps after completing the data collection.

REVIEW OF OPERATIONS Task: CM remote DTOC MC Date: 5 Sep 96		
Description		
Equipment	:	1 x AN/TRC-145 and 2 x AN/GRC-142
Supply	:	MRE for 7 SM x 14 days
Personnel	:	C-E PSG from 105th MI BN, C-SIGINT spec from CIAS
Command and Control	:	Cdr, C Co , 105th MI BN; ACofS G2
SOP	:	C-E Annex, OPORD 10-96
Operations Type	:	Defense of PL Gray and Counterattack

Figure B-V-2. Data collection format.

(f) Interview personnel who took part in the operations. Usually, your information needs are met by analyzing operations.

(g) May request permission to interview others identified as key personnel in the reports. Enter the results of the interview on the form.

(3) Review and finalize data:

(a) Review the data, assuring all requirements are met.

(b) Request additional information from the operations officer if conflicting information exists.

(c) Enter final information on the form.

(4) Compare and summarize data about conduct of operations:

(a) Complete a final review of the data collected.

(b) Compare the actual conduct of operations with the OPLAN and OPORD.

(c) Note where operations proceeded as planned and where they deviated from plans.

(d) Write a summary statement of the differences for later analysis.

B-V-4. **Determine Actual Countermeasures Implementation.**

a. The MDCI analyst gathers information about countermeasures implementation operations. The analyst can collect information about implementation any time after the countermeasure has been initiated. The preferred scheme is to collect information about implementation at regular intervals.

b. If the countermeasure is part of general peacetime operations, evaluations of the countermeasure operations should be ongoing. If the countermeasure is specific to an operation, the minimum number of evaluations is two. Accurate information about countermeasures implementation is necessary for evaluating how well the countermeasures were implemented. The analyst may request information from the operations staff, adjacent or higher echelon assets supporting a command, and participants in an operation.

c. The procedures for determining actual countermeasures implementation follow:

(1) Determine data requirements to implement countermeasures:

(a) Determine the preferred countermeasures implementation procedures.

(b) Examine the preferred tasks and expected results, responsibilities, equipment, operational characteristics, weather and terrain impacts, and effects of the countermeasure on adjacent or higher echelon commands.

(c) Enter the information on the countermeasures implementation worksheet shown in Figure B-V-3. Specific questions must be tailored to each situation.

(d) Answer the following types of questions to determine data requirements:

1 Are there SOPs for the operations? Are they affected by other countermeasure operations?

2 Who are the personnel responsible for the countermeasure? Have they performed the requisite duties?

3 What are the specific tasks? What operations will be affected? By whom? In what time frame?

4 What are the expected results? Will they affect operations?

(2) Identify data sources. Review the data requirements and determine what data are stored in the database; what new data are required; and the best, most complete, and valid sources for the new data. Written reports, memorandums, or findings of an operation are a primary source information. The analyst must verify and supplement this documentation from—

(a) The analyst's own experience.

(b) Interviews of participants in the operation.

CM: Remote DTOC MC
Last update : 14 Sep 96

CHARACTERISTICS OF DATA	PREFERRED CM ACTIVITIES	DATA REQUIREMENTS	FINDINGS	DATA SOURCES
Equipment AN/TRC-145	Move to neutral location	Spot check and review of comm log	Too little supervision Assign additional NCO	C-E Plt Sgt
Equipment AN/GRC-142 2 each	Place at DTOC and above AN/TRC-145 site	Spot check and review of comm log	Need best operators Large msg volume Good OJE	C-E Plt Sgt
Adequate and higher echelon impacts	Additional MC to communicate with corps will increase size of site	Spot check and review of comm log	Doubled msg volume of RATT Need more operators	C-E Plt Sgt

Figure B-V-3. Countermeasures implementation worksheet.

(c) Interviews of staff members.

(d) Reviews of the actual conduct of operations.

(e) Queries of other commands in the theater.

(3) Collect and summarize data:

(a) Review the C-SIGINT database and other documentation to fulfill the data requirements.

(b) Identify data supporting the needs and enter the data in the Findings column of Figure B-V-3.

(c) Enter the data sources in the last column. Upon completion of this first data survey, identify information shortfalls by gaps in the rows.

(d) May have to request information from other sources, such as the operations staff, adjacent commands, or participants in the operation.

(e) Review for completeness before beginning the next task.

B-V-5. **Compare the Actual and Preferred Countermeasures Implementation.**

a. The comparison of actual and preferred implementation shows successes and shortfalls in countermeasures actions. The MDCI analyst uses these successes and shortfalls in later evaluations of countermeasures options to manage ongoing countermeasures activities and to determine whether new vulnerabilities exist.

b. The comparison may be performed during an ongoing operation or upon completion. The completion provides needed information and analysis about countermeasures implementation in different operational situations. The comparison is based on information generated during the identification of countermeasures options and the internal processes in countermeasures evaluation.

c. The procedures for comparing the actual and preferred countermeasures implementation follow:

(1) Review data on countermeasures application. Review the data collected and organized in the development of countermeasures options and in the previous implementation. Simple countermeasures will have limited support and few activities or tasks; more complex countermeasures, such as deception, have numerous activities and relationships. In the latter case, analyze key activities first. If they are not met, the countermeasures are not effective and subsequent analysis is unnecessary. For example, the remoting of the multichannel supporting the Division Tactical Operation Center (DTOC) requires a separate site with NCO supervision. The personnel components of the evaluation are, therefore, examined first, since they represent the largest impact on the determination of effectiveness.

(2) Estimate the degree preferred countermeasures actions were completed. Determine the degree of completion by comparing the actual with preferred countermeasures performance.

(a) Match actual and preferred:

1 Review the preferred countermeasures implementation from the analysis of the relative benefit.

2 Match data from the actual implementation with the preferred implementation.

3 Review the countermeasures implementation review worksheet shown in Figure B-V-4, focusing first on the key activities.

4 Identify areas where the actual countermeasures activities were similar to the preferred actions.

CM : Remote DTOC MC Date: 4 Sep 96				
TASKS			**PERCENT COMPLETE**	**REMARKS**
Key	:	Allocate MSE to provide communications with remoted MC.	100	MSE provided by C Company, 105th MI.
Median	:	Provide NCO supervision at remote site.	50	DTOC and corps MCs had NCOs, but the MSE were operated by PFCs. MSE operators were not efficient in sending msgs.
Support	:	C-E Plt Sgt reviewed division logs, but not corps logs due to time. MREs were consumed twice as fast as expected due to additional corps personnel.	70 50	Additional data gatherer needed. Conduct additional liaison with corps and adjacent divisions before next implementation of this CM to ensure sufficient MREs are available.

Figure B-V-4. Countermeasure implementation review worksheet.

5 Estimate the percent of the preferred completed actions.

6 If the actual countermeasure is at least 50 percent of the preferred countermeasures operations, enter the countermeasure in the implementation review worksheet.

7 If the countermeasures have not been implemented as planned, according to the preferred operations, the percent completion of the standard is determined to be zero, and the analysis is complete.

(b) Develop an overall estimate of completion of the preferred countermeasures operations. For multitask countermeasures or situations including more than one countermeasure—

1 Review the individual key estimates listed in Figure B-V-4.

2 Review support activities to determine the general level of success and failures.

3 Look for trends and specific cases decreasing full countermeasures activity.

4 Find the median percent estimate and describe the level of overall success using the median and a verbal description of general support.

B-V-6. **Review and Validate Current Threat.**

a. Validation of the current threat provides a baseline for subsequent analysis of changes in threat operations. For short-term countermeasures operations, the validation should be completed before evaluation of the countermeasures implementation. The analyst must work with the best and most current threat data available. Validated threat is a necessary baseline for evaluation of threat SIGINT/EW operations, and, ultimately, the effectiveness of countermeasures.

b. The operations staff receives and analyzes current information to generate the threat assessment. The information is requested by and transferred to the MDCI analyst for countermeasures evaluation. The procedures for reviewing and validating current threat follow:

(1) Review expected impacts on threat.

(a) Review the objectives and expected results of the countermeasure. Identify any expected impacts of the countermeasure on the threat by asking the following types of questions:

1 Is the countermeasure objective to impair or destroy the capabilities of a known-collector rather than to protect friendly EEFI?

2 Is the threat able to redirect assets toward another friendly vulnerability?

3 Have similar countermeasures worked in other situations against similar threats?

4 How important is the collector to the operations or doctrine of the threat?

5 Is the threat asset an EEFI for friendly operations?

(b) Then complete the review of information by identifying specific threat assets mentioned as targets, and listing these targets for further analysis.

(2) Review threat assessment. Review the threat assessment to determine whether the threat targets are examined and evaluated in the product. if included, quickly review supplemental intelligence reports. If not included, request additional intelligence support to complete a threat review specific to the targets.

(3) Review other intelligence products about threat actions. As necessary, identify recent intelligence reports describing changes in location, capabilities, and intentions of the threat systems.

(4) Validate the threat assessment:

(a) Compare the current threat assessment with the previous threat assessment.

(b) Prepare a list of the existing pre-countermeasures implementation threat.

(c) Validate the list of key indicators by reviewing them for consistency, checking the sources, and if necessary, requesting assistance from the operations staff.

B-V-7. **Identify Changes in Threat Operations.**

a. Current intelligence data collected after countermeasures implementation are used to estimate the effects of implemented countermeasures on the targets identified shown in Figure B-V-5. The MDCI analyst performs this process after the countermeasure has been applied, if it is a short-term operation. In a continuing operation, the analyst performs the process at regular intervals to identify significant changes potentially affecting other countermeasures or operations. If the countermeasure is directed against the threat, the analyst must determine whether the threat has changed and whether friendly vulnerabilities have changed. The analyst integrates the threat information into the countermeasures evaluation.

		CM: Remote DTOC MC Date: 10 Nov 96		
	PRE-CM THREAT INDICATORS	**POST-CM THREAT INDICATORS**	**REMARKS**	**PERCENT CONFIDENCE LEVEL**
Capabilities	Intercept and DF of MC	Increased IMINT and HUMINT		80
Operations	Low level of threat SIGINT Low SIGINT site movement	Increased traffic in threat C^3 Five site movements in a week		80
Intentions	Attack imminent MC jammer in proximity to MBA	No jamming reported for 8 days		100

Figure B-V-5. Countermeasures impact on threat worksheet.

b. The procedures for identifying changes to the threat operations follow:

(1) Compare current and assessed actions. Compare the most recent information in situation reports, intelligence reports, messages, or verbal conversations with the validated threat assessment.

(a) Review the list of threat indicators identified in Figure B-V-5 and the expected impact of the countermeasure on the threat:

1 Examine current intelligence information about the indicators.

2 Examine capabilities, such as the organization of threat resources, their readiness, deployment, equipment, and the introduction of new capabilities to the opposing unit.

(b) Enter any changes in Figure B-V-5. Include any remarks about the implications of the changes, including whether the changes correlate with the expected result of the countermeasure. For example, you receive an intelligence report describing a decrease in threat attempts to intercept allied tactical communications because of electronic protection (EP) built into new radios. The implication is that the friendly vulnerabilities have decreased, causing a change in threat capabilities. The level ranges from 50 percent for a guess to 100 percent for certainty. Higher confidence levels are given for more specific information about an indicator, multiple sources of information, multiple disciplines, or corroboration by another analyst.

(c) Next, review the current intelligence to determine whether any information suggests change to other operations. Examples might include increased IMINT, more active HUMINT, sabotage, or other active pursuits. The redirection of threat efforts increases the estimate and confidence in countermeasures effectiveness against their target. (Although the redirection may also mean changed friendly vulnerabilities.) Update Figure B-V-5.

(d) Review and evaluate intentions:

1 Review the threat assessment for past intentions and examine the current intelligence for indicators of threat intentions.

2 Identify changes by examining whether any current intelligence documents changed intentions and by examining patterns of behavior to see whether they match doctrine. You can attribute the changes in operations to the countermeasures if the changes cannot be explained by doctrine or no documentation of changes exists.

3 Include a confidence level for the interpretation. For example, personnel redeployment following the implementation of countermeasures.

4 Request assistance, if needed, from other members of the intelligence or operations staff knowledgeable about doctrine and plans to help identify changed intentions.

(e) After you complete the identification of changes in the threat, review the results listed in Figure B-V-5. All areas with consistent information about threat changes are highlighted. Any contradictions are noted. Attempt to resolve any contradictions by reviewing data or by requesting assistance from intelligence sources.

(2) Identify and evaluate the significance of changes. A second analysis follows the determination of any changes. Determine how significant the changes are: whether they represent a major change of threat capabilities and intentions, and the overall importance of the change.

(a) Compare past examples of changes in operations, capabilities, and estimate of intentions with the current data. The comparison uses current information compiled in Figure B-V-5, past compilations, and supplementary documentation stored by the analyst. Then review the documents, collect similar threat indicators (for example, types of collectors), and list indicators for threat changes by countermeasures review worksheet shown in Figure B-V-6. Complete this form by entering descriptions of findings. In the search for changes in patterns, ask specific questions about particular threat systems and countermeasures:

1 Does the threat tend to alter collection operations consistently (for example, redirecting assets toward another target or using different assets toward the supported commander's EEFI)?

2 Are threat changes matched with the type of friendly situation?

3 Do threat changes occur after a certain time period of countermeasures application or are they immediate?

4 Does the threat attempt to use EA or EP?

(CLASSIFIED WHEN FILLED IN)					
	Current Threat Changes		Past Changes		
Date	Description	Situation	Description	Situation	Source

Figure B-V-6. Format for threat changes by countermeasures review worksheet.

(b) Use the results from the evaluation of the countermeasures impacts on the threat in the final evaluation of threat indicators. Estimate the significance of a change in threat capabilities and intentions by examining the following five characteristics:

1 Scope of change (how wide is the impact)?

2 Effects of change (how many assets does the change affect)?

3 Level of change (at what echelon in the chain-of-command)?

4 Direction of type of change (what COA was taken)?

5 Overall evaluation of the significance of the change (in comparison with historical data filed in CI database).

(c) Enter each change documented in Figure B-V-5 in the significance of threat changes worksheet shown in Figure B-V-7. Then determine the magnitude of each change (based on a comparison of the previous actions and the actual change identified in the threat indicators).

Classified when filled in							Date _____	
	A	B	C	D	E	F	G	H
Capabilities								
Operations								
Intentions								

Figure B-V-7. Format for significance of threat changes worksheet.

(d) Use a scale of 1 to 5 for ranking the change of each of the six indicators. If the change is large, enter a 5; if small, enter a 1. Then compile and review the individual assessments; a significant change is one in the 4 to 5 range in at least three of the five characteristics or any composite change factor totaling at least 15.

(e) The final step is to estimate the confidence of the assessment of change. Use the 50 to 100 percent scale using the following guide to determine the confidence level:

1 Multiple sources used.

2 Multiple disciplines applied.

3 Multiple analysts agreeing with the assessment.

4 An assessment of the changes in threat operations due to implementation of the countermeasures.

(f) Confidence is high if two of the above criteria are met. Confidence is low if none are met. The confidence level is then entered in Figure B-V-7.

(3) Summarize the analysis in a two-part format. The first part is a short summary of the applied countermeasures, current intelligence reports, and an assessment of the areas of

threat change due to countermeasures implementation. The second part includes the detailed estimate of changes presented in Figures B-V-5 and B-V-7.

B-V-8. **Review Expected C-E Profiles.**

a. The analyst requires a base line of expected friendly profiles to determine whether a countermeasure has had the expected effect on the profiles by reviewing expected patterns and signatures. The data are initially collected to perform the vulnerability a&eskment and are applied during this process.

b. The MDCI analyst—

(1) Reviews expected patterns and signatures by identifying profile information associated with the countermeasures during the validation of the commander's guidance and the summarization of the operation.

(2) Searches the friendly forces database for information about the equipment and operational profiles associated with the countermeasures.

(3) Enters countermeasures-related profile data collected into the profile comparison worksheet shown in Figure B-V-8.

(4) Checks to ensure data are current and complete. If not, requests additional information from the operations and logistic sections.

CM: Remote MC
Date: 10 Nov 96

	EXPECTED		ACTUAL	
	Command and Control	Operations	Command and Control	Operations
Physical Signature	2 x M35A2	1 x M104 1x M35A2	1 x M35A2 1 x M1008	1 x M104 1 x M35A2
Electronic Signature	AN/VRC-46 AN/TRC-145	AN/GRC-142 AN/MRC-108B AN/GRC-106	AN/VRC-46 AN/GRC-142	AN/GRC-142 AN/MRC-108B AN/GRC-106
Pattern Data	MC to DISCOM and DIVARTY		Additional MSE for communication with remote MC	

Figure B-V-8. Profile comparison worksheet.

B-V-9. **Determine Actual C-E Profiles.**

a. The analyst requires valid data about actual C-E profiles after countermeasures application to evaluate the successful change of a command's C-E profile. The analyst needs specific data for comparison with expected profiles to evaluate countermeasures. The analyst updates and maintains the friendly forces C-E profile information. Data sources include the CI database, interviews with personnel, reviews of reports, and review of operations.

b. The procedures for determining actual C-E profiles follow:

(1) Determine data requirements.

(a) Identify specific data requirements to compare the actual and expected profiles. Review this data and ask the following types of questions:

1 What types of equipment are used?

2 What logistic channels are used?

3 Are there SOPs?

4 What doctrinal requirements result in profiles?

(b) Identify specific questions for each countermeasures evaluation.

(2) Collect data about actual C-E profiles. Identify command-specific sources of data to fill the requirements. Common sources include actual participation in operations, new evaluations of equipment and procedures resulting from site surveyor new equipment information, interviews of personnel, and reviews of operational reports. Begin by—

(a) Reviewing reports.

(b) Identifying information about actual profiles.

(c) Matching the data requirements.

(d) Entering data in Figure B-V-8.

(3) Summarize data. After preliminary reviews, information gaps remaining are filled by other sources. This depends on the applied countermeasures and resources available (sufficient personnel and equipment vital to the determination of C-E profile are not available and require EAC augmentation). Verify the descriptions of the profile by using data from at least two sources.

B-V-10. **Compare Expected and Actual C-E Profiles.**

a. The analyst compares what should happen with what does happen to determine whether the countermeasures were effective and whether stated countermeasure results are valid. The comparison contrasts expected C-E profiles, based on historical data, with actual profiles. The analyst performs the comparison and analysis using the CI database and the data collected in paragraph B-V-9.

b. The procedures for comparing expected and actual C-E profiles follow:

(1) Analyze actual command profile:

(a) Review the data generated in paragraphs B-V-8 and B-V-9.

(b) Compare the expected and actual C-E profiles.

(c) Summarize the differences for each attribute.

(d) Note the differences between expected and actual profiles.

(e) Review the comparison to answer the following questions and include these findings in a report to the commander.

1 What attributes most closely matched expected profiles?

2 Were any elements in an organization successful in matching expected C-E profiles?

3 Have adjacent commands or OPSEC policies affected the C-E profiles?

(2) Analyze the relationship between countermeasures expected profile, and actual profile.

(a) Complete an additional evaluation of the countermeasures and profiles to provide an overall review of the countermeasures effect on C-E profiles and to identify additional vulnerabilities as a result of the countermeasures. Note the continuing C-E profile vulnerabilities; list new vulnerabilities identified in the countermeasures review; and document the evaluation.

(b) This information becomes part of the recurring lessons-learned reviews conducted at theater level and is stored locally for continued evaluation.

B-V-11. **Evaluate Countermeasures Effectiveness.**

a. The final process reviews and combines all previous countermeasures evaluations. Both ECB and EAC elements use the information to modify ongoing countermeasures

operations, as summary information for subsequent countermeasures options development, and for training analysts.

b. The procedures for evaluating countermeasures effectiveness follow:

(1) Evaluate the success of countermeasures in meeting specific objectives defined in paragraph B-V-2. Review the findings of each countermeasures evaluation, listing the cases where results of countermeasures implementation met the expectations identified during development of countermeasures options. Compare these successes with the number and type of failures. Repeat this procedure for each type of analysis. A scale for comparing success to failure follows:

(a) 0 percent - Failure.

(b) 25 percent - Marginal success.

(c) 50 percent - Moderate success.

(d) 75 percent - Substantial success.

(e) 90 percent - High level of success.

(2) Evaluate overall success of countermeasures. Using the countermeasures finding-worksheet shown in Figure B-V-9, enter the estimates of success for each of the countermeasures evaluation criteria. For each countermeasure, review the level of success per objective. Count the number of cases where the countermeasure has a greater than 50 percent success rate and divide this number by the total number of cases. The resulting ratio provides an overall estimate of success, supplemented by specific success rates for particular objectives estimated in paragraph B-V-11(1).

Vulnerability: Intercept and DF of DTOC MC				Date: 10 Nov 96
CM APPLIED	**PERCENT ESTIMATE OF CM SUCCESS**	**STRENGTHS**	**WEAKNESSES**	**PERCENT TOTAL SUCCESS RATIO**
Remote MC	50	Causes threat to move often, increasing the chances of friendly observation	Does not remove vulnerability Increases amount of MSE traffic	50

Figure B-V-9. Countermeasures finding worksheet.

(3) Identify strengths and weaknesses. Using this analysis—

(a) Complete a listing of strengths and weaknesses of a given countermeasure in the situation examined.

(b) Use the definition of the situation from paragraphs B-V-2 and B-V-3.

(c) Develop and maintain a list of countermeasures strengths and weaknesses to support countermeasures development in subsequent operations.

(4) Identify assumptions for revalidation. Compare current findings with previous countermeasures analyses. This helps identify continuing problems that require review. For example, regular changes of call signs may have been a sufficient countermeasure in a particular location because the threat was unable to intercept clear voice and was unable to identify stations within the net with any degree of accuracy. Changes in technology, threat operations, and net radio traffic may cause the effectiveness rating of the applied countermeasure to decline. The analyst must recommend a review of the countermeasure as threat operations become more successful. Continual revalidation is a necessary procedure.

(5) Summarize findings. Summarize findings for quick responses to the commander; and produce a lessons-learned review for EAC and theater.

B-V-12. **Produce Output From Countermeasures Evaluation.** Output may consist of reports, briefings, or messages. Many of the forms used as working aids in CI analysis may be attached as summary statements.