copy 3
(18 May 93)

FM 34-7

INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO LOW-INTENSITY CONFLICT OPERATIONS

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

FIELD MANUAL
No. 34-7

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 18 May 1993

INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO LOW-INTENSITY CONFLICT OPERATIONS

Table of Contents

Page

PREFACE iv

CHAPTER 1—THE FUNDAMENTALS OF LOW-INTENSITY CONFLICT 1-1
Definition 1-1
The Low-Intensity Conflict Environment 1-1
The Influences on Low-Intensity Conflict 1-1
The Imperatives of Low-Intensity Conflict 1-2
Operational Categories 1-3
The Continuum of Military Operations and Low-Intensity Conflict 1-7
The Low-Intensity Conflict Continuum Applied 1-9

CHAPTER 2—THE INTELLIGENCE AND ELECTRONIC WARFARE MISSION AND SYSTEM 2-1
The Intelligence and Electronic Warfare Mission 2-1
The Intelligence System of Systems 2-1
The Intelligence and Electronic Warfare Team 2-1
The Intelligence and Electronic Warfare Tasks 2-2
The Intelligence Cycle 2-4
Intelligence and Electronic Warfare Architecture in Low-Intensity Conflict 2-6

CHAPTER 3—INTELLIGENCE PREPARATION OF THE BATTLEFIELD 3-1
Development and Use of Intelligence Preparation of the Battlefield Products 3-1
Battlefield Area Evaluation 3-2
Terrain Analysis 3-5
Weather Analysis 3-8
Threat Evaluation 3-9
Threat Integration 3-16

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Page

CHAPTER 4—ANALYSIS IN LOW-INTENSITY CONFLICT 4-1
Analysis in Depth 4-1
Techniques of Analysis 4-5
Factors of Analysis 4-13
General Conclusions 4-17
Courses of Action 4-17

CHAPTER 5—INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO INSURGENCY AND COUNTERINSURGENCY 5-1
Human Intelligence 5-1
Imagery Intelligence 5-2
Signals Intelligence 5-3
Counterintelligence 5-4

CHAPTER 6—INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO COMBATTING TERRORISM 6-1
Human Intelligence 6-1
Imagery Intelligence 6-2
Signals Intelligence 6-2
Counterintelligence 6-2

CHAPTER 7—INTELLIGENCE SUPPORT TO PEACEKEEPING OPERATIONS 7-1
Information Operations Guidelines 7-2
Predeployment Intelligence Planning 7-2
Information Support 7-2
Command Security 7-3

CHAPTER 8—INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO PEACETIME CONTINGENCY OPERATIONS 8-1
Human Intelligence 8-1
Imagery Intelligence 8-2
Signals Intelligence 8-3
Counterintelligence 8-3

APPENDIX A—ECHELONS ABOVE CORPS INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO LOW-INTENSITY CONFLICT OPERATIONS A-1

APPENDIX B—ELECTRONIC WARFARE SUPPORT TO LOW-INTENSITY CONFLICT OPERATIONS B-1

APPENDIX C—MULTIDISCIPLINE COUNTERINTELLIGENCE SUPPORT TO LOW-INTENSITY CONFLICT OPERATIONS C-1

APPENDIX D—COLLECTION PLAN FORMATS AND INSTRUCTIONS D-1

Page

APPENDIX E—REQUIREMENTS, SOURCES, AND AGENCIES E-1

APPENDIX F—REPORT FORMATS F-1

APPENDIX G—LOW-INTENSITY CONFLICT INTELLIGENCE PREPARATION OF THE BATTLEFIELD GRAPHICS G-1

APPENDIX H—IMAGERY INTELLIGENCE SUPPORT TO LOW-INTENSITY CONFLICT H-1

APPENDIX I—INTERROGATION SUPPORT IN LOW-INTENSITY CONFLICT I-1

APPENDIX J—S2 CHECKLIST FOR COUNTERINSURGENCY OPERATIONS J-1

APPENDIX K—S2 CHECKLIST FOR COMBATTING TERRORISM K-1

APPENDIX L—S2 CHECKLIST FOR PEACEKEEPING OPERATIONS L-1

APPENDIX M—S2 CHECKLIST FOR PEACETIME CONTINGENCY OPERATIONS M-1

GLOSSARY Glossary-1

REFERENCES References-1

INDEX Index-1

PREFACE

The purpose of this manual is to provide doctrine and tactics, techniques, and procedures (TTP) for intelligence and electronic warfare (IEW) in support to low-intensity conflict (LIC) missions. It further provides doctrine and TTP for the organization and operations of IEW assets assigned to units involved in LIC missions.

This manual also emphasizes the support roles that the military intelligence (MI) brigade echelons above corps (EAC) or theater and national level assets play in a variety of LIC missions. It amplifies doctrine contained in FM 34-1, FM 34-2, FM 34-3, FM 34-36, FM 34-37, FM 34-60, and FM 34-130. It is consistent with MI issues of LIC operational doctrine in FM 100-20.

This manual is designed for use by all commanders and their staffs. It is intended for use by Active Component (AC), Reserve Components (RC), and Army National Guard (ARNG) units.

The proponent of this publication is the United States Army Intelligence Center and Fort Huachuca, Fort Huachuca, Arizona. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, US Army Intelligence Center and Fort Huachuca, ATTN: ATZS-TDL-D, Ft Huachuca, AZ 85613-6000.

This manual does not implement any international standardization agreements.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

CHAPTER 1

THE FUNDAMENTALS OF LOW-INTENSITY CONFLICT

This manual is about IEW support to LIC operations. The purpose of this chapter is to provide framework for the subsequent discussion of how IEW supports LIC in each of the four operational categories: support for insurgency and counterinsurgency, combatting terrorism, peacekeeping operations (PKO), and peacetime contingency operations (PCO).

This chapter also defines LIC, describes the LIC environment and its critical elements, the operational continuum, and the LIC imperatives. The level of detail is structured to assist you in understanding the doctrine and TTP described in this manual. For more information on military operations in LIC, see FM 100-20.

DEFINITION

LIC is a political-military confrontation between contending states or groups below conventional war and above the routine, peaceful competition among states. It frequently involves protracted struggles of competing principles and ideologies. LIC ranges from subversion to the use of armed force. It is waged by a combination of means employing political, economic, informational, and military instruments. LICs are often localized, generally in the Third World, but contain regional and global security implications.

THE LOW-INTENSITY CONFLICT ENVIRONMENT

Many people associate LIC with involvement in countries such as El Salvador, Nicaragua, or Vietnam. These are examples of insurgencies, and an insurgency is only one of several forms which LICs can take. Many natural and manmade disasters and international confrontations short of war will present the United States with a constant flow of political-military missions in the LIC environment. To deal with these, we must understand the driving political and socio-economic forces behind them.

THE INFLUENCES ON LOW-INTENSITY CONFLICT

Major factors feeding LICs are change, discontent, poverty, violence, and instability. The interaction or combination of these conditions create environments conducive to LIC. If, for example, a hurricane devastates an impoverished nation, the change and instability may contribute to a LIC environment. In this case, a need for rescue and recovery operations (RRO) and disaster relief—both being PCO—may be required.

CHANGE

Socio-economic changes raise tensions in a society. Governments must be aware of the feelings of the people and react, within reason, to their desires. By being proactive and keeping in touch with popular demands, a government can make changes and yet maintain order.

For example, prior to the fall of Nicaraguan leader Anastasio Somoza, in 1979, the population of that country had endured decades of repression. The ruling Somoza family ignored the needs and desires of the population. The opposition party, Frente Sandinista Liberacion Nacional (FSLN), proclaimed it would bring popularly desired democratic political reforms and economic improvements to the masses. With popular support, the FSLN ousted the Somoza regime.

Ironically, the population became discontented with the FSLN's communist state. Again, political and economic change brought turmoil to the country. Ultimately, a democratic election was held in which the FSLN was defeated.

This situation highlights the point that a government not in touch with, or even concerned with, the wishes of the people will experience internal strife.

DISCONTENT

Discontent takes on many forms. Any time people think or feel they have been cheated or wronged, and given the opportunity, they will take action. As noted above, the Nicaraguan people felt cheated over the years by the Somoza family and wanted change. To bring about this change, a violent, bloody conflict followed.

Not all forms of discontent will be violent. The amount of perceived injustice often determines the level of discontent. The critical factor influencing the level of discontent is the number of people with the same feeling or the impact of outside pressure.

For example, the people of Panama were unhappy for years with General Manuel Noriega's stranglehold on their country, yet they did not have enough support to overthrow him. For nearly two years a sector of the Panamanian people openly, but mildly, opposed Noriega. It was only with US intervention and assistance that they were able to rid themselves of him.

POVERTY

As mentioned before, poverty or unstable economic conditions are influencing factors on LIC. Impoverished nations are ripe for change and revolution. The masses are anxious for an improved standard of living.

The smart revolutionary leader determines what the populace wants from economic change. He will not second guess nor attempt to read their minds and force unwanted reforms.

Typically, the populace desires only what they consider to be their fair share: a few more hectares of land perhaps. It is easy for the revolutionary to promise such things and gain the popular support of the people.

Consider the labor movement led by Lech Walesa in Poland a few years ago. While some violence was encountered through demonstrations; economic advances, labor reforms, and ultimately freedom were accomplished.

VIOLENCE

The danger of violence is a dominant force in any LIC mission. Do not consider the threat as the only source of violence. You may encounter a repressive host nation (HN) or third-party country that engages in violence against its detractors as well as its own population. The violence created by a natural disaster combined with the HN lack of humanitarian relief (by intent or lack of resources) also will be a negative force. Violence produces instability.

INSTABILITY

Instability within the general population, the military, or the government of a nation develops from any or all of the preceding forces. Instability, a force in any LIC mission, is not always bad. Consider instability created by a counterinsurgency operation. The insurgency element will consider instability an asset; the HN will not.

The Somoza regime in Nicaragua did not like the instability created by the FSLN. The FSLN, however, relished the inactivity of the Somoza regime following the earthquake of 1972 because they mobilized the impoverished, disaster-stricken populace to revolt.

THE IMPERATIVES OF LOW-INTENSITY CONFLICT

The following five imperatives are common to each LIC category. Success in LIC requires the use of these as a checklist in your mission planning stage.

POLITICAL DOMINANCE

Civil authority and political objectives drive military decisions at every level. These political objectives must be understood as they affect military operations and influence selected courses of action (COAs). Civil authority must adopt COAs that legally support those objectives even if the COAs appear to be outside the traditional military doctrine.

UNITY OF EFFORT

Consider how military actions integrate with, and contribute to, initiatives of other government agencies. Interagency coordination is critical. Commanders may answer to civilian chiefs or employ the resources of civilian agencies.

ADAPTABILITY

This is the skill and willingness to change or modify structures and methods to meet different situations. Adaptability is more than merely tailoring or the built-in flexibility of common techniques and organizations. It means developing new ones appropriate to each situation.

LEGITIMACY

Legitimacy stems from the willing acceptance by the governed of the right of the government to rule. It comes from the belief that authority is genuine and effective and uses the proper agencies for reasonable purposes. Legitimacy is the central concern of all parties involved in a conflict.

PERSEVERANCE

LIC, by nature, typically involves protracted struggles. Perseverance requires careful, informed analysis to select the right time and place for decisive action. Perseverance is the patient, resolute, and persistent pursuit of goals and objectives for as long as it takes to achieve them.

OPERATIONAL CATEGORIES

US military operations in LIC fall into four broad categories. They are—

- Support for insurgency and counterinsurgency.
- Combatting terrorism.
- PKO.
- PCO.

LIC operations may involve one or more of these categories. Understanding the similarities and differences between the operational categories helps establish priorities in actual situations.

SUPPORT FOR INSURGENCY AND COUNTERINSURGENCY

US security interests may lie with an incumbent government or with an insurgency. Both insurgencies and counterinsurgencies concern themselves with mobilizing the support of the people. How they distribute their efforts between building support for themselves and undermining the support and legitimacy of their opponents is the central dilemma for both insurgents and counterinsurgents.

This point is highlighted by the situation in El Salvador leading up to the cease-fire implemented 1 February 1992. The opposition force, Frente Farabundo Marti de la Liberacion Nacional (FMLN), tried to build support for itself with the population while at the same time discrediting the government. This was a difficult task, as the FMLN did not want to discredit itself by conducting actions against the government that offended the populace.

Insurgency

An insurgency is an organized and armed political struggle, the goal of which may be to seize power through revolutionary takeover and replace the existing government. In some cases insurgency goals may be more limited. For example, the insurgency may intend to break away from government control and establish an autonomous state within traditional ethnic or religious territorial bounds. The insurgency may also only intend to extract limited political concessions unattainable through less violent means.

There are seven elements common to all insurgencies:

- Leadership.
- Ideology.
- Objectives.
- Environment and geography.
- External support.
- Phasing and timing.
- Organizational and operational patterns.

These elements provide a framework for analysis which can reveal the insurgency's strengths and weaknesses. Although you examine them separately, you must understand their interaction to fully understand the insurgency. Chapter 5 and FM 100-20, Appendix C, explain this fully.

The US supports selected insurgencies opposing oppressive regimes working against US interests. We coordinate this support with our friends and allies. Feasibility of effective support and the compatibility of US and insurgent interests are major considerations.

Support for insurgency is often covert, and many of the operations connected with it are special activities. Special operations forces (SOF) are well-suited to provide this support because of their extensive unconventional warfare (UW) training.

General purpose forces may be called upon when the situation requires their functional specialties. Their tasks may include support and advice. Command and control (C^2) relationships are normally situation-specific.

When ordered, US armed forces provide equipment, training, and services to the insurgent force. Types of operations in which US forces can assist insurgents include—

- Recruiting, organizing, training, and equipping forces to perform UW or guerilla warfare.
- Psychological operations (PSYOP).

- Institution and infrastructure development.
- Intelligence gathering.
- Surreptitious insertions.
- Linkups.
- Evasion and escape of combatants.
- Subversion.
- Sabotage.
- Resupply operations.

Counterinsurgency

Counterinsurgency is all military, political, economic, psychological, and civic actions taken by a government focused on defeating an insurgency. It can provide guidance for the organization and conduct security force operations based on the HN internal defense and development (IDAD) strategy.

A nation's IDAD strategy is the full range of measures taken by them to promote their growth and to protect themselves from subversion, lawlessness, and insurgency. It focuses on building viable political, economic, military, and social institutions that respond to the needs of society. Its fundamental goal is to prevent insurgency. It does this by forestalling and defeating the danger from insurgent organizations, and at the same time working to correct those conditions that foster instability.

The government mobilizes the population to participate in IDAD efforts. IDAD is, ideally, a preemptive strategy against insurgency. However, if the insurgency develops, it provides a framework for counterinsurgency activities.

The IDAD concept uses all the leadership, organizational, and material resources available to the HN. The HN identifies the real or imagined grievances of its people and takes political, economic, and social actions to redress them. It acts in an orderly way within its constitutional system. The actions it takes should gain popular support for the HN and forestall insurgent efforts. HN security forces (military, paramilitary, and police) defeat insurgent combat elements, neutralize their leadership, and establish a peaceful environment in which social progress develops.

The HN cannot depend upon outside combat forces to wage their battles for them. HN security forces support the development effort through civil-military operations conducted in accordance with the HN IDAD plan.

The US uses its military resources to support HN counterinsurgency operations under a foreign internal defense (FID) agreement. FID is the participation by civilian and military agencies of one country in any of the action programs another government takes to free and protect its society from subversion, lawlessness, and insurgency. The US ambassador, through his country team, provides the focal point for interagency coordination and supervision of FID.

Military support to FID is provided through the unified Commander in Chief (CINC). The US conducts FID operations in accordance with the HN's IDAD concept. The US may provide materiel, advisors, trainers, and security assistance forces to support the HN counterinsurgency operations through the security assistance office (SAO). More direct forms of support may be provided when required, such as advisors and trainers and FID augmentation force.

The US provides support to counterinsurgency based on a National Command Authorities (NCA) decision. US support to HN counterinsurgency programs is a balanced effort of both civil and military support.

The principal US role is to augment security assistance programs by providing military training, technical training, and intelligence and logistical support. The objective of military involvement is to—

- Improve the efficiency of the supported security force and its military operations.
- Help stop external support to the insurgency.
- Augment other US government agency efforts.

US forces activities in support of HNs that conduct counterinsurgency include—

- Intelligence operations.
- Joint-combined command post (CP) exercises.
- Civil-military operations, including civil affairs (CA) and PSYOP.
- Humanitarian or civic assistance.
- Logistical support.
- Populace and resources control.
- Counter-drug operations.
- Tactical operations.

COMBATTING TERRORISM

Terrorism is the calculated use of violence or threat of violence to inculcate fear; it is intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

It is often difficult to distinguish the acts of politically motivated terrorists from acts performed by criminals. Criminal acts create similar tactical problems for security forces, but normally have no political intent nor effect. Some criminal organizations, especially drug traffickers, have become powerful enough to have broad political interests. When they pursue these interests by terrorism, they become a military concern like any other political terrorist group.

The terrorist neither needs nor necessarily wants popular support. Terrorist organizations and movements require secrecy. Their activities do not conform to rules of law or warfare. Their victims are frequently innocent bystanders, or symbolic persons and places, and usually have no role in either causing or correcting the terrorist's grievance. Terrorist acts include threats of (or actual) hostage taking, hijacking, sabotage, assassination, arson, hoaxes, bombings, and armed attack.

The aim of combatting terrorism is to protect innocent lives and property. Combatting terrorism includes both antiterrorism (AT) and counterterrorism (CT) actions throughout the entire continuum of military operations. The combatting terrorism program is designed to provide coordinated action before, during, and after terrorist incidents.

Antiterrorism

AT involves all measures taken by installations, units, or individuals to reduce the probability of their falling victim to terrorist acts. Educational programs, physical security, personal protection techniques, and operational patterns are all examples of making a target less appealing to a terrorist. Announcing military police (MP) searches of cars entering installations and the hardening of facilities by using fences, walls, and other protective devices are forms of AT.

Counterterrorism

CT is the full range of offensive measures to prevent, deter, and respond to terrorism. Participation in CT actions is normally limited to specially trained and equipped forces kept on alert status for that purpose. One example of this is the Israeli operation to rescue the airline passengers held hostage in Entebbe, Uganda, in 1976.

PEACEKEEPING OPERATIONS

PKO are military operations conducted with the consent of the belligerent parties to a conflict to maintain a negotiated truce and to facilitate a diplomatic resolution. The US may participate in PKO under the auspices of an international organization, in cooperation with other countries, or unilaterally. PKO support diplomatic efforts to achieve, restore, or maintain the peace in areas of potential or actual conflict. PKO include—

- Withdrawal and disengagement.
- Cease-fire.
- Prisoner-of-war exchange.
- Arms control.
- Demilitarization and demobilization.

When an operation is approved, Department of Defense (DOD) designates a service to be executive agent for the specific operation. The executive agent provides administrative personnel, together with operational and logistic support. It also provides command, control, and communications (C^3) support for committed US military forces. It may also assist forces of other nations when in accord with diplomatic agreement.

The three key administrative documents used to address problems the force will face are discussed below.

Terms of Reference (TOR)

The TOR, similar to an operations order (OPORD), is published by the executive agent. It describes how the US will implement its portion of the operation. The TOR, which may be subject to approval by each party to the dispute, describes—

- The mission.
- Command relationships.
- Organization.
- Logistics support.
- Accounting procedures.
- Responsibilities of the US contingent to the peacekeeping force.
- Coordination and liaison arrangements.

Your force will operate strictly within the parameters of its TOR, doing neither more nor less than it mandates. A distinguishing feature of these operations is that the peacekeeping force normally is forbidden to use violence to accomplish its mission. In most cases, it can use force only for self-defense. The multinational force and observers in the Sinai region are examples of this type of mission.

Letter of Instruction (LOI)

LOIs are prepared by the major organization tasked with providing units and elements of the US peacekeeping force contingent. LOIs amplify information contained in the TOR. Each LOI contains information on—

- Organization and equipment.
- Operations.
- Intelligence.
- Personnel.
- Logistics.
- Communications-electronics (C-E).
- Public affairs.
- Finance.
- Air operations.
- Nuclear, biological, and chemical (NBC) defense.
- Command relationships.

Area Handbooks

You will directly produce area handbooks. They contain, at a minimum, information on—

- The peacekeeping organization.
- History and culture of the people.
- Terrain.
- Weather.
- Local armed forces.

You may decide to include graphic information on the insignia, markings, and identifying characteristics of armed forces, military weapons, and equipment.

PEACETIME CONTINGENCY OPERATIONS

PCO are politically sensitive military operations normally characterized by short-term, rapid projection or employment of forces in conditions short of war. They are often undertaken in crisis avoidance or crisis management situations requiring the use of military power to enforce or support diplomatic initiatives. PCO include, but are not limited to—

- Shows of force and demonstrations.
- Noncombatant evacuation operations (NEO).
- RRO.
- Strikes and raids.
- Peacemaking.
- UW.
- Disaster relief operations (DRO).
- Counter-drug operations.
- Security assistance surges (SAS).
- Support to US civil authorities.

Military efforts in PCO complement political and informational initiatives. This relationship distinguishes PCO from contingency operations in war, which are often conducted for purely military objectives. Clear command relationships and communications procedures must be established by agreement, because the lead organization varies according to the type of mission. Your understanding of C^3 matters is necessary to ensure smooth coordination of the effort.

PCO use tailored forces, are usually short in duration, and are joint or combined. Military forces employed in PCO will normally use service-specific tactical doctrine or joint tactics, techniques, and procedures (JTTP) in executing their mission.

A basic tenet is to rapidly project military forces consistent with the factors of mission, enemy, terrain, troops, and time available (METT-T) in order to bring the contingency to an immediate close under conditions favorable to the US.

The forces employed will be chosen from designated contingency forces who have planned and trained for these types of operations. The time available will rarely allow any other forces to train to the required standard necessary for the successful conduct of the operation.

As a result, it is your responsibility to have all current intelligence products and graphics on hand to support an operation. Mapping, charting, and geodesy (MC&G) products should also be on hand and in sufficient quantities to support your contingency.

The unifying feature of these disparate actions is the rapid mobilization of assets to focus on a specific problem. This usually is a crisis and guided at the national level. Frequently, these operations take place away from customary facilities, requiring deep penetration and temporary establishment of long lines of communication (LOC) in a threatening or hostile environment.

PCO may require the exercise of restraint and the selective use of force or concentrated violent actions. A wide array of options for US force employment exists. Limited in duration and usually focused on a specific objective, they do not always require combat operations. Two examples follow:

- Operation BLAST FURNACE was the 1986 aviation task force support of the Bolivian Narcotics Police involving six UH-60 helicopters with an accompanying support security and intelligence package. The mission was to assist in targeting cocaine production laboratories and to transport HN security personnel to conduct raids.
- Operation HAWKEYE was the XVIII Airborne Corps Task Force deployment to the island of St. Croix to assist local law enforcement following hurricane Hugo in 1989. The task force (TF) included C^3, MP, CA, and medical personnel.

THE CONTINUUM OF MILITARY OPERATIONS AND LOW-INTENSITY CONFLICT

With these missions in mind, we can examine the continuum of military operations. This review highlights the possibility of your being involved in two or more missions at the same time. It also shows you the possibility of being involved in different levels of conflict at the same time.

Routine peaceful competition is the normal desired end state of global interests. The states of the world pursue their own interests, sometimes in harmony, but with enough common interests to avoid violence. This is the relationship of nations, both internally and externally, during what is commonly referred to as *peacetime.*

To preserve this peaceful environment and to achieve US goals, our military focuses on deterring war, but supports political, economic, and informational efforts.

Figure 1-1 shows the continuum of military operations in LIC. Do not define boundaries between the categories when you view the continuum. This allows you to realize that you may have different levels of conflict at the same time. For example, in Vietnam conventional US forces were battling conventional North Vietnamese forces in one area, while at the same time US Special Forces were conducting UW and civic action in others.

It is possible to jump across the continuum, either escalating or decreasing the scope of the conflict without stopping at intermediate points on the scale.

It is likely that the cessation of hostilities at one level will not result in the resumption of routine peaceful engagement but in a move to some level of LIC. This was the case following the conclusion of the 1973 Arab-Israeli war, with the 1979 Camp David Accords resulting in the ongoing United Nations (UN) PKO in the Sinai.

Within this continuum, the US can find itself in peacetime engagement with one nation, at war with another, and in hostilities short of war with still another nation—all at the same time.

As PCO of the past decade reveal, the operational continuum is nonlinear. This permits operations to flow in all directions. This is a key point of the operational continuum: operations do not end after the cessation of hostilities—just as they do not begin with the firing of the first shot.

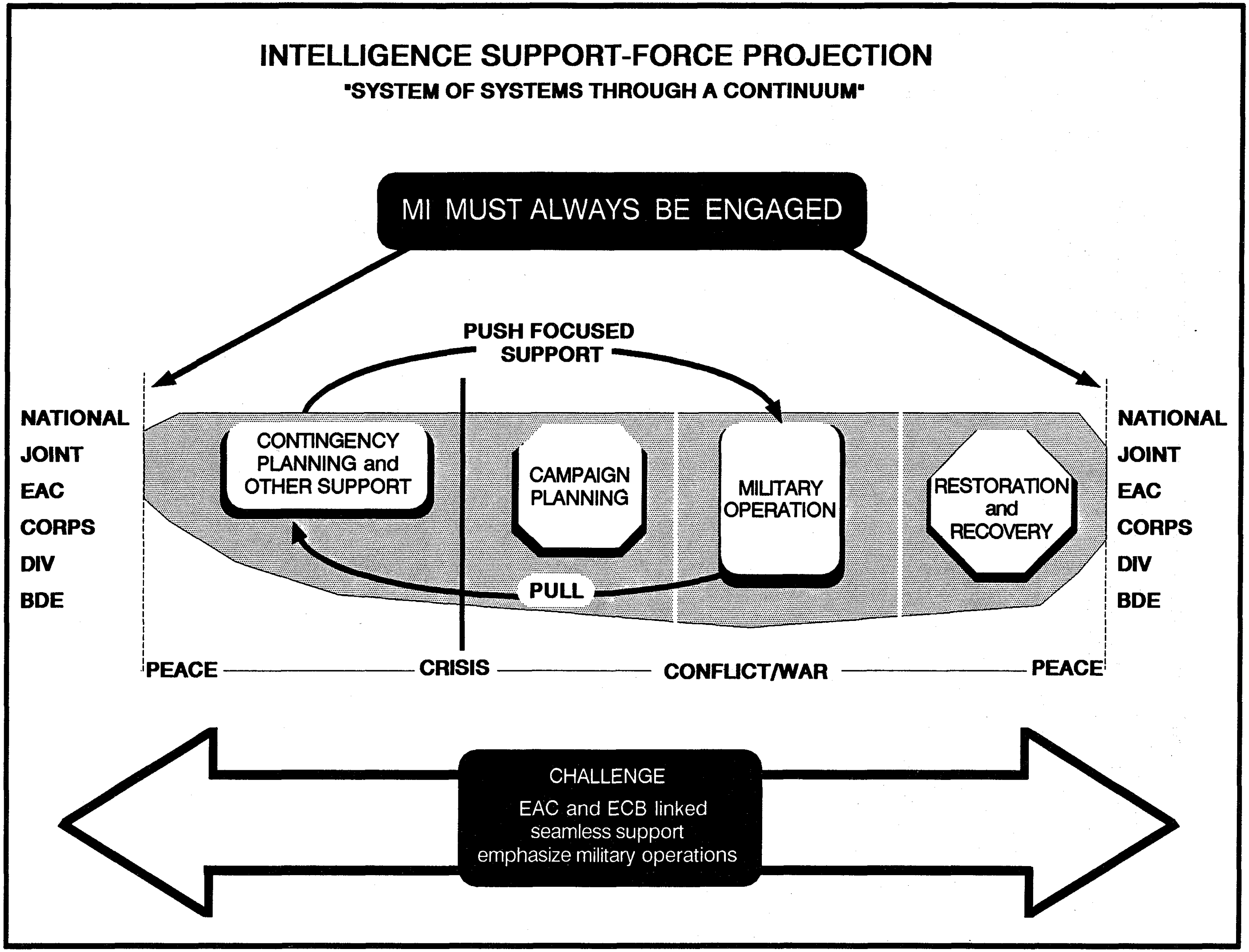


Figure 1-1. Continuum of military operations in LIC.

THE LOW-INTENSITY CONFLICT CONTINUUM APPLIED

The US and Iraq were in peacetime engagement following the Iran-Iraq war. The US was hoping to influence Baghdad and pull it out of the Soviet sphere. But in July 1990, Iraq massed troops on the Kuwaiti border and threatened to invade if Kuwait did not cut its oil production.

The US response was mostly in the diplomatic arena; however, we held joint air defense exercises with our Persian Gulf allies, which placed us on the brink of hostilities short of war. When Iraq appeared to back off, it looked as though the situation would revert to peacetime engagement.

However, after Iraq's invasion of Kuwait and the subsequent execution of Operation DESERT SHIELD, the US and Iraq entered into hostilities short of war. Had Operation DESERT SHIELD succeeded in convincing Iraq to withdraw from Kuwait, it would not have been necessary to move into the next environment of the continuum—War.

However, after months of diplomatic and military maneuvering, the US and its allies initiated Operation DESERT STORM, and we crossed over into war. Initially, the allies limited their actions to aerial bombing hoping to persuade Iraq to withdraw.

Again, it was Iraq's failure to withdraw that forced the allies to move deeper into the war environment of the continuum with the initiation of ground operations. After the 100-hour ground war, the allies called a halt to offensive operations but maintained forces inside Iraq—thus moving back into hostilities short of war.

Still within that area on the continuum, the situation with the Kurdish refugees in northern Iraq caused the US to initiate Operation PROVIDE COMFORT and Operation GALLANT PROVIDER. The ultimate allied goal is to work through the operational continuum while rebuilding Kuwait and Iraq, and to reestablish the environment of peacetime engagement.

CHAPTER 2

THE INTELLIGENCE AND ELECTRONIC WARFARE MISSION AND SYSTEM

This chapter describes the IEW mission, the intelligence system of systems, the IEW team, and the six IEW tasks that support the commander. It also outlines the intelligence cycle, order of battle (OB) factors, analysis, and some of the assets available in a LIC environment.

THE INTELLIGENCE AND ELECTRONIC WARFARE MISSION

The IEW mission is to provide timely, relevant, and accurate support to tactical, operational, and strategic commanders across the scope of military operations. It reduces uncertainty and risk to US Forces and permits effective application of combat power.

THE INTELLIGENCE SYSTEM OF SYSTEMS

As the IEW mission states, all intelligence efforts are designed to support commanders. Army intelligence assets are integrated with other national and theater intelligence assets to operate as a system of systems. The system of systems provides responsive, tailored, balanced, all-source intelligence to support the mission planning and execution needs of theater, operational, and tactical commanders across the scope of military operations.

The intelligence system is a seamless system flowing from the national level down to and including the individual soldier in the field. This system is extremely flexible and can support theater, corps, or discrete units from brigade TFs to joint task force (JTF) levels. The entire system focuses on the force commander and *pushes* intelligence to the echelons that need it, while retaining the capability to respond to specific intelligence requirements in a *pull* mode.

THE INTELLIGENCE AND ELECTRONIC WARFARE TEAM

At each echelon, the force commander is the IEW team leader. He directs the intelligence process through his intelligence battlefield operating system (BOS). The IEW BOS consists of the basic intelligence tasks with the addition of EW and CI. By understanding the intelligence BOS capabilities and limitations, the commander can synchronize it to support his concept of the mission. Under his direction, the intelligence BOS becomes a significant combat multiplier.

Before the operations begin, the force commander focuses his intelligence effort by establishing priority intelligence requirements (PIR). When these initial PIR are answered, the commander uses the resulting information and intelligence to—

- Seize the initiative.
- Eliminate or reduce the risk of surprise.
- Begin to shape the battlefield.

As current PIR are answered, the commander continues to direct his intelligence BOS by developing new PIR, based on current and projected METT-T factors. In this way, the commander ensures the system remains tightly focused on providing the intelligence and targets he needs throughout the operation.

The G3 and S3 work closely with the G2 and S2 to make sure they thoroughly understand the commander's mission objectives and possible COAs. Based on this knowledge, the senior intelligence officer (SIO) develops predictive intelligence that is synchronized with the commander's scheme of maneuver. The SIO then advises his commander on ways to focus and leverage combat power during the battle.

At brigade, the intelligence and electronic warfare support officer (IEWSO) serves as liaison between the MI units and the G2 or S2 and G3 or S3. Appendix A contains information on MI Brigade (EAC). The IEWSO also can request information from special intelligence channels.

MI commanders lead, train, fight, and sustain their IEW units. They provide MI assets to support the effort. MI commanders provide direct support (DS) and general support (GS) assets, as well as combat information and intelligence from other sources, to support their ongoing organic collection efforts. Regardless of rank, the MI unit commanders respond to the S2's or G2's intelligence taskings. The MI unit commander must answer each tasking no later than the suspense set by the S2 or G2.

THE INTELLIGENCE AND ELECTRONIC WARFARE TASKS

There are six IEW tasks, which are discussed below. These tasks are interdependent, concurrent, and synergistic and support the IEW mission.

All echelons from maneuver brigade to the Army component have the basic capability to do these tasks, but in varying levels of detail depending upon the echelon, situation, and operational environment. When necessary, the force commander prioritizes these functions.

INDICATIONS AND WARNING (I&W)

I&W gives the commander as much early warning of hostilities as possible. It is used to develop and refine indicator lists of threat activities and possible intentions. It is derived from any source that detects and reports time-sensitive threat information.

At operational and tactical levels, I&W is a product of the situation development and force protection functions. It concentrates on avoiding surprise and in detecting enemy actions that prove or run counter to planning assumptions. Proper use of I&W helps the SIO select and put in place the right combination of collection and analysis support assets before the battle begins.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD (IPB)

IPB applies across the scope of military operations. At the strategic and operational levels, IPB is used to focus the intelligence effort and, at theater, build a basic intelligence data base. IPB also is used to focus the intelligence effort in theater, as well as support strategic and campaign planning, and build a data base. At the operational and tactical levels, IPB is the key to focusing and integrating the intelligence effort within a commander's specific area of operation (AO) and area of interest (AI).

IPB integrates the environment with the enemy's fighting doctrine. It reveals his capabilities and vulnerabilities and allows the commander to systematically predict enemy actions. It also helps the commander to understand the battlefield and synchronize the BOS for maximum effect.

The SIO (G2 or S2) coordinates the IPB process for the commander, but IPB involves all staff elements because it supports the commander's decision-making process. IPB products are integrated into situation development and support current situation and predictive intelligence requirements.

In LIC, as in other combat environments, IPB is continuous. The standard IPB process will work when applied to a LIC operation, but requires some alteration, primarily in focus and thought processes. For example, in LIC, demographic information and analysis must be added into the IPB process.

Demographic information is simply information about the population. Analysis is the process used to determine the significance of raw data, relative to information and intelligence already known, and to draw deductions about the meaning of the evaluated information (see Chapter 3).

IPB draws upon intelligence efforts at all levels, but the best tactical intelligence is often built *bottom up* from subordinate units. Information flow and reports from below are vital to developing detailed intelligence pictures. Even events that do not happen and an enemy who is absent can serve as valuable indicators for the commander.

In the end, these details must be integrated into a clear picture on which the commander can base his decisions. Using overlays, graphic displays, and templating techniques, the IPB process increases the accuracy and timeliness of intelligence by making it easier to synchronize intelligence support.

SITUATION DEVELOPMENT

Situation development is a dynamic process. It is the basic overarching and continuous process used to develop intelligence. It folds in all the information and intelligence produced or derived from the other five tasks as well as from the intelligence BOS and other combat, combat support (CS), and combat service support (CSS) sources.

Situation development confirms or denies enemy. COAs predicted in IPB. This enables the commander to make timely decisions. It provides the commander and his staff with concise, successive, and objective *snapshots* of the situation within his AO.

During military operations, situation development takes the place of tactical and operational level I&W functions. The situation development process (guided by the IPB process, the intelligence estimate, and current intelligence reporting) allows the SIO to project threat intentions and the effects of political, economic, and social factors, as well as weather and terrain. This gives the commander the time to plan in detail. The process also supports strategic and national I&W.

At the conclusion of, or a halt in, military operations, the tactical and operational level situation development and I&W functions concentrate on helping the commander avoid surprise, protect the force, and support follow-on operations.

TARGETING AND TARGET DEVELOPMENT INCLUDING SUPPORT TO ELECTRONIC WARFARE (EW)

Targeting and target development identify high-value targets (HVTs) and high-payoff targets (HPTs) that support the commander's concept of the operation. Then they detect and locate those targets with sufficient accuracy for attack by fire, maneuver, psychological, and electronic means. This task is integrated with situation development to provide the commander with accurate, timely locations of threat activities, locations, and weapon systems.

Because the commander's intent may be satisfied by delaying, disrupting, destroying, or dissuading an enemy target, targeting data must be accurate and timely enough to support an effective attack by maneuver, fire, or electronic means.

Target acquisition priorities are established before the operation begins. These priorities are firmly based on the commander's concept, a thorough understanding of the enemy, and how the enemy is most likely to present his forces on the battlefield.

In LIC, MI units directly support dynamic target development and target acquisition by precisely locating and nearly simultaneously disseminating the information needed to strike targets effectively. A high priority in LIC (as well as other conflict environments) is to identify critical enemy vulnerabilities that can be exploited. Weaknesses that can be turned into exploitable vulnerabilities also have a high priority.

As in all military operations, LIC target priorities may change dynamically, based on the progress and success of the operation. Continuous interactive situation and target development throughout the operation support this target acquisition requirement.

EW supports targeting and target development by disrupting, exploiting, and deceiving enemy C^2 systems while protecting friendly use of communications and noncommunications systems. EW is both offensive and defensive in nature. Proper application of its three primary components—electronic warfare support (ES), electronic combat (EC), and electronic protection (EP)—represents a significant contribution to command, control, and communications countermeasures (C^3CM). The three EW components (formerly known as ESM, ECM, and ECCM) are discussed in Appendix B.

BATTLE DAMAGE ASSESSMENT (BDA) INCLUDING POST STRIKE ASSESSMENT (PSA)

BDA is a timely and accurate all-source analysis product developed as part of the collection management and analysis production process. It is developed at strategic, operational, and tactical levels—from national level agencies down to division. (See the glossary for definitions of each level of BDA.)

In large or joint operations, the bulk of BDA generally is developed and disseminated at the operational level as a joint intelligence product. However, in LIC operations, BDA will generally be produced by the division G2.

In LIC, the G2 or S2 uses BDA to confirm or deny changes to enemy transportation methods or patterns of activity that directly affect friendly operations. This makes BDA a predictive tool, as well as a measurement tool for evaluating the degree of success of a military operation, engagement, or battle.

The SIO also uses BDA to evaluate the results of a military operation or battle in terms of the damage done to the enemy and as a baseline to estimate the enemy's remaining combat effectiveness, capabilities, and intent.

The commander uses BDA to reduce risk and uncertainty. BDA gives the commander a continual assessment of enemy strength and the effect of friendly operations on the enemy. It is a means to measure progress, to determine if restrike is necessary, and to determine how close the commander is to accomplishing his targeting goals, strategy, and plan.

This makes BDA a force multiplier, as well as a measurement tool.

PSA is a subset of BDA. A PSA is a running tally of enemy weapons systems and units destroyed or rendered ineffective. All SIOs at all echelons and levels perform PSA. Initial PSAs are integrated into BDAs. They are also used to support BDA post-mission assessments and after-action reports (AARs).

FORCE PROTECTION INCLUDING COUNTERINTELLIGENCE AND SUPPORT TO OPERATIONS SECURITY

Force protection identifies the elements of your force most important to the threat and those elements most vulnerable to detection and attack. It denies the threat the opportunity to engage friendly forces, and lets the commander achieve maximum surprise on the battlefield.

Force protection is a difficult task in LIC. That is why in LIC the essence of counterintelligence (CI) is force protection. CI operations counteract insurgent, foreign intelligence, and terrorist threats to the friendly force.

CI operations include identifying multidiscipline intelligence collection and terrorist threats, determining friendly vulnerability to those threats, and recommending and evaluating appropriate operations security (OPSEC) countermeasures. Multidiscipline counterintelligence (MDCI) operations collect on and neutralize foreign intelligence and security services (FISs) and support friendly OPSEC, deception, and rear area operations. CI agents must be language qualified so they can conduct low-level source operations (LLSO) and HN liaison activities.

Generally, CI units at EAC have area, regional, or subject matter responsibilities. CI units at corps and below are part of the tactical force and have a clearly defined primary responsibility to their parent unit. They may be called upon to support EAC elements in their operations or to participate in EAC CI operations. Appendix C provides details of MDCI support and MDCI analysis in LIC.

THE INTELLIGENCE CYCLE

Intelligence operations at all echelons and levels of war generally follow a four-step process known as the intelligence cycle. This cycle includes directing, collecting, processing, and disseminating intelligence.

Although the cycle involves sequential steps, it is a continuous process and functions often occur at the same time. For example, while available information is processed, collection assets can be tasked for more information. At the same time, finished intelligence, combat information, and target acquisition data are disseminated as they become available.

To maximize the effectiveness of the intelligence cycle, the commander must select two or three PIR that focus on his most critical needs. Properly designating PIR and target acquisition priorities substantially contribute to the quality and timeliness of intelligence products and targets.

Although no commander can know everything he would like to know, he can count on the intelligence system to meet his most critical needs if he focuses his limited intelligence assets on them sequentually.

The SIO at each echelon develops an intelligence synchronization matrix to ensure the intelligence effort fully supports the commander's concept of the operations by providing relevant intelligence to the commander when he needs it and in the desired format. (See Figure D-10 for a sample synchronization matrix.)

STEP 1. DIRECTING

The commander, through his S2 or G2, directs the intelligence effort. The S2, G2, or collection manager performs collection management planning before the operation begins. He also guides the effective employment of collection assets during the operation.

The intelligence section develops and maintains graphic data bases through research and IPB. IPB, coupled with available data bases, provides a foundation for situation and target development. This gives the G2 or S2 a way to project events or activities in the operational area and to predict threat COAs. Comparing these projections with actual events provides commanders with timely, complete, and accurate intelligence.

Intelligence agencies from national level down constantly develop and maintain intelligence data bases. G2s and S2s can access these data bases to prepare initial intelligence estimates and to analyze the AO. G2s and S2s must ensure their analysis is based on mission requirements and the commander's PIR.

The resulting product is an intelligence estimate. It is integrated with other staff estimates and presented to the commander. He then decides what must be done to accomplish his mission. The S2 or G2 determines what IEW assets, out of those available, will be tasked to satisfy the commander's requirements. The S2 or G2 bases his selection on the initial intelligence estimate, his commander's intent, and PIR.

G2s and S2s develop a set of information requirements (IR) to support the commander's concept of operations. These IR are based on the HN, demographics, threat, AO, and mission. The commander approves PIR; the S2 or G2 approves IR.

PIR represent critical information the commander needs to accomplish the mission. IR represent specific information needs required to answer PIR. PIR and IR focus the collection and production effort, and they must be integrated into your collection plan.

The S2 or G2 focuses efforts on answering the commander's PIR. To do this, he must—

- Access data bases.
- Task assets.
- Direct, process, and disseminate intelligence and combat information. A tool for tracking changing requirements and directing the continuing collection process is a synchronization matrix.
- Forecast threat intent, COAs, and vulnerabilities.

You will develop new PIR and IR based on—

- Changing mission requirements.
- Meeting old requirements.
- Establishing new requirements.

Appendix D contains sample collection plan formats and instructions. Appendix E contains requirements for LIC operations and a listing of sources. For more information on collection management and dissemination (CM&D), see FM 34-2.

STEP 2. COLLECTING

Collecting is the process of gathering information from all sources. Your collection plan is driven by PIR and IR. You focus your effort on named areas of interest (NAIs) and target areas of interest (TAIs). NAIs are points or areas where activity confirms or denies a COA. TAIs are engagement points or areas where the interdiction of a threat will reduce or deprive that element of certain capabilities.

Your threat will not always be related to a hostile force. If you are involved in a disaster relief mission, your threat may be mud slides from a hurricane. Your TAI may be hillsides prone to mud slides near LOC. These hillsides may need manmade support to prevent major LOC from being closed.

As in all operations, collection in a LIC begins when the mission is identified. You must use all assets available to you—strategic, operational, and tactical. Do not limit yourself to the IEW community. Other sources such as US Agency for International Development (USAID) or the Drug Enforcement Administration (DEA) can provide valuable information.

Your information request will follow your standing operating procedure (SOP). Because the range of request processes is too great to be identified here, refer to FM 34-2 for specifics on requesting and receiving information.

STEP 3. PROCESSING

This is the step of the intelligence cycle where information and raw data become intelligence. It consists of recording, evaluating, and analyzing. (See Chapter 4 for a discussion on analysis.) FM 34-3, Chapter 2, describes information processing.

Recording

Local variations in recording and displaying intelligence affect the use of annotated overlays and working files. The incident map or overlay provides historical information on trends and patterns. The entries will help determine—

- The nature and location of threat targets.
- Intensity level of threat activity in an area.
- Degree of threat control over, or support from, the population.
- Potential areas of threat operations.

Evaluating

Evaluating determines—

- The pertinence of information to the operation.
- Reliability of the source.
- Accuracy of the information.

Your knowledge and judgment play a critical role in evaluation. When you determine the validity of information, do not be misled because it has never been received before, or that previously it was deemed impossible. Confirm reports with other information when possible. As your data base expands, you will be able to confirm new data with greater ease. This assists you in recognizing threat trends and patterns.

Analyzing

The processing of information continues with analysis, which consists of three steps: Assessing, integrating, and interpreting. It is during this phase of the intelligence cycle that information becomes intelligence.

Assessing. Assessment is the sifting and sorting of evaluated information to update significant elements on mission and operations of the unit.

Integrating. Assessed information is integrated with other information and interpreted to determine its significance. This involves combining selected data to form patterns and establishing a basis for interpretation.

Interpreting. Interpretation is making deductions as to the probable meaning of new information and determining its relevance to future activities. The meaning of the information is determined relative to the current situation and the threat's probable COAs.

STEP 4. DISSEMINATING

One critical aspect of intelligence is the need for rapid dissemination of information to the users. Each information report is scanned quickly to see if it is of immediate concern. If so, it needs to be forwarded to interested parties without delay.

Successful intelligence reporting communicates the results of analysis (and combat information) to the right people, at the right time, and in the right format. It provides commanders with the information and intelligence needed to reduce risk and uncertainty.

Some LIC missions will require dissemination to both US and HN military and civilian agencies. For example, during any outside continental United States (OCONUS) counter-drug operation, dissemination will be made to the US country team. Then the country team makes dissemination to supporting US agencies and their HN counterparts.

Including nonmilitary topics is vital to accurate reporting in LIC. Appendix F shows LIC mission report formats. They emphasize the need to report demographic information as well as the different types of threat and levels of hostilities.

When disseminating intelligence information, be sensitive to the lack of maps available to local operational field elements. Grid coordinate locations also should be reported in reference to local landmarks to facilitate use in the field.

INTELLIGENCE AND ELECTRONIC WARFARE ARCHITECTURE IN LOW-INTENSITY CONFLICT

The IEW architecture in LIC will be as diverse as the mission. Here we discuss—

- US assets (strategic, operational, and tactical).
- Non-DOD assets.
- HN assets.
- US sources within HN.

US ASSETS

US assets are strategic, operational, and tactical. Their use is subject to limitations. The S2 or G2 is your first point of contact.

Strategic Assets

Strategic intelligence is produced by national intelligence agencies and sent to operational forces. The IEW system connects strategic and tactical intelligence activities and supports combat forces at all echelons. There are three primary agencies: Defense Intelligence Agency (DIA), National Security Agency (NSA), and Central Intelligence Agency (CIA). Each of these provides—

- Analytical services.
- Finished intelligence products.
- Extensive data bases.
- Other services required by deployed units.

Do not think that these agencies are out of reach. Your collection manager can access each agency and request necessary assistance. Too often a product or report has been completed by one of these agencies, and analysts in the field are unaware of its existence.

Operational Assets

EAC IEW organizational and operational capabilities are tailored regionally and functionally to fit the specific needs of the theaters involved. When a theater command is established in a given AO, it will have an organic MI brigade (EAC) available for IEW support. This brigade may be augmented with a military intelligence battalion, low intensity (MIBLI).

The MI brigade (EAC) is organized to provide support in each of the following disciplines:

- Human intelligence (HUMINT).
- Imagery Intelligence (IMINT).
- Signals intelligence (SIGINT).

It also provides intelligence support in the form of technical intelligence (TECHINT) and measurement and signature intelligence (MASINT). The MI brigade (EAC) employs CI assets to support the overall command effort in the area of force protection (see Appendix A).

Tactical Assets

Due to the diversity of LIC missions, MI assets are task organized. Typically, MI LIC missions are HUMINT intensive. This is due to heavy involvement with the HN populace. Linguists and interrogators may be in high demand and short supply.

Document exploitation is also useful, especially in counterinsurgency and PCO. CI assets conduct MDCI operations to support force protection, deception, and OPSEC.

At the tactical level, SIGINT assets are characterized by low-level voice intercept (LLVI) teams. They are employed primarily for early warning when the threat possesses a measurable capability to communicate. You can use 98Gs or language qualified 98Cs when the mission allows or requires the augmentation of interrogation teams or document exploitation cells. They can also assist PSYOP and CA teams in evaluating the effectiveness of their programs.

In LIC missions, finished IMINT products flow down from the operational level for tactical exploitation. These IMINT products support data base development, mission planning and, in some instances, BDA. Additionally, we use IMINT to assess damage resulting from manmade and natural catastrophes.

IMINT has great value in collecting information significant to political, economic, or social events. An example of this would be imagery analysis of a topographic feature near an earthquake fault line. By fusing IMINT data with that from seismology, analysts can alert local authorities to potential catastrophes. In turn, lives may be saved, embattled governments receive popular support, and economic aid delivered.

NON-DOD ASSETS

Virtually any LIC mission will demand information and assistance from a number of non-DOD agencies. Some missions, nation building or disaster relief, will be in DS of one of these agencies. For example, during the counter-drug mission Operation BLAST FURNACE, assistance was provided to the DEA.

The following agencies may be of assistance to you:

- Department of Justice (DOJ).
  - DEA.
  - Federal Bureau of Investigation (FBI).
  - US Marshals Service.
  - Immigration and Naturalization Service (INS).
  - US Border Patrol.
- Department of Treasury.
  - Internal Revenue Service (IRS).
  - US Customs Service.
  - Bureau of Alcohol, Tobacco, and Firearms (ATF).
- Department of Transportation (DOT).
  - US Coast Guard.
  - Federal Aviation Administration (FAA).
- Department of the Interior.
  - National Park Service.
  - Bureau of Indian Affairs.
  - Bureau of Land Management.
  - US Fish and Wildlife Service.
- Department of Agriculture. (US Forest Service).
- Department of State (DOS).

  - USAID.
  - US Information Agency.
  - Bureau of International Narcotics Matters.
  - Bureau of Intelligence and Research.
- Department of Commerce (DOC).
- Foreign Broadcast Information Service.

As with national intelligence agencies, use the collection management officer (CMO) to contact these agencies for assistance. Remind the commander, G3, and S3 that these agencies are available. They are great assets in your planning phase as well as during the operation.

HN ASSETS

Various HN agencies may be available to assist you. Typically, each nation has agencies similar to those in the US. For access to these agencies, work through your collection manager to the US embassy or consulate located in the HN. They will assist you in establishing liaison with the appropriate agency. As for military resources, a member of the HN military should be attached to the G2 or S2. If not, request that one be attached.

US SOURCES WITHIN HN

Some missions may require you to rely on support from DOD and non-DOD elements stationed within the HN. You will also want to consider assistance from agencies of the HN.

DOD security assistance elements within the HN typically fall under the control of the SAO. These elements (not to be confused with embassy guards, attaches, and staff) represent an array of specialties such as combat arms, engineers, logistics, intelligence, or medical services. As a result of these missions, they possess valuable information for the planner and you.

Consider the prospect of your unit's moving to a country needing assistance following an earthquake. Critical to the HN populace will be the basic needs of life. Paramount to your mission will be medical and engineer support. Check with the SAO before deployment. Most likely it will be your point of contact.

In addition to the SAO, there may also be other DOD elements located in the HN, such as national intelligence centers (NICs), regional intelligence centers (RICs), and tactical analysis teams (TATs). All are formed and established in the HN at the request of the HN leader. A NIC or RIC provides advice, assistance, and finished intelligence support to the HN. A TAT provides analytical advice and assistance to a specific tactical mission.

Non-DOD agencies will be represented at each embassy or consulate. They, too, possess a wealth of information and will most likely represent the lead agency that you support.

CHAPTER 3
INTELLIGENCE PREPARATION OF THE BATTLEFIELD

This chapter describes the IPB process and provides IPB TTP to support LIC operations.

As in other environments, the IPB process must be an effort driven by the commander that involves his entire staff. IPB, when applied in a LIC environment, integrates threat doctrine and operational patterns with weather and terrain and political, social, and economic information. Then it relates these factors to the specific mission and situation.

IPB provides a basis for determining and evaluating the capabilities, vulnerabilities, and probable COA of the threat, local population, HN government, and military. It also serves as the planning basis for the commander's concept of operations and for allocating resources. This allocation could be engineers for disaster relief, special forces for FID, or a Ranger battalion for an airfield seizure.

IPB is interdependent with the intelligence cycle and the factors of analysis. It is not a stand-alone process. It relies on the functions and steps in the intelligence cycle for information. In turn, it provides input to the factors of analysis.

Information becomes intelligence in the processing phase of the intelligence cycle. This information comes from all available sources and agencies. The information processed includes, but is not limited to, demographics, OB, weather, terrain, personality, PSYOP, NBC, air defense, aviation, transportation, and logistics data.

The process of piecing together bits of intelligence into a usable product is done during the factors of analysis process. The end products of IPB are critical because they are the building blocks for recommendations to your commander. (See Chapter 4.)

DEVELOPMENT AND USE OF INTELLIGENCE PREPARATION OF THE BATTLEFIELD PRODUCTS

IPB is formally conducted at division or higher. A more informal approach occurs below division. In LIC, the formal process may begin at any level depending upon the situation. In support of a PCO (Operation JUST CAUSE), the process would be formally conducted at each echelon. In a counterinsurgency mission (El Salvador), the formal process starts at the RIC supporting a specific brigade.

Regardless of the mission, each level of command provides IPB support and products to its subordinate elements. Subordinate elements refine and expand these IPB products based on their specific mission requirements.

Developing IPB products in LIC is labor intensive. It requires cooperation from all staff elements, the commander's direction and planning guidance, mission focus, and the involvement of outside resources such as HN elements and US DOD and non-DOD agencies.

The commander and his mission drive IPB. The G2 or S2 is the staff IPB coordinator. The all-source production section (ASPS) and the battlefield information coordination center (BICC) assemble the threat data base, convert it to graphics, and integrate it with demographic, weather, and terrain data.

However, the critical responsibility in IPB remains with the commander who actually guides the process based on his mission, AO, and AI. The AO and AI will differ greatly in size and scope based on the force employed, echelon, and specific mission. For example, an AO may be a fairly small contained area, such as Army Special Operations Forces (ARSOF) mission areas within a Joint Special Operations Area (JSOA). Or it could be large enough to cover an entire country or geographic region.

The commander's primary concerns are the mission, threat, weather, and terrain. In LIC these are expanded to include the HN population, government, and military. A commander involved in a counterinsurgency mission, where the insurgents receive external support from a third nation, expands his AI to include the supporting nation and logistical LOC. He has similar concerns in a counter-drug mission determining—

- Where precursor elements used by the producer originate.
- How and where they arrive in country.

- The producer's logistics and transportation structure.

Following the commander's analysis of the mission, he restates the mission to his staff and provides planning guidance. The staff may be augmented by external agencies and the HN. The planning usually contains the commander's PIR. In the event it does not, the IPB process will help identify critical gaps and assist the staff in identifying suggested PIR. An example of this is a mission where the force is assisting a HN in PCO or DRO.

The SIO briefs the staff on the current threat situation including potential threat COAs. This input becomes the basis of staff estimates. The threat differs by mission, ranging from armed insurgents to criminal gangs.

In some instances, the threat is represented by nonviolent forms such as propaganda or, possibly, elected officials within the supported government. The threat does not have to be an armed force. If something is hostile, it is a threat.

When staff estimates for all potential threat COAs have been prepared, the staff analyzes and wargames the potential friendly and threat COA and determines the most probable COA based on all known factors. The staff then develops event templates and matrices and, if possible, decision support templates (DSTs) or decision support matrices (DSMs), whichever applies.

The commander is briefed on the DST and DSM. He reviews both DST and DSM to ensure all potential threat COAs and all friendly actions and intentions have been considered. The commander then updates his PIR based on the DST and DSM and issues a decision and concept of operations. This includes updating the DST and DSM.

Graphic products are the end result of IPB. In LIC, you produce graphics not normally found in the conventional process. A portion of these LIC-oriented graphics is shown at Figure 3-1. These and others are explained in Appendix G.

BATTLEFIELD AREA EVALUATION

The first step of the IPB process is battlefield area evaluation (BAE). In this step, you assess the overall nature of the HN population, friendly forces, threat, and operating environment.

This evaluation should address key areas such as significant personalities, ethnic, political, economic, or religious sectors of the populace and specific population centers. This helps you determine what information, products, and support you need to complete IPB. You can then issue IR to fill in basic information gaps.

INFORMATION REQUIREMENTS

Tailor these IR to the specific battlefield area and to the threat you expect to encounter within the AO and AI. This helps you determine threat capabilities in relation to the HN population, government, military, weather, terrain, and friendly mission.

In LIC, this is difficult since we usually have no threat doctrinal templates to consider when making recommendations to the commander. As a result, we create, manage, and evaluate our data base early. This assists us in developing threat operational patterns and doctrine early.

DATA BASES

Data bases differ from mission to mission, but the basic needs remain. Data requires tailoring to apply to a specific LIC mission. For example, the threat presented in counterinsurgency is different from that presented by a drug producer. Yet they both require some of the same basic logistics to operate: food, clothing, and batteries. Your data base would be the same for logistics but would differ for threat, weapons, and tactics.

As discussed above, we have to consider support provided by outside elements when involved in any of the missions in LIC. The data base should also illuminate topographic areas and features that must be considered during the IPB effort.

THE BATTLEFIELD

The battlefield consists of the AO and the AI. These areas are typically viewed in terms of width, depth, height (airspace), electro-optical (E-O) factors, and time—with time being the most critical.

In LIC, these factors stay important and are evaluated along with the TTP of friendly and HN forces. To these, however, we must add the HN population, threat, and friendly mission. Typical battle frontages and formations

IPB GRAPHICS: STANDARD VS LOW- INTENSITY CONFLICT	
STANDARD PROCESS	LIC PROCESS
TERRAIN OVERLAY (MCOO)	POPULATION STATUS OVERLAY LOGISTICS SUSTAINABILITY OVERLAY CONCEALMENT AND COVER OVERLAY LINES OF COMMUNICATION OVERLAY KEY FACILITIES AND TARGETS OVERLAY
WEATHER OVERLAY	WEATHER OVERLAY
THREAT OVERLAY	INSURGENT THREAT OVERLAY CRIMINAL THREAT OVERLAY PSYOP THREAT OVERLAY EXTERNAL SUPPORT OVERLAY COUNTER-DRUGS THREAT OVERLAY
NA	HN GOVERNMENT OVERLAY
NA	HN MILITARY DISPOSITION
DOCTRINAL TEMPLATE	DOCTRINAL TEMPLATE (SELECT USES) OPERATIONAL PATTERNS OVERLAY
SITUATION TEMPLATE	INCIDENT MAP KEY FACILITIES AND TARGETS OVERLAY
EVENT TEMPLATE	EVENT TEMPLATE AND MATRIX
DST	DST, DSM

Figure 3-1. Dispersed IPB graphics.

are not common to LIC; however, they may occur in certain PCO or PKO.

Ground Operations Areas

As mentioned, your AO will vary in size from very small, as in the case of an ARSOF mission area (which may be located well within a denied area) to a very large area. An AO is determined by the TTP of the force, mission, population, and threat. During Operation JUST CAUSE, a light infantry brigade's AO encompassed hundreds of square miles.

Mission planning does not end with initial success or termination of threat operations; rather, it extends through the follow-on nation building phase. With this kind of planning, the AO takes on a different perspective.

Your commander's assigned AO is based on METT-T factors in addition to the TTP of the unit. For example, if he has the mission to pacify and control the populace in an extremely large area, his first choice may be to use an ARSOF operating detachment alpha (ODA). Yet this unit is too small and does not have the necessary transportation assets. However, by attaching an ODA to a light infantry brigade, the mission is possible.

The LIC mission commander looks at the battlefield in the conventional way and keeps an eye on those areas which are not in conflict (countries, states, regions). The primary difference in application is that in LICs the political, social, and economic characteristics of the AO are addressed in more detail.

Air Operations Areas

The air AO is similar to the ground AO because air bases, refueling points, landing zones (LZs), drop zones (DZs), and air defense weapons and radars operate within the command's boundaries.

One major difference between air and ground operations is the height or operating ceiling (within which fixed- and rotary-wing aircraft operate and defense weapons can fire) and the enormous distances that can be covered by aircraft.

Many of the special operations aircraft (SOA) are capable of self-deploying to combat zones or conducting stealth infiltrations covering thousands of miles. The AO for SOA must cover the home base, the initial staging base (ISB), the forward staging base (FSB), and the target.

Numerous infiltration and exfiltration routes may be developed based on the mission. Infiltration routes may cross several countries or various political alignments and areas with severely different climatic conditions and must be included in the AI.

Rear Operations Areas

In most conventional operations, the rear AO differs from the forward AO (close and deep) because it includes geographical areas where higher and lower support, security, and air defense elements are conducting operations simultaneously.

Specific factors about the civil population, CI, security, PSYOP, and CA also impose special considerations. In LIC, these specific factors are considered by all units at any location and in any mission. Again, some missions of PCO or PKO can result in the unit's having a rear operations area.

In certain PCO and PKO missions the rear operations AI may include an area as large as a theater of operations, a theater rear area, or a communications zone (COMMZ). The area must extend into threat territory, as CS and CSS units must be prepared to move into areas formerly occupied by the threat. The rear AI may overlap the AIs of other rear area commanders, as well as other rear AOs.

Most LIC operations have a 360-degree AO. Therefore, considerations normally found in a rear operations area take on added importance to the maneuver commander.

Areas of Interest

Time remains a crucial factor in many ways: Tactical, operational, and strategic concerns are all related to time. A Ranger battalion seizing an airfield is concerned with the reaction time of a response force. A theater CINC is concerned with the timeliness of a logistics flow to a country in need of disaster relief. Assistance for nation building using nationally appropriated funds may take years to complete. In LIC, time is viewed in immediate, near term, and future frames.

The G2 or S2 recommends the AI to the commander based on METT-T and the commander's concept of the operation. It includes all threat activities that might affect the friendly force from the time the operation begins through follow-on missions.

An AI is developed based upon its importance to the threat; friendly force; the HN population, government, and military; or how it corresponds tactically to other selected targets in terms of criticality and importance.

An additional factor in determining your AI may be that the area includes a portion of another country where the commander cannot interdict the threat and the G2 or S2 cannot easily gather data. When your AI includes another country, then cross-theater coordination for collection and dissemination of intelligence will be required. This increases reliance on the HN's (or possibly a third nation's) ability to provide detailed information that is not obtainable with organic collection assets. Combatting terrorism, for example, may require the monitoring of a country that exports terrorism and is located thousands of miles from your AO.

Following the commander's approval, the G2 or S2 forwards the boundaries of the AI to the next higher echelon, where it serves as a guide for supporting intelligence requirements. The AI will be larger than the AO and differs in size and magnitude from mission to mission. At the operational or strategic level, the AI may extend to other countries thousands of miles away if they are seen as a source of external support to the threat encountered. Tactically, the AI will include all infiltration and exfiltration routes to be used.

The air AI is normally larger than the ground AI, primarily because of the great distances threat aircraft can rapidly cover and the speed with which they can influence friendly operations. The air AI encompasses threat airfields, refueling and rearming points, surface-to-air missile (SAM) sites, air defense early warning radar (EWR) locations, and ground-controlled intercept (GCI) sites.

The air AI extends upward to the maximum ceiling of threat aircraft and to the maximum effective altitudes of friendly and threat air defense systems. The AI for SOA are specific, narrowly defined target areas. In the BAE step, demographics are important for areas around the ISB or the FSB.

The G2 or S2 evaluates the demographics, terrain, weather, and threat and makes recommendations regarding the determination of subordinate unit boundaries to the G3 or S3. He uses these recommendations to suggest subordinate unit boundaries and resource allocations to the commander.

Analyst Considerations

When the AO and AI are defined, the analyst determines and assembles the data requirements—demographics, terrain, weather, and threat—along with materials needed to complete the IPB process. Basic requirements include maps and material to prepare templates and overlays. The data base includes current reporting and a library of finished products.

Expand your holdings to include finished products such as doctrinal and theological writings, captured manuals, open-source articles, recorded newscasts, area studies, gazetteers, and nautical almanacs. Unique products may be required such as—

- Geological surveys.
- Charts for areas prone to earthquakes (disaster relief).
- Hydrographic studies for NEO.
- Telephone directories for military operations in urban terrain (MOUT).
- Any local gazetteer or commercial directory.

Standard military topographic products (at a scale corresponding to the echelon conducting the IPB) are essential. When available, airspace analysis may be accomplished using the standard 1:250,000 air and radar joint operations graphic (JOG) specifically designed for this purpose. For detailed analysis of an aircraft's approach to a target, standard 1:50,000 topographic maps are useful. MOUT requires maps at scales of 1:12,500 or larger. Certain missions, especially those in support of ARSOF elements, require the use of products at a scale of 1:2,500, blueprints, floor plans, and photographs for precise collection and planning.

You may find that there is no map coverage of your AO and AI, especially at the 1:50,000 scale or larger. This requires you to collect MC&G products from DOD or non-DOD agencies. The Defense Mapping Agency (DMA) may be of some assistance; however, the best source is usually the HN you are supporting. But do not overlook sources such as The National Geographic Society, oil company road maps, and tire company touring guides.

During Operation BLAST FURNACE, HN hydrographic maps at extremely small scale had to be used as no other MC&G products were available. Commercially procured topographic satellite (LANDSAT) imagery was used for a short time until it was determined that the imagery was taken during the rainy season. This altered the look of the terrain during the time of the operation.

If you are involved in an operation where there are no HN graphics, DMA will provide whatever support it can. But you may have to exercise some local initiative to satisfy the command's needs.

TERRAIN ANALYSIS

The second step of IPB is terrain analysis. This looks at the effects of terrain on military operations. In LIC, consider the military aspects of observation and fields of fire, concealment and cover, obstacles, key terrain, avenues of approach, and mobility corridors (OCOKA), as you do in conventional missions. But in addition, you must also consider the local population. The impact of population on a LIC mission is critical.

When you look at population, you must evaluate HN demographics, government, and military. By evaluating these factors you will be better prepared for the diversity of LIC missions. Chapter 4 lists those demographic factors that must be included in your evaluation.

You should understand the historical development of the country. Make sure you know those precedent-setting events that evoke or inspire pro- or anti-nationalist feelings. You may find that the threat conducts operations on historically significant dates.

The population study will be diverse and in-depth. At a minimum you will want to identify pro-government, anti-government, and neutral population sectors. Categorize population by—

- Boundaries.
- Political subdivisions.
- Natural features.
- Settlement patterns.
- Structure.
- Migration patterns.
- Labor.
- Known problems.

Ethnic, language groups, and languages (subsets of the population) are critical factors in any LIC mission and require your specific attention. Evaluate the social system to determine class structure, family, kinship relations, religion, and social values.

Examine the education system in terms of—

- Literacy rates by region.
- Age.
- Government financing.
- Government view on the importance of education.
- The education system.
- Teaching profession.

The evaluation of the economy will include the economic system itself, public finance, financial institutions, agriculture, industry, foreign trade, transportation; together with domestic issues such as housing, health, and welfare.

When evaluating the HN government—

- Review the legislative and judicial structures, functions as authorized by law, and the constitutional framework.
- Look at the political structure governing the country including key personnel.
- Determine its legitimacy, dogma, beliefs, and intent.
- Evaluate each political party or faction that is active within the country.
- Examine special interest groups and their impact on local politics.
- Understand the HN foreign policies and relations.

When you evaluate the HN military, develop and evaluate the generic data base of all military organizations. Look at—

- Composition.
- Disposition.
- Strength.
- Tactics.
- Weapons.
- Equipment.
- Personalities.

Your evaluation should also include national policy and laws which govern the use of the military. Check their adherence to these laws, association with political groups (as well as external influences or support), and any division or rift within the ranks. Consider the capability of the military to accomplish the mission at hand.

In addition to the OCOKA factors described above, you must also consider—

- Strategic location.
  - Neighboring countries and boundaries.
  - Natural defense, including frontiers.
  - Points of entry and strategic routes.
- Size and dimensions.
- Relief.
- Beach data.

- Hydrography.
  - Oceans.
  - Lakes.
  - Rivers.
- Other surface water sources.
- Land use.
- Geological basics.
- Forests and vegetation.
- Water.
- Natural foods.
- Wildlife.
- Demographics.
  - Population centers.
  - Social analysis (History, Ethnics, Languages, Social system, Education).
- Living conditions.
- Cultures.
- Religions.
- Taboos.
- Grievances.
- Political analysis.
- National government.
  - Structure.
  - International orientation.
  - Degree of popular support.
- Political parties.
- Foreign dependence or alliances.
- Controls and restrictions.
- Laws (civil and religious).
- Economic analysis.
- Current value of money, wage scales.
- Financial structure, to include national or international banking system.
- Foreign dependence.
  - Assistance programs.
  - In-country business.
- Agriculture and domestic food supply.
- Natural resources and degree of self-sufficiency.
- Industry.
  - Types (base and main industries).
  - Production levels.
  - Consumer demands.
  - Unions.
- Black market and illicit trades (drugs, weapons, contraband).
- Technology.
  - Capabilities.
  - Expertise.
- Foreign trade.
  - Type.
  - Level.
  - Transportation.
- Fuels and power.
  - Locations.
  - Quality.
  - Production system.
- Mass communications.
  - Telephone.
  - Telegraph.
  - Television.
  - Radio.
  - Microwave systems.
  - Satellite and laser systems.
- Transportation.
  - Railroads.
  - Highways and roads.
  - Trails and paths.
  - Waterways.

  - Aircraft LOC.
  - Airports.
  - Airfields.
  - Air strips.
  - LZs.
- Sea LOC to include port studies.
- Tunnel systems.
- Host national security analysis.
  - Public order and internal security.
  - Armed forces.
  - External support and dependency.
- Friendly neutral third-party analysis.
  - Embassies and consulates.
  - Military.
  - Business interests.

While the last two categories may not always lend themselves to templating, they can be graphically represented on matrices. You must consider these categories when viewing the LIC battlefield. This list is far from conclusive; expand or delete items as necessary. The intelligence estimate (Appendix F) has been expanded to reflect these considerations.

WEATHER ANALYSIS

The third step in IPB is weather analysis. Weather analysis in LIC does not differ greatly from that conducted during regular operations. However, the primary focus of weather analysis shifts to supporting the G2 or S2 on reconnaissance and surveillance (R&S) capabilities.

Weather effects still apply on mobility, observation, fields of fire, camouflage, helicopter LZs, and line-of-sight (LOS) radio and radar equipment. See FM 34-81-1 for details on weather effects on systems, operations, and personnel, to include—

- Climatic conditions.
- Weather effects.
- Weather forecasts.

In areas of great seasonal climatic change, terrain intelligence produced during one season may be useless in others. Therefore, weather analysis based on current observations or forecasts, together with terrain intelligence, must be reviewed and updated continuously.

Weather may have a unique impact on LIC missions and account for some unusual indicators. For example, in tropical areas during wet seasons, it is probable that it will rain at the same time every day. The G2 or S2 can usually rely on this information to predict occurrences of threat activity.

An insurgent force may time its attack to coincide with the daily tropical rain knowing that military aircraft will not respond. This also applies to counter-drug operations, as inclement weather provides excellent cover for the movement of illicit drugs.

In PKO, it may become evident that threat organizations do not conduct demonstrations or rallies during inclement weather. This allows you to put together another piece of the projected threat activity puzzle.

Weather affects PSYOP. Rain and heavy winds disrupt or stop an otherwise effective leaflet drop. Weather also impacts on CA operations; heavy rain easily disrupts construction projects or a medical and veterinary assistance program.

Another key aspect of weather is light data. For example, you may have to perform pattern analysis on freshly cut trails and related threat activities. While reviewing the data for those activities, examine the light data as well. You will probably find that the percent of illumination during each period was low, providing the threat with the greatest degree of darkness.

Consider the following weather effects:

- Subversives normally use bad weather or darkness to their advantage. These conditions reduce the effectiveness of HN surveillance, direct and indirect fire, air support, and logistics.
- Inclement weather affects the availability of food supplies.
- It is difficult for insurgents to cache supplies in frequently flooded areas.

- Mass demonstrations use good weather to get maximum turnout.
- Seasonal weather effects may determine if farmers or fishermen are available to participate in insurgency operations.
- Bad weather further degrades poor road networks common in lesser developed countries.
- For additional information on the military application of weather, see FM 34-81/AFM 105-4.

THREAT EVALUATION

The threat evaluation in LIC begins early. You will cover a wide range of factors in building an accurate model. These include all aspects of—

- Leadership.
- Objectives.
- Organization.
- Tactics.
- Timing.
- Environment.

Doctrinal templates developed during conventional threat evaluation are difficult to use in LIC due to a lack of defined TTP.

However, threat operational patterns are determined and templated for exploitation during threat integration.

Threat evaluation is a three-step process as shown at Figure 3-2.

DEVELOPMENT

The first step is the development of the threat data base. The LIC threat data base is similar to that developed for a conventional military unit with some modifications. These include—

- External training.
- External travel.
- Political and religious beliefs.
- Other support.

This data base will be further modified when applied to other LIC missions such as counter-drugs. Here you still require an organizational structure, personalities, equipment, and tactics. Modifications include—

- Specifics on the production of the drug.
- Growing season of the base plant.
- Methods of transport.
- Required precursor chemicals.
- Source and availability.

As stated earlier, LIC threat data bases are developed in much that same way as conventional threat data bases. Consequently, use OB factors to develop and evaluate LIC threat.

There are certain OB considerations unique to a threat encountered in LIC operations. Recognize the differences in types of threat, strategy, modus operandi, and tactics as well as equipment, materiel, and personnel. There are as many differences when applying OB to the phases of an insurgency as there are when analyzing looters, drug traffickers, and terrorists.

OB intelligence factors are interdependent and considered as a whole. Information on one of the elements often leads to a reevaluation or alteration of information previously received on another. Furthermore, the general rule that OB intelligence is developed and maintained down to and including two echelons below the analyst's own level of command does not apply to LIC operations.

LIC threat requires OB intelligence to be produced in greater detail and at lower echelons than found in conventional operations. Many times you will focus down to individuals. In LIC the category *personalities* is added to the usual list of OB factors.

These factors, which are viewed from the same perspective as in *war,* include—

- Composition.
- Disposition.
- Strength.
- Tactics.
- Training.
- Logistics.

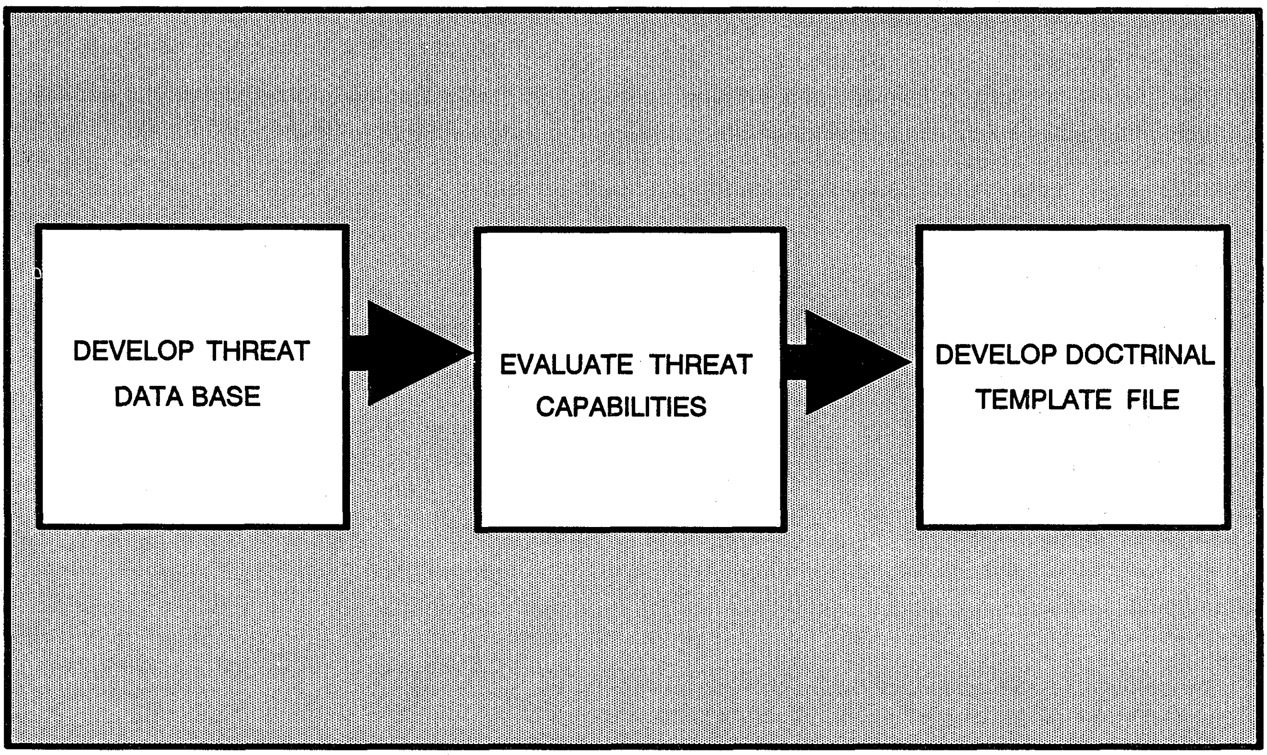


Figure 3-2. Threat evaluation.

- Combat effectiveness.
- Electronic technical data.
- Personalities.
- Miscellaneous data.

Composition

Composition is the identification of units, organizations, or possibly families involved in illicit activities such as drugs. Unit identification consists of the complete designation of a specific entity by name or number, type, relative size or strength, and subordination.

Similar information is required on organizations, families, and individuals. Often you will be dealing with a name only. Instead of a unit type, you may be dealing with a type of activity. For example, a family involved in drugs may only be a front for money laundering and never have anything to do with the actual drug production. Composition includes—

- Criminals.
  - Gangs.
  - Families.
  - Organized crime.
- Drug traffickers.
  - Families.
  - Organizations, cartels.
  - Structured similar to a military unit with *staff sections* responsible for specific functions, such as logistics, transportation, and security.
- Terrorists.
  - Cells.
  - Echelons.
  - Staffs.
  - Political, religious, ideological, and military aims.
  - External support.

Here is a look at the activity thresholds of insurgencies by phases.

During Phase I, threat activities range from being only a potential problem to frequently occurring activities displaying an organized pattern. No major outbreak of violence or uncontrolled insurgent activity exists. The insurgent is primarily concerned with organizing infrastructure, conducting PSYOP, and conducting limited terrorist attacks during this phase, and may include—

- Infrastructure: political, religious, and ideological.
- New organizations.
- Internal and external C^2.
- Operational organizations.
- Internal and external support structure.

Phase II begins when the insurgent has gained sufficient local or external support to initiate organized guerilla warfare against the government or military units, including—

- Internal and external support structure.
- New organizations.
- C^3.

Phase III of an insurgency becomes primarily a conventional conflict between the organized forces of the insurgents and the established government. The insurgents may continue guerilla operations as well.

An important point to remember is that the insurgent may be operating outside the boundaries of the HN during all three phases. Geographic boundaries cannot limit collection and analysis of conventional military units, such as C^3.

Political Structure

- Criminal. Typically not a factor; may be motivated by oppressive regime to support insurgency or terrorism.
- Drug trafficker. Typically not a factor.
- Terrorists.
  - Political, religious, or ideological initiatives.
  - External ties.
- Insurgents.
  - Formal structure.
  - Political, religious, or ideological initiatives.
  - Parallels existing government hierarchy.
  - Usually forms an *umbrella* organization over the military arm.

Combat Forces

- Criminal (may have *hit squads* that are responsible for enforcement).
  - Gangs.
  - Families.
- Drug traffickers. Security elements.
- Terrorists.
  - Assassination squads.
  - Bomb and demolition squads.
  - Attack or hit squads.
- Insurgents.
  - Maneuver units (cells, companies, battalions).
  - Special forces (assassination, demolition). All combat units should be identified by number, commander's name, commander's nickname, unit nickname, code designation, and name of area in which it operates.

Disposition

Disposition consists of the geographic location of threat elements and the manner in which they are deployed, employed, or located. Additionally, disposition includes the recent, current, and projected movements or locations of these threat elements. Disposition includes—

- Criminal.
  - Residences (impoverished or poor neighborhoods).
  - AOs (target areas; for example, high cost areas).
- Drug trafficker.
  - Residences.
  - Production and growing areas of base product.
  - Areas of control.
  - Safe houses.
  - Transshipment points.
  - Manufacturing locations of synthetic drugs.

  - Laboratory sites for processing base products.
  - Logistics camps.
  - Front organizations and companies.
- Terrorists.
  - Training camps.
  - Base camps.
  - Logistics camps (external and internal).
  - Headquarters (external and internal).
  - Areas of control.
- Insurgents.
  - Training camps.
  - Base camps.
  - Logistics camps (external and internal).
  - Headquarters (external and internal).
  - Areas of control.
  - PSYOP locations (radio transmitters and printing presses).
  - Emphasis in rural areas compared to city areas.

Strength

Strength conventionally is described in terms of personnel, weapons, and equipment. However, in LIC you augment this definition with combat forces, strike teams, hit squads, political cadres or cells, and, most importantly, popular support. Popular support can range from sympathizers to assistance in conducting operations, moving logistics, or just withholding information.

Tactics

Tactics include strategy, modus operandi, and doctrine. Each refers to the threat's accepted principles of organization and employment of forces. Tactics also involve political, military, psychological, and economic considerations.

Remember that the threat modifies its activities based on the abilities and tactics of friendly forces. A good example of this was the mine-countermine situation in El Salvador in the 1980's. The insurgent force developed a new type of mine or booby trap; the government forces countered with new tactics or detection devices; to which the insurgents replied with a different device. Tactics include—

- Criminal.
  - Patterns of activity (for example, windows for operations).
  - Methods of operation (methods of entry, looting).
- Drug trafficking.
  - Growing methods.
  - Concealment methods.
  - Transportation methods.
  - Money laundering.
  - Extortion.
  - Civic actions.
  - Political endeavors.
- Terrorists.
  - Threats.
  - Sabotage.
  - Extortion.
  - Violence (bombing, assassination).
  - Civic actions.
  - PSYOP.
  - Economic targets.
  - Political and religious targets and motivators.
- Insurgents.
  - Subversive patterns.
  - Critical-cell patterns.
  - Mass-oriented patterns.
  - Traditional patterns.
  - Urban warfare.
  - Rural warfare.
  - Small-scale operations.
  - Major offensives.
  - Mines and booby traps.
  - Recruitment.

  - PSYOP.
  - Economic targets.
  - Political and religious targets and motivators.

Training

Training is tied closely to combat force and threat tactics. Those supporting the threat receive some type of training. Persons who mix the precursor elements in the manufacture of cocaine or those that build satchel charges have to be trained. You can predict potential activities by monitoring the types and levels of threat training.

Higher education also plays a role in threat tactics and training. Some threat elements intentionally recruit university students, either to join the movement or to prepare for future leadership roles.

An example of this is Omar Cabezas, a medical student in Nicaragua. He was recruited by the FSLN while attending medical school in Leon, Nicaraugua, in the late 1960's. His education and political convictions made him a prime recruitment target of the FSLN. By monitoring the training he received, Nicaraguan government forces were able to measure his contribution to FSLN readiness. Following are examples of threat training:

- Drug trafficking.
  - Growing cycle.
  - Production cycle.
  - Manufacturing cycle.
  - Techniques and procedures in shipping and marketing.
- Security of operations.
  - Armed forces.
  - Deception.
  - Concealment.
- Terrorists.
  - Weapons (individual and crew-served).
  - Demolitions (manufacture and placement).
  - Tactics.
  - Indoctrination and strategy (political, ideological, or religious).
  - Operations.
  - Transportation (covert movement).
  - Logistics.
  - Communications.
  - R&S.
  - Media manipulation.
  - PSYOP.
  - Education (military and civilian).
- Insurgents.
  - Weapons (individual and crew-served).
  - Demolitions (manufacture and placement).
  - Tactics.
  - Indoctrination and strategy (political, ideological, or religious).
  - Operations.
  - Transportation.
  - Logistics.
  - Communications.
  - Media manipulation.
  - PSYOP.
  - Medical.
  - R&S.
  - Education (military and civilian).

Logistics

As in conventional warfare, threat effectiveness in LIC depends heavily on logistics. This dependency fluctuates horizontally between the various threat groups and also vertically between levels of intensity. You also see activity trends based on logistic support or nonsupport.

For example, a resupply surge into an area controlled by an insurgent may indicate an upcoming offensive. Or the upcoming harvest of opium poppies in a specific region will indicate a resupply surge in support of the stepped up production process. These indicators, when combined with IPB, help you predict possible threat COAs.

Logistic indicators include—

- Drug trafficking.
  - Precursor elements and chemicals.
  - Base products (coca leaf, poppies, synthetics).
  - Plastic medical waste bags.
  - Tarp (heavy quality).
  - Plastic sheets (heavy quality).
  - Microwave ovens.
  - High wattage light bulbs.
  - Generators and fuel.
  - Aircraft and fuel.
  - Small boats.
  - Food.
  - Water.
  - Medical.
  - Weapons and ammunition.
- Terrorists.
  - Weapons and ammunition.
  - Bomb components.
  - Food.
  - Water.
  - PSYOP materials (paper, ink, printing press).
  - Medical.
- Insurgents.
  - Weapons and ammunition.
  - Bomb components.
  - Communications equipment.
  - Clothing.
  - Generators and fuel.
  - Food.
  - Petroleum, oils, and lubricants (POL).
  - Water.
  - PSYOP materials (paper, ink, printing press).
  - Medical.

Combat Effectiveness

Combat effectiveness in LIC is not the same as combat effectiveness in conventional operations. Rather, we view it from the standpoint of effectively controlling the population and the political situation. An upswing in support for a local drug lord indicates a level of effectiveness over that of the government. Government deficiencies may be economic, social, or political. Whatever the case, the drug lord fills voids the government cannot. Combat effectiveness indicators include—

- Criminal.
  - Extortion of business owners.
  - Disrupting tourism, affecting local businesses.
  - Blackmail.
- Drug trafficking.
  - Support to local populace the government cannot or will not give.
  - Extortion.
  - Intimidation.
  - Corruption.
- Terrorists.
  - Fear.
  - Intimidation.
  - Political change.
  - Popular support.
  - International support and furor.
- Insurgents.
  - Fear.
  - Intimidation.
  - Political change.
  - Popular support.
  - International support and furor.

Electronic Technical Data

In LIC, there is often a lack of threat signal operating instructions (SOI). This impedes the development of an extensive threat electronic OB data base and an electronic technical data base.

The threat use of radar tends to be situation specific. While not playing a large role in insurgency, it cannot be completely overlooked. Threats often use high frequency (HF) shortwave or ham radio sets. Citizen band sets play a role in early threat operations. Equipment available to the threat ranges from the most primitive to the most modern.

Propaganda activities may result in threat-sponsored commercial or clandestine radio broadcasts. Covert broadcasts normally originate outside the national boundaries or from remote, inaccessible areas. Commercial radio broadcasts may use code words to control and coordinate threat operations. Television broadcasts may be used similarly.

Personalities

Personalities are a critical factor in LIC operations. We have to focus our attention on the individual. Through link analysis (determining relationships between personalities), we can *build* organizations. This applies to virtually any threat represented in LIC. Once you have determined relationships and the level of contact or knowledge the personalities have of each other, you can determine their activities.

For example: If you know that an individual is responsible for train-the-trainer missions on mortars, you would track him to see who he comes into contact with and who he trains. By doing this, you will not only determine the capabilities of the insurgents but may also help to identify cells within the faction. This, in turn, helps determine organizational structure. Personality files include, but are not limited to—

- Criminals.
  - Gang leaders.
  - Family leaders.
  - Nicknames.
- Drug traffickers.
  - Family leaders.
  - Organization, cartel leaders, and staffs.
  - Nicknames.
- Terrorists.
  - Leaders (political, ideological, religious, and military).
  - Staff members.
  - Experts in demolitions, weapons, and assassinations.
  - Media manipulation. Alerting the press to gain exposure.
  - PSYOP.
  - Trainers.
  - Nicknames.
- Insurgents.
  - Leaders (political, ideological, religious, and military).
  - Staff members.
  - Nicknames.
  - Demolitions.
  - Weapons.
  - Assassinations.
  - Civic actions.
  - PSYOP.
  - Communications.
  - Economics.
  - Logistics.
  - Transportation.
  - Recruitment.
  - Trainers.
  - Emissaries for external support.

Miscellaneous Data

Miscellaneous data includes supporting information needed by analysts but not covered by an OB factor. This could include unit, organization, or family history; false unit identifications (IDs), names or designators; methods of operation; political and military goals; propaganda and PSYOP; and demographics.

Propaganda and PSYOP files contain—

- Copies of leaflets, posters, and other printed material.
- Video recordings of television broadcasts.
- Audio recordings of radio broadcasts.
- Copies of speeches.

- Background material.
- Analysis of local grievances.

Reference material, such as a reference library to support your backup working files, will complete your data base. This library needs to contain at a minimum—

- Material on the area.
- Manuals or writings on threat doctrine, tactics, and methods.
- Newspapers and magazines.

EVALUATION

The second step of the threat evaluation process is the evaluation of threat capabilities. These capabilities are evaluated based on their impact on the battlefield and friendly mission. You determine the ability of the threat to conduct specific actions. For example, does the threat have sufficient popular support to conduct an offensive in the capital? Is the threat organized well enough to be able to kidnap a local judge without causing casualties in the immediate area? This evaluation provides the basis for doctrinal templating.

PRODUCTION

The final step is the production of doctrinal templates. Generally, the templates you develop in a conventional conflict will be modified for LIC. For example, generic practices or patterns throughout all insurgencies do not lend themselves to templating.

As a result, we build threat models based on our data base and fuse that with pattern analysis developed from historical incident overlays which portray threat activity. This is typical of most LIC threats: insurgents, terrorists, drug traffickers, or criminals.

THREAT INTEGRATION

What we determine about the battlefield through data evaluation is now integrated (fused) with the evaluation of the terrain and weather. At this point in the conventional process, we would normally develop the situation template and NAIs.

As there are no doctrinal templates available during the early stages of LIC, we base the situation template on types of activity, when and where it will occur, and the disposition of the threat to conduct the activity—not on enemy formations and movement.

In counterinsurgency, for example, we construct the situation template by layering or fusing incident overlays covering a specific period. From these you determine what preliminary movements and actions were conducted by the enemy prior to an action.

To capture data on enemy tactics used during the attack, we produce a second situation template using a large-scale map of the immediate area. You can now accurately determine patterns or practices used to conduct operations. You can then compare them to known enemy composition, disposition, training, and personnel levels at the time of the attack.

At the same time, factor in the other facets of the BAE as they were prior to and during the time of the attack. Was there a recent presidential election? Is the date of the attack a significant date in the history of the country or revolution? Was there a recent increase in foreign assistance to the government?

Templating requires continuous refinement to accurately portray enemy patterns and practices. You develop situation templates for the other facets of LIC through this same process.

PKO requires similar data to predict where demonstrations may occur. In this instance, layer or fuse incident overlays for a specific timeframe and you will determine such things as—

- Rally or gathering points for crowds.
- March routes used to move from rally points to demonstration sites.
- Recurring demonstration locations such as churches, embassies, and universities.

The same holds true in counter-drugs. There are no doctrinal templates for the emplacement of cocaine laboratories. However, through the above process you can determine laboratory profiles. They will be located in isolated areas, near water and an airstrip.

By plotting all features of the drug laboratory area onto a large-scale map, monitoring activity, and factoring in production processes and growing seasons, you will collect useful information, such as—

- When the laboratory is active.
- Transshipments of chemicals.
- Movement of base plants.
- The transfer of illicit drugs.

RESIZING THE AREA OF OPERATIONS

You can now reduce the size of the AO to likely areas of subversive concentrations by merging the population status, concealment and cover, and logistic sustainability overlays. By determining areas that provide the support of the populace—concealment, cover, and sustenance—we can now focus on a number of small geographic areas rather than on one large country or a major city.

These likely areas of subversive concentrations are now viewed as NAIs, allowing us to efficiently task our collection assets. We then add the LOC overlay to determine the location of possible threat targets in or near the NAIs. This aids collection, R&S, and analysis of the NAIs.

Due to the absence of time phaselines and other doctrinal concerns, DSTs or DSMs cannot always be produced in LIC. But you can produce supporting matrices to assist the commander. You build these using information gained from your version of the situation template and your evaluation of the AO. Once you determine the requirements and actions of an insurgent force prior to an attack, develop a matrix that reflects these key events.

In the case of counterinsurgency, you will require a separate matrix for each insurgent faction encountered. This same process applies to all facets of LIC: in counter-drugs for determining the movement of illicit drugs or the activation of a processing laboratory, and in PKO to determine preliminary activities for demonstrations or terrorist attacks. Through this analysis we develop TAIs, some of which may have been NAIs.

TARGET AREA OF INTEREST CATEGORIES

We place TAIs into two categories: point and area.

Point TAIs are specific areas for fire support, EW, or possibly HUMINT assets. Or, for that matter, any system that requires a moderate degree of accuracy.

Area TAIs are generally more terrain dependent; for example, sanctuaries near international borders, areas of anti-government sentiment, and estuaries serving as resupply LOC.

TARGET VALUE ANALYSIS

Once you have identified TAIs, you can then conduct target value analysis (TVA) to determine if the threat can seize the target, attack the target, or if the target fits into his COA. You can now predict subversive intentions throughout the spectrum of LIC and hinder or deny threat success.

DISSEMINATION AND USE

As a result of IPB, you will produce a variety of—

- Templates.
- Overlays.
- Association and event matrices.
- Flow charts.

You will provide them to the commander and G3 or S3 for approval and guidance. Once approved, the G3 or S3 integrates IPB with other staff products and applies them to mission planning and execution.

Your job is to ensure that accurate products are promptly provided to consumers. You also use your IPB products internally to identify gaps in the intelligence data base and provide input to the CMO to help refine his collection effort.

CHAPTER 4
ANALYSIS IN LOW-INTENSITY CONFLICT

This chapter provides guidance for analysis in LIC and is in three parts: Analysis in depth, techniques of analysis, and factors of analysis. MDCI analysis process is addressed in Appendix C.

ANALYSIS IN DEPTH

Information is transformed into intelligence at the processing step of the intelligence cycle. This intelligence supports the commander's needs and guides his decision-making process. It also allows him to successfully complete his mission and at the same time protect his own force. Of course, the analyst does not make decisions for the commander. But the commander cannot make quality decisions without the input analysts provide.

Analysis determines the significance of raw data, relative to information and intelligence already known. And then it draws conclusions about the evaluated information. All analysts, whether OB, MDCI, imagery, or traffic go through this mental process.

Analysis in LIC involves a combination of tools and skills. Some of these tools have been developed to support one discipline and are now used by others. This is true for certain techniques—specifically, link and pattern analysis.

This chapter follows the pattern for analysis outlined in FM 34-3, Chapter 5, but has been tailored to address applications in LIC.

MEETING USER REQUIREMENTS

The ultimate user of intelligence is the commander. However, in LIC this may not always seem to be the case—at least not a commander in the sense we are accustomed to. There are situations when you may support an HN commander, a DEA special agent-in-charge, or an ambassador. They, too, need intelligence to form decisions; yet, each has unique requirements.

We need to ensure the HN commander understands the terms and products you present to him. Always remember to produce what the user needs. Make sure you are responding to stated PIR and IR. By doing so, you respond directly to the user's needs.

You must understand these needs in order to satisfy them. If the analyst and the user do not view PIR and IR from the same perspective, the intelligence product will not support the mission. You must feed back to the user your understanding of what he needs or wants. You must also be visionary and proactive.

For example, if you are involved in a forced entry mission, such as Operation JUST CAUSE, look beyond the immediate mission's PIR and IR. Ask yourself the following questions:

- What will be needed to support a nation assistance operation following hostilities?
- Will a threat remain against US forces?
- What information needs of a displaced person (DP) will the commander and civil military officer have?
- Will there be IR from non-DOD agencies such as USAID or DOS? If so, what will they need?

In conventional operations, the commander and his staff view the mission in similar terms: usually a tactical situation with an identifiable threat within an AO and AI.

In LIC, your end-user may not possess the same focus or views that you do. Your considerations of threat to the force are more detailed than those of some non-DOD agencies.

For example, in preparation for a counter-drug operation, an analyst was informed by the DEA special agent-in-charge that he maintained over 100 target folders on potential laboratory sites in the proposed AO. When the analyst was presented with the folders, they contained jumbled information in no set format. Later, the special agent-in-charge was presented a number of military style target folders. The special agent-in-charge was initially flabbergasted; he had never seen intelligence products of that caliber and detail before.

DETERMINING THE RISK FACTOR

Defining the degree of uncertainty, or filling in information gaps, is the job of intelligence. To succeed, analysts handle uncertainty from many sources. While objective ground truth is found in the laboratory, it is not a part of analysis of the battlefield. The analyst frequently deals with ambiguous or even misleading information.

The analyst's greatest concern is uncertainty; the commander's is risk. Good analysts translate uncertainty into risk. Figure 4-1 shows the relationship between lethality and risk.

Risk increases as threat lethality moves from low to high. When a degree of uncertainty is added to the estimate of lethality, the potential danger becomes even greater. The degree of risk a commander will accept governs the amount of uncertainty the analyst reports.

Risk is the voluntary exposure to danger. In combat, there is always risk in not preparing responses to potential threat action—whether or not that action has a high possibility of execution. Risk increases in response to possible danger and decreases when the threat potential goes down.

The analyst's uncertainty plays a key role in the evaluation of the enemy and the amount of risk accepted. Uncertainty may arise for many reasons:

- There is uncertainty about the enemy's intent. For example, what is the enemy's real objective? What are the various means of achieving this objective?
- There is uncertainty in evaluating the capabilities of the enemy force to achieve these objectives.
- There is uncertainty in other factors: lethality, warning time, enemy and friendly options, and environment conditions.
- There is uncertainty that the method of response will produce the desired outcome.

In the past, the strength of El Salvadoran efforts against the FMLN was its ability to quickly move troops by helicopter. There were sporadic reports of the FMLN's possessing shoulder-fired SAMs or their members' receiving training on the weapons. This information was never supported nor confirmed. The range of uncertainty was high and the risk was low.

However, in 1991 shoulder-fired SAMs were used against El Salvador Air Force (ESAF) helicopters. The level of uncertainty became low, although it was not known when or where the weapons would be used next. Therefore, the risk was high. As a result, analysts supporting tactical operations had to consider the risk SAMs presented. One way to reduce this risk was to develop air mobility corridor overlays and select routes that were not channelized.

THE THREAT MODEL

As an analyst, you develop a model to portray the threat you may encounter in an operation. It allows you to piece together information; identify gaps; and speculate, predict, and solve problems. More importantly, it assists you in lowering some of the risk.

There will always be some information gaps in your threat model; thus, you will always have some degree of uncertainty. However, by comparing the model to current activity you can identify patterns, trends, and activity levels. Your model consists of five color-coded categories:

- Battlefield environment (including terrain, hydrology, and weather)—WHITE.
- Organizational structure of threat—RED.
- Organizational structure of friendly forces—BLUE.
- Population—GREEN.
- Physical objects such as weapons, vehicles, aircraft, and drug laboratories—BLACK.

The model forms an organizational structure from which the analyst can mentally picture the AO and AI. Once the model is developed, it is refined and updated to maintain its validity.

First, *think WHITE*. This is your framework for the model. This portion of the model relates to time and space. Here, time is a sequence of periodic snapshots within which events will occur. This will present problems when your threat is an insurgent or terrorist organization.

It may be difficult to determine time when countering these groups. You want to key on significant dates to the HN or threat; they may want to conduct an action in concert with a specific date; for example, HN's independence day. You may also know certain events that will occur before this group conducts an operation. You do not know the time, but you do know the sequence. Herein lies the uncertainty.

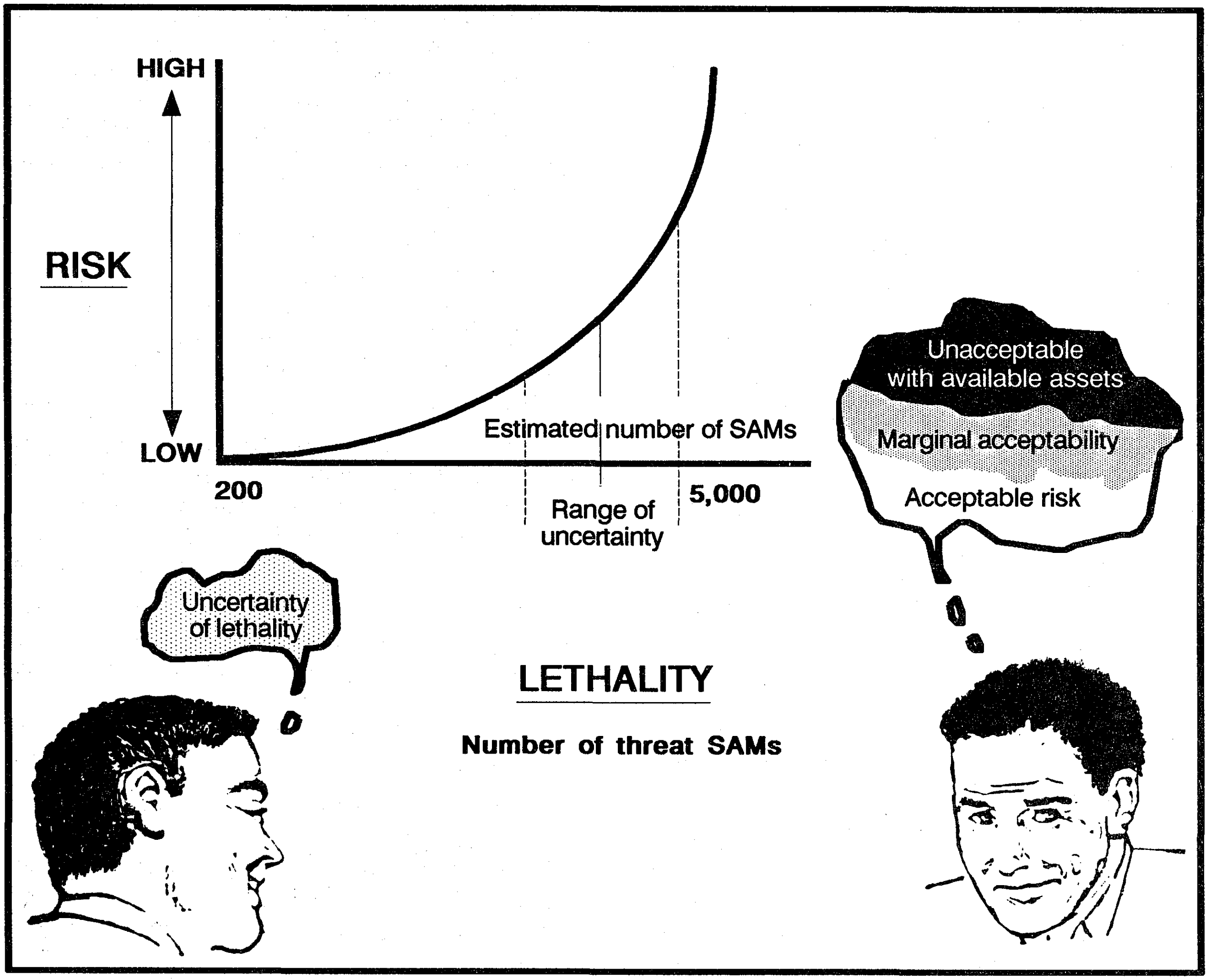


Figure 4-1. Translating uncertainty to risk.

In a counter-drug operation, time will not be such a problem. Determine growing patterns and cycles in your AO and AI. For example, if coca, the leaf will have to be moved to a base laboratory within a certain period.

Your map is a model of the real world. It contains valuable information about the battlefield environment. Use it as a base for your model. Overlay the time period snapshots to highlight patterns and changes.

Thinking RED is seeing the current situation in the AO and AI from the threat's point of view. This color anchors your model to the current situation. Remember that the combat arm of the insurgent or terrorist group is an extension of the political or religious faction. Therefore, actions on the battlefield follow the political or religious strategy of the organization.

Counter-drug operations may be tethered to production cycles or economic concerns. The security elements of the drug producer will follow basic site defense tactics. Plot the threat locations, known and perceived. This will help you view the AO from his vantage.

Thinking BLUE refers to seeing the operation from the friendly commander's viewpoint. Friendly forces may become the threat target in an insurgency or terrorist environment. Plot friendly locations; determine effect on threat positions and likely threat COA.

The concept of *thinking GREEN* is new to the threat model. Consider the impact the populace has on the threat and friendly forces as well as their location in the AO and AI. Will they impede operations? Will they assist the threat? Are there areas pro-government or anti-government?

This information affects the uncertainty of the situation. It is an added dimension to analysis not considered on the dispersed battlefield. Plot the disposition of the population by type of support (pro, anti, or neutral) and ethnic, racial, religious, and even economic divisions.

Thinking BLACK pertains to manmade objects that are displayed on any map. When you think black, consider al‡ structures whether they are buildings, bridges, towers, or transportation routes. For example:

- In insurgency and counterinsurgency operations, these objects may provide concealment and cover or targets for both friendly and threat forces.
- In search and rescue or DRO, you will need to know key structures for planning purposes.
- In NEO, knowing the locations and condition of structures such as hospitals, police stations, and governments aids in planning and executing NEO.

TESTING THE MODEL

With a model of how the AO appears, the analyst can test hypotheses of how threat and population may interact. A hypothesis is an explanation for a set of facts that can be tested by further investigation. It should consist of a set of logically related propositions and an expected outcome.

A hypothesis can be proven false based on evidence, but it can never be proven correct in advance. The best that you can do is to rank order several hypotheses or assign rough probabilities to them. When seeking evidence to support or reject a hypothesis, consider the following:

- The threat may be engaged in deception or disinformation.
- Sensors and platforms may not be able to operate in all areas or situations.
- Indicators may be common to several hypotheses.
- A number of assets may collect the same or very similar information. This gives undue validity to a hypothesis.
- A seemingly insignificant indicator may be vital to a specific COA.

BIASES

Errors in thinking can lead to false alarms or rejecting good ideas. Other errors that affect analysis are biases. There are four types of biases:

- Cultural.
- Organizational.
- Personal.
- Cognitive.

Cultural biases are formed at an early age and continue through life. They are based on your cultural or social perceptions. Remember, you will view certain areas—religion, customs, or even local dress codes—from a different point of view than the threat and the local populace.

Organizational biases are based on your knowledge of how your organization operates and the personalities of your commander and supervisors. This bias makes it easy to *idealize* a situation. Be careful not to alter your deductions or recommendations in an attempt to please the commander.

Personal biases come from your own experiences. If you previously had success using a particular analytical process, you may continue to try to fit every situation to this model. Do not attempt to put square pegs in round holes. Alter your thinking to accommodate different situations.

Cognitive biases have strengths and weaknesses. These vary from source-to-source and sometimes from message-to-message. This variance creates doubt about the reliability of some sources. Contributing to this are—

- Vividness. A clear and concise report will receive more attention than something vague, even if it is wrong.
- Absence of evidence. Do not hold back information because it is not conclusive.
- Oversensitivity to consistency. Do not validate information simply due to consistent reporting. Instead, consider if the information is representative of the potential total of information available.

TECHNIQUES OF ANALYSIS

There are two primary analytical techniques that help the analyst identify the presence of indicators—pattern and link.

PATTERN ANALYSIS

This technique is based on the premise that threat COAs reflect certain characteristic patterns that can be identified and interpreted. Ideally, paragraph 3 of the intelligence estimate (see Appendix F) should identify the presence of these indicators.

Analysts are faced with problems of organizing and recording incoming information and adding it to existing information so that meaningful relationships are clarified. The working situation map (SITMAP) and IPB templates are the primary tools used to organize information. Indicators can be ambiguous and incomplete. The analyst identifies patterns of activity or tip-offs which characterize specific threat units.

For example, you are supporting a counter-drug operation. You have data available concerning previous raids. This data, plotted on an overlay, gives you trends and patterns. You then apply these trends or patterns to other locations, predicting possible laboratory sites.

Current information is posted to your incident map as received. This map is a working aid allowing you to graphically show threat activity in both AO and AI that you consider important. Information on the incident map can provide a good foundation for the more formal SITMAP.

In another example, you are supporting a disaster relief mission following an earthquake. Your IPB process reveals certain high-cost areas that may be prone to looters. Information from your incident map reveals a trend in looting within two areas. These areas would go onto your SITMAP as confirmed threat target areas.

Working files are critical to properly store the extensive research material you will generate. You may be fortunate to be in a unit that has its files on computer; otherwise, you will have to do this manually. Either way, you must ensure that your filing system is easily understood, information is easy to retrieve, and includes cross-referencing.

The *hot file* is your most important working file. Here you will keep all available material pertaining to a specific incident, as well as information from related incidents. Reports of planned demonstrations, sabotage, or attacks all initiate hot files. A hot file becomes inactive when the event occurs, does not occur, or your priorities change.

It is critical that you stay alert and recognize all possible patterns that may be formed. The following illustrates the possible fusion of information:

- A tactical analysis team supporting counter-drug operations OCONUS receives a report from the FAA that three new Cessna aircraft have been registered by an export company located in the HN.
- Information from the personality files reveals that the owner of the export company is a relative of a major drug trafficking family residing in a neighboring country.
- The drug trafficking organization and family files reveal that the family in the neighboring country recently decided to move its export base to another country, location unknown.
- A review of the front company files reveals that the export company is a subsidiary of a US corporation.
- A request for information from the DOJ and DOT reveals that the corporation is being investigated for a number of federal offenses.

Once all related items of information from the intelligence files, sources, and agencies are obtained, the analyst begins to assemble the available information to form as many logical solutions or hypotheses as possible.

Assembly of information to develop logical hypotheses requires good judgment and considerable area expertise. When you develop hypotheses, avoid reaching conclusions based on prejudices or preconceived notions. In the above example, it would be easy to assume that the owner and relative are actually the export link for the drug trafficking family.

There are still some information gaps you must explore. Are there other family members of the traffickers in the same country or surrounding countries? In what illicit market is the front company involved? At a minimum, you have linked the owner of the front company to new aircraft, a drug trafficking family, and a US corporation suspected of federal offenses.

In the example above, if the owner is involved in the shipment of drugs, first you will have to determine from where the shipments originate. This will dictate your future actions. If it is from your country, you will be involved directly. If not, you will be on the periphery. In either case, you wil! be in direct contact with the DEA.

If the owner is not involved in drug trafficking, you will report the situation to the appropriate HN and US agencies. You will also search for other information that may link the drug trafficking family to other personalities residing within your AO.

A resource file includes all material which is important but not of immediate value. It includes hot files that are overcome by events (OBE), inactive incident files, inactive personality and organization files, and photographs.

The coordinate register is a valuable analytical tool. It keeps track of threat activity in a given area over time. Each page represents an important geographic area or town. This register has two parts: written entry record, Figure 4-2, and a blowup of the map grid, Figure 4-3. Both products help identify trends and patterns.

Figure 4-4 shows the personality card format which is maintained on each threat personality and organization. The correct identification of threat personnel will help you *build* the threat data base. Therefore, you must include all personalities, not just leaders. For example, you are supporting a counterinsurgency mission. You know that the threat is acquiring shoulder-fired SAMs.

Your PIR are focused on where the SAMs will be located and which force will receive them. A review of personality files will reveal which individuals have been trained on the weapon. With this data, you can focus your collection assets on specific people and areas. By identifying personalities and activities, you can construct organizational line-and-block charts and other data.

LINK ANALYSIS

Link analysis is used to depict contacts between persons, events, activities, and organizations. It can be used with four different recording devices:

- Association matrix.
- Activities matrix.
- Time event charts.
- Link diagrams.

The association matrix, Figure 4-5, is used to determine the degree of relationships, contacts, or knowledge between individuals. It is used to register members of a threat organization and chart their relationships with each other. The structure of the threat organization is formed as connections between personalities are made. (Acronyms and names used therein are fictional.)

The activities matrix, Figure 4-6, is used to connect individuals to any organization, event, entity, address, activity—anything other than people. Information from this matrix, fused with information from the association matrix, assists you in linking personalities as well.

For example, you may determine that three people who have never been seen together are all involved in the finance section of an insurgency. By linking their common activities, you can request surveillance to determine association. You may find that each is in charge of finances for separate cells of the same faction.

Time event charts are shown at Figure 4-7. This is a chronological record of individual or group activities designed to store and display large amounts of information in a small space.

Link diagrams are a graphic display used to assist the analyst conducting link analysis. It allows the analyst to show linkage between individuals and various sections of the threat organizations. An example is at Figure 4-8.

COMBINED ANALYSIS

Link and pattern analysis are often combined. For example, over a period of two months you have determined that every time a shipment of cocaine has been made from the AO, a request for plastic medical refuse bags emanated from that specific laboratory. By linking the two activities—request for medical refuse bags and the shipment of cocaine—you have established one pattern in the shipment of cocaine.

You should attempt to link another activity or possibly a person to this activity for the development of other indicators. If you know that medical plastic bags are ordered, you should also know who receives the order. Most likely that person is the logistician of the organization. You now link the logistician to other activities and personalities.

ITEM	TIME	COORDINATE	ACTIVITY	NOTES
1	101428	XK124679	COCAINE LAB	15 KILOS COCAINE
2	121544	XK179600	PRECURSOR ELEMENTS CACHE	ACETONE, ETHER
3	130523	XK155693	CESSNA 172 SEIZED	300 KILOS COCAINE

Figure 4-2. Written entry coordinate register.

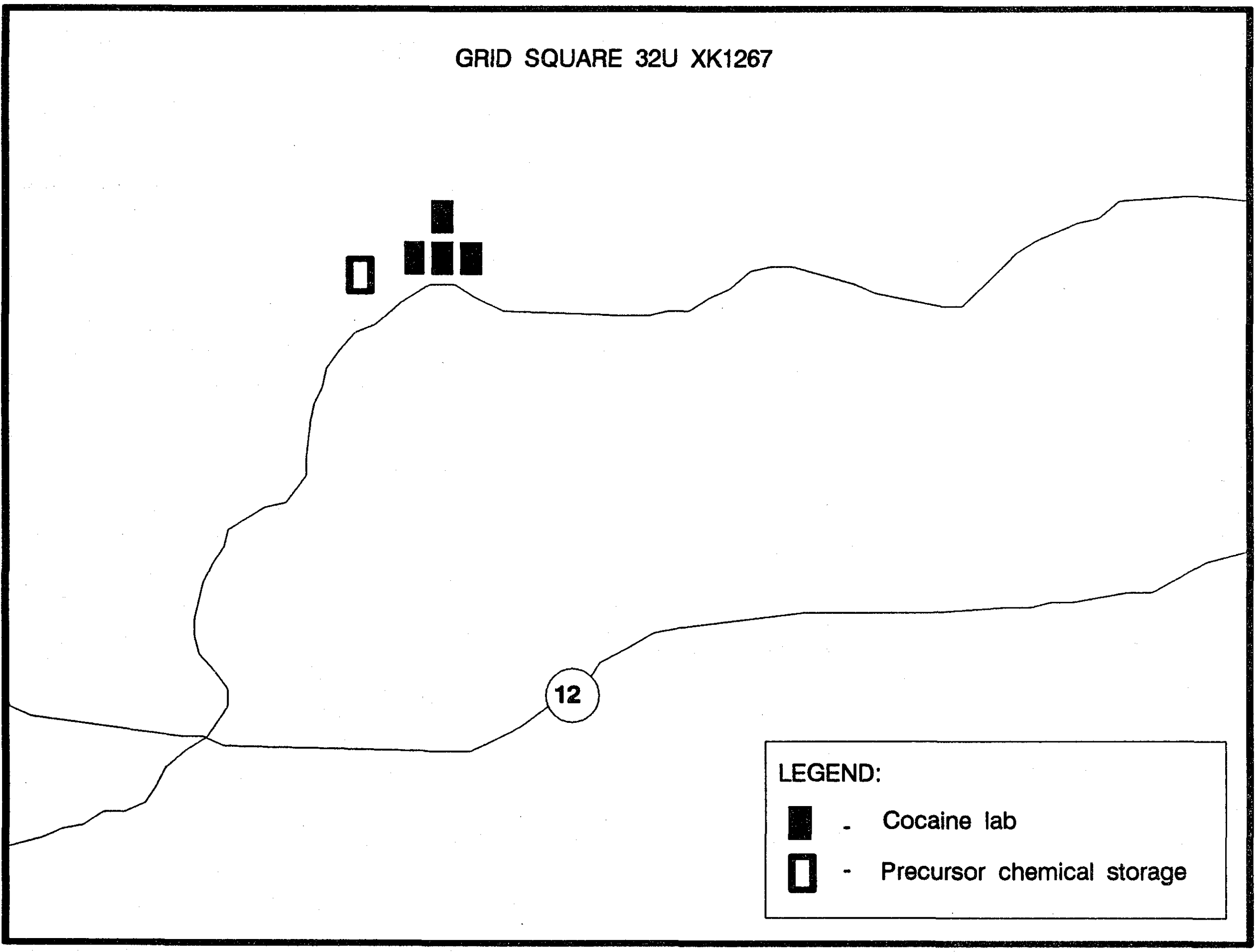
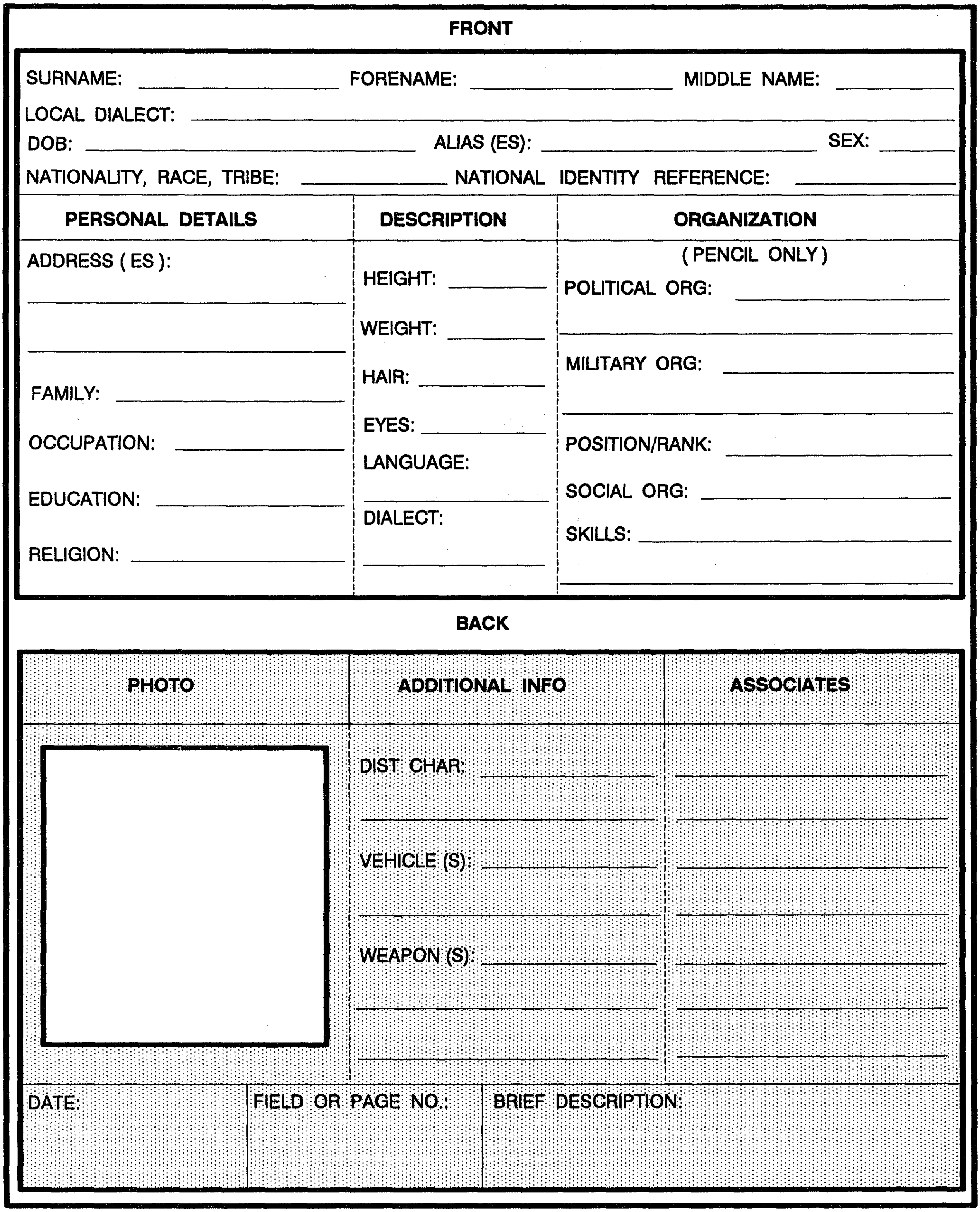


Figure 4-3. Coordinate register map grid.



FRONT

SURNAME: ____ FORENAME: ____ MIDDLE NAME: ____

LOCAL DIALECT: ____

DOB: ____ ALIAS (ES): ____ SEX: ____

NATIONALITY, RACE, TRIBE: ____ NATIONAL IDENTITY REFERENCE: ____

PERSONAL DETAILS

ADDRESS (ES): ____

____

FAMILY: ____

OCCUPATION: ____

EDUCATION: ____

RELIGION: ____

DESCRIPTION

HEIGHT: ____

WEIGHT: ____

HAIR: ____

EYES: ____

LANGUAGE:

____

DIALECT:

____

ORGANIZATION

(PENCIL ONLY)

POLITICAL ORG: ____

____

MILITARY ORG: ____

____

POSITION/RANK: ____

SOCIAL ORG: ____

SKILLS: ____

____

BACK

PHOTO

ADDITIONAL INFO

DIST CHAR: ____

____

VEHICLE (S): ____

____

WEAPON (S): ____

____

____

ASSOCIATES

____

____

____

____

____

____

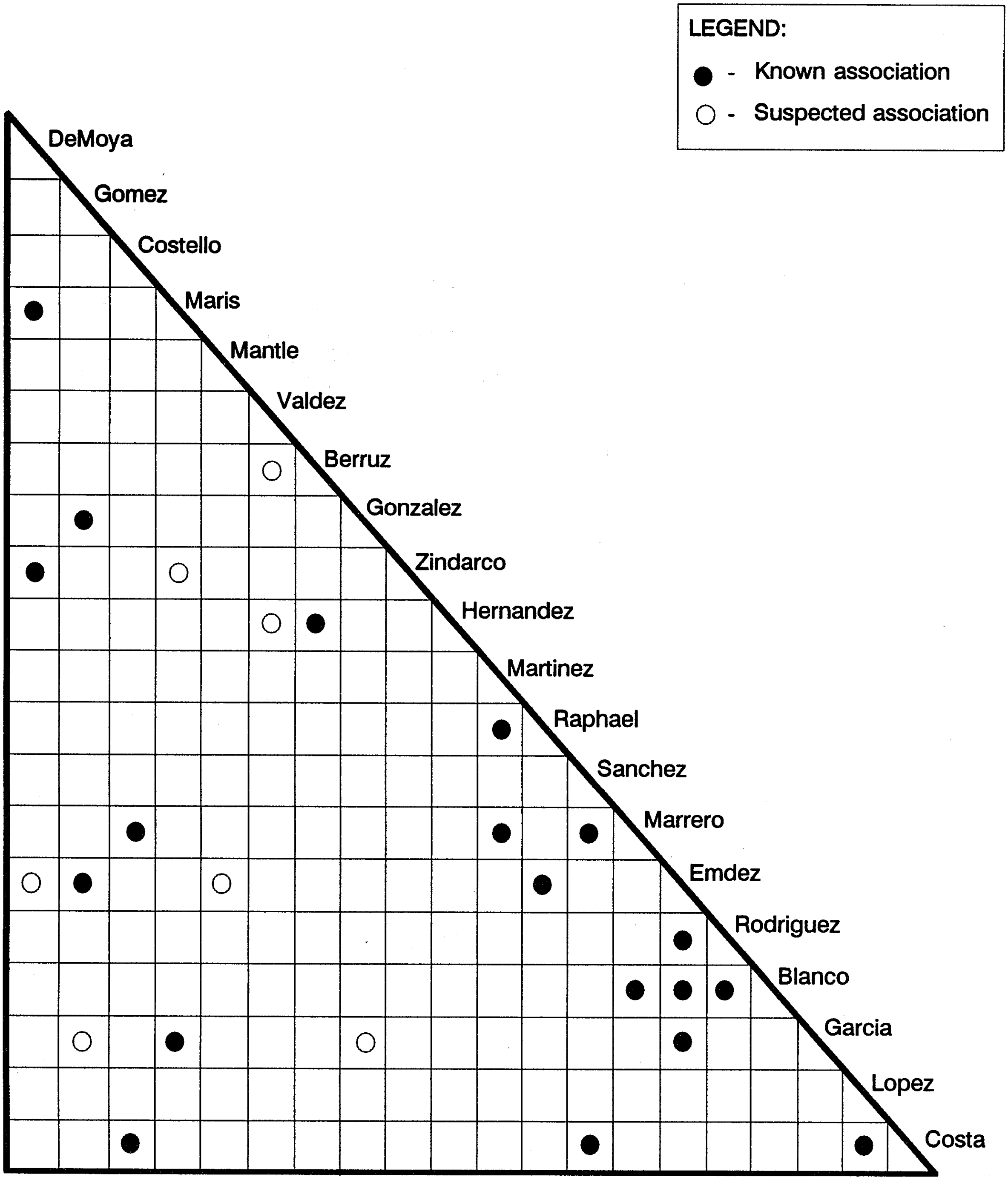
____

DATE:

FIELD OR PAGE NO.:

BRIEF DESCRIPTION:

Figure 4-4. Personality card format.



LEGEND:

● - Known association

○ - Suspected association

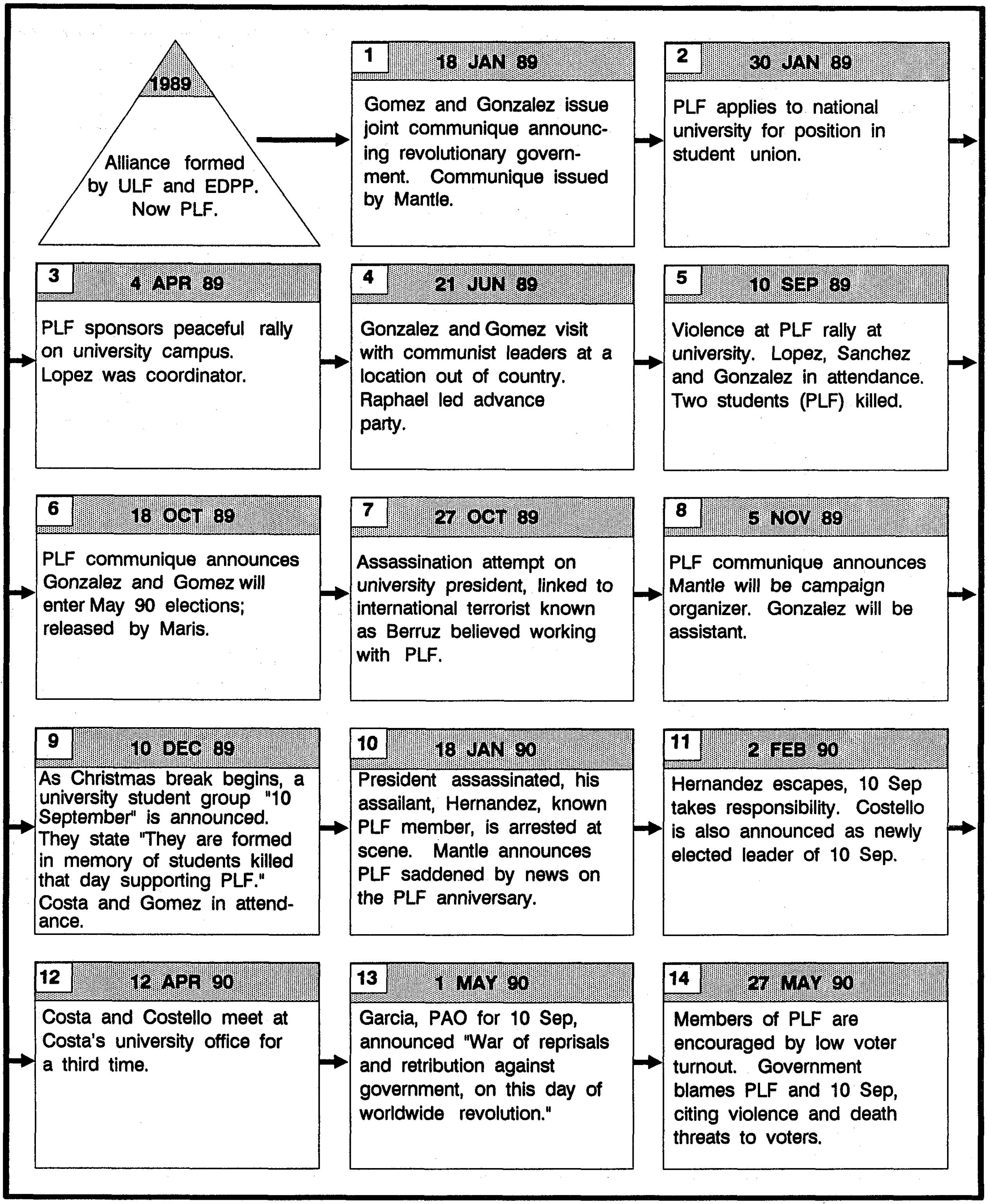
	DeMoya	Gomez	Costello	Maris	Mantle	Valdez	Berruz	Gonzalez	Zindarco	Hernandez	Martinez	Raphael	Sanchez	Marrero	Emdez	Rodriguez	Blanco	Garcia	Lopez
Gomez																			
Costello																			
Maris	●																		
Mantle																			
Valdez																			
Berruz						○													
Gonzalez		●																	
Zindarco	●			○															
Hernandez						○	●												
Martinez																			
Raphael											●								
Sanchez																			
Marrero			●								●		●						
Emdez	○	●			○							●							
Rodriguez															●				
Blanco														●	●	●			
Garcia		○		●				○							●				
Lopez																			
Costa			●										●						●

Figure 4-5. Association matrix.

	Political Trainer	Crew Served Wpn Trainer	Recruiter	External Logistics	External Travel	Propaganda	Registered Communists	News Media	External Business Trade	Political Tng Received	External University Ed.	Finance	Logistics	Assassination	Illicit Drugs	External Media Support	Weapons Buyer	Weapons Supplier
DeMoya				●		○	●				○					●		
Gomez						●	○				●							
Costello										●								
Maris								●								○		
Mantle						●	○				●							
Valdez														●				
Berruz														●				
Gonzalez						●	○				●							
Zindarco																●		
Hernandez														●				
Martinez					●													
Raphael					●				●									
Sanchez			●				○											
Marrero					●				●		●	●						
Emdez					○	●	●		●		●		●		●		●	
Rodriguez																		●
Blanco				●									●					
Garcia						●	●	●			●				●			
Lopez		●			●		●			●	●							
Costa	●				●		●			●	●							

LEGEND:
● - Known association
○ - Suspected association

Figure 4-6. Activities matrix.



1989

Alliance formed by ULF and EDPP. Now PLF.

1 — 18 JAN 89

Gomez and Gonzalez issue joint communique announcing revolutionary government. Communique issued by Mantle.

2 — 30 JAN 89

PLF applies to national university for position in student union.

3 — 4 APR 89

PLF sponsors peaceful rally on university campus. Lopez was coordinator.

4 — 21 JUN 89

Gonzalez and Gomez visit with communist leaders at a location out of country. Raphael led advance party.

5 — 10 SEP 89

Violence at PLF rally at university. Lopez, Sanchez and Gonzalez in attendance. Two students (PLF) killed.

6 — 18 OCT 89

PLF communique announces Gonzalez and Gomez will enter May 90 elections; released by Maris.

7 — 27 OCT 89

Assassination attempt on university president, linked to international terrorist known as Berruz believed working with PLF.

8 — 5 NOV 89

PLF communique announces Mantle will be campaign organizer. Gonzalez will be assistant.

9 — 10 DEC 89

As Christmas break begins, a university student group "10 September" is announced. They state "They are formed in memory of students killed that day supporting PLF." Costa and Gomez in attendance.

10 — 18 JAN 90

President assassinated, his assailant, Hernandez, known PLF member, is arrested at scene. Mantle announces PLF saddened by news on the PLF anniversary.

11 — 2 FEB 90

Hernandez escapes, 10 Sep takes responsibility. Costello is also announced as newly elected leader of 10 Sep.

12 — 12 APR 90

Costa and Costello meet at Costa's university office for a third time.

13 — 1 MAY 90

Garcia, PAO for 10 Sep, announced "War of reprisals and retribution against government, on this day of worldwide revolution."

14 — 27 MAY 90

Members of PLF are encouraged by low voter turnout. Government blames PLF and 10 Sep, citing violence and death threats to voters.

Figure 4-7. Time event chart.

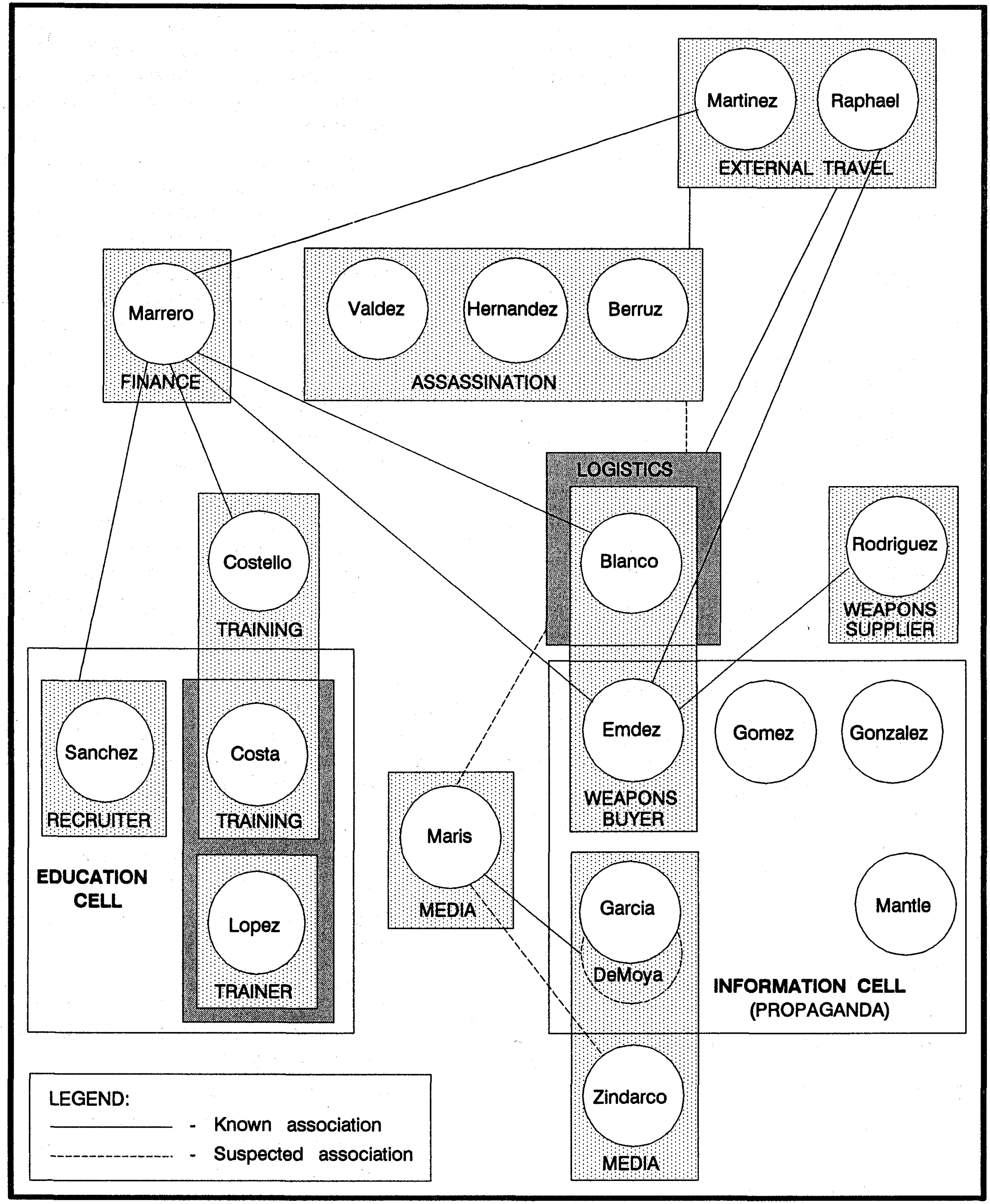


Figure 4-8. Link Diagram.

FACTORS OF ANALYSIS

FM 100-20/AFP 3-20 provides an excellent model for the factors of analysis when analyzing an insurgency or counterinsurgency. We follow that guide but tailor it for LIC. Areas addressed are—

- Mission analysis.
- Nature of the society.
- Nature of the threat.
- Nature of the government.
- General conclusions.
- COAs.

You must identify the principal factors for these broad areas and study each in turn. Then you weigh and compare the factors in each area and reach tentative conclusions. These conclusions lead to development of possible COAs. You can then rank the probability of each COA and select the most likely one.

Figure 4-9 shows a threat analysis worksheet. This worksheet provides a guide to collection and analysis. The worksheet can also serve as a model for factor analysis.

MISSION ANALYSIS

Mission analysis requires a concise, but encompassing, description of the final outcome wanted. Consider all constraints and restrictions affecting mission achievement. Among these are material and human resource constraints, as well as the demands of politically active groups in the society. You will first use assumptions and then replace them with facts as the situation develops.

NATURE OF THE SOCIETY

Demographics of the HN society includes these five areas:

- Social organization.
- Economic organization and performance.
- Political organization and dynamics.
- History of the society.
- Political environment.

Social Organization

In evaluating social organization, look at—

- Density and distribution of population by identifiable groups; balance between urban and rural groups; sparsely populated areas; and concentrations of predominantly racial, linguistic, or cultural groups.
- Race, religion, national origin, tribe, economic class, political party by group affiliation, ideology, education level, union memberships, management class, occupation, and age of the populace.
- Overlaps among classes and splits within them. For example, do union members belong to one or many religious or racial groups? Are there ideological divisions within a profession?
- Composite groups based on their political behavior and the strength of each. For example, who actively or passively supports the HN, the insurgents, or remains neutral.
- Current or potential issues driving the political, economic, social, or military behavior of each subgroup—group and population growth or decline, age distribution, and changes in location by groups; for examples, economic benefits, social prestige, political participation, and perception of relative deprivation.

Determine which activities and programs accommodate the common goals of politically and socially active groups. You then determine which groups and composite groups support (or are inclined to support) the government, the threat, or remain neutral.

Economic Organization and Performance

Factors to consider when evaluating economic organization and performance are—

- The principal economic ideology of the society and local innovations or adaptations.
- The economic infrastructure. Examples: Fuel and mineral resource locations, bulk electric power production and distribution, transport facilities, and communications networks.
- Economic performance. Examples: Gross national product, gross domestic product, foreign trade balances, per capita income, inflation rate, and annual growth rate.
- Performance of productive segments. Examples: Public and private ownership patterns; concentration

1. US objective (immediate, short-term, long-term).

2. Nature of the society.

   a. Social, economic, political, and security conditions.

   b. Causes of discontent.

   c. Issues.

   d. Groups (segments of the population) and forces (groups trying to influence actions of others).

   e. Variables likely to influence the level of violence (coercive potential, institutions, legitimacy of the regime).

3. Nature of the threat.

   a. Leadership.

   b. Objectives (immediate, short-term, long-term).

   c. Organization.

   d. Target groups.

   e. External support (third party).

   f. Timing.

   g. Mass support.

   h. Relationship to legitimate political processes.

   i. Use of violence.

   j. Urban or rural base.

4. Nature of government.

   a. Objectives (immediate, short-term, long-term).

   b. Description of program (counterinsurgency, counter-drug, and so forth.)

   c. Evaluation of program.

      (1) Balanced, neutralization, and mobilization programs.

      (2) Preemptive and reinforcing aspects of threat strategy.

      (3) Adherence to operational guidelines.

      (4) Evaluation of each program in terms of likely impact on each segment of the population.

5. Government response (US, HN, third party).

   a. Possible COAs.

   b. Evaluation of each COA.

   c. Recommendation.

Figure 4-9. Threat analysis worksheet.

and dispersal; distribution of wealth in agriculture, manufacturing, forestry, information, professional services, transportation, mining, and others.

- Public health factors. Examples: Birth and death rates, diet and nutrition, water supply, sanitation, health care availability, and endemic diseases.
- Foreign trade patterns. Examples: Domestic and foreign indebtedness (public and private) and resource dependencies.
- Availability of education. Examples: Access by individuals and groups sufficient for national needs; groupings by scientific, technical, professional, liberal arts, and crafts training; surpluses and shortages of specific skills.
- Unemployment, underemployment, exclusion of groups, and horizontal and vertical career mobility.
- Taxing authorities, rates, and rate determination.
- Economic benefit and distribution, occurrence of poverty, and concentration of wealth.
- Population shifts and their causes and effects. Examples: Rural to urban, agriculture to manufacturing, and manufacturing to service.

You can now identify economic programs with values and resources which might increase favorable HN support, stabilize neutral groups, or neutralize threat groups.

Political Organization and Dynamics

When evaluating political organization and dynamics, look at—

- The formal political structure of the government and the sources of its power. Examples: Pluralist democracy based on the consensus of the voters, strong-man rule supported by the military, others.
- The informal political structure of the government and its comparison with the formal structure. Example: Is the government legally a democracy but in reality a political dictatorship or oligarchy?
- Legal and illegal political parties and their programs, strengths, and prospects for success. Also, the prospects for partnerships and coalitions between parties.
- Nonparty political organizations; motivating issues, strengths, parties or programs they support, and political action groups.
- Nonpolitical interest groups and the correlations of their interests with political parties or nonparty organizations. These include churches, cultural groups, professional organizations, and unions.
- The mechanism for government succession and the integrity of the process; roles of the populace; regularity of elections; systematic exclusion of identifiable groups; voting blocks; and patron-client determinants of voting.
- Independence or subordination and effectiveness of the judiciary. For instance: Does the judiciary have the power of legislative and executive review; does it support constitutionally guaranteed rights and international concepts of human rights?
- Independence or control of the press and other mass media and alternatives for the dissemination of information and opinion.
- Centralization or diffusion of essential decision-making process and patterns of inclusion or exclusion of specific individuals or groups.
- Administrative organization and competence of the HN civil service bureaucracy. For example, are they altruistic public servants or self-serving crooks? Can individuals and groups make their voices heard within the bureaucracy?

You now correlate those social, economic, and political factors and identify political programs which will neutralize opposition and promote a supporting majority.

History of the Society

When evaluating history, look at the—

- Origin of the incumbent government and its leadership. Examples: Was it elected? Has it been in power long? Have there been multiple peaceful successions of government?
- History of political violence. Examples: Is violence a common means for the resolution of political problems? Is there precedent for revolution, coup d'etat, assassination, or terrorism? Does the country have a history of consensus building? Does the present threat have causes and aspirations in common with historic political violence?

Political Environment

In evaluating the political environment, determine the legitimacy of the government. Observe and analyze acceptance of violent and nonviolent remedies to political problems by the populace; the type and level of violence exhibited by friendly and threat forces; and the groups or subgroups which support or oppose the use of violence.

NATURE OF THE THREAT

Studying the nature of the threat includes their objectives, organization, operational patterns, leadership, tactics, and external support.

In evaluating threat, look at the—

- Desired end state of the threat. Clarity of its formulation. Openness of its articulation. Commonality of point of view among the elements of the threat. Differences between this end view and the end view of the government.
- Groups and subgroups supporting the general objectives of the threat.
- Divisions, minority views, and dissensions within the threat.
- Groups which may have been deceived by the threat concerning the desired end state of the threat.
- Threat organizational structures and patterns; their variations, combinations, shifts, and trends.

Determine the stage and phase of the threat, and how far and for how long it has progressed or regressed over time. You also identify and evaluate unity and disagreement within front groups.

NATURE OF THE GOVERNMENT

Here we address the HN government. Areas to examine are—

- National strategy.
- Coercive measures.
- Balanced development.
- Administrative competence.

In evaluating the nature of the HN government response, examine the—

- General planning or lack of planning for countering the threat, comprehensiveness of planning, and correctness of definitions and conclusions.
- Organization and methods for strategic and operational planning and how these plans are executed.
- Strengths, weaknesses, resource requirements and constraints, and the validity of priorities.
- Use of population and resources, and the effects on each group.
- Organization, equipment, and tactical doctrine for security forces. For example, how does the government protect its economic and political infrastructure?
- Areas where the government has maintained the initiative.
- Population and resource control measures.
- Economic development programs.

Next, correlate HN and threat strengths and weaknesses and identify necessary changes in friendly security force programs, plans, organization, and doctrine.

In evaluating the effects on nonbelligerents, look at—

- Mechanisms for monitoring nonbelligerent attitudes and responses.
- Common objectives of groups neither supporting nor opposing the threat.
- Effects of HN military, political, economic, and social operations and programs on the populace. For example, does it kill civilians in counter-threat operations? Are benefits of government aid programs evenly distributed?
- Whether the populace is inclined to provide the threat or the HN with intelligence.

You also determine the strengths and weaknesses of the nonbelligerents; the depth of their commitment to remain neutral; and programs to keep them neutral or to support HN initiatives and forces.

In evaluating the COA for threat, HN, and nonbelligerents, you must consider and integrate the above factors into a comprehensive, flexible report.

GENERAL CONCLUSIONS

You must now try to put your analyses of society, threat, and government together. Your conclusions must accommodate and reflect the interaction of all factors.

You determine the methods with which each side attempts to mobilize human and materiel resources in its favor. This methodology affects specific groups of people in diverse ways. Analysis identifies issues which concern key political, social, and economic groups.

Both government and insurgents offer solutions to the people's problems and attempt to deliver on their promises, within various constraints.

A measured mix of benefits, persuasion, and coercion motivate groups to conform their behavior to the will of the provider. Remember the first principle of people management: Things that are rewarded are things that get done.

COURSES OF ACTION

Conclusions lead to COAs. Determine what is necessary to—

- Persuade a majority of identified groups to support the HN.
- Neutralize opposition groups.
- Prevent unaligned groups from supporting the opposition.

Whether you are actively involved in the operation, or on the periphery, you must keep the COA in balance. Consider the effect of each COA on each targeted group. Frequently, a benefit to one group has a negative effect on another. Consider all group dynamics. Assign priorities to groups in proportion to their importance in influencing the balance of power.

As the analyst, you must also consider using force against groups totally committed to the opposition. You may recommend the use of violence appropriate to the nature of the group's involvement in the conflict.

In general, select COAs which hold the greatest promise of moving groups to your side and the least risk of driving groups into the threat camp.

CHAPTER 5

INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO INSURGENCY AND COUNTERINSURGENCY

US forces require intelligence information to operate either in support of a US-backed insurgency against an oppressive regime or on behalf of a friendly HN fighting an insurgent group. This chapter provides TTP needed to conduct missions and functions of each of the intelligence disciplines and CI support in these kinds of operations.

HUMAN INTELLIGENCE

HUMINT plays a major role in insurgency and counterinsurgency operations. In support of an insurgency, HUMINT sources provide information on the intentions and operations of the threat government. In counterinsurgency operations, HUMINT provides information on the insurgent capabilities, intentions, deliberations, and decisions.

In these environments, the struggle is between the government and the insurgents for the loyalty and support of the populace. The population is key to success or failure. As the conflict revolves around the population, they usually have a wealth of information that can be exploited. This information can be collected through liaison, controlled collection, interrogation, and document exploitation.

In counterinsurgency operations, civilian sources provide information on the—

- Ideological motivation and sympathies of local residents.
- Logistical support available, or potentially available, to insurgents.
- Potential insurgent targets and objectives.
- Identification of rank and file supporters of the insurgency.
- Insurgent sabotage, espionage, terrorist techniques, and activities.
- Underground support, structure, and activities.
- Insurgent weaknesses and vulnerabilities.
- Insurgent PSYOP and the impact on local populations.
- Insurgent location, size, strength, and organization.
- Insurgent key members.

There are many sources for this information available to military and civilian government intelligence agencies. Some examples include—

- Leaders of dissident groups (ethnic, religious, labor, political).
- Merchants.
- Native religious groups.
- Medical personnel (doctors, nurses, hospital employees).
- Ordinary citizens.
- Insurgent defectors.
- Captured insurgents.
- Local police departments and other local agencies.

Liaison is established with HN law enforcement, intelligence, and government agencies. Your primary liaison and coordination is with local law enforcement agencies (LEAs). Insurgent activities often look like criminal activities. This is particularly true during the earlier stages of the insurgency. LEA activities include developing informants and informant nets which feed them intelligence and information. Liaison with HN military and paramilitary organizations can also provide valuable HUMINT information.

The US role in support of counterinsurgency is based on the principles of the IDAD strategy. When directed, US military support includes CSS, CS, and even combat forces. When, or if, this escalation occurs, additional HUMINT assets will be available. These US forces, by their very presence, become involved in the collection of intelligence on the insurgents. Some examples of HUMINT collection activities include—

- PSYOP, CA, and civil-military operations.

- Observation posts (OPs), patrolling, and reconnaissance.
- Long-range surveillance (LRS) detachments.
- MP.
- CS and CSS operations.
- SOF.

HUMINT, particularly low-level tactical HUMINT, may well be your most important intelligence discipline. It provides short-term tactical intelligence to support military and civil-military operations. It can also provide crucial I&W on a threat that operates in small numbers, normally avoids confrontation, and selects targets based on careful understanding of friendly vulnerabilities.

HUMINT has the capability of defeating the insurgency by identifying the insurgent's reason for (and degree of) popular support.

IMAGERY INTELLIGENCE

IMINT plays a big role in the support of insurgency and counterinsurgency operations. Typically used to track threat disposition, it also supports political, economic, and social efforts. Tasking of imagery assets is based on their availability and ability to support the commander's mission.

These assets include national, theater, and tactical sensors and platforms and can include civil imaging capabilities as well. They are used to obtain information the analyst uses to answer the commander's PIR and IR, and to create the imagery-derived products used for mission planning and references. See Appendix H for details on IMINT support in LIC.

Imagery collected against threat targets is examined by the imagery analyst (IA). He is looking for current indicators of threat activities. He then weighs the implication and significance.

Imagery collection in support of insurgency operations is more covert than in counterinsurgency operations.

IMINT systems used in support of an insurgency have the capability to monitor and collect against a number of threat targets. They include, but are not limited to—

- Deployment of government artillery.
- Deployment of government helicopters.
- Out of garrison (or out of area) deployment of maneuver units.
- Movement of government logistics and ordnance forward or into uninhabited areas.

IMINT systems support counterinsurgency operations more openly and directly. Examples of targets include—

- Storage facilities.
- Transshipment points.
- Main supply routes.
- Recurring roadblocks or road tax collection points.
- Training, refugee, or operational encampments.

IMINT support in the three phases of insurgent activities are discussed below.

PHASE I—LATENT AND INCIPIENT

In Phase I a limited number of targets can be collected against since this phase is normally conducted clandestinely. Targets might include arms, logistics, shipping, and delivery activities plus roadblocks and tax collection points.

National level collection is predominantly in support of an eventual tactical unit intervention. Tactical units with the mission to support LIC operations in this category will be able to obtain intelligence and supporting products from national sources.

IAs study the imagery in order to detect, classify, and identify the above targets regardless of technique. Collection against these targets will contribute to the AO intelligence data base.

IMINT may also be used to update existing map products. Many insurgent areas are very remote, and maps may be inadequate or nonexistent.

Most of the insurgent activity in this phase will likely be found in rural areas as HN forces tend to be stationed in and around major cities.

Imagery support during this phase is almost totally restricted to the development of a baseline data base.

PHASE II—GUERRILLA WARFARE

Here IMINT targets expand to include insurgent training and more detailed logistic activities. As the activities initiated in Phase I continue, newly recruited guerrillas need both physical and weapons training. IMINT can reveal locations used for physical training such as running tracks which may show up as rough oval shapes on the ground. Firing ranges can be detected and are good indicators of a possible insurgent presence in an area.

Insurgent activity indicators may include changes in crop sizes, new or unexplained agricultural areas, and recently cleared fields.

However, you must not confuse legitimate farming activities with those in support of the insurgents. Comparative coverage (coverage of the same area or object taken at different times and by different sensors to show changes) would help to identify the legitimate areas as opposed to the areas used by the insurgents. Sensors capable of supporting counterinsurgency operations include optical, E-O, infrared, multispectral, and radar. Selection depends on availability.

PHASE III—WAR OF MOVEMENT

Insurgents expand on activities conducted on the previous phase and the struggle becomes a conflict between military forces. These activities will continue to drive the imagery collection effort.

Long-term aerial surveillance operations collect information over a long period of time to note any changes in the AI and AO, while aerial reconnaissance operations collect information over specific targets at a particular time.

SIGNALS INTELLIGENCE

SIGINT can play an important role in support of either insurgency or counterinsurgency operations.

SIGINT efforts against insurgencies offer the commander a chance to collect information in both close-in and stand-off postures. Limited threat air defense allows airborne platforms to get closer to the target and provides better coverage. Platforms are restricted by maintenance, bad weather, and allowable flight time.

Although ground-based systems operate longer and require less maintenance than airborne systems, they need frequent resupply and are physically closer to the target. To pinpoint threat targets in counterinsurgency operations, a combination of air and ground-based systems is best.

ESM intercept, identify, and locate targets of interest. The technical information gained from ESM is one SIGINT source developed during operations against insurgents. (The systems in Appendix B show the variety of man packed, vehicular, and airborne collection systems available to the commander.)

In counterinsurgency operations these systems are used to locate C^3 elements as well as infiltration, exfiltration, and resupply routes.

Insurgents are usually organized into small cells of three to five people. To the SIGINT and EW unit this means that there may be a target-rich environment. The analytic techniques used to chart an insurgent C^3 structure are the same as those used for any communications structure.

SIGINT provides early I&W of insurgent intentions. Prior to an operation, you may find that an insurgent group employs radio silence. This may not be readily noticeable at first, but through pattern analysis you should eventually be able to predict threat actions.

Exploitation of captured command, signal, and code-related materials is also imperative. SIGINT helps the commander through target development of threat C^3 and logistics activities.

In the offense, EW measures include the exploitation, disruption, and deception of threat command, control, communications, and intelligence (C^3I) through—

- ECM (jamming and deception).
- ESM (intercept, identify, and locate).

The technical data gained from these activities allows you to effectively carry out ECM operations.

Defensively, ECCM protect friendly C^3 systems through the use of the meaconing, intrusion, jamming, and interference (MIJI) program and the proper deployment of ground-based systems. (Appendix B has more on defensive EW.)

IEW SIGINT support to counterinsurgency operations is applied in three phases.

PHASE I—LATENT AND INCIPIENT ACTIVITIES

During the initial phase, US ground forces are not likely to be committed but they will make specific requests for information to the national community. In the initial stage of our involvement there may not be many SIGINT targets. This lack of targets makes it difficult to establish or verify technical data bases. You need to verify existing data first. Then, as new data is collected, you can add it to existing data bases or start a new one.

Logistic networks develop during the first phase. As this occurs you need to identify routes as well as locate camps. The collection and verification of this information feeds the requirements of the national system and, this in turn, ensures that their focus is on your tactical needs. Units with counterinsurgency SIGINT missions can access national sources.

PHASE II—GUERRILLA WARFARE

During the second phase, activities outlined above continue. SIGINT targets will continue to be verified. Resupply activities will increase. Concurrently, you may see infiltration and exfiltration routes develop.

The threat will begin to strike at its opposition. You may see insurgents conduct traffic stoppages for propaganda purposes or attack government installations to test their own and HN capabilities. Training camps may develop. Throughout all of this, you will probably see an increase in threat communication levels and a rise in the number of communication stations and networks. Use this time to—

- Build your data bases.
- Provide input to the target acquisition process.
- Identify your gaps in collection.
- Increase your knowledge of the threat.

PHASE III—WAR OF MOVEMENT

During the third phase, the above activities will occur more frequently. The scope of each event will vary. One day a target may be a power substation, and the next a bank or military post.

During this stage SIGINT is extremely active. The insurgents have developed their capabilities and moved to open warfare. C^3 nets are present. Anomalies in their operation will be very obvious. These could indicate a change in operation procedures or simply a mistake by the threat radio operator.

Take advantage of the anomalies and mistakes when you can. They sometimes provide information that you would otherwise not get.

As a final note, radio direction finding (RDF) is valuable during all phases. Use your RDF capabilities to pinpoint known threat locations and identify new ones. Confirmation of threat locations is vital for target development.

COUNTERINTELLIGENCE

The likelihood of direct US military general purpose ground force involvement in an insurgency is remote. However, the NCA may deem it necessary to use as a policy option *the threat of force*—such as that employed against Nicaragua in the 1980's.

A *be prepared to* mission is sufficient justification for initiating MDCI support actions as early in the planning phase as possible. This early-on effort becomes more important in those areas where our CI activities have been minimal.

INSURGENCY SUPPORT

If the US decides to support an insurgency, then the MDCI target becomes the intelligence and security apparatus of the hostile government and any third parties that may be assisting. This includes the potential for Level I (enemy agents or guerrillas) and Level II (diversionary and sabotage) threat activities.

US support to the insurgents may be covert. Consequently, many of the operations connected with it may be special activities. Depending on the sensitivity of the operation, initial CI support from the national level may be covered by special access programs (SAP).

MDCI focuses its interest on the counterinsurgency threat posed by the hostile government and third-party IDAD support. Some peculiar situations may exist. Examples include:

- The US government may still maintain diplomatic relations with the hostile government.
- Elements of a country team may be resident in the target country.
- The insurgents may be based in the target country or have sanctuary in an adjacent country.

Whatever the situation, MDCI attempts to catalog the threat intelligence and security infrastructure which poses a danger—danger not only to the insurgent's agenda but also to the success of the US support program.

Insurgencies rely on personnel and resources from within the target country to be successful. They build their legitimacy in the eyes of the people in direct competition with the threat government. Therefore, their efforts include—

- Political.
- Social.
- Economic development.
- Reform.

Consequently, the basic principles of IDAD apply to those areas under insurgent control.

Figure C-1 identifies those tasks that the supporting CI element can perform. The senior CI officer or noncommissioned officer determines which tasks support the insurgents. In addition, the senior CI officer ensures that MDCI products and support are provided for all aspects of OPSEC for the protection of the force.

The senior CI officer supporting the US force commander ensures that investigations of US personnel are coordinated with the appropriate intelligence staff CI element (FM 34-37) at the MI Brigade (EAC). This CI element is responsible for—

- Providing information on enemy and internal security threats to theater forces.
- Coordinating the Subversion and Espionage Directed Against the US Army (SAEDA) program.
- Reporting deliberate security violations to CI agencies or other services in accordance with AR 381-12.
- Establishing a theater control office for CI investigations and operations.

Threat Assessment

The MDCI analyst must be concerned with the functions and capabilities of the hostile government intelligence and security services. These concerns include—

- Leadership and organization.
- C^3 system.
- All-source collection capabilities.
- Third-country intelligence and security IDAD support.
- CI capabilities and countermeasures.
- Counterinsurgency doctrine and infrastructure.
- Military and paramilitary forces.
- Area and local police methods of operation.
- Public information and PSYOP agencies.
- Demographics.

Neutralizing the intelligence and security agencies of a hostile government engaged in counterinsurgency operations is a prime objective of insurgents. A hostile intelligence and security service, although possibly smaller than either the police or military forces, and with no apparent physical means of intervention, is paradoxically the most dangerous threat to an insurgency. This is because the intelligence services' objective is to gather information which protects the government from insurgent activities.

Foreign HUMINT Threat. Effective HUMINT operations are probably the greatest threat to insurgents. Sooner or later, in order to gain the support of the people, the insurgent must surface in hamlets, villages, and work places. He must further his cause and confront hostile local, state, and national forces whether military, paramilitary, or police.

The intelligence information collection effort by the hostile government to support its IDAD operations will not be successful without a viable and timely national level HUMINT network. As the hostile government implements its IDAD strategy, it seeks to achieve the following objectives:

- Isolate or protect the people from covert insurgent agencies (the infrastructure).
- Isolate or protect the people and physical targets from overt insurgent forces (the guerrilla units).
- Defeat the insurgency forces.

Foreign SIGINT Threat. The SIGINT threat to insurgent operations is not usually as extensive as one directed against a conventional threat. But you must identify, quantify, and qualify the hostile communications and noncommunications intercept, RDF, and EW capabilities.

Your inventory includes ground based (fixed and mobile) units, airborne systems, and associated C^3I. Threat target country SIGINT capabilities may be augmented by a third country. Actual equipment may vary from known worldwide military standard items to off-the-shelf components available from local or foreign commercial suppliers.

Refer to FM 34-60 for details on the counter-SIGINT data base process. The minimum PIR of concern are—

- Equipment sensitivity.
- Quantities.
- Antenna capabilities.
- Data processing capability.
- Dissemination scheme.
- Employment considerations.
- The degree to which information processing is integrated into the hostile C^3 system.

You are also concerned with the scope of threat SIGINT capabilities and the operational effectiveness of personnel and equipment. It is important for you to know to what degree the threat intelligence service CMO relies on SIGINT-derived information as compared to other sources. This could expose a vulnerability in their decision-making process.

Foreign IMINT Threat. The threat IMINT effort could range from handheld cameras with extra lenses to airborne platforms, LANDSAT, or other satellites operated by the threat government or a third party. Other IMINT systems include—

- Radars.
- Infrared sensors.
- Optical sensors.
- E-O sensors.
- Multispectral sensors.

Vulnerability Assessment

The MDCI analyst must thoroughly understand the insurgent's situation and the supporting US forces' mission. Minimum concerns are—

- Leadership.
- Ideology.
- Objectives.
- Communications.
- Logistics.
- Environment, geography, and demographics.
- External support such as economic aid.
- Phasing and timing.
- Organization.
- Patterns of activity.

Information in these areas is translated into the MDCI insurgent vulnerability assessment (IVA). The IVA examines the threat government's HUMINT, SIGINT, and IMINT capabilities to detect, identify, locate, and track the insurgents. This includes—

- All insurgent sanctuaries.
- Routes to and from target areas.
- Logistic bases.
- Training sites.
- Villages and areas known to be sympathetic or actively supporting the insurgent cause.
- Ethnic groups having an affinity to the insurgent group.
- Radio stations, newspapers, and other media which overtly or covertly support the insurgent effort.

Population is the key factor in a LIC insurgency. It represents the only key *terrain* feature which must be seized, controlled, or defended. The population may provide vital moral, logistical, and security support to the insurgent.

However, you must recognize that the various tribal, ethnic, economic class, religious, and political groups are also the *nodes* which threat intelligence and security services target to penetrate and exploit.

Another factor you consider in the IVA is the role of the insurgent as either a rural or an urban guerrilla. This role dictates the insurgent's AO and targets. These areas and targets become the objectives of the threat government's counterinsurgency program.

Over time, as the insurgent experiences success, it is possible that it may transition from rural to urban AOs. As insurgent LOC and logistics support expand and their base areas move from third-country sanctuary to the target country, the scope and capabilities of threat intelligence and security services must be constantly reassessed.

Attention is focused on insurgent activity and signatures that will ultimately emerge during the development of the insurgency. Such phenomena provide the *indicators* of insurgent intentions that enable the hostile government to predict insurgent COAs.

Your job, based on the threat assessment and IVA, is to recommended countermeasures that should be adopted by insurgent and supporting US forces. MDCI support to OPSEC increases the success and safety of insurgent operations and supporting US forces (see Appendix C).

COUNTERINSURGENCY SUPPORT

MDCI support to counterinsurgency starts during the planning phase and continues to the end of US involvement. The primary focus of MDCI support is on protecting US and friendly HN forces.

The MI brigade (EAC) supporting the CINC of the unified command initiates MDCI support actions through the echelons above corps intelligence center (EACIC).

MDCI aid to counterinsurgency focuses on—

- Insurgents.
- Terrorists.
- FISs.
- Drug-traffickers.

Emphasis is on the infrastructures and intelligence collection capabilities of these organizations. One primary concern is the type and level of external support to the insurgency.

Additionally, the MDCI effort focuses on the HN intelligence and security forces. Primary emphasis is on their intelligence collection capabilities and MDCI operations.

MDCI support begins with the development of an MDCI data base on the AO. It addresses local and regional conditions. It also provides the basis for threat and friendly vulnerability assessments and the development of effective force protection countermeasures.

Data Base

The MDCI data base will contain information on both the HN and the threat. It addresses political, economic, social, geographic, demographic, and military conditions in the HN. MDCI data base development is part of the MDCI LIC area evaluation process. MDCI data base also contains detailed information on—

- The insurgency.
- Known terrorist organizations.
- Drug-trafficking organizations.
- FIS threat.

Threat Assessment

The MDCI analyst conducts a detailed and continual assessment of each type of threat targeted against US and HN forces. Threat capabilities, objectives, doctrine, and methods of operations need to be analyzed. Your goal is to determine threat capabilities, intentions, and activities with the primary focus on—

- Intelligence collection.
- Espionage.
- Subversion.
- Sabotage.
- Terrorism.

Your analysis includes information on insurgent, terrorist, FIS, and drug-trafficking threats. This information equates to the MDCI analyst's PIR and, as a minimum, includes—

- Leadership.
- Ideology.
- Internal and external support.
- Organization.
- Logistics.
- HUMINT, SIGINT, and IMINT disciplines.
- Goals and objectives.
- Capabilities.

- Methods of operation.
- Communications.
- CI.

Informational gaps are identified and requirements are submitted through CM&D for national level tasking.

The threat will place a heavy reliance on its HUMINT collection capability. HUMINT is its most productive asset, particularly if the local population supports the insurgency.

External support determines the level of insurgent SIGINT and IMINT collection capabilities. These capabilities could range from very unsophisticated to highly sophisticated. You need to understand the threat's intelligence collection limitations, vulnerabilities, and weaknesses. Additionally, you need to identify any interoperability between the threat and any third party in intelligence collection and exchange.

Vulnerability Assessment

MDCI analysts need to identify friendly centers of gravity and critical operational nodes that require OPSEC protection. This is critical to successful US and HN counterinsurgency operations.

You need to thoroughly understand the friendly military commitment to the IDAD strategy for counterinsurgency. You also need to know the HN and US military structure, concepts, conditions, and missions for conducting counterinsurgency operations. As a minimum, focus on—

- Leadership and organization.
- C^3.
- All-source intelligence collection systems and capabilities.
- Counterinsurgency doctrine and infrastructure.
- Military and paramilitary forces.
- Area and local police methods of operation.
- CA and PSYOP agencies.
- Third-country intelligence and security IDAD support.
- CI capabilities and friendly countermeasures.

This whole assessment process determines friendly weaknesses and vulnerabilities that might be detected and exploited by threat collectors and targeting team. If you understand friendly vulnerabilities, you can recommend appropriate countermeasures.

Figure C-1 identifies the different types of tasks that CI personnel perform in support of counterinsurgency. The actual CI support provided will be based on—

- NCA policy decisions.
- CINC intent.
- HN-US bilateral agreements.
- Country team guidance on IDAD concepts and strategy.

CI personnel provide advice, assistance, and training to HN intelligence and security services (military, paramilitary, police) through SAOs. CI personnel function as advisors, members of mobile training teams (MTTs), or training assistance field teams (TAFTs).

CI personnel can also be supporting a joint or combined command. Whatever your role, the primary objectives are to increase the HN capabilities to—

- Deny intelligence information to insurgents.
- Identify and neutralize insurgent infrastructure.
- Neutralize insurgent intelligence effort.

The type and scope of training assistance provided will be based on HN needs and US regulatory limitations. The intent is to ensure that support is within legal authorizations and that unauthorized information and processes are not compromised.

SECURITY ADVICE AND ASSISTANCE

Security advice and assistance (A&A) is conducted by security managers and CI and MP personnel to improve the security posture of US and HN commands. A&A can help identify threats from—

- Intelligence collection.
- Insurgent and terrorist activities.
- Sabotage.
- Assassination attempts.

Specific vulnerabilities and recommended countermeasures are provided to the commander through surveys and assessments.

Personnel Security

Your personnel security activities include investigations, screening, and foreign local hire programs. Personnel security applies to all military and civilian individuals working for US military forces. You will need to see that all personnel receive adequate background investigations.

Personnel security investigations (PSIs) for US personnel will be conducted in accordance with AR 380-67; PSIs for local nationals will be in accordance with Status of Forces Agreements (SOFAs). Your security investigations of local hire nationals involve additional information such as—

- Local national (LN) travel or residency in threat-controlled countries.
- Prior residency in insurgency-controlled areas.
- Relatives in threat- and insurgent-controlled areas.
- Prior employment.

In order to do effective PSIs on local civilians, you need a good working relationship with HN intelligence and security agencies. These agencies normally keep the records for current criminal investigations and, in most instances, are responsible for investigating and clearing local personnel. As you know, these agencies vary from excellent to nonexistent but you still need whatever they can provide.

The employment of local nationals is a security risk and should be kept to a minimum. To minimize and prevent undue security risks, consider the following precautionary measures:

- Use the *guarantor system* to determine a person's loyalty and reliability.
- Use the quartering and messing of indigenous employees within the US base area for activity and movement control.
- Use polygraph examinations for initial preemployment checks and periodic reexamination.

Insurgents use local nationals to collect information on friendly installations and activities. Local hires can collect sensitive information simply by keeping their eyes open. Thus, a viable, continuing personnel security program is critical to the security and protection of US and HN forces.

Information Security

US forces routinely have daily contact with HN military and civilian personnel. These contacts involve unavoidable security risks and the potential for unauthorized disclosure of classified information. Thus, a viable information security program that stresses strict compliance with AR 380-5 is essential.

Additional procedures are needed to ensure that HN and foreign classified material is safeguarded. This applies regardless of personal opinions about the validity of HN classification.

You need to do security checks and sweeps of classified areas when base camps or units are moved, or when US occupied facilities are vacated.

The inadvertent disclosure of unclassified military information can be as dangerous as the willful disclosure of classified information. It is almost impossible to distinguish between friendly and insurgent supporters among the local populace, and this magnifies the problem of *loose talk*. The careless discussion of unclassified military information can lead to ambushes, surprise raids, and acts of terrorism. You need to constantly remind your soldiers that the local populace is the primary source of intelligence for insurgents.

An information security SOP needs to be written that addresses the emergency evacuation and destruction of classified material. The SOP must be workable, coordinated with base camp security personnel, and physically rehearsed. You can provide A&A by examining these SOPs for three factors:

- They contain effective and up-to-date emergency destruction procedures.
- Procedures are established for frequent review and update.
- They conform to requirements and directives levied from higher headquarters.

All used paper, whether classified or unclassified, should be destroyed. Many unclassified documents (such as morning reports, orders, or personal letters) can be exploited by insurgents for propaganda or intelligence purposes. Burning all paper waste saves a sorting process and reduces the danger of anything usable slipping into insurgent hands.

Physical Security

The effective protection of military installations, personnel, and activities from the threat of espionage and sabotage is the essence of physical security.

The G3 or S3 and provost marshal's office (PMO) have primary responsibility for perimeter defense and installation security. CI personnel recommend security procedures for visitor control, restricted areas, and perimeter inspections.

Minimum physical security measures outlined below should be implemented to protect US forces from insurgent and terrorist activities. (FM 19-30 provides details on physical security measures.)

Examine the perimeter defensive system to see that every possible means of access has been controlled. Pay attention to culverts, gullies, and streambeds which could provide surreptitious entry. You must establish an effective R&S plan to detect and deter insurgent or terrorist threats to the perimeter. Frequent patrolling and available tactical IEW equipment, such as ground surveillance radars and remote sensors, should be in the plan.

Designate all sensitive areas of the installation as restricted areas. These include—

- Your G2, S2, or CI section.
- Tactical operations center (TOC).
- CP.
- POL storage.
- Communication facilities.
- Ammunition dumps.

These areas should be off limits to all but authorized personnel and must be marked as *Restricted Areas*.

Putting up large red signs is not the smartest way to handle the problem. Such obvious markings make it easier for local hire nationals to pass critical information to the insurgents. Instead of conspicuous markings, you might divide the compound into quadrants, assigning each a color code.

Issue civilian employees a colored tag authorizing them to work only in a specific quadrant. The compound should be organized so that civilian employee traffic to and from their authorized quadrants require them to pass by as few restricted areas as possible.

This method limits access to restricted areas and avoids using large red signs. The color codes for the quadrants should be changed periodically. It is also smart to conduct periodic technical sweeps of restricted areas to look for electronic bugs.

Always establish a strict visitor control system including passes, tag systems, and searches. Everyone working or visiting the compound should be subject to this system.

Your pass and tag system is essential to control visitors. Tags are issued at the gate upon entry.

Every employee entering a camp or compound must produce a special pass which is collected at the gate by a guard. The employee is given back the pass at the end of the day when leaving. Only by collecting the pass at night and presenting it the next day can the employee be readmitted. This system can also be color coordinated with quadrant colors.

Regardless of the type system you use, each pass and tag needs to be strictly controlled and each should contain a photograph and identifying data. All HN civilians should be monitored by stationary and roving interior guards.

When entering a facility, all HN civilians should be searched for concealed weapons or explosives. They may also be searched on the way out to prevent theft.

If available, use local police to conduct searches. Make special provisions for females. This is a normal police function and civilians will have less resentment towards them than military personnel.

Additionally, procedures should be established to randomly search military personnel. Trustworthy local HN personnel can be used for gate security. In addition to personnel searches, vehicles need to be searched for explosives.

Wherever possible, locate troop-associated facilities, washing areas, and sanitary fills within the containment. Ammunition and POL points should not be collocated with a hospital or close to the installation perimeter. This avoids compact and lucrative targets where one, well-placed satchel charge could destroy everything.

All obsolete or unserviceable military equipment should be evacuated or destroyed. This keeps discarded materiel out of insurgent hands. Cans, brass cartridge casings, and dead batteries have been used as mines, booby traps, and detonators.

In addition to physical security measures outlined above, care must be taken to prevent establishing operational profiles. Unless warned, all units get into set routines that can be exploited. Examples are POL trucks that drive to the fuel dumps and refuel at the same time each day or convoys that always assemble 12 hours before a combat operation. Steps that screen the staging, grouping, training, and planning of military operations are extremely important.

Avoid establishing individual activity profiles. Personnel can be targeted not only because of their position but also because of their established routines. On 25 May 1983, the deputy chief of the American military advisors to El Salvador was assassinated. He was killed because he picked up his girlfriend at the university in San Salvador the same way every day. He was probably targeted because of his position, but he made it possible because of his profile or pattern.

All security measures should be viewed and undertaken with the knowledge that there is no rear area in counterinsurgency. Rather, you have a 360-degree dispersed battlefield.

Security Education and Training

The ultimate objective of a security education and training program is the ongoing protection of classified information, personnel, and materiel. This is achieved when security awareness is established in the minds of all US forces personnel. Your program must be tailored to the unique security requirements of each organization and unit present.

Training is conducted in personnel, physical, and information security. Emphasis is placed on the intelligence, espionage, and security danger to US personnel and operations.

CI personnel support security education and training programs with briefings on—

- SAEDA.
- FIS multidiscipline intelligence collection capabilities.
- Threats (insurgent or terrorist).

Your security education program focuses on defensive security. The basic philosophy is to deny unauthorized access to classified information together with personnel, physical, and information security.

INTELLIGENCE OPERATIONS

Intelligence provides the basis for all US and HN plans and operations in counterinsurgency. To a large extent, intelligence marks the difference between success or failure in reaching civil-military objectives. Intelligence is fundamental to any successful counterinsurgency operation.

MDCI supports US and HN intelligence operations through the use of—

- Controlled HUMINT operations.
- LLSO.
- Counter-HUMINT operations.
- Liaison.

At EAC, the MI brigade (EAC) has the mission and capability to conduct these types of MDCI operations.

Classified directive DCID 5/1 governs HUMINT collection, LLSO, and counter-HUMINT operations in counterinsurgencies. FM 34-60A(S) and FM 34-5(S) provide details on MDCI operations.

HUMINT operations provide valuable intelligence and I&W on threat activities and operations. HUMINT provides timely information on insurgent capabilities and intentions. HUMINT collects information by—

- Penetration.
- Observation.
- Elicitation of personnel.
- Exploitation of documents and material.

LLSO provides I&W on potential security dangers to US and HN forces. It also provides information on personalities and activities in an area of CI interest. LLSO provide information on terrorist, insurgent, drug trafficking, and indicators of sabotage and subversion.

Counter-HUMINT operations neutralize insurgent espionage, sabotage, and subversion activities. Counter-HUMINT operations include—

- Counterespionage.
- Countersubversion.

- Countersabotage.
- Investigations.

Close liaison with a variety of US and HN military and civil organizations is mandatory. This liaison is critical for coordination, intelligence collecting, and information sharing. As a minimum, you must coordinate with—

- Members of the US country team.
- HN regional and urban area coordination centers.
- HN intelligence and security forces.
- HN military, paramilitary, and local police.
- US MI units.
- US MP, CA, and PSYOP units.

TACTICAL OPERATIONS

MDCI support to tactical operations includes participation in cordon and search operations. Cordon and search operations ferret out the insurgent infrastructure. They are also used against units or groups which may use a community or area as cover or a support base. Cordon and search operations are conducted with HN intelligence and security forces and are not unilateral US efforts. US forces, to include CI personnel, provide support to the HN official conducting the operation.

The purpose for conducting cordon and search operations is to identify and detain persons hostile to the US and HN. A by-product is to gather information. You should know that this type of operation may be politically destructive.

Before participating in cordon and search operations, you must coordinate with the regional or local HN area coordination center. If none exists, coordinate with host-country intelligence and police organizations to—

- Update existing black and gray lists.
- Have insurgent defectors, agents, and other knowledgeable personnel present to identify insurgents and their supporters.
- Update all intelligence on the community or area.

Coordination is necessary with unit commanders who will be involved in the operation. Your main task is to get an update of all current intelligence on the community or area.

The senior tactical unit commander is responsible for the conduct of the operation. With advice from CI, interrogation, CA, and PSYOP personnel, he plans the cordon, which is usually set up at night; and the search, which normally begins at first light.

Community Operations

Figure 5-1 shows the basic community cordon and search operation. As the screening element sets up the collection or screening station, the sweep element escorts the residents toward the station. If required by law, leave one resident behind to care for family belongings.

The search element follows behind the sweep element searching everything (houses, storage areas, cemeteries) with dogs and metal detection equipment. You are looking for evidence of intelligence collection operations, such as radios, cameras, and communications codes.

Each search element consists of a CI team and an interrogator team. They are given a list of persons of CI interest. Enroute to the screening station, search each individual for weapons.

In the collections or screening station, the residents are brought to the collection area (or holding area) and then systematically moved to specific screening stations. Move the residents past the mayor, community leaders, enemy defectors, or cooperating prisoners (who will be hidden from view so that they can uncompromisingly identify any immediately recognizable enemy). These informants will be told how to notify a nearby guard or screener if they spot a threat member.

You must immediately segregate those identified and interrogate them. At specific screening stations, ask the residents for identification, check their names against the black list, and search for incriminating evidence.

Photograph suspects and set up further interrogation. Or if time is a problem, put them in the screening area detention point and take them back to a base area for more intensive interrogation later.

Pass innocent residents to the general screening area where you may have helped arrange medical check-ups, civic assistance, entertainment, and friendly propaganda.

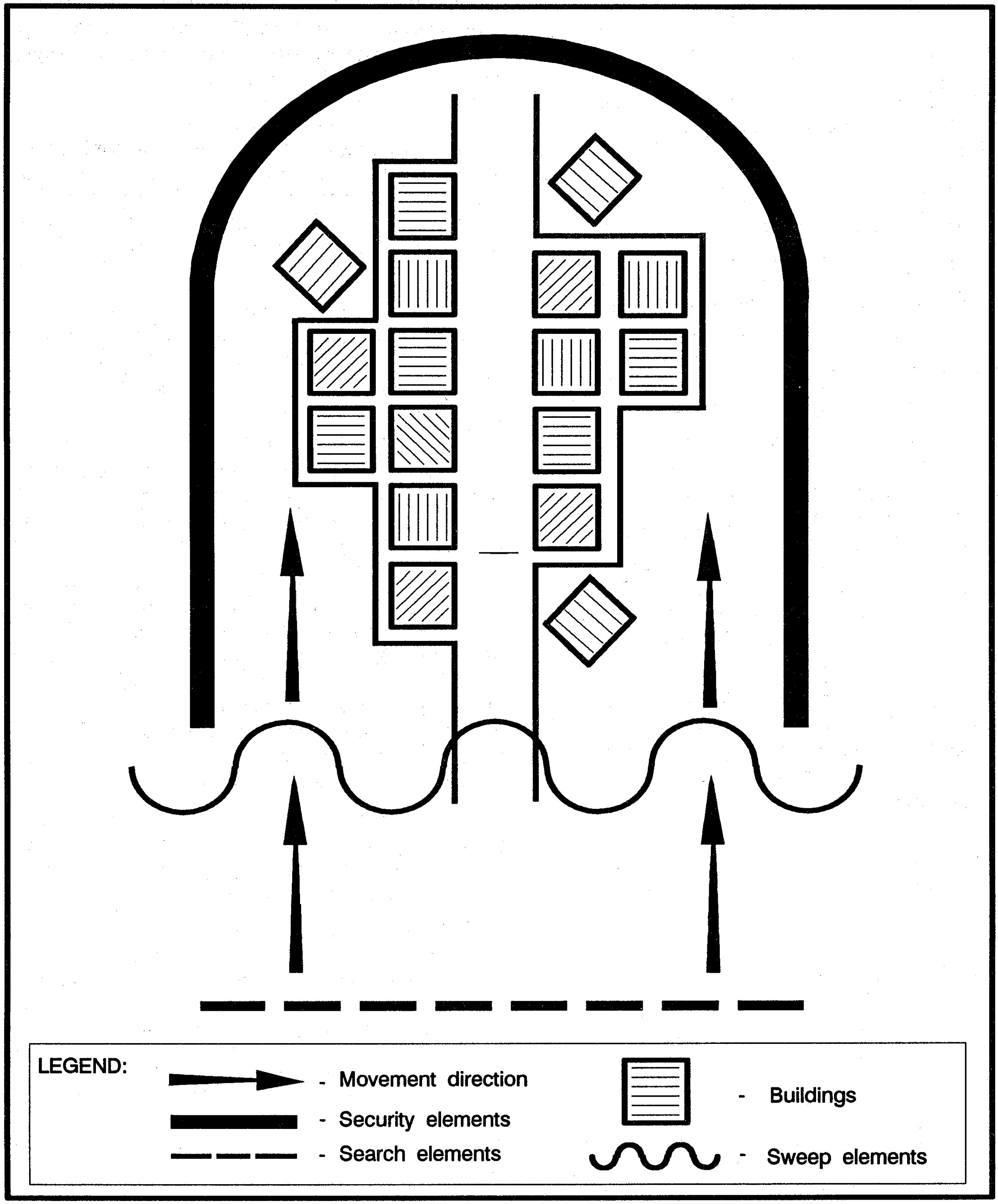


Figure 5-1. Community cordon and search.

Immediately return persons caught attempting to escape or break through the cordon to the detention area.

When the operation is over, allow all innocent people to return to their homes, and remove the threat suspects under guard for further interrogation. Photograph all members of the community for compilation of a village packet which will be used in future operations.

Soft or Area Operation

The second type of cordon and search operation is frequently referred to as the *soft* or area cordon and search. This operation includes the cordoning and searching of a relatively large area. One example is a populated area incorporating a number of hamlets, boroughs, towns, or villages which are subdivisions of a political area beneath country level. This operation requires—

- A large military force to cordon off the area.
- A pooling of all paramilitary, police, and CA elements.
- Intelligence resources sufficient to conduct the search and screening.
- An extensive logistical effort.

This operation extends over days and may take a week or longer.

While screening and search teams systematically go from community to community and screen all residents, military forces sweep the area outside the communities over and over again to seek out anyone avoiding screening. As residents are screened, they will be issued documents testifying that they were screened and, if necessary, allowing them limited travel within the area.

Effective information control and OPSEC plans are essential in area cordon and search. The threat's HUMINT collection capability easily detects this type of operation due to its size, scope, and amount of coordination required.

Other population and resources control measures are used as well. These opportunities allow you to issue new identification cards and photograph all area residents.

As each community screening proceeds, individuals who were designated for further interrogation are sent to a centralized interrogation center in the cordoned area. Here, you will work with intelligence interrogation personnel (both US and HN), police, and other security service interrogators.

In addition to field files and other necessary facilities, a quick reaction force is located near the interrogation center. This force can react immediately to perishable intelligence from interrogations or informants planted with the detainees.

CHAPTER 6
INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO COMBATTING TERRORISM

This chapter provides TTP needed to conduct the missions and functions of the intelligence disciplines to combat terrorism. It also addresses CI support to force protection in combatting terrorism.

Terrorism is generally described as the calculated use of violence, or the threat of violence, to inculcate fear intended to coerce or intimidate governments or societies in the pursuit of goals that are political, religious, or ideological. This is done through intimidation, coercion, or instilling fear. Terrorism involves a criminal act that is often symbolic in nature and intended to influence an audience beyond the immediate victims.

HUMAN INTELLIGENCE

In combatting terrorism, HUMINT is the first line of defense. Primary objectives are deterring, detecting, and preventing terrorist acts. The collection and development of HUMINT information on the terrorist threat is critical. HUMINT sources provide valuable information on terrorist organizations, capabilities, tactics, and targets. HUMINT collection operations include document exploitation, interrogations, and liaison.

Usable information can come from a variety of HUMINT sources including open sources, LEA, government intelligence agencies, and informal local contacts. These need to be accessed and exploited by the installation intelligence officer or combatting terrorism officer.

OPEN INFORMATION SOURCES

This information is publicly available, often overlooked, and reliable. Local and national news media and government and private sector publications are excellent open sources on terrorism. Also, terrorist groups, and their affiliates, may publish a variety of manuals, pamphlets, and newsletters that reveal their objectives, tactics, and possible targets. Information on specific groups and individuals must be collected and maintained in accordance with AR 381-10.

CRIMINAL INFORMATION SOURCES

Both military and civil LEA collect criminal information. Criminal information can be a valuable source of intelligence on terrorists. LEAs maintain informants and informant nets to collect intelligence on criminal activities. They can also provide information concerning terrorist plans, capabilities, recruitment, and targets.

Intelligence officers need to conduct effective liaison with the provost marshal, MP investigators, and local US Army Criminal Investigation Command (USACIDC) agents. These military LEAs can assist in liaison or in obtaining information from HN local, state, or federal counterparts and security agencies. They can also assist in assessing the local terrorist threat.

GOVERNMENT INTELLIGENCE AGENCIES

Military and governmental intelligence and investigative agencies maintain extensive terrorist threat data. Intelligence threat analysis centers (ITACs) produce MDCI and terrorist threat summaries. Periodic regional threat packets are available from the local US Army Intelligence and Security Command (INSCOM) representative. The US Air Force Office of Special Investigations (OSI), DIA, and CIA maintain comprehensive terrorist data bases, which can be accessed.

Intelligence officers need to establish routine liaison with the CI covering agents who support their organization. These individuals are a good source for obtaining terrorist information from local US military and governmental intelligence agencies. They also can assist in obtaining information from national level assets. CI personnel overseas can obtain terrorist data from HN intelligence and security agencies.

INFORMAL LOCAL SOURCES

Other valuable sources of information are individual soldiers, family members, or civilian employees. When approached and made aware of the potential terrorist threat, they can become valuable sources of information. These informal sources provide information on unusual or suspicious activities in their area.

You also need to ensure that the reporting of terrorist-related indicators is stressed during periodic terrorist threat briefings and SAEDA training.

Additionally, family members and employees need to be encouraged to report useful information through an active crime prevention program.

IMAGERY INTELLIGENCE

Imagery assets can provide timely information to operational units once terrorist activities have been initiated. Indeed, optical imagery or prints of terrorist training facilities can be studied to learn how a particular terrorist organization trains and operates. Facilities such as swimming pools (frogmen, underwater training), towers (airborne training), firing ranges, and physical training areas are some indicators used by the IAs to determine the terrorist group's operating characteristics.

The initial identification of terrorist training facilities is usually made by IAs at the national level. However, units involved in combatting terrorism should have on file imagery or prints of targets for reference. (See Appendix H.)

SIGNALS INTELLIGENCE

EW and SIGINT provide a limited contribution to combatting terrorism. From an offensive standpoint, ESM may be possible during terrorist criminal acts such as sabotage and kidnappings. Due to the nature of terrorist groups, the use of ECM will be minimal.

Because today's terrorists are well trained and well equipped, combatting them is best done before the fact, not after. The way to do this is to take all countermeasures possible. The proper use of ECCM will go a long way in deterring terrorist actions. Make sure you—

- Secure your equipment. Stolen equipment gives added capabilities to terrorist groups. If weapons and communications gear are discovered missing, make every effort to recover them. Stolen weapons have been used in actions against US forces and installations. Likewise, stolen communications equipment can be used by terrorists to target our people by conducting radio intercept operations.
- Use the telephone carefully. Today's terrorists have the capability and know-how to tap telephone systems, particularly overseas. Use a secure telephone to discuss classified information, visiting dignitary itineraries, and key personnel travels. Do not try to talk around issues. If a secure means of communications is not available, find another way to conduct business or do not do it.

Above all, if you or your unit is involved in combatting terrorism, remember that MI jurisdiction is limited by executive orders, federal laws, Army regulations, directives, international agreements, and SOFAs. One example of these is Title 18 of the US Code. Verify the legality of pending operations with the legal officer of the local MI brigade.

COUNTERINTELLIGENCE

MDCI support to combatting terrorism focuses on protecting the force and is primarily preventive in nature. MDCI support ranges from strategic to echelons corps and below (ECB). This support is accomplished through the four functional areas of investigations, operations, collection, and analysis and production. MDCI support includes—

- Preparing and maintaining a threat data base pertaining to terrorist and FIS multidiscipline intelligence collection capabilities (HUMINT, IMINT, and SIGINT).
- Preparing terrorist threat analysis.
- Providing MDCI threat evaluations of foreign intelligence and terrorist organizations.
- Alerting Army commanders to terrorist threats against their personnel, facilities, and activities.
- Assisting operations personnel in assessing vulnerabilities and recommending protective countermeasures.
- Investigating terrorist incidents for intelligence value.
- Conducting liaison with federal, state, and local agencies; and HN federal, state, and local agencies,

to exchange information on terrorist and FIS activities.

- Conducting CI operations to include SAEDA briefings, investigating deliberate security violations, and providing security A&A.
- Conducting collection operations to include LLSO.

The senior CI officer will determine specific tasks that need to be performed in accordance with regulatory requirements and SOFAs with the HN. Appendix C describes the MDCI analytical process used in—

- Combatting terrorism.
- Terrorist assessments.
- Friendly force assessments.
- Countermeasures recommendations.
- Countermeasures evaluations.

The MDCI analyst needs to evaluate the supported command's OPSEC program and make recommendations to improve force protection measures. Force protection needs to be tailored to fit each installation or separately deployed unit.

CHAPTER 7
INTELLIGENCE SUPPORT TO PEACEKEEPING OPERATIONS

This chapter defines PKO and describes the unique missions and functions of MI in PKO.

PKO are efforts taken with the consent of belligerent parties in a conflict. The object is to maintain a negotiated truce and let diplomatic efforts achieve and maintain a permanent peace. Such consent represents an explicit agreement permitting the—

- Introduction of the force.
- Type and size of force.
- Kinds and amount of equipment.
- Type of operation to be conducted.

PKO may take many forms, including—

- The supervision of free territories.
- Cease-fires.
- Withdrawals.
- Disengagements.
- Election supervision.
- Prisoner-of-war exchanges.
- Demilitarization and demobilization.
- Maintenance of law and order.

FM 100-20/AFP 3-20 and Joint Publication 3-07.3 discuss PKO doctrinal procedures and techniques in detail.

The US provides military support to PKO with either UN or multinational forces. While possible, it is unlikely that US military would be involved in PKO unilaterally.

Participating units may include naval, air, or ground forces; a combination of all of these; or be limited to selected individuals.

Tailored support packages may include communications, logistical, medical, engineer, MP, or combat arms units. IEW support, as we know it, will not be conducted. However, mission requirements such as language or area knowledge may require the limited use of MI personnel.

PKO have three broad missions:

- Peacekeeping support, of which financial support is the most predominant US form, particularly to peacekeeping sponsored by the UN. The US may provide logistical support, such as equipment and supplies, as well as airlift and sealift to support PKO.
- Observer missions, which include acting as individual observers or as functional area experts under the command of the UN. Military personnel observe, record, and report on implementation of truces and any violations. They also carry out tasks such as patrols in sensitive areas. Observer groups usually operate under an open-ended mandate which, in the case of UN operations, can be terminated only by the UN Security Council.
- Peacekeeping forces, which may be a combat, CS, or CSS unit. US personnel may be used individually as members of a multinational staff, or as unit members. A typical peacekeeping force is a combat unit in a peacekeeping role supported by logistics and communications units under a joint headquarters.

Typical missions for a peacekeeping force include—

- Internal pacification. This requires the force to end violence by peaceful means and to prevent a renewal of violence. This requires placing observers or units between belligerents in order to stop the fighting. The peacekeeping force must remain neutral so diplomatic efforts can succeed. Violence may be used only in self-defense.
- The buffer force. The force occupies and patrols an established demilitarized zone in accordance with the terms of the peacekeeping mandate. The zone physically separates belligerents.
- The border patrol. The unit operates along an armistice line to detect and report violations. It interposes itself where possible to prevent violent incidents.
- A peacekeeping force. Observers occupy fixed sites to both visually and electronically monitor a cease-fire line. They observe, report, effect liaison, mediate, and supervise a cease-fire between the parties involved.

INFORMATION OPERATIONS GUIDELINES

There are threats in PKO. Under many circumstances the atmosphere is hostile. Each side watches the other, as well as the PKO force, with suspicion. In fact, some elements may not desire peace at all. They may target the peacekeeper in order to rekindle hostilities.

The command may not conduct intelligence operations nor will it include an intelligence section when it deploys. However, there will be an information section. This section may not be authorized to receive, process, or store classified information. The terms of reference established by the executive agent provides authorization for this. The information section focuses on analyzing reports obtained from within the command. Intelligence support systems, in most cases, do not exist. The command will be without traditional SIGINT, IMINT, and HUMINT support.

In an effort to compensate, diplomatic authorities instruct the command to rely upon Multinational Force Headquarters and the HN to provide required information. This is helpful, but these sources are seldom able to provide the threat information needed.

PREDEPLOYMENT INTELLIGENCE PLANNING

Predeployment intelligence operations focus on collecting information necessary for staff planning. The information officer must be ready to provide estimates to update or deal with changed conditions.

PKO are designed to achieve military, political, or psychological objectives. Therefore, the quality of available information is no less important than the quality of the forces themselves.

During the preparation for PKO, the information officer should ask the following questions:

- Does the information exist?
- Where can I find it?
- Is it valid, organized, and accessible?
- Who has been there?
- Who speaks the language?

With time and effort, all of these questions can be answered. In order to expand the breadth and depth of knowledge pertaining to the target area, new assets are required. These assets must include—

- Sources within the area (indigenous or foreign).
- Sources outside the area (direct or indirect access).
- Technical sources capable of *covering* the target from within or outside the area.
- A means of rapid and secure communications.

These assets, however, are often a luxury not readily available in most PKO. As the information officer, you know that information assets need to be among the first committed, and these assets must be tailored to the situation and the AO.

Politically motivated attacks by the more radical elements of belligerent forces or terrorists can never be completely eliminated. But they can be reduced by proper information and security operations.

Undue attention cannot be given to any radical element. Your understanding of the basic conflict, convincing the populace of your neutrality, and displaying strength through nonviolence, will allow the PKO to be effective.

INFORMATION SUPPORT

To meet PKO challenges, we must make-do with collection assets that are limited and sometimes unsuitable. National priorities, which determine the use of these assets, predominantly focus on the most dangerous, but less likely, threats to the defense of the United States.

Once deployed, the unit receives little or no external intelligence support and functions virtually alone.

PKO amplify your role as the force information officer in both training and operations. The nature of PKO demands a complete mental reorientation of each soldier. He has been trained to go to war; in PKO we task him to keep the peace at all costs.

The information section must be prepared to assist the commander in developing this change. You will be looked upon as the resident historian and will be expected to provide information on—

- Threat.
- Economic conditions.
- History.
- Social conditions.
- Political situations.

In addition, they look to you for a definition of the threat. You help reorient the soldier by teaching him about the conflict from the perspectives of all parties.

By understanding both sides, and the root cause of the conflict, the soldier will have empathy for each side. Hopefully, this will help him keep the neutral perspective he needs in PKO.

All PKO forces must realize that, while there may be threats, there is no enemy! We train our soldiers in absolutes: GO or NO-GO, right or wrong. In PKO, every soldier must understand that two conflicting ideas may both be correct.

COMMAND SECURITY

Mission success and the security of the command depends almost entirely upon the observational skills of each soldier. Individual soldiers, observation and listening posts, and patrols become your primary source of timely information.

The information officer recommends all reconnaissance efforts, supervises processing and dissemination of reports, and redirects patrols to fill gaps. The system you direct is the first line of defense against threats and is critical in mission success.

CHAPTER 8

INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO PEACETIME CONTINGENCY OPERATIONS

This chapter defines IEW support to PCO and describes the missions and functions of each of the intelligence disciplines and CI support in PCO.

PCO are politically sensitive military activities normally characterized by—

- Short term.
- Rapid projection or employment of forces.
- Conditions short of war.

They are undertaken in crisis avoidance or crisis management situations that require the use of military force to back up diplomacy.

Military efforts in PCO complement political and informational initiatives. PCO are usually—

- Political and time sensitive.
- Conducted by tailored forces.
- Joint or combined in scope.

They are sometimes conducted at the request of another government. Some recent examples of LIC PCO are disaster relief (San Salvador 1986, Bangladesh 1991), peacemaking (Grenada 1983 and Panama 1989), and NEO (Liberia 1990).

HUMAN INTELLIGENCE

HUMINT is potentially the most important and productive intelligence discipline in support to PCO. Strategic, operational, and tactical level HUMINT collection operations provide valuable intelligence and I&W of threat operations.

HUMINT uses penetration, observation, elicitation of personnel, and exploitation of material and documents to collect information on the threat. HUMINT activities vary from controlled operations, liaison, interrogations, and document exploitation to the debriefing of reconnaissance patrols.

Your well-developed HUMINT collection effort is critical to providing intelligence support to your commander.

HUMINT collection operations provide continuous support through all phases of PCO by—

- Concentrating on collection operations that contribute to identification and analysis of the potential threat.
- Filling gaps in the commander's intelligence requirements.
- Providing intelligence support to US forces during actual operations.
- Supporting US forces in follow-on missions, particularly in support of CA.
- Identifying and neutralizing threat infrastructure.

Additionally, they provide intelligence which contributes to the development of changes to US doctrine and tactics.

HUMINT in a variety of forms and sources is available to the intelligence elements conducting PCO. The quality and quantity of HUMINT depends on US forces organization, operating environment, and the extent of HN support. Additional considerations are the attitudes of the belligerents and the local population.

The following are some examples of HUMINT sources available to US, HN, and allied forces conducting PCO:

- US soldiers.
- US and HN civilians.
- CA specialists.
- PSYOP specialists.
- SOF.
- CI agents.
- Enemy prisoners of war (EPWs).
- MI organizations.
- HN and allied military.
- HN and allied governmental agencies.

- US, HN, and allied MP.
- HN and allied LEA.
- HN FIS.

Information provided by HUMINT sources must be processed. The greatest danger is that received pertinent information may not be recognized as such and is ignored, discarded, or not reported. Also, you need to ensure that HUMINT analysis is fused with IMINT and SIGINT data. FM 34-60A(S), TC 34-5(S), and FM 34-52 contain details on HUMINT collection activities.

IMAGERY INTELLIGENCE

Imagery and imagery-derived products can be used to support some of the PCO. Reference imagery of the AO is used to support mission planning. Some operations, such as disaster relief and counter-drug, require both reference imagery and current coverage in order to monitor the AO for significant changes. These changes could include—

- New structures.
- Defenses.
- Changes in status of LOC.
- Communication activity levels.
- New or additional military equipment.

Target coverage required to support PCO, in general, include—

- LOC.
- Bridges.
- Airfields.
- Ports.
- Border areas.
- Main government centers.
- Key military installations.

DISASTER RELIEF

Disaster and emergency relief is provided after droughts, floods, earthquakes, and war. US forces involved in disaster relief and humanitarian assistance operations benefit from both reference and current imagery of the AO.

Imagery analysis provides baseline information for initial damage assessment. Progress of relief and rebuilding efforts can also be monitored by optical imagery collection. For example, before and after photographs of Bangladesh destroyed by a series of typhoons in March 1991 were used to brief representatives of US Government agencies. These agencies were involved in damage assessment and planning for rebuilding this residential area.

SUPPORT TO COUNTER-DRUG OPERATIONS

US forces can be involved in counter-drug operations. This includes the detection, disruption, interdiction, and destruction of illicit crops and the drug-trafficking infrastructure. National level imagery assets are able to obtain important information to support this mission. (See Appendix H.)

IAs must be knowledgeable about illicit drug activities. Indicators change over time as drug operators change their methods in order to avoid detection. Indicators also differ by geographic area. For example, illicit crop patterns may vary by country depending on legality of the crop's cultivation. Analysis of reference and current imagery is done in an attempt to establish operational patterns and locations of transshipment points.

Imagery analysis also provides examples of cultivation patterns and crop sizes. Appearance of recently cleared fields or new, unexplained cultivated areas may indicate areas of illicit crop cultivation. However, such areas can be confused with legitimate farming activities. Comparative analysis, such as knowledge of how each crop appears on imagery and the growth period and harvesting cycles, aids in identifying legitimate areas.

Optical sensors are suitable for—

- Basic collection.
- Detection.
- Identification of illicit drug crops.
- Related facilities.
- LOC.
- Transshipment points.

These sensors are less effective against heavily vegetated areas.

Infrared sensors are better able to detect and identify objects day or night, except in areas of very dense vegetation and during heavy precipitation.

Radar sensors are often used for surveillance. The APG-66 radar used on the Small Airborne Surveillance System (SASS) can detect land, sea, or air targets.

Multispectral imagery (MSI) can provide information on areas, size, and possible yield of illicit crops. This analysis is usually performed by specialists at national level and some non-DOD elements. MSI can satisfy collection requirements against very large areas. Repetitive coverage of some AOs may be difficult to obtain with sensors on aerial platforms due to the size or inaccessibility of the AO.

SIGNALS INTELLIGENCE

SIGINT contributes to the planning and execution of PCO by providing early warning of threat intentions and surveillance of threat C^2 elements. SIGINT supports the primary categories of PCO as outlined here:

- Shows of force. Provides information on the threat's reaction to the operation.
- NEO. Provides a picture of the threat's reaction.
- RRO. Provides locational information.
- Strikes and raids. Delays and disrupts threat reaction to an operation without violating restrictive rules of engagement (ROE).
- Peacemaking. Contributes to the assessment of threat forces by providing the necessary data needed to conduct ESM and ECM operations.
- UW. Helps assess the effectiveness of UW actions.
- SAS. Contributes to force protection.
- Support to US civil authorities. Supports operations against national security such as illegal immigration and customs violations by detecting, disrupting, and interdicting the infrastructure of drug-trafficking entities.

COUNTERINTELLIGENCE

MDCI support to PCO focuses on the commander's mission of protecting the force. PCO missions include, but are not limited to—

- Shows of force and demonstrations.
- NEO.
- RRO.
- Strikes and raids.
- Operations to restore order.
- UW.
- DRO.
- SAS.
- Support to US civil authorities.
- Counter-drug operations.

MDCI support must be integrated into the planning process as early as possible. MI brigades (EAC) supporting the CINCs have the resources and capability to provide MDCI support to units entering the AO. They also coordinate the smooth transition of MDCI operational support to MI units assigned to the contingency force.

PCO force MI units arriving in theaters where the MI brigade (EAC) is not forward based should expect only limited MDCI support until EAC MI assets deploy. Additionally, these assets will arrive gradually in three tiers, with each tier successively increasing the capabilities and scope of support.

In PCO of short duration, deploying forces will not have the full degree of support the MI brigade (EAC) can provide. PCO forces in MI units should include this fact in their planning.

The CINC's statement of the mission, his intent, and the ROE are the basis for determining the type and scope of MDCI support required and permitted. The senior CI officer must know and understand the constraints imposed by the NCA, HN, and other countries together with the effects these constraints have on force deployments and operations. This is important where cooperation between US Army CI and HN intelligence and security services is one of your objectives.

See Figure C-1 for the essential tasks CI performs in support of PCO. The MDCI estimate, and other products, are integrated into the staff planning process. They support your commander's requirements for maintaining OPSEC during all phases of the operation. MDCI products also support his deception plans.

MDCI support to force protection is consistent with the three principles unique to PCO: Coordination, balance, and planning for uncertainty.

COORDINATION

Coordination is required between CI elements of the MI brigade (EAC) supporting the CINC, and the CI elements organic to the MI brigade or battalion supporting the PCO force. A key coordination element is the need to clearly delineate the responsibility for intelligence and CI liaison between EAC intelligence support elements (ISEs), the EAC CI battalion, and the contingency force CI element.

CI liaison is important among EAC, ECB, and members of the country team in the HN. This includes CI liaison among the US Army, other government intelligence and security services, and HN security entities.

BALANCE

Balance is a factor that your MDCI support achieves by portraying to the friendly commander *how he looks* to the threat. This includes a thorough analysis of the HN and adversary intelligence and security system.

Your MDCI analysts may not have direct access to this information and may have to rely on other national level agencies and departments. For example, there must be a balance between political goals and the scale, intensity, and nature of military operations supporting those goals.

PLANNING

PCO require detailed, flexible planning incorporating the principles of coordination and balance. Intelligence support to planning must be comprehensive.

MDCI preparation of the PCO battlefield begins with the MI brigade (EAC) supporting the theater CINC.

PCO can transition from one type to the other. Operations to restore order transition into PKO; noncombatant operations transition to peacekeeping and peacemaking operations.

The planning and training phases of PCO may require special protection such as that afforded by the SAP.

Open sources of information such as the news media, both in the base area and the HN, should be scrutinized to determine if essential elements of friendly information (EEFI) have been compromised. Pay particular attention to political factions that are opposed to US and HN cooperation. A primary concern to the MDCI analyst is any potential for terrorist activity targeted against the US Army presence in the host country.

PCO CONSIDERATIONS

Various PCO require you to be sensitive to special needs. Not all PCO are created equal; each has its own collection of special circumstances. Each type of PCO requires separate consideration of the potential threat to the success of the mission. The MDCI analyst uses the MDCI analysis process described in Appendix C to determine the threat or friendly vulnerabilities and countermeasures.

Shows of Force and Demonstrations

Shows of force and demonstrations include—

- Forward deployment of military forces.
- Combined training exercises.
- Aircraft and ship visits.
- The introduction or buildup of military forces in a region.

These missions will provide opportunities for the threat and third-country supporters to exploit the presence of US forces to their political advantage. Such exploitation may include violence such as terrorist activities or the intelligence exploitation of US soldiers in contact with local nationals.

You must ensure that unit security education programs and SAEDA orientations are emphasized and integrated into unit training plans and programs.

Noncombatant Evacuation Operations

NEOs may cause hostile reactions when they involve using US forces to relocate threatened civilian noncombatants, selected HN natives, and third-country nationals. Air and ground routes of evacuation may provide targets of opportunity for terrorist interdiction or public demonstrations that might cripple the mission.

CI element liaison and coordination with other US agencies resident in the HN and with HN intelligence, security, and LEA offices will be necessary. Your job is to ensure that the threat is properly assessed and friendly vulnerabilities have been protected.

Rescue and Recovery Operations

RRO may include the rescue of US or friendly foreign nationals and the location, identification, and recovery of sensitive equipment or materiel.

Threat forces may oppose RRO. Therefore, a thorough assessment of threat intelligence and security systems is essential for force protection. RRO may be either clandestine or overt. Stealth, speed, surprise, and sufficient force to overcome the threat are the characteristics of RRO. MDCI supports the commander's need for timely intelligence, extraordinary OPSEC measures, and the use of deception.

Strikes and Raids

Strikes and raids can support RRO or seize and destroy equipment and facilities which threaten US interests. They can also support counter-drug operations. Consider putting planning, organizing, training, and equipping under SAPs. Deliberate and inadvertent disclosure of the commander's intent requires special attention.

Threat and third-country intelligence and security service collection capabilities must be thoroughly assessed. MDCI will support the commander's OPSEC program and the deception plan. The plans will assist in disguising rehearsals through integration with routine training. The MDCI analyst should anticipate a threat all-source collection effort with national and technical assets available.

Operations to Restore Order Transitions

Operations to restore order include the unilateral employment of US forces, or a US and foreign JTF. Typically, operations to restore order PCO are undertaken at the request of the HN. ROE can be restrictive because the purpose of the force is to establish and maintain law and order. Your operations to restore order mission may rapidly transition to PKO. MDCI supports operations to restore order, which include—

- Consistent mission analysis.
- Clear C^2 relationships.
- Effective communications facilities.
- Effective public diplomacy and PSYOP.

Continuity of MDCI operations is essential during all phases of the operations to restore order and transition to and during the PKO. The threat may consist of elements of the HN intelligence and security system, other FIS, or terrorist and other paramilitary or guerilla elements aligned with various political factions.

The stopping of hostilities, and the following period of negotiated settlement, is a time in which opposition factions will be maneuvering for power. US forces will be susceptible to terrorist activities and possible low-level interdiction by guerilla or paramilitary elements.

Unconventional Warfare Operations

Unconventional warfare operations (UWO) may include the use of both SOF and general purpose forces. Unlike most PCO, UWO are usually a long-term effort. Support to UWO is similar to support to insurgencies. A major difference is that in UWO the emphasis is on military actions while support to an insurgency focuses on infrastructure and political development.

Disaster Relief Operations

DRO provide emergency assistance to victims of natural or manmade disasters abroad. They may include—

- Refugee assistance.
- Food programs.
- Emergency medical treatment.
- Assistance to other civilian welfare programs.

CI elements coordinate with agencies dispensing services to ensure that the situation is not being exploited by threat intelligence and security services. Coordination is between CI, MP, and CA elements supporting the operation.

Security Assistance Surges

SAS require MDCI threat assessments to determine threat intentions toward the security assistance effort. These surges are usually for a limited time. However, US forces involved in SAS may be subject to terrorists' attempting to degrade the effectiveness of the operation.

Support to Civil Authorities

Support to US civil authority involves the use of military forces to support federal and state officials under (and limited by) the Posse Comitatus Act and other laws and regulations. US Army CI elements are guided by AR 381-10 and AR 381-20.

Counter-Drug Operations

DOD and Department of the Army (DA) policy regarding US Army CI support to DOD counter-drug operations is stated in DA letter, DAMI-CIC (381-20), Subject: Guidance for Army Counterintelligence Elements Supporting DOD Counternarcotics Missions, dated 20 September 1990.

Planning Considerations

Figure 8-1 is a functional matrix for PCO and guides MDCI support planning. This matrix was developed from FM 100-20/AFP 3-20, Chapter 5.

Since Chapter 5 is not an exhaustive list of all major functions accomplished during the planning and execution of the various types of PCO, many functions are not cross-walked to a type operation with an X. This does not mean that the function is not important to a particular type PCO. Add your own X if you see a relationship not marked. (Figure 8-1 expands the CI functional steps in Figure C-1.)

The senior CI officer (commissioned, warrant, or noncommissioned officer) involved in planning MDCI support to PCO uses this matrix to identify key areas where additional support and attention are needed. PCO functional areas correlate to the four basic MDCI functions of—

- Investigation.
- Operations.
- Collection.
- Analysis and production.

HN and belligerent nation security forces include intelligence and security services and Level I and Level II threats in the area of responsibility (AOR). The MDCI data base should contain a complete description of friendly and threat FISs.

Dossiers and files on key personnel in the structure should be maintained. In PCO, there may be a fine line between military, paramilitary, and LEA operations.

Terrorism, for example, is a criminal activity but requires heightened security when US military personnel, civilian noncombatants, and facilities are targets. Guerrillas, who employ terrorist tactics, may be countered by a combination of military, paramilitary, and police means.

US CI personnel must be fully apprised of the threat situation in any PCO. This attention is important because these operations can transition quickly to another level.

The senior CI officer is responsible for recommending countermeasures to protect EEFI. You must be thoroughly familiar with the mission statement, the commander's intent, and METT-T factors. You must also understand how friendly forces will operate in the AO. Most PCO are short term and are executed swiftly. MDCI support must be *front-loaded* into PCO as early as possible in the contingency planning phase.

Aggressive CI liaison is a major contributor to accomplishing the MDCI mission. You are responsible for ensuring that close coordination is effected with the EACIC ISE resident in the AOR.

Intelligence liaison officers assigned to ISEs need to be trained to report information of MDCI interest. Records should be maintained of ISE liaison contacts with foreign military, paramilitary, and police personnel (sources) and organizations. Biographic data must be recorded and filed. This information will provide valuable input into the HUMINT data base in the counterintelligence analysis section (CIAS).

You must be completely familiar with the ROE and the political sensitivities that are part of each type of PCO. ROE includes constraints on the military imposed by the NCA, the US ambassador and his country team, the CINC, and caveats contained in the SOFA.

Force protection efforts may require special MDCI collection activities such as LLSO within the AOR. If LLSO are already being conducted in support of the CINC, you may want to consider augmenting the effort with additional resources or you may recommend refocusing the collection effort.

In any case, reporting from the LLSO must be incorporated into MDCI support to PCO. FM 34-60 and FM 34-60A(S) contain additional information on LLSO.

TYPE OPERATION

PCO FUNCTIONS	SHOW			STKS	OP TO				SPT
	FORCE			AND	RESTORE				US
	DEMO	NEO	RRO	RAIDS	ORDER	UW	DRO	SAS	CA
Advisory personnel									X
Collection operation				X					X
-informational									X
-detection									X
-surveillance									X
C^2 relationships	X			X	X				
-communications					X				
-effective facilities						X			
Force protection	X	X	X	X	X	X			
-OPSEC			X	X					
-deception			X	X					
-extraordinary security means				X	X				
-PSYOP				X	X				
HN security forces	X	X	X	X	X	X			
-role and status		X	X	X					
Intelligence	X		X	X	X				
-intelligence support				X					
-timely	X		X	X					
Legalities	X	X			X				
-Posse Comitatus Act									X
-illegal immigrant									X
-ROE	X	X	X	X	X	X	X	X	X
-customs violations									X
Liaison	X	X			X				
-joint					X				
-combined					X				
-US ambassador		X							
-country team		X							
-CIA									
-DOS		X					X		X
-DEA									X
-INS/Border Patrol									X
-Customs Service									X
-FBI									X
-Coast Guard									X
-CINC	X	X	X	X	X	X	X	X	X

Figure 8-1. PCO functional matrix.

PCO FUNCTIONS	SHOW			STKS (2)	OP TO (1) (3)				SPT
	FORCE	(1)	(2)	AND	RESTORE				US
	DEMO	NEO	RRO	RAIDS	ORDER	UW	DRO	SAS	CA
Maneuver	X				X				
-general purpose									
forces	X		X	X	X	X			
-discrete appl/force		X		X	X				
-swift execution		X	X	X					
-SOF						X			
-highly trained									
special units			X	X					
-forward deploy/									
military forces	X								
-combined training									
exercises	X								
-introduction/buildup									
military forces	X								
-visits	X								
aircraft	X								
ships	X								
Logistics/CSS	X					X	X	X	X
-airlift		X						X	
-sealift	X							X	
Mission analysis	X	X	X	X	X	X	X	X	X
-ROE	X	X	X	X	X	X	X	X	X
-operations									
long term						X			
short term	X	X	X	X	X		X	X	X
-politically complex	X			X					
-public diplomacy				X					
-swift execution		X	X	X					
-threats/pub property									X
-counter-drug									X
-detailed planning		X	X	X	X				X
-civic action									X
-disasters		X				X			
manmade		X						X	
natural		X						X	
Training				X					
-MTT									X
-offshore									X
-combined training									
exercises									

(1) NEO can transition into operations to restore order or PKO.
(2) Strikes and raids can support RRO, counter-drug operations. CINC plans and executes.
(3) Operations to restore order may transition to PKO.

Figure 8-1. PCO functional matrix (continued).

APPENDIX A
ECHELONS ABOVE CORPS INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT TO LOW-INTENSITY CONFLICT OPERATIONS

This appendix describes the MI brigade (EAC) and its capability to provide IEW support to LIC operations.

Since no single IEW echelon can meet all of its intelligence requirements with assigned resources, each must integrate its resources into the entire IEW system. This interdependency requires regular and detailed coordination and applies equally to producers and executors. The CMO centrally manages coordination at each echelon.

When a theater command is established in an AO, it will have an organic MI brigade (EAC) available to provide IEW support. The MI brigade (EAC) is part of the IEW architecture at theater and is organized and regionally tailored according to the theater's mission and its geographic area.

The MI brigade (EAC) may be augmented with an MIBLI. A *type* of MI brigade (EAC) is shown in Figure A-1. This brigade manages, collects, processes, and disseminates SIGINT, HUMINT, IMINT, CI, and TECHINT.

The MI brigade (EAC) commander employs available organic and attached MI assets to execute the IEW mission. IEW employment must be in the broad context of the Army commander's overall campaign and not in the narrow sense of the capabilities of the assets themselves. It provides—

- Transition-to-war planning.
- IEW support to battalion managers at the joint and allied command levels.
- Reinforcement of IEW support to all theater MI units or staffs.

BRIGADE ORGANIZATION

Each MI brigade (EAC) is tailored to meet specific regional mission requirements and may consist of—

- A headquarters company or detachment.
- An EACIC, which may be subordinate to the operations battalion.
- An operations battalion or company.
- A TECHINT battalion or company.
- An imagery analysis battalion or company. This also may be a unit subordinate to the operations battalion.
- A SIGINT battalion or company.
- An interrogation and exploitation battalion or company or a HUMINT battalion or company. If there is no HUMINT, interrogation and exploitation battalion, or CI element, there is a collection and exploitation battalion or company.
- A CI battalion or company.

HEADQUARTERS

The brigade headquarters company or detachment provides—

- C^2 subordinate brigade elements.
- Staff planning, control, and supervision of attached units.

OPERATIONS BATTALION

In LIC, the operations battalion of the MI brigade (EAC) is the focal point for brigade operations. It is organized with a headquarters, headquarters service company (HHSC), an EACIC, a TECHINT company, and a strategic imagery company. The battalion provides—

- C^2 of assigned and attached unit.
- All-source intelligence analysis, production, and dissemination.
- Intelligence analytical support to battlefield deception.
- Near-real-time (NRT) exploitation, reporting, and rapid dissemination of national level collected imagery.
- Collection and data base management, tasking guidance, and tasking for EAC sensor cueing.

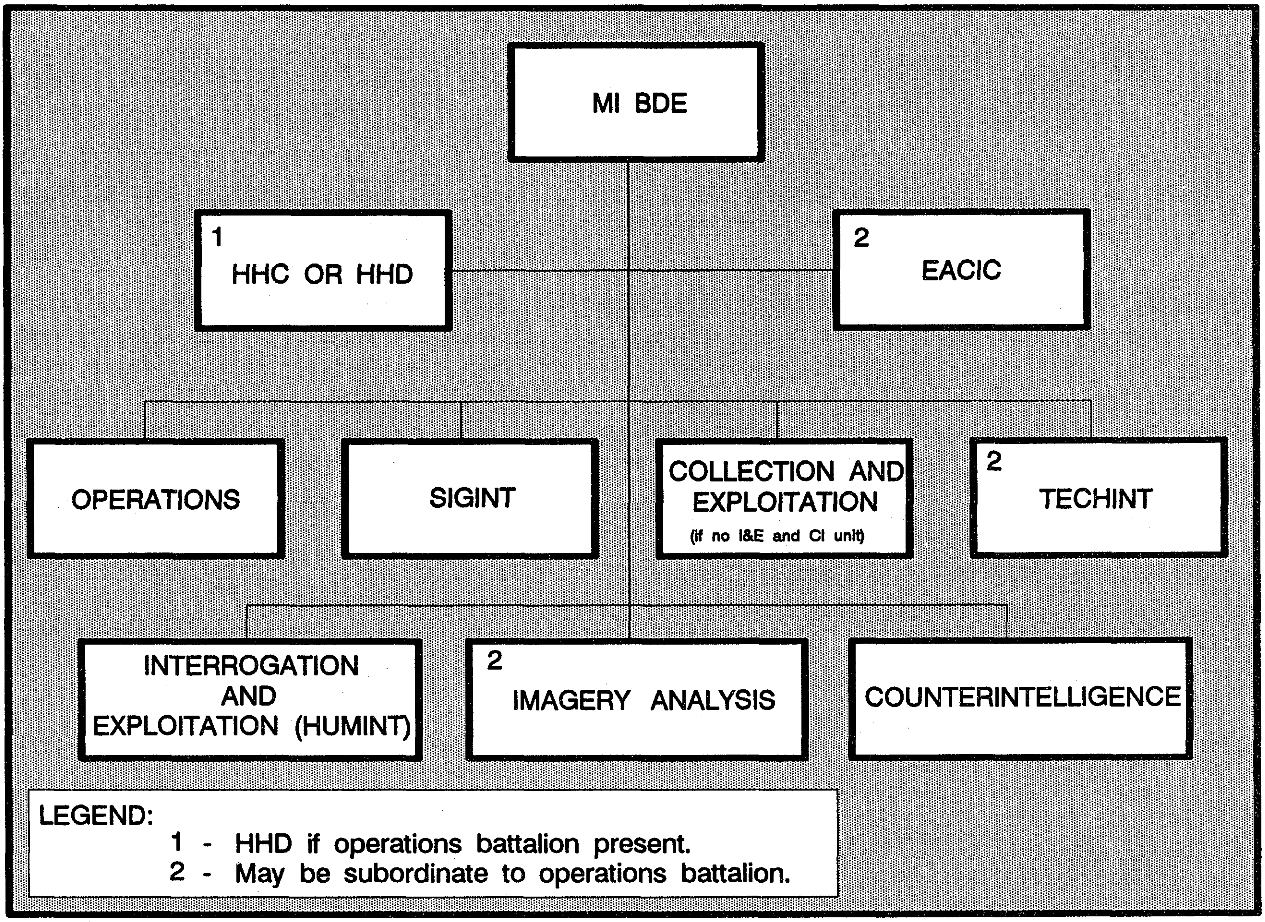

MI BDE
1 HHC OR HHD
2 EACIC
OPERATIONS
SIGINT
COLLECTION AND EXPLOITATION (if no I&E and CI unit)
2 TECHINT
INTERROGATION AND EXPLOITATION (HUMINT)
2 IMAGERY ANALYSIS
COUNTERINTELLIGENCE
LEGEND:
1 - HHD if operations battalion present.
2 - May be subordinate to operations battalion.

Figure A-1. Type MI brigade (EAC) organization.

- Army TECHINT support to the EACIC and other users in the theater.
- Mechanical and electronic maintenance.
- IEW support to wartime reserve mode (WARM) and reprogramming operations.

TECHINT BATTALION OR COMPANY

The TECHINT battalion or company's support can range from identifying routine modifications of existing equipment to processing and evaluating threat items that reflect major advances in offensive or defensive capabilities. During war it is concerned with high priority items that require immediate field exploitation to determine major capabilities, limitations, and possible friendly countermeasures.

The TECHINT battalion or company provides—

- Analysis and exploitation of captured enemy documents (CEDs) and equipment, weapon systems, and other war materiel.
- Analysis of the capabilities, limitations, and vulnerabilities of enemy materiel.
- Feedback on the tactical threat posed by technological advances in new or recently discovered foreign and enemy materiel.
- Countermeasures to any enemy technical advantages.

IMAGERY ANALYSIS BATTALION OR COMPANY

The imagery analysis battalion or company exploits tactical, theater, and national level imagery. The imagery analysis company provides first-, second-, and third-phase analysis; exploitation; and reproduction of radar, infrared, photographic, E-O, multispectral, and digital imagery products.

SIGINT BATTALION OR COMPANY

The SIGINT battalion or company has from 2 to 5 collection companies and a control and processing company, which conducts—

- SIGINT operations against skywave HF signals.
- Communications intelligence (COMINT) processing and analysis.
- RDF operations.
- Target exploitation (TAREX) collection activities.
- ECM operations.

HUMINT BATTALION OR COMPANY

The HUMINT interrogation and exploitation battalion or company interrogates EPWs, high level political and military personnel, civilian internees, refugees, DPs, and other non-US personnel. They also translate and exploit selected CEDs. Typical EAC HUMINT collection activities include—

- Exploiting EPWs and detainees.
- Exploiting CEDs.
- Conducting debriefings.
- Conducting long-range surveillance operations (LRSO).
- Conducting overt elicitation activities to include liaison with local military or paramilitary forces.
- Collecting information from friendly troops.
- Conducting controlled collection operations.
- Supporting other intelligence agencies and disciplines operating within the AO.

CI BATTALION OR COMPANY

The CI battalion's special operations teams conduct counterespionage, countersubversion, and countersabotage operations and investigations. The polygraph teams support investigations; the security support section works automated data processing (ADP) security, technical surveillance countermeasures, and counter-SIGINT. Other CI battalion or company functions include—

- Collecting intelligence information through LLSO.
- Providing MDCI support to other units.
- Providing CI support to rear area operations and CT.

MIBLI AUGMENTATION

MIBLIs are organized to support Army component commanders, CINCs, and national intelligence requirements under LIC conditions. There currently is one MIBLI with three companies, which are—

- A Company — SASS.
- B Company — CRAZY HORSE (airborne SIGINT system).
- C Company — GUARDRAIL (airborne SIGINT system).

APPENDIX B
ELECTRONIC WARFARE SUPPORT TO LOW-INTENSITY CONFLICT OPERATIONS

This appendix defines SIGINT and EW. It explains the relationship of SIGINT to EW, the component parts of EW, and describes the basic tactical IEW equipment which may be available in LIC.

SIGINT results from collecting, locating, evaluating, and analyzing intercepted emissions, as well as from the fusion of other intelligence. SIGINT sources include both communications and noncommunications emitters.

It combines the following intelligence disciplines: COMINT, electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). The SIGINT contribution to LIC is usually in the form of COMINT. COMINT provides technical and intelligence information that comes from the analysis of threat communications.

Technical SIGINT information enhances the data bases required to provide EW support in a LIC environment. Effective EW provides combat information, disrupts the threat electromagnetic spectrum, and allows unhampered use of the same spectrum to friendly forces. EW has both an offensive and defensive component.

OFFENSIVE ELECTRONIC WARFARE

Offensive EW consists of ES and EC. ES gives us the ability to intercept, identify, and locate enemy emitters. ES provide combat and technical information required for jamming (FM 34-40-7), deception operations (FM 90-2A(S)), targeting, and the tactical employments by combat forces. The primary function of ES is to provide the tactical commander with perishable combat information he needs to conduct his operations.

DEFENSIVE ELECTRONIC WARFARE

Defensive EW or EP are actions taken to ensure friendly use of the airwaves. These actions are both preventive and remedial. Preventive techniques include—

- Terrain masking.
- Selecting correct antennas.
- Transmitting only when necessary.
- Using minimum transmitting power.
- Using correct radio procedures.

Remedial techniques are the actions used after the threat has started to exploit friendly communications.

In LIC it is unlikely that you will be jammed. But if it happens, begin remedial techniques in accordance with unit SOPs and report it under the MIJI program.

It is more likely that your radio net will be intruded upon. This is likely if the threat possesses captured friendly communications equipment or if their communications gear is compatible with current issue. When this occurs, it will usually be on a nonsecure radio net.

Preventive measures include using proper radio procedures and the authentication tables in your unit SOI. One remedial measure is to change frequencies.

If you suspect that your crypto-variables or your SOI have been compromised, report it immediately and take the actions needed to correct the problem. Consult your unit SOP and C-E staff officer for advice.

TACTICAL ELECTRONIC WARFARE EQUIPMENT

Figure B-1 shows current tactical IEW equipment according to nomenclature, function, prime mover, and unit and quantity. Figure B-2 shows EAC and Corps IEW assets.

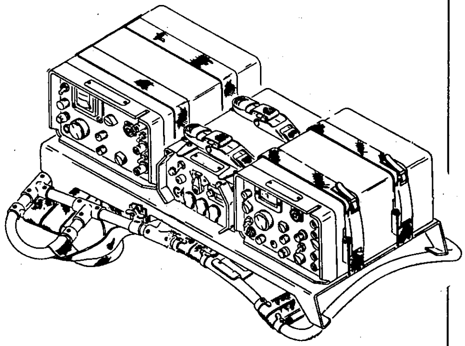
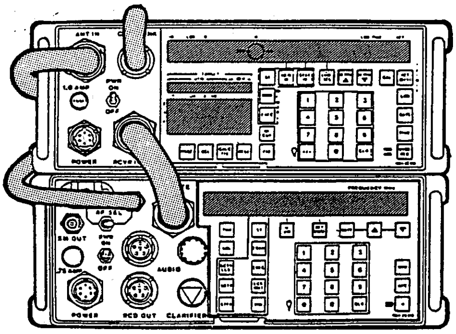
NOMENCLATURE	FUNCTION	PRIME MOVER	UNIT and QUANTITY
AN/TRQ-30 Receiving Set 	HF/VHF Intercept (VHF LOB)	Man Packed	HVY DIV: 3 Systems. 1/C&J Plt, C&J Co, MI Bn. LT DIV: 9 Systems. 3/Voice Coll Plt, Coll Co, MI Bn. AASLT DIV: 12 Systems. 4/C&J Plt, C&J Co, MI Bn. ABN DIV: 3 Systems. 3/C&J Plt, MI Co (Gen Spt), MI Bn. ACR: 2 Systems. 1/C&J Plt, MI Co. CORPS: 6 Systems. 3/Voice Coll Plt, EW Co, MI Bn (TE), MI Bde. 3/Voice Coll Plt, EW Co (Coll), MI Bn (TE)(RC), MI Bde.
AN/PRD-10 Receiving Set (MPRDFS) 	HF/VHF/UHF Intercept (VHF DF when netted w/other PRD-10 or TRQ-22's)	Man Packed	ABN DIV: 9 Systems. 3/C&J Plt, MI Co (Fwd Spt), MI Bn.

Figure B-1. Tactical IEW equipment capabilities and quantities.

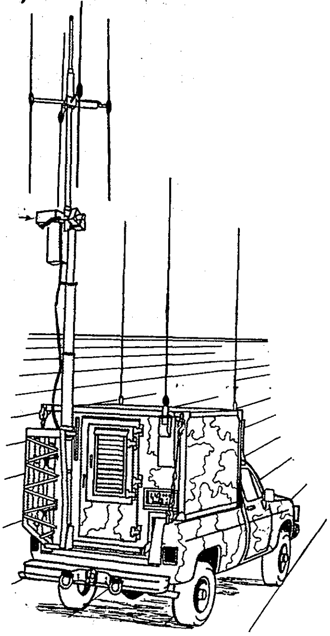
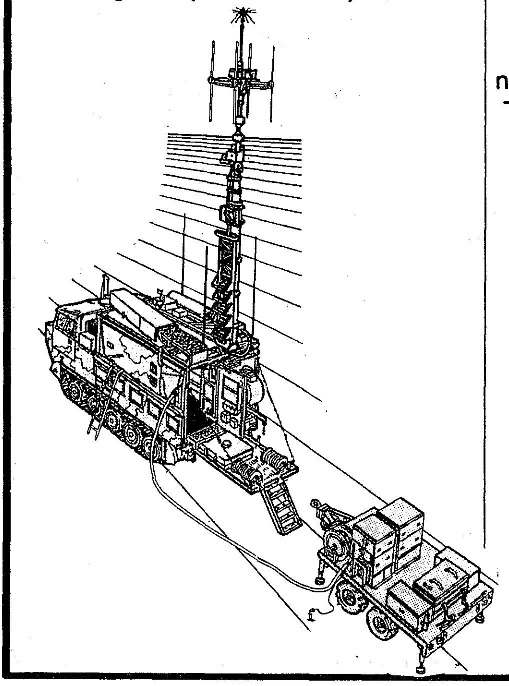
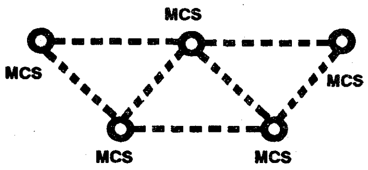
NOMENCLATURE	FUNCTION	PRIME MOVER	UNIT and QUANTITY
AN/TRQ-32 (V)2 Receiving Set (TEAMMATE) 	HF/VHF/UHF Intercept (VHF DF when netted w/other TRQ-32's)	CUCV/ HMMWV	HVY DIV: 3 Systems. 1/C&J Plt, C&J Co, MI Bn. LT DIV: 3 Systems. 1/C&J Plt, Coll Co, MI Bn. AASLT DIV: 3 Systems. 1/C&J Plt, C&J Co, MI Bn. ABN DIV: 3 Systems. 3/C&J Plt, MI Co (Gen Spt), MI Bn. ACR: 2 Systems. 1/C&J Plt, MI Co. CORPS: 6 Systems. 3/Voice Coll Plt, EW Co, MI Bn (TE), MI Bde. 3/Voice Coll Plt, EW Co (COLL), MI Bn (TE)(RC), MI Bde.
AN/TSQ-138 Special Purpose Detecting Set (TRAILBLAZER) 	VHF DF (HF/VHF/UHF Intercept) DF when netted w/other TSQ-138's or ALQ-151	M1015	HVY DIV: 1 System (5 vehicles) 1/SIGINT Proc Plt, EW Co, MI Bn. DEPLOYMENT: 

Figure B-1. Tactical IEW equipment capabilities and quantities (continued).

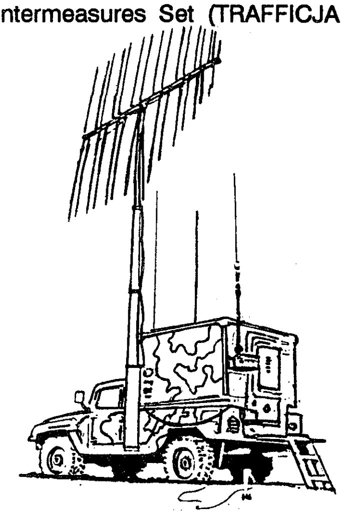
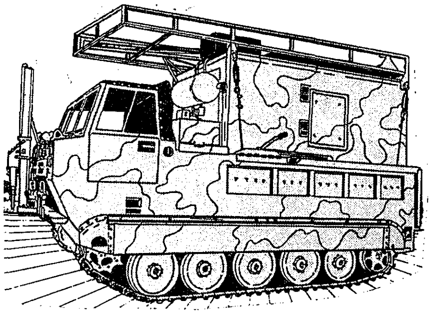
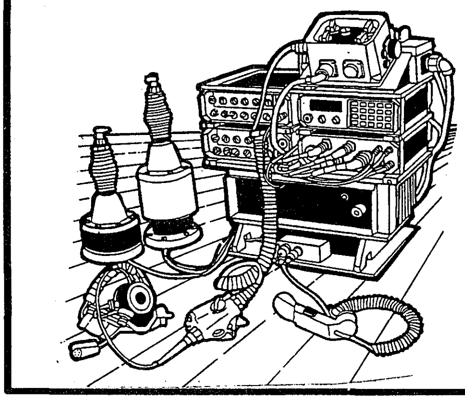
NOMENCLATURE	FUNCTION	PRIME MOVER	UNIT and QUANTITY
AN/TLQ-17A(V)3 Countermeasures Set (TRAFFICJAM) 	VHF EC (HF/VHF Intercept)	CUCV/ HMMWV	HVY DIV: 3 Systems. 1/C&J Plt (3), C&J Co, MI Bn. AASLT DIV: 3 Systems. 1/C&J Plt (3), C&J Co, MI Bn. ABN DIV: 3 Systems. 3/C&J Plt, MI Co (Gen Spt), MI Bn. ACR: 2 Systems. 1/C&J Plt (2), MI Co. CORPS: 3 Systems. 1 EC Plt (3), EW Co (EC), MI Bn(TE)(RC), MI Bde.
AN/MLQ-34 Special Purpose Countermeasure Set (TACJAM) 	VHF EC (VHF Intercept)	M1015	HVY DIV: 3 Systems. 1/C&J Plt (3), C&J Co, MI Bn. ACR: 2 Systems. 1/C&J Plt (2), MI Co. CORPS: 9(AC), 6(RC) Systems. 3/VHF EC Plt (3), EW Co, MI Bn (TE), MI Bde. 2/EC Plt (3), EW Co (EC), MI Bn. (TE)(RC), MI Bde.
AN/ULQ-19(V)2 VHF Responsive Jammer (RACJAM) 	VHF EC (VHF Intercept)	CUCV/ HMMWV	ABN DIV: 3 Systems. 1/C&J Plt (3), MI Co. (MI Co (Fwd Spt)), MI Bn (Training device).

Figure B-1. Tactical IEW equipment capabilities and quantities (continued).

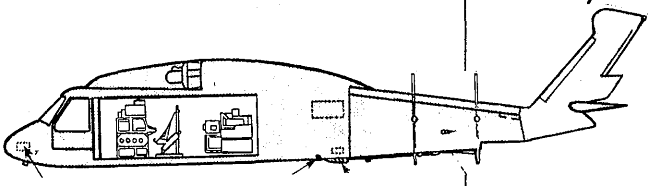
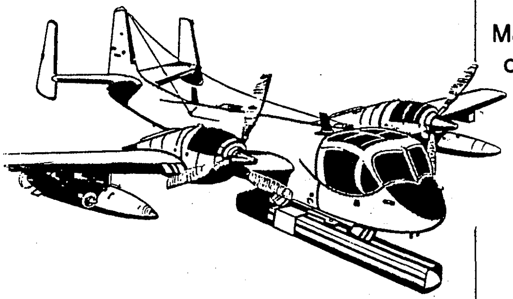
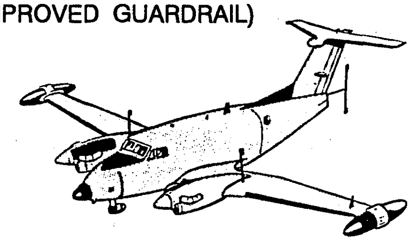
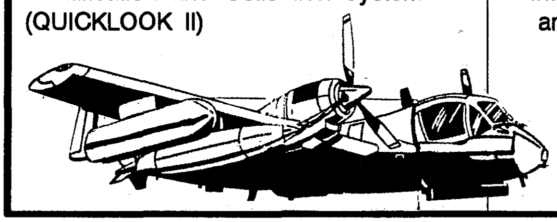
NOMENCLATURE	FUNCTION	PRIME MOVER	UNIT AND QUANTITY
AN/ALQ-151(V)1 Special Purpose Countermeasures System (QUICKFIX IIA) AN/ALQ-151(V)2 (QUICKFIX IIB) 	VHF Intercept VHF EC VHF DF (Can net w/ TRAILBLAZER for DF)	EH-60A (BLACKHAWK)	HVY DIV: 3 Systems. 3/Flt Plt, Avn Bde. LT DIV: 3 Systems. 3/Flt Plt, Avn Bde. AASLT DIV: 3 Systems. 3/Flt Plt, HHOC, MI Bn. ABN DIV: 3 Systems. 3/Flt Plt, Cbt Avn Squadron. ACR: 3 Systems. 3/Flt Plt, Cbt Avn Squadron.
AN/APS-94F Radar Surveillance Set (MOHAWK) 	Moving Target Indicators on Radar Maps (SLAR) or PHOTO	OV-1D	CORPS: 10 Systems. 5/Flt Sec (2), Flt Plt, Avn (AS Co) MI Bn (AE), MI Bde.
AN/USD-9 Special Purpose Detecting System (GUARDRAIL V) (IMPROVED GUARDRAIL) 	VHF/UHF Intercept VHF/UHF DF	GRV RU-21 IGRV RC-12D	CORPS: 6 Systems. 6/COMINT Acft Sec, Flt Plt, Avn (EW) Co, MI Bn (AE), MI Bde.
AN/ALQ-133 Noncommunications Identification and Collection System (QUICKLOOK II) 	Noncomms Intercept and DF	RV-1D	CORPS: 6 Systems. 6/Noncomm Acft Sec, Flt Plt, Avn (EW) Co, MI Bn (AE), MI Bde.

Figure B-1. Tactical IEW equipment capabilities and quantities (continued).

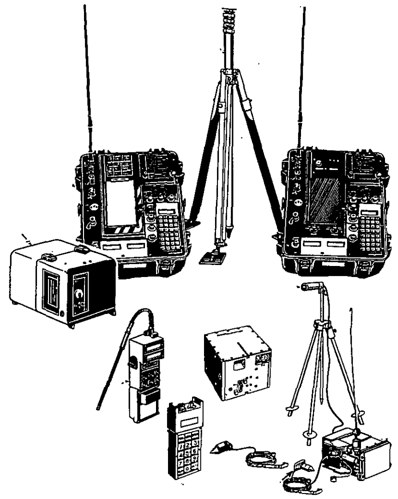
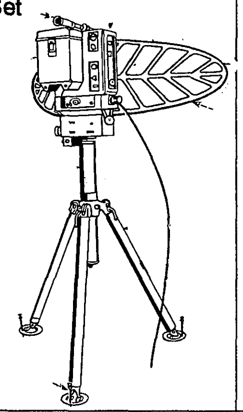
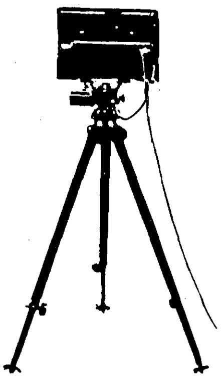
NOMENCLATURE	FUNCTION	PRIME MOVER	UNIT and QUANTITY
GSQ-187 Remotely Monitored Battlefield Sensor System (REMBASS) 	Seismic/ Acoustic/ Magnetic/ Infrared	Man Packed and Vehicle	LT DIV: 5 Systems. 5/GS Plt, I&S Co, MI Bn. AASLT DIV: 5 Systems. 5/GS Plt, I&S Co, MI Bn. ABN DIV: 5 Systems. 5/GS Plt, MI Co (Fwd Spt), MI Bn.
AN/PPS-5B Radar Set 	Moving Target Indicators Range: 6 km-Pers 10 km-Veh	Man Packed and Vehicle	HVY DIV: 12 Systems. 4/GSR Squad (3), Survl Plt, I&S Co, MI Bn. AASLT DIV: 3 Systems. 1/GSR Squad (3), Survl Plt, I&S Co, MI Bn. ACR: 9 Systems. 3/GSR Squad (3), Survl Plt, MI Co.
AN/PPS-15A(V)1 Radar Set 	Moving Target Indicators Range: 1.5 km-Pers 3 km-Veh	Man Packed and Vehicle	LT DIV: 12 Systems. 3/GSR Squad (4), Survl Plt, I&S Co, MI Bn. AASLT DIV: 9 Systems. 3/GSR Squad (3), Survl Plt, I&S Co, MI Bn. ABN DIV: 9 Systems. 3/I&S Plt (3), MI Co (Fwd Spt), MI Bn.

Figure B-1. Tactical IEW equipment capabilities and quantities (continued).

NOMENCLATURE	FUNCTION	PRIME MOVER	UNIT
AN/MSA-34 Mobile Operations and Electrical Facility	HF SIGINT collection	V-348 low bed semitrailers w/tractor	EAC-SIGINT Bn
AN/TRD-23 Radio Direction Finding Set	HF Skywave DF	5-ton cargo truck	EAC-SIGINT Bn
AN/TSQ-152 (Track Wolf)	SIGINT operations and DF	5-ton cargo truck	EAC-SIGINT Bn
Sandcrab	EW	HMMWV	EAC-SIGINT Bn
AN/TSQ-163 (55P-5) Single Source Processor SIGINT	SIGINT processor	2-M931A1 tractors	EAC-Op Bn
Crazyhorse	Airborne SIGINT operations and DF	C-12 aircraft and 5-ton ground station	EAC-MI Bn (LI)
Aerial Reconnaissance Low (ARL)	Airborne SIGINT operations and DF. EO/FLIR DA-1 TV DF	DASH-7	EAC-MI Bn (LI)
AN/TSQ-134(V) Electronic Processing and Dissemination System (EPDS)	ELINT processing	2 (5-ton) tractor trucks	EAC, Corps
Army HF EW System (AHFEWS)	HF EW		EAC
TROJAN	SIGINT readiness	Fixed site	EAC, Corps
AN/TSQ-132 Joint Surveillance Target Attack Radar System Ground Station Module (Joint STARS)	Radar Processor	M923A1 cargo truck	EAC, Corps
Small Airborne Surveillance System (SASS)	Radar Sensor	Tethered balloon	EAC-MI Bn (LI)
Imagery Exploitation System (IES)	Imagery processing and dissemination	Tractor trailor	EAC-Op Bn
Enhanced Tactical Users Terminal (ETUT)	ELINT and IMINT processing	5-ton truck	EAC, Corps
Mobile Imagery Tractical Terminal	ELINT and IMINT receiver	HMMWV	Corps

Figue B-2. IEW and Corps IEW assets.

APPENDIX C

MULTIDISCIPLINE COUNTERINTELLIGENCE SUPPORT TO LOW-INTENSITY CONFLICT OPERATIONS

This appendix describes the types of MDCI support available to US military involved in LIC operations. It addresses the key aspects of EAC and ECB support.

MDCI support to forces in LIC encompasses a wide range of capabilities from strategic to tactical level. MDCI support provides the capability to counter threat, HUMINT, SIGINT, and IMINT collection, and security measures. We accomplish this through analysis that brings together threat, friendly forces vulnerabilities, and existing security programs. The four functional CI tasks of investigations, operations, collection, and analysis and production are applied to each type of LIC operation.

Figure C-1 is a matrix which correlates these CI tasks to the four types of LIC operations. Mission analysis, and a review of the force's mission-essential task list (METL), is matched to the subtasks identified in this matrix for planning and allocating MDCI support.

Tasks that are not within the capability of the CI element assigned to the MI unit supporting the force are converted into unresourced requirements and passed to higher echelon.

Key aspects of higher echelon support are discussed below.

INVESTIGATIONS

The Commanding General (CG), INSCOM, is responsible for—

- Maintaining centralized control of all CI operations and investigations.
- Conducting CI operations and investigations in accordance with AR 381-47(S) and AR 381-20.
- Providing CI-related security support to US Army OPSEC programs.
- Ensuring appropriate foreign intelligence and physical security information, derived from CI operations and activities, is provided to the support installation security officer.
- Collecting and reporting CI information in response to approved CI collection requirements.
- Conducting liaison with the FBI, CIA, host and other foreign country agencies, and other federal and local agencies.
- Providing the nearest Criminal Investigation Division (CID) office with terrorism information as developed.

OPERATIONS

MI brigades (EAC) perform theater IEW support missions for operational commanders in Europe, Southwest Asia, the Americas, Northeast Asia, the Pacific, and the continental United States (CONUS). They are responsible for—

- Providing a subcontrol office for CI investigations within their AOR.
- Coordinating CI operations and collection activities within their AOR.
- Performing CI and terrorism analysis and production.
- Conducting CI-related liaison with HN and other foreign country agencies plus representatives of other US agencies. See FM 34-37 for more information.

COLLECTION

The CG, INSCOM, is responsible for—

- Conducting foreign intelligence and CI activities to collect and disseminate information on all aspects of terrorism and related threats against the Army and DOD. These activities are conducted in accordance with AR 381-10, AR 381-20, AR 381-47(S), and AR 381-100.

CI FUNCTIONS	INSURGENCY	COUNTER-INSURGENCY	PKO	COMBATTING TERRORISM	PCO
INVESTIGATIONS					
Espionage	X	X	X	X	X
Sabotage	X	X	X	X	X
Treason					
Sedition					
Subversion		X			X
Personnel security (OCONUS)	X	X	X		X
Terrorism		X	X	X	X
Technology transfer					
Deliberate security violations and compromises	X	X	X	X	X
COMSEC insecurity	X	X	X	X	X
Incident investigation	X	X	X	X	X
Unexplained absence and suicide	X	X	X	X	X
Walk-in	X	X	X	X	X
Assessment of sources	X	X	X	X	X
Impersonation of intelligence personnel	X	X	X		X
Technical penetration		X			X
Investigation control	X	X	X	X	X
OPERATIONS					
Penetration operations (OFCO)		X		X	X
Surveys			X	X	X
CI support to cover		X			
Technical support and services			X	X	
COMSEC monitoring		X			
Crypto facility inspections					
Crypto netting approval					
SAEDA training	X	X	X	X	X
SAP	X	X		X	X
Security A&A	X	X	X	X	X
COLLECTION					
Liaison	X	X	X	X	X
LLSO	X	X	X	X	X
Casual source	X	X	X	X	X
EPWs, refugees, detainees	X	X			X
Foreign contact debriefings	X	X	X	X	X
ANALYSIS					
MDCI data base development	X	X	X	X	X
Prepare plans, products, reports	X	X	X	X	X
FIS threat assessments	X	X	X	X	X
Friendly vulnerability assessment	X	X	X	X	X
Countermeasures recommendation	X	X	X	X	X
Countermeasures evaluation	X	X	X	X	X
Conduct MDCI IPB	X	X	X	X	X

Figure C-1. MDCI functional matrix for LIC.

- Providing Army commanders with information on terrorist threats against their personnel, facilities, and operations.
- Investigating terrorist incidents for intelligence purposes in cooperation with the FBI or HN authorities.
- Serving as the Army's liaison to US and HN national, state, and local agencies.

MULTIDISCIPLINE COUNTERINTELLIGENCE ANALYSIS AND PRODUCTION SUPPORT

INSCOM serves as the Army's analytic representative for terrorism and is responsible for—

- Analyzing information on all aspects of terrorism and the threat it poses to US Army personnel, facilities, and activities; and forwarding that information and intelligence to commanders at all echelons.
- Providing terrorism analysis and assisting in developing area situation assessments.
- Providing all-source threat evaluations of foreign intelligence and terrorist organizations that threaten US Army security.
- Preparing multidiscipline threat data pertaining to SIGINT, EW (less manipulative electronic deception [MED] and ECCM), HUMINT, and IMINT, for inclusion in supported commands' OPSEC training programs.

THE THREAT

FIS threats to US forces in LIC are multidiscipline. The MI forces countering that threat must also be multidiscipline.

This multidiscipline approach is achieved by executing the four MDCI functional tasks. This approach applies to all echelons from battalion to EAC.

Commanders of friendly forces involved in LIC are also concerned with the threat posed by enemy agents or guerrillas (Level I), and diversionary and sabotage operations conducted by threat UW forces (Level II).

OPERATIONS SECURITY

OPSEC in LIC is concerned with keeping a high security posture. It also aims at achieving surprise by protecting friendly capabilities and intentions from exploitation. Its ultimate objective is to prevent a threat from getting enough advance information to degrade the operations of US, HN, or other forces.

COUNTERINTELLIGENCE AND SECURITY SUPPORT TO OPERATIONS SECURITY IN LOW-INTENSITY CONFLICTS

The level of CI and security support to OPSEC in LIC is tailored to the supported organization's mission and its vulnerability to foreign intelligence collection or terrorist attack. This support is provided by MI units at both EAC and ECB.

To determine the degree of CI and security support required, supporting MI units routinely consider—

- All aspects of the supported unit's mission in LIC (as derived from the METL).
- The total threat from foreign intelligence collection and terrorist attack capabilities.
- Specific identification of forces or agency vulnerabilities to foreign intelligence collection and terrorist attack.
- Recommendation of countermeasures for the supported unit.
- Evaluation of the effectiveness of the countermeasures.

SPECIAL ACCESS PROGRAMS

SAPs are established to provide extra protection and limited access to various programs and missions. The CG, INSCOM, provides CI support to SAPs and develops and maintains capability, methods, and expertise to meet Army requirements. For more information on SAPs, refer to TC 34-5(S) and FM 34-60A(S).

OPERATIONS SECURITY SUPPORT TO ECHELONS CORPS AND BELOW

Organic elements of the MI battalion, brigade, or other MI units within the Army's tactical force structure are responsible for providing direct CI support to OPSEC for units at ECB in LIC. This support includes CI and limited signals security (SIGSEC) service support.

COUNTERINTELLIGENCE PRODUCTION

Analysis and production of CI information to meet the needs of the LIC commander take place at all levels with organic CI support. National level MDCI analysis and production are provided by the United States Army Intelligence Agency (USAIA). Information from all intelligence collection disciplines is used to develop a complete analysis of foreign intelligence and threat activities. Certain key production objectives include—

- Collating, analyzing, and evaluating information of CI significance.
- Preparing studies, estimates, and analysis of FISs and threat activities.
- Supporting contingency planning and major exercises.
- Providing analysis and summary of foreign collection and threat activities by geographic areas.
- Providing analysis and studies in support of major Army commands (MACOMs) and contingency mission forces dealing with the organization, methods of operation, personnel, and activities of FISs that pose a current or potential threat to US forces.
- Providing analysis and estimates of intelligence on the organization, location, funding, training, operations, and intentions of terrorist organizations.

COUNTERINTELLIGENCE COLLECTION

National level collection requirements for CI information are validated and issued by DIA. These consist of—

- Information objective: Tasking requiring input to complete intelligence production, maintain data bases, and support friendly planning and operations.
- Time-sensitive collection requirements: Tasking designed for use when collection and initial reporting must begin within 48 hours.
- Source-directed requirements: Tasking designed for a specific source or collection opportunity.

Guidelines for validating collection requirements for CI information are in DIAM 58-13, Volume I.

COUNTERINTELLIGENCE LIAISON AND COORDINATION

In overseas areas, MACOMs establish liaison programs with US, HN, and foreign agencies consistent with—

- Conducting strategic and operational liaison by EAC MI units.
- Conducting tactical MI unit liaison with LEAs and security agencies when liaison coverage is not otherwise available. Such local liaison is limited to matters within the operational charter of the tactical MI unit.

MULTIDISCIPLINE COUNTERINTELLIGENCE DATA BASE

The MDCI analyst develops the data base for the commander's AI in LIC. This data base includes the three disciplines of counter-HUMINT, counter-SIGINT, and counter-IMINT and is tailored to each operation, mission statement, and unit METL.

The MDCI analyst should be aware that one type of LIC operation may flow into another type of operation. For example, when supporting PCO, you will also be concerned with terrorism. Consequently, the MDCI data base requires constant updating and attention until mission completion.

This data base allows the MDCI analyst to produce MDCI threat and friendly vulnerability assessments in support of force protection. As a result, the MDCI analyst will also recommend that counter-HUMINT, counter-SIGINT, and counter-IMINT countermeasures be integrated into the commander's OPSEC and deception plans.

Lastly, the MDCI analyst will, as best he can, monitor the effectiveness of those countermeasures.

Ideally, the MDCI analyst has the opportunity to start the MDCI data base before the deployment or involvement of US forces. The MDCI data base is integrated into the main IPB data base of the ASPS.

MDCI analysts requires manual or automated access to many of the IPB products prepared by the all-source intelligence analyst. Details on IPB products are in Chapter 4. See FM 34-60 for details on counter-HUMINT, counter-SIGINT, and counter-IMINT data bases and sources.

MULTIDISCIPLINE COUNTERINTELLIGENCE ANALYSIS PROCESS

The MDCI analysis process follows the pattern of the counter-SIGINT process but has been expanded to include counter-HUMINT and counter-IMINT. The integration of counter-HUMINT, counter-IMINT, and counter-SIGINT analysis is a job for MDCI analysts with experience in one or more of those disciplines.

The MDCI analysis process provides input to the following intelligence products:

- Analysis of the area of operations (AAO); paragraph 2c, Additional Characteristics; and paragraphs 4a and 4b, Effects of Characteristics of the Area (on COAs). The AAO provides much of the pertinent information later included in the command and staff estimates, operations plan (OPLAN), and OPORD.
- MDCI annex to the AAO.
- MDCI annex to the Intelligence Estimate, and portions of the OPSEC, deception, PSYOP, and CA estimates.
- Intelligence annex to the OPLAN and OPORD; paragraph 6, Counterintelligence, and MDCI appendix.

The MDCI analysis process is accomplished by the CIAS at EACIC, corps main CP (intelligence cell), and division main CP. The CIAS must coordinate its efforts closely with the ASPS and G3 and S3 staff.

The MDCI analysis process in LIC is a five-step process which includes—

- Area evaluation.
- Threat assessment.
- Vulnerability assessment.
- Countermeasures options development.
- Countermeasures evaluation.

AREA EVALUATION

The purpose of area evaluation is to describe the threat, terrain, weather, and other characteristics of the LIC environment that will affect or influence mission accomplishment. The primary emphasis is on how terrain, weather, and other characteristics will affect FIS employment of its collection capabilities and security countermeasures. The impact of these conditions on Level I and Level II threat operations is also evaluated.

You also include the base area from which the LIC operation will be staged (for example, CONUS) as an extension of the LIC area evaluation. The FIS threat directed against the base area, prior to the deployment of the contingency force, cannot be ignored.

In order to accomplish this evaluation, you need the use of the AAO prepared by the ASPS. Also you must be thoroughly familiar with the IPB process described in Chapter 3 and FM 34-3.

The four tasks accomplished during area evaluation are shown in Figure C-2 and discussed below.

Task 1. Identify Pertinent IPB Terrain and Weather Products

The analysis of terrain and weather in the LIC area is necessary to determine their compound effects on friendly and threat collection systems. HUMINT, IMINT, and SIGINT sensors must have the capability to detect, locate, and track or monitor critical nodes in NAIs and TAIs.

It is important for you to know to what degree terrain and weather are affecting optical and electronic LOS of FIS systems to friendly critical nodes. HUMINT, IMINT, and SIGINT sensors, regardless of whether they are FIS or friendly, have different means of accessing the target. Terrain features work to the advantage or disadvantage of FIS systems.

Bad weather combined with air and ground movement problems may keep your sensors from

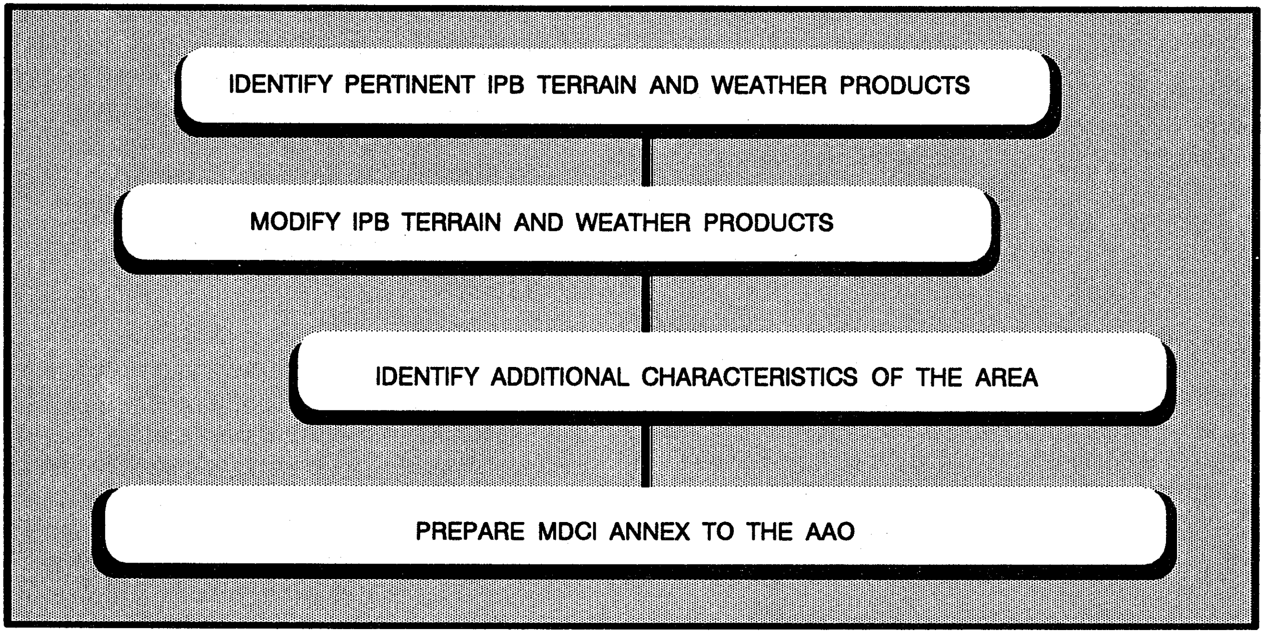

IDENTIFY PERTINENT IPB TERRAIN AND WEATHER PRODUCTS
MODIFY IPB TERRAIN AND WEATHER PRODUCTS
IDENTIFY ADDITIONAL CHARACTERISTICS OF THE AREA
PREPARE MDCI ANNEX TO THE AAO

Figure C-2. Area evaluation.

getting to vantage points or LOS positions to targets. You work to become as much an expert on terrain and weather as the local FIS and Level I and Level II threats operating in the area.

Task 2. Modify IPB Terrain and Weather Products

You may need to modify certain IPB overlays to a higher resolution or greater detail. The need for modifications is situation dependent. Support from the staff weather officer (SWO) and the engineer terrain analysis team may be required.

You may want to request current imagery of the area during various seasons of the year to update maps and other graphics. At a minimum, updates are necessary for those areas where manmade changes have occurred, such as new LOC or expansion of built-up areas.

Task 3. Identify Additional Characteristics of the Area

This is a key task. You tailor your effort to the specific LIC condition and operation identified in mission analysis. One such characteristic is the demographics of the area. This includes the ethnic, linguistic, religious, and education status of the people. People are *key terrain* in insurgency and counterinsurgency conditions and are usually the targets of influence in most types of LIC conditions.

There are centers of gravity (HN and hostile element) that you must identify. These are the social, political, economic, security, and organizational factors that generate and sustain the LIC condition. FIS and Level I and Level II threats will try to exploit these and other characteristics to their advantage.

Task 4. Prepare MDCI Annex to the AAO

You prepare the MDCI annex to the AAO in essentially the same format as the AAO (FM 101-5 and FM 34-3). The major goal is determining the effects of the AO on friendly and threat FIS COAs.

THREAT ASSESSMENT

Threat assessment is a continuous process that starts during the staff planning and does not end until the mission is completed. MDCI threat assessment is an integral part of the IPB process of threat evaluation (FM 34-130).

You are the commander's expert on how and with what systems the threat *sees* friendly forces and agencies in LIC. You know that complete information on the FIS and hostile intelligence and security services may be difficult to obtain. Facts and assumptions concerning the threat must be clearly understood relative to Who, What, When, Where, Why, and How.

The following is a list of the PIR and IR concerning the functions and capabilities of a threat FIS. Both internal and external capabilities must be addressed:

- Leadership and organization.
- C^3 system.
- All-source collection capabilities.
- Third-country intelligence and security IDAD support.
- CI capabilities and countermeasures.
- Counterinsurgency doctrine and infrastructure.
- Military and paramilitary forces.
- Public information and PSYOP agencies.
- Demographics.

The MDCI threat assessment includes the six tasks shown in Figure C-3 and discussed below.

Task 1. Identify Threat Systems in the Geographic AOR

The following specific threat capabilities should be identified within the geographic AO:

- HUMINT, SIGINT, and IMINT systems of the threat FIS.
- Espionage.
- Subversion.
- Terrorism.

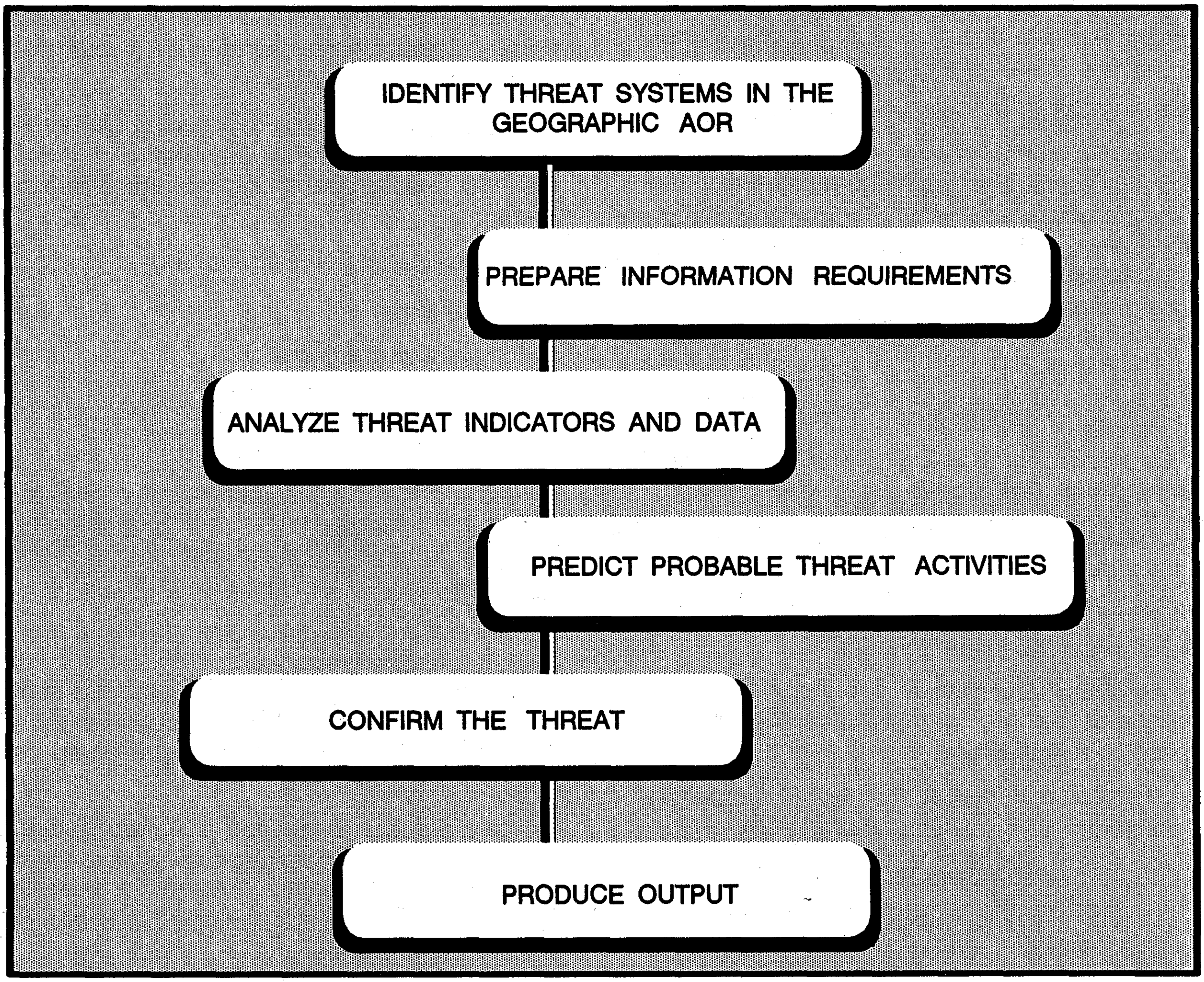

IDENTIFY THREAT SYSTEMS IN THE GEOGRAPHIC AOR
PREPARE INFORMATION REQUIREMENTS
ANALYZE THREAT INDICATORS AND DATA
PREDICT PROBABLE THREAT ACTIVITIES
CONFIRM THE THREAT
PRODUCE OUTPUT

Figure C-3. MDCI threat assessment.

- Sabotage.

The primary objective of this task is to determine the specific FIS threat faced by friendly forces. One or more of the above threats may be present in each of the four operational categories of LIC. You anticipate the use of both human and technical means when considering each category of threat.

You will consult all-source intelligence products of national producers, such as INSCOM and DIA, for this information.

The SOF area study described in FM 34-36 is an excellent source on threat forces in the AO.

Task 2. Prepare Information Requirements

You identify information gaps and submit requests for information through the CM&D to national level agencies. These agencies include DIA, INSCOM, DOD collectors, and country teams in the AO and AI.

Task 3. Analyze Threat Indicators and Data

You review, organize, and evaluate all key information components relative to each hostile intelligence system capability. The purpose is to identify the signatures, patterns, and profiles of each FIS and hostile intelligence and security service. Included are indicators that technical collection means are being changed or upgraded. Lastly, you attempt to determine hostile intentions.

Task 4. Predict Probable Threat Activities

The purpose of this task is to identify the threat activities. To do this, you—

- Correlate FIS system capabilities and intentions to target US forces and supported units' critical nodes.
- Use doctrinal and situation templating techniques to assist in this predictive process.
- Integrate, through the use of overlays, the effects of terrain and weather on hostile intelligence collection capabilities.
- Use standard or specially produced IPB products in this process (FM 34-3 and FM 34-60).

Task 5. Confirm the Threat

You verify the threat prediction. You also validate existing data and information concerning FIS systems, request additional data, as necessary, and evaluate and integrate new information into the threat prediction. New requests for information are forwarded to the appropriate CM&D.

Task 6. Produce Output

The final MDCI threat assessment product is integrated into the MDCI annex to the AAO, SOF area studies, and the MDCI annex to the intelligence estimate. It also provides input to the G3 OPSEC estimate and various other staff estimates. (The format for the MDCI annex in Figure F-3 is similar to the format for the OPSEC estimate prepared by the G3.)

VULNERABILITY ASSESSMENT

The MDCI vulnerability assessment determines the centers of gravity and critical operational nodes of the LIC operation, and the specific areas where the threat FIS can be most damaging to friendly forces.

You (with the assistance of the G2, G3 staff, and the C-E officer) examine the technical and operational characteristics of the LIC force.

You prepare doctrinal templates of LIC friendly force critical nodes for each COA identified in the OPLAN. Initially, you will focus on five areas of concern:

- Command and communications.
- Intelligence.
- Operation and maneuver.
- Logistics.
- Administrative support.

These doctrine templates portray the physical and electronic characteristics of friendly force critical nodes. This is the same analytical technique the intelligence analyst uses in IPB to template the threat.

General purpose forces employed in LIC may retain their signature and pattern of activity. It is the combination of signature and patterns that produces the profile that FISs attempt to detect and evaluate. It is also the profile that Level I and Level II threats target against.

Each civilian, military, and police activity in LIC has an electronic and physical signature. People adopt habits over time which provide a basis for predicting what the unit or agency will do next. SOPs are a good example of habit patterns.

Threats at Level I and Level II exploit the *profile* of a unit or agency as the basis for espionage, subversion, and sabotage targeting. Guerrillas and terrorists also exploit profiles of individuals, units, and activities. FIS systems target both physical and electronic signatures to locate and identify units and agencies.

You, and your G3 counterpart, must work together to become experts on how friendly forces *look* to the threat. Your goal is to ensure that friendly profiles remain obscure and ambiguous.

The MDCI vulnerability assessment shown in Figure C-4 is described below. (You will complete tasks 5 through 10 as part of the wargaming COA process conducted by the G3 or S3.)

Task 1. Compile Friendly Force Characteristics

You determine the mission, task organization, and deployment scheme for the particular type of LIC forces and operation under assessment. If the operation is conducted in phases, then the assessment will focus on characteristic force profiles during each phase. You have an advantage over your threat counterpart due to 100 percent knowledge of *ground truth.*

Consult FM 34-60 for details concerning the C-E equipment characteristics of friendly forces. Additional sources of information include doctrinal publications and pertinent tables of organization and equipment (TOE), modified tables of organization and equipment (MTOE), tables of distribution and allowance (TDA), and unit SOPs.

You use imagery in assessing the physical characteristics of the command. Imagery products can be requested from national level production centers of all facilities, training areas, logistics sites, marshalling yards, and unit locations in the base area. Photographs are also requested of the AI and the AO for a look before, during, and after deployment of US forces.

You are not the only user of this imagery. Tasking for this support should be coordinated through your G2.

Your assessment of the human characteristics of the command is more ambiguous. You should refer to INSCOM and command security A&A program reports, the command security SOP, and consult with the security officer about the status and effectiveness of the following programs:

- Personnel security.
- Information security.
- ADP security.
- SAEDA.
- Physical security.

Task 2. Determine Friendly Force Profiles

The MDCI analyst conducts analysis of the signatures and patterns of C-E equipment, physical layouts, and human security activities to produce an MDCI profile of the force (signatures + patterns = profile). FM 34-60, Appendix A, provides details on the subtasks to be performed in this analytical process. You will adapt the process for physical and human applications as required.

Figure C-5 is a template of how the vehicles and equipment constituting a corps main CP might be arranged on the ground. You construct templates to map scale and arrange antennas, vehicles, and supporting equipment according to command guidance, terrain limitations, and other conditions. The template may portray a *type,* planned, or actual arrangement.

Task 3. Identify Force Susceptibilities

A susceptibility is defined as the degree to which a profile consisting of an item of C-E equipment, a weapon system, physical feature, or human entity is open to effective FIS exploitation due to weaknesses. Any susceptibility is a potential vulnerability.

C^3I, operations, and maneuver nodes and elements have both physical and electronic signatures. How these nodes and elements are arranged in a geographical area during each phase of the LIC operation (base area to target area) is governed by doctrine and the elements of METT-T. Hence, a profile is established which may be unique to a particular unit and aid in identification and location.

A certain type of vehicle or antenna associated with SOF units and operations are examples of physical signatures. These items are subject to both hostile human and imagery verification. When the antenna is transmitting, it exhibits an electronic signature and is open to hostile electronic intercept and exploitation.

Groups of vehicles, antennas, weapon systems, and associated equipment establish identifiable patterns. Humans create the observable patterns of activity that provide indicators of *intentions.* These patterns need to be protected from threat exploitation.

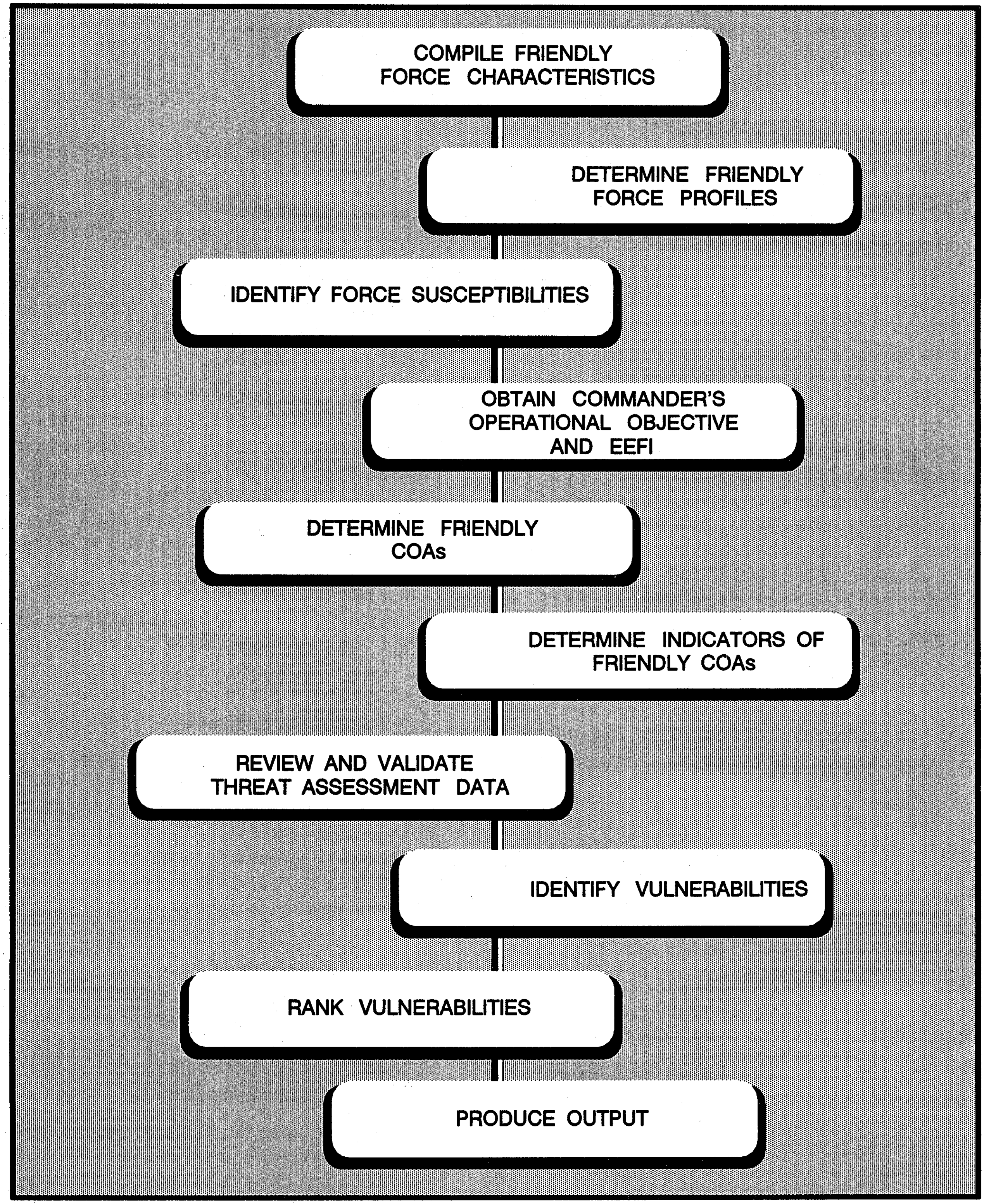

COMPILE FRIENDLY FORCE CHARACTERISTICS
DETERMINE FRIENDLY FORCE PROFILES
IDENTIFY FORCE SUSCEPTIBILITIES
OBTAIN COMMANDER'S OPERATIONAL OBJECTIVE AND EEFI
DETERMINE FRIENDLY COAs
DETERMINE INDICATORS OF FRIENDLY COAs
REVIEW AND VALIDATE THREAT ASSESSMENT DATA
IDENTIFY VULNERABILITIES
RANK VULNERABILITIES
PRODUCE OUTPUT

Figure C-4. Vulnerability assessment.

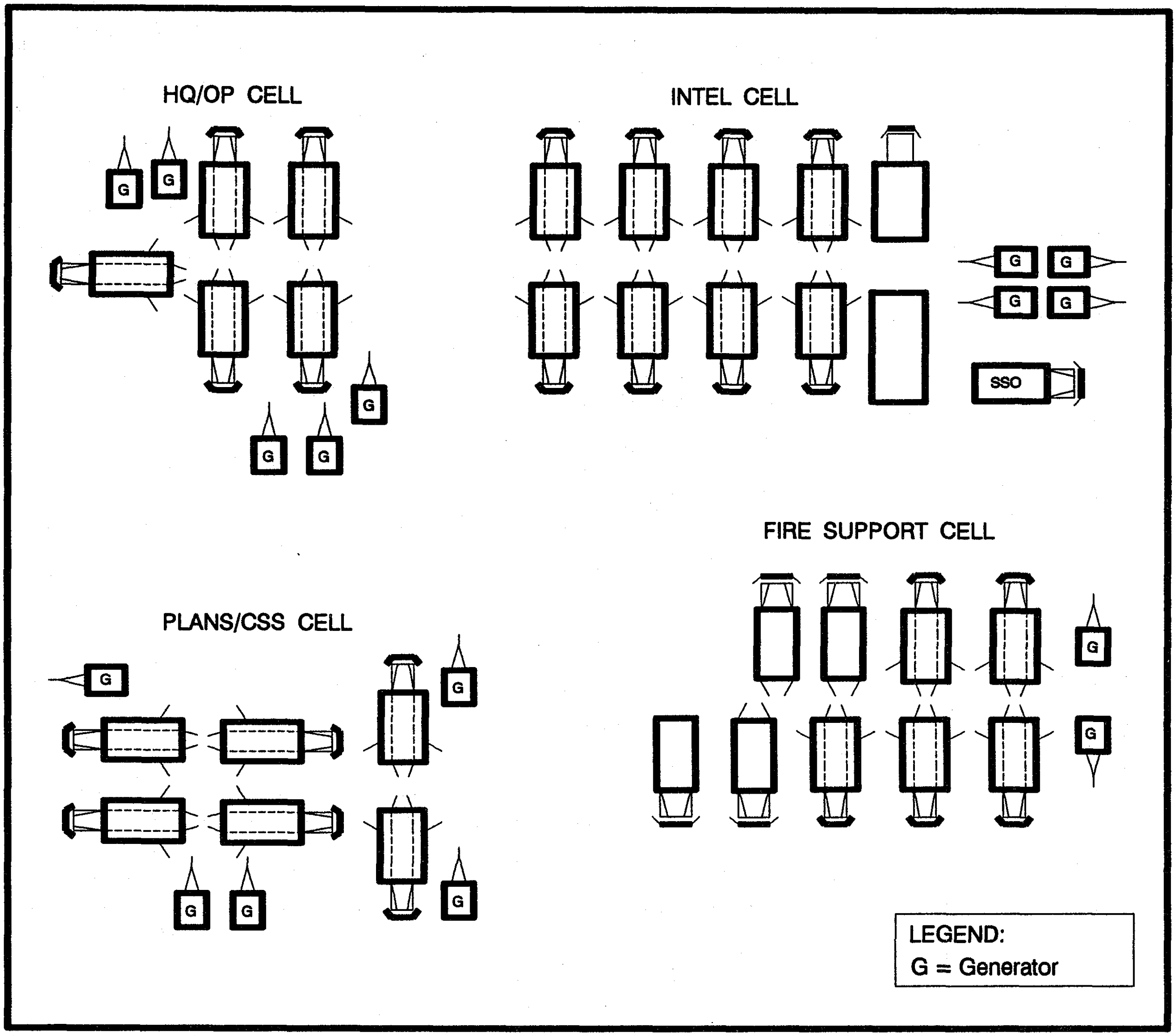


Figure C-5. Type template suggesting a corps main CP.

You need to construct friendly critical node templates. The details needed to construct these templates come from a variety of sources:

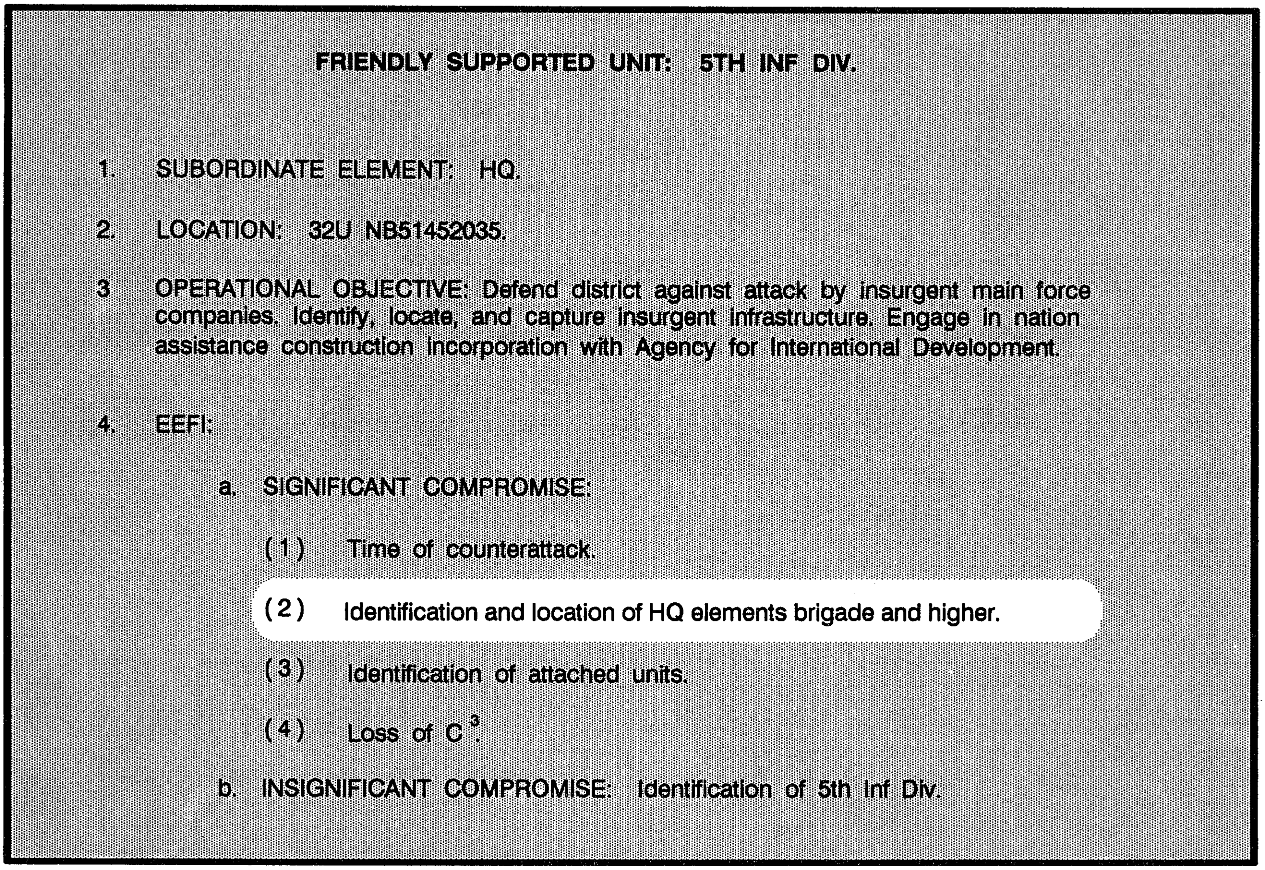
- Operations element.
- Unit SOP.
- Installation engineer.
- Personal observation.
- Imagery products.

Events such as a field training exercise (FTX) or a command post exercise (CPX) can also provide opportunities for collection and evaluation efforts prior to friendly deployment in LIC.

Task 4. Obtain Commander's Operational Objective and EEFI

In coordination with the G2 and G3, review existing OPLAN and OPORD to determine the commander's intent, operational concept, and pertinent EEFI relative to COA. EEFI are also identified as a result of the war-gaming of the COA process.

Figure C-6 is an example of a statement of EEFI. In paragraph 4a, four EEFI have been listed as *indicators*



FRIENDLY SUPPORTED UNIT: 5TH INF DIV.

1. SUBORDINATE ELEMENT: HQ.

2. LOCATION: 32U NB51452035.

3 OPERATIONAL OBJECTIVE: Defend district against attack by insurgent main force companies. Identify, locate, and capture insurgent infrastructure. Engage in nation assistance construction incorporation with Agency for International Development.

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 C-6. Sample essential elements of friendly information statement.

of a friendly COA. Paragraph 4a(2) is highlighted and will be referred to throughout the following discussion.

This information enables you to evaluate the indicators of a friendly COA which the commander considers essential to the success of the mission. These EEFI, therefore, require protection from hostile intelligence collection systems.

Task 5. Determine Friendly COAs

A COA consists of—

- One or more units.
- A series of events accomplished.
- Various locations on the ground, or in the air.
- Certain times.
- A given duration.

The commander's operational objective is described briefly in paragraph 3; for example (5th Inf Div), "Defend to PL Gray, counterattack at 300001Z Oct 92." You can request other supporting materials such as overlays that describe the scheme of maneuver in more detail through the G2 or S2 from the G3 and S3.

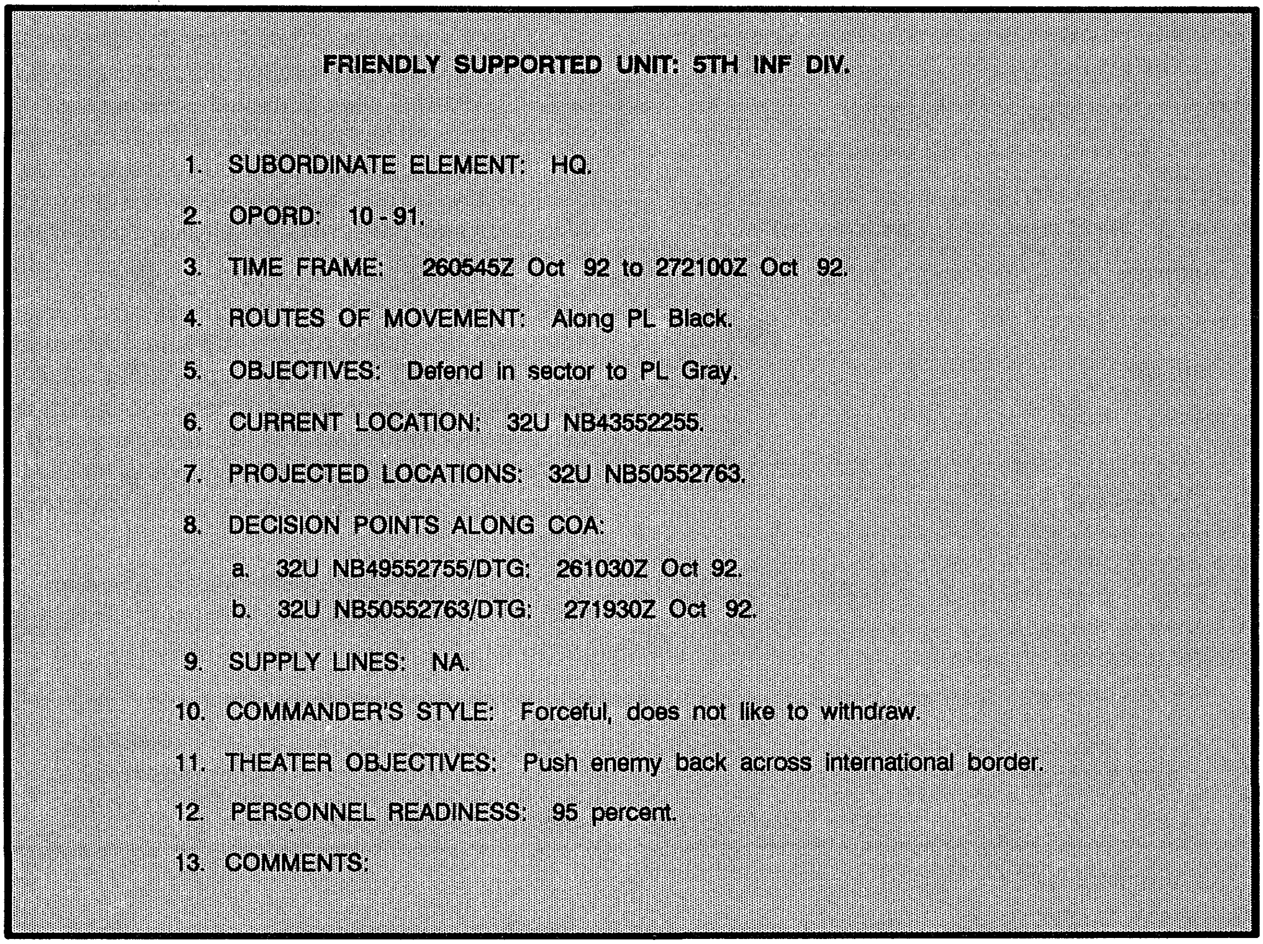
A COA may also have built-in options. The COA adopted by the commander receives priority attention. A COA may also include elements of a deception plan as well as SOP OPSEC measures.

Figure C-7 is an example of a friendly COA event list similar to the one the MDCI analyst might prepare. The use of map overlays is recommended. The G2 or S2 should cross-walk the COA with the G3 and S3 to ensure accuracy.

You compare the COA elements to EEFI and determine which elements, if detected by threat intelligence or target acquisition systems, might compromise the EEFI.

Task 6. Determine Indicators of Friendly COAs

You correlate friendly force profiles (Task 2) to the COA. As units execute a COA, they will be shooting,



FRIENDLY SUPPORTED UNIT: 5TH INF DIV.

1. SUBORDINATE ELEMENT: HQ.
2. OPORD: 10 - 91.
3. TIME FRAME: 260545Z Oct 92 to 272100Z Oct 92.
4. ROUTES OF MOVEMENT: Along PL Black.
5. OBJECTIVES: Defend in sector to PL Gray.
6. CURRENT LOCATION: 32U NB43552255.
7. PROJECTED LOCATIONS: 32U NB50552763.
8. DECISION POINTS ALONG COA:
   a. 32U NB49552755/DTG: 261030Z Oct 92.
   b. 32U NB50552763/DTG: 271930Z Oct 92.
9. SUPPLY LINES: NA.
10. COMMANDER'S STYLE: Forceful, does not like to withdraw.
11. THEATER OBJECTIVES: Push enemy back across international border.
12. PERSONNEL READINESS: 95 percent.
13. COMMENTS:

Figure C-7. Friendly course of action event list.

moving, and communicating. They will enter into threat NAIs which provide opportunities for threat intelligence collection or targeting.

In a LIC operation, friendly COA analysis is not as complex as COA analysis for general purpose forces in a mid-intensity conflict (MIC) or high-intensity conflict (HIC). On the other hand, COA options may be more limited depending on which of the four LIC conditions is involved.

Protecting vital EEFI is important to the success of any mission. Indicators are combinations of EEFI relative to a COA that, if known to the threat and properly interpreted, would compromise the COA.

You will also evaluate the effects of METT-T on the indicators in each COA and will determine the degree to which indicators may be masked to threat detection. You will use IPB terrain and weather effects overlays in this effort. Combinations of indicators tend to reveal friendly intentions to the threat commander.

Task 7. Review and Validate Threat Assessment Data

You use the threat IEW systems templates and overlays prepared during threat assessment and determine which threat HUMINT, SIGINT, and IMINT systems are likely to be directed against a friendly COA.

You include in your threat assessment any new data that might apply. You select only those threat capabilities that are relevant to the situation and COA.

Task 8. Identify Vulnerabilities

You compare the FIS collection effort to the friendly unit susceptibilities (Task 3) to determine vulnerabilities. A susceptibility that is *targetable* by a specific threat collector becomes a vulnerability.

You must correlate indicators to each vulnerability. Then you identify the specific COA elements affected (for example, time and location).

Task 9. Rank Vulnerabilities

You rank the vulnerability according to its bearing on the success of the mission. These ranks are—

- Unimportant.
- Important.
- Significant.
- Critical.

Figure C-8 is an example of an MDCI vulnerability matrix. The threat is assumed to have a viable HUMINT, SIGINT, and IMINT capability. The division tactical operations center (DTOC) is the critical EEFI to be protected. Its profile is the indicator that, if known to the enemy, will reveal the COA and the friendly commander's intention.

DTOCs and other C^2 and C^3I nodes have profiles consisting of C-E equipment (radios, antennas, and vehicles), assorted work tents, and other types of vehicles arranged in a standard doctrinal arrangement. The situation template of a DTOC contains all the essential physical and technical characteristics of that node integrated into a weather, terrain, and operational condition profile.

Knowing this, the analyst can determine if the node, at a certain time and place, is more vulnerable to threat HUMINT, IMINT, or SIGINT exploitation. Human observation and reporting of antenna configurations pose a greater initial threat in LIC than the probability of intercept; particularly during periods of planned radio silence or given the absence of a viable threat DF capability.

Analysts rank the vulnerabilities within each intelligence discipline and then prepare an integrated

VULNERABILITY		CRITERIA			OVERALL NUMERICAL RATING
	EEFI	UNIQUENESS	IMPORTANT	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
Indigenous work parties have visual or escorted access to DTOC area.	4 a (1)(2)(3)	5	5	5	15

CRITERIA RATING VALUES

0 - 2 = Low
3 = Medium
4 - 5 = High

OVERALL RATING VALUES

0 - 4 = Unimportant
5 - 8 = Important
9 - 11 = Significant
12 - 15 = Critical

Figure C-8. Multidiscipline counterintelligence vulnerability matrix.

MDCI rank listing. (See Figure C-8 for a numerical scale that can be used or modified as required.)

Task 10. Produce Output

Figure C-9 is a format for an MDCI vulnerability assessment. Vulnerability assessments for each intelligence discipline are integrated into the MDCI vulnerability assessment. You may prepare this as a document or as a graphic. It is integrated into the MDCI annex to the intelligence estimate and the OPSEC estimate.

COUNTERMEASURES OPTIONS DEVELOPMENT

The MDCI countermeasures options development steps are shown in Figure C-10 and are discussed below.

During countermeasures development, review the C-E, physical, and human entity vulnerabilities. Identify, analyze, prioritize, and recommend specific options for controlling, eliminating, or exploiting the vulnerabilities. Countermeasures are required to prevent or degrade FIS exploitation of friendly force vulnerabilities. Collect the data and analyze it to determine countermeasures.

Task 1. Identify MDCI Countermeasures Options

Construct MDCI vulnerability to countermeasures matrices for profile (C-E, physical, and human entity) vulnerabilities. Figure C-11 is an example of this matrix. Two or more can be combined when the same countermeasures apply. Each vulnerability should have at least one countermeasure option.

Vulnerabilities with the highest numerical rating should be listed accordingly in the countermeasures matrix.

Task 2. Determine Relative Benefit of Each Option

Figure C-12 is an example of an MDCI relative benefit options table. Each vulnerability is analyzed relative to each countermeasure option (CM-O), as well as—

- Human, equipment, logistical resources, and time required to implement the CM-O.
- Expected results if a specific CM-O is implemented.
- Impact on operations.
- Shortfalls.

Task 3. Perform Risk Assessment

Risk assessment is a judgmental effort that you use to predict the element of risk to operations when CM-Os are not applied or do not successfully protect the EEFI. Figure C-13 is an example of risk factor (RF) calculations.

Task 4. Produce Output

The CM-O process is completed when you review and recommend countermeasures to the G3 OPSEC element. Countermeasures recommendations for each COA are coordinated with the G3 during the staff estimate sequence.

COUNTERMEASURES EVALUATION

MDCI countermeasures evaluation includes the four tasks shown in Figure C-14 and discussed below.

Attempt to determine how well the countermeasures that were implemented actually achieved the expected results. Since each CM-O was developed in consonance with the commander's intent, EEFI, and COAs, first determine if any of those factors changed prior to or during the time frame that the CM-O was in effect.

Task 1. Determine Changes in the Commander's Guidance

Check for modifications made during the execution of the OPORD that would impact on the effectiveness of the CM-O.

Review fragmentary orders (FRAGOs) or verbally debrief the G3 and S3. You also review the results of specific OPSEC surveys conducted in coordination between the G2 and G3.

Task 2. Evaluate the Accomplishment of the CM-O Relative to the Execution of the Pertinent COA and Any Changes Identified in Task 1

Analysts review current intelligence reports during the period under review to determine threat reaction to the CM-O and the effectiveness of the CM-O.

You review pertinent IEW operational reports to verify that the CM-O was implemented, that adequate resources were available, and that the impact on operations was within expectations.

Your evaluation becomes more complex if CM-Os from two or more intelligence disciplines were implemented to protect the same EEFI.

For example: A counter-SIGINT CM-O to protect EEFI, paragraph 4a(2), may have been implemented but was negated because a counter-HUMINT CM-O failed. Since there are limited numbers of CM-Os within the HUMINT, IMINT, and SIGINT disciplines, you will have to be objective when evaluating the effectiveness of CM-Os.

Task 3. Summarize the CM-O Evaluation and Identify Fixes

You may be unable to verify CM-O effectiveness due to the lack of data. You can, however, identify shortfalls that you can fix. You can also assign a numerical rating from 0 to 5 to indicate how successful a countermeasure was for your next risk assessment.

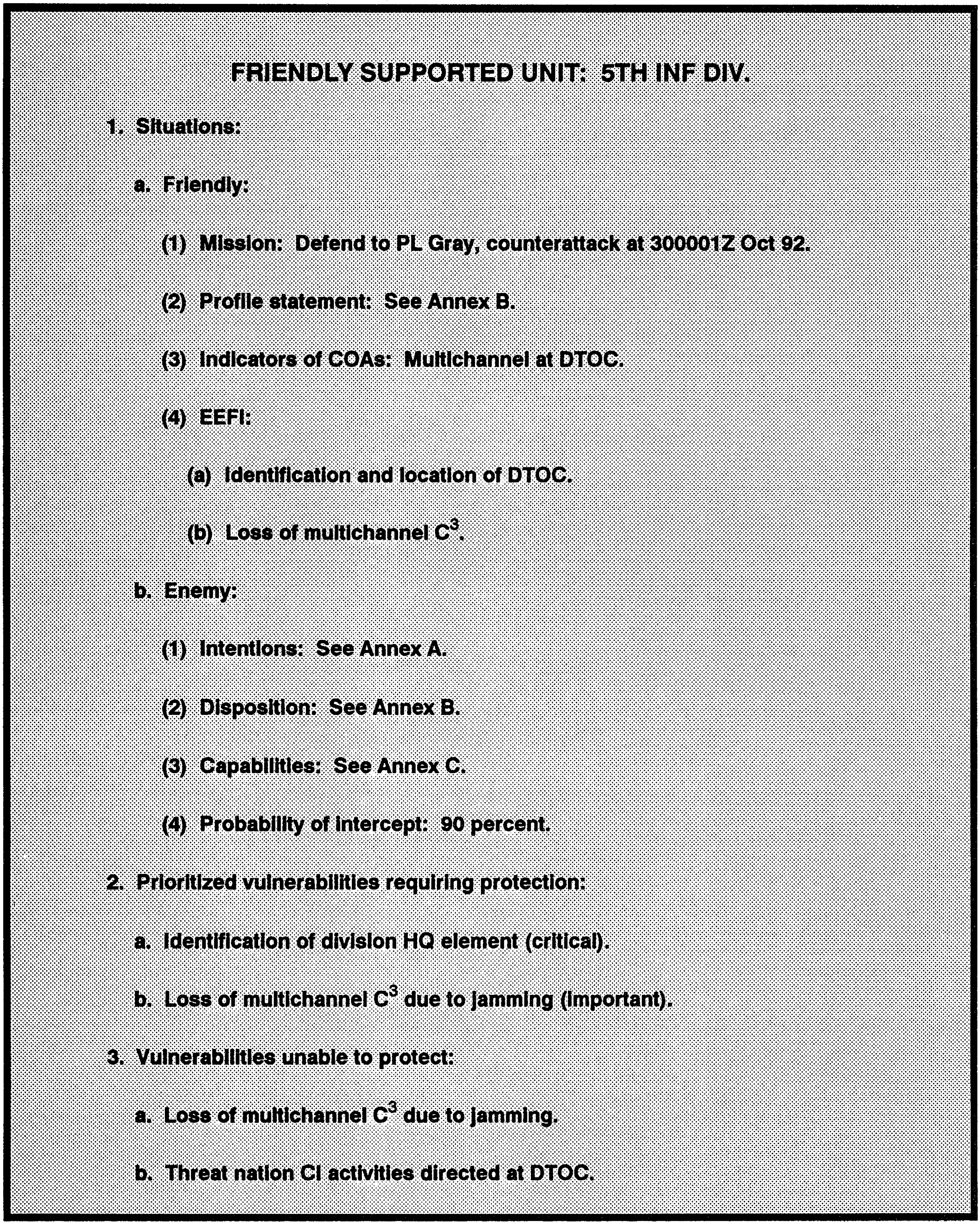
Task 4. Prepare an AAR

Prepare an AAR in accordance with local SOPs for the G2, G3, and other designated staff elements. The AAR is provided to assist in—

- Modifying countermeasures.
- Developing countermeasures.
- Analyzing training.
- Reviewing lessons learned.

POST MISSION ACTIONS

After the mission is completed, you must update threat HUMINT, IMINT, and SIGINT data bases with pertinent data. This includes reviewing and revising templates of threat intelligence collection systems and friendly critical nodes.



FRIENDLY SUPPORTED UNIT: 5TH INF DIV.

1. Situations:

a. Friendly:

(1) Mission: Defend to PL Gray, counterattack at 300001Z Oct 92.

(2) Profile statement: See Annex B.

(3) Indicators of COAs: Multichannel at DTOC.

(4) EEFI:

(a) Identification and location of DTOC.

(b) Loss of multichannel C^3.

b. Enemy:

(1) Intentions: See Annex A.

(2) Disposition: See Annex B.

(3) Capabilities: See Annex C.

(4) Probability of intercept: 90 percent.

2. Prioritized vulnerabilities requiring protection:

a. Identification of division HQ element (critical).

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

3. Vulnerabilities unable to protect:

a. Loss of multichannel C^3 due to jamming.

b. Threat nation CI activities directed at DTOC.

Figure C-9. Format for MDCI vulnerability assessment.

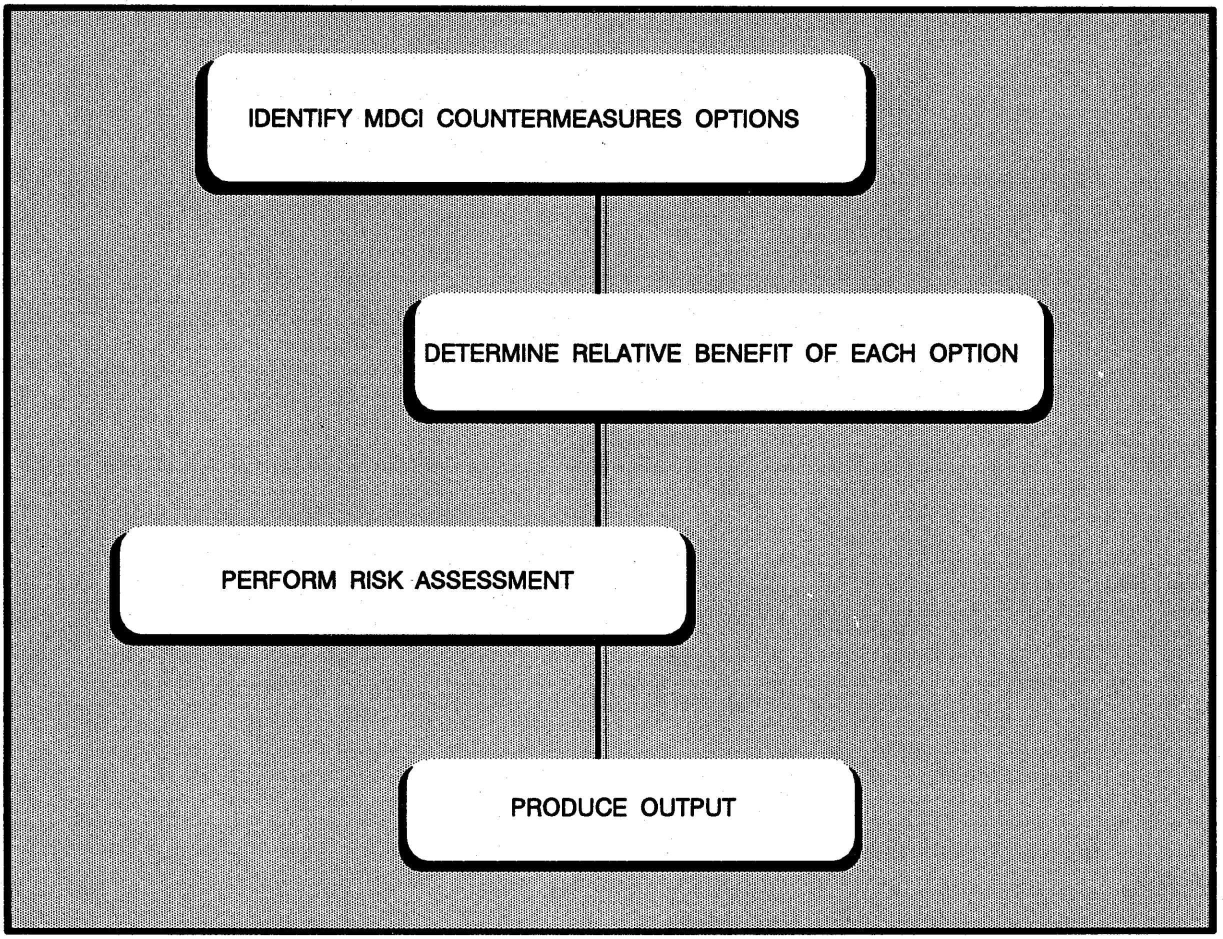

IDENTIFY MDCI COUNTERMEASURES OPTIONS
DETERMINE RELATIVE BENEFIT OF EACH OPTION
PERFORM RISK ASSESSMENT
PRODUCE OUTPUT

Figure C-10. Countermeasures options development.

COUNTER-MEASURES OPTIONS VULNERABILITY	REMOTE EQUIPMENT	USE DESTRUCTION	PLACE EQUIPMENT AT ANOTHER ECHELON	USE OTHER EQUIPMENT	USE DECEPTION	LIMIT HN ACCESS
Indigenous work parties have visual or escorted access to the DTOC area.						X
Multichannel vulnerable to intercept.	X	X	X		X	
Multichannel vulnerable to jamming.		X		X	X	

Figure C-11. Vulnerability to countermeasures matrix.

VULNERABILITY OF DTOC MULTICHANNEL EQUIPMENT TO INTERCEPTION

COUNTER-MEASURES	RESOURCES	EXPECTED RESULTS	IMPACT ON OPERATIONS	SHORTFALLS
Remote multichannel. CMS = 5 (High) R F = 0 (Low)	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.	Communications needs high maintenance. May have to replace wire. Wire needs to be guarded.
Use destruction. CMS = 5 (High) R F = 0 (Low)	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. CMS =3(Medium) R F =0(Medium)	Personnel Time Vehicles Fuel Food	Make the threat think the other echelon is the division.	SIGINT and DF may not think the division moved.	Fired upon before reaching new location. New location may not have trained personnel for multichannel equipment.
Use deception. CMS = 0 (Low) R F = 5 (High)	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.

CMS = Countermeasures past success

R F = Risk factor

Formula: EEFI/V –CMS = RF

EEFI - 4a(2)

EEFI - Vulnerability (EEFI/V = 5)

Figure C-12. Relative benefit options table.

THE MDCI ANALYST PREPARES THE FOLLOWING TWO SCALES:

EEFI VULNERABILITY SCALE	CM-O PAST SUCCESS SCALE
5 = Critical	5 = High
3 = Significant	3 = Medium
1 = Important	1 = Marginal
0 = Unimportant	0 = Failure

The CI analyst applies the following formula to determine the numerical RF:

EEFI/V – CMS = RF

The calculations can be incorprated into the existing MDCI relative benefit options table. A numerical RF of 4 to 5 equates to High Risk; an RF of 2 to 3 is Medium Risk, and an RF of 0 to 1 is Low Risk.

Figure C-13. Risk factor calculations.

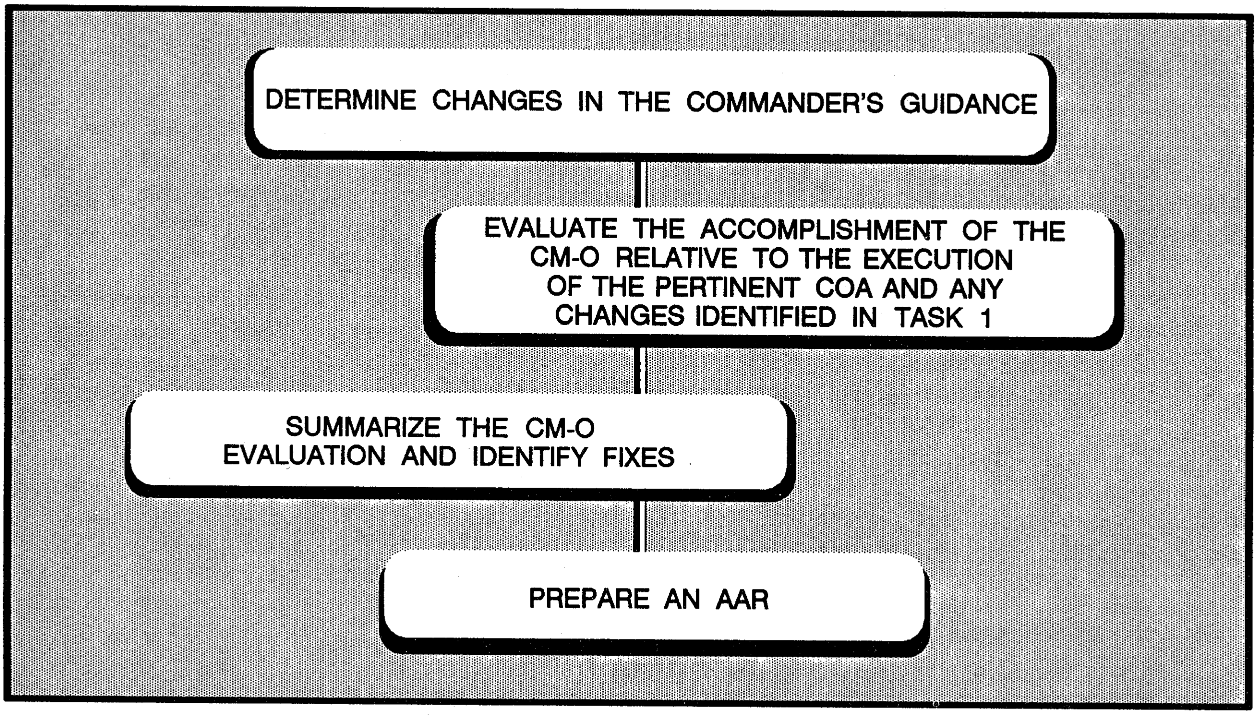

DETERMINE CHANGES IN THE COMMANDER'S GUIDANCE
EVALUATE THE ACCOMPLISHMENT OF THE CM-O RELATIVE TO THE EXECUTION OF THE PERTINENT COA AND ANY CHANGES IDENTIFIED IN TASK 1
SUMMARIZE THE CM-O EVALUATION AND IDENTIFY FIXES
PREPARE AN AAR

Figure C-14. Countermeasures evaluation.

APPENDIX D
COLLECTION PLAN FORMATS AND INSTRUCTIONS

Although there is no prescribed collection plan format, we recommend the two formats described here for two reasons: They can be easily tailored to support your mission or unit requirements, and they list the collection assets available to you.

STANDARD COLLECTION PLAN FORMAT

The first format is designed to support most conventional battlefield collection management (CM) requirements and some specific military combat operations in a LIC environment. Figure D-1 shows an example of this type of collection plan format.

Figure D-2 gives instructions on how to fill out the major parts of the collection plan format. Additional details on the CM process and this collection plan are in FM 34-1 and FM 34-2.

The standard collection plan format is a valuable aid during all phases of the CM process. Written collection plans help the CMO focus his efforts and work toward solving PIR and IR, such as threat capabilities and vulnerabilities.

The amount of detail needed, of course, depends on the particular requirement to be satisfied and the amount of overall collection effort required. For some operations, a collection plan might be as simple as a list of available collection resources, brief notes, reminders about current intelligence requirements, or specific information that must be collected. For other operations, more complex plans may be required.

LIC operations often have several PIR and IR that require detailed analysis and extensive collection effort over longer periods. Figure D-3 shows examples of LIC PIR and IR developed for support to a counterinsurgency.

THE DISPERSED BATTLEFIELD COLLECTION PLAN FORMAT

The second format is designed to support dispersed battlefield collection management requirements. This format is particularly suited to meet LIC CM requirements and is the tool you use to manage and answer the large amount of highly diverse PIR and IR generated in a dispersed environment.

Although detailed, the format simplifies CM tasks and can be filled out manually or by computer. It assists in identifying, collecting, and reporting tasks during all phases of the CM process as shown in Figure D-4.

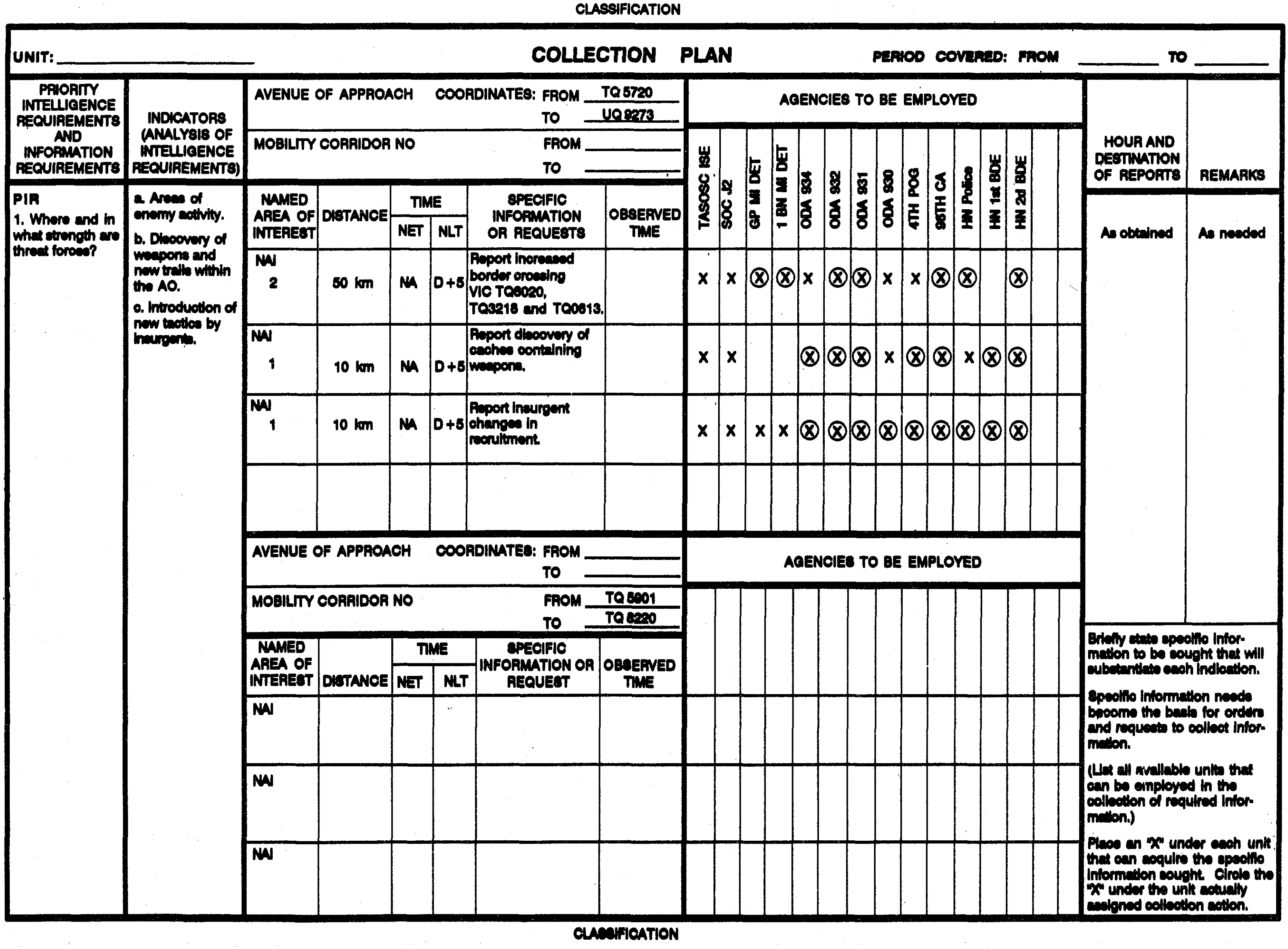
The format is easy to use and requires only four steps:

- List and prioritize PIR and IR—assign PIR numbers and IR letters for control and prioritization.
- Determine potential indicators—prioritize those that will answer the PIR and IR. Any indicator that does not answer the PIR or IR is deleted.
- Determine specific information requirements (SIR)—analyze the indicators and target characteristics. Then prioritize the SIR and determine the appropriate collectors.
- Prepare the tasking list—task the various collectors with an easy-to-read and understandable prioritized SIR list.

LIST AND PRIORITIZE PIR AND IR

The first step is to list and prioritize the PIR and IR. As in all collection plans, the dispersed battlefield collection plan format is designed to assist the G2 or S2 in answering the commander's PIR.

However, these PIR and IR are not immediately added to the collection plan. Instead, they are posted next to the plan and given numerical and alphabetical designators, as shown in Figure D-5. The most important PIR is 1, the next is 2, and so on. IR are given alphabetical designators and prioritized the same way as PIR. This allows collection managers to continually add, revise, and reprioritize PIR and IR. Use these numbers and letters in the PIR and IR column on the collection plan to cross-reference specific PIR or IR.



CLASSIFICATION

UNIT: ____________ **COLLECTION PLAN** PERIOD COVERED: FROM ________ TO ________

AVENUE OF APPROACH COORDINATES: FROM TQ 5720 TO UQ 9273

MOBILITY CORRIDOR NO FROM ________ TO ________

AGENCIES TO BE EMPLOYED

PRIORITY INTELLIGENCE REQUIREMENTS AND INFORMATION REQUIREMENTS	INDICATORS (ANALYSIS OF INTELLIGENCE REQUIREMENTS)	NAMED AREA OF INTEREST	DISTANCE	TIME		SPECIFIC INFORMATION OR REQUESTS	OBSERVED TIME	TASOSC ISE	SOC J2	GP MI DET	1 BN MI DET	ODA 934	ODA 932	ODA 931	ODA 930	4TH POG	96TH CA	HN Police	HN 1st BDE	HN 2d BDE			HOUR AND DESTINATION OF REPORTS	REMARKS
				NET	NLT																			
PIR 1. Where and in what strength are threat forces?	a. Areas of enemy activity. b. Discovery of weapons and new trails within the AO. c. Introduction of new tactics by insurgents.	NAI 2	50 km	NA	D+5	Report increased border crossing VIC TQ6020, TQ3218 and TQ0613.		X	X	⊗	⊗	X	⊗	⊗	X	X	⊗	⊗		⊗			As obtained	As needed
		NAI 1	10 km	NA	D+5	Report discovery of caches containing weapons.		X	X			⊗	⊗	⊗	X	⊗	⊗	X	⊗	⊗				
		NAI 1	10 km	NA	D+5	Report insurgent changes in recruitment.		X	X	X	X	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗				

AVENUE OF APPROACH COORDINATES: FROM ________ TO ________

MOBILITY CORRIDOR NO FROM TQ 5901 TO TQ 6220

AGENCIES TO BE EMPLOYED

NAMED AREA OF INTEREST	DISTANCE	TIME		SPECIFIC INFORMATION OR REQUEST	OBSERVED TIME
		NET	NLT		
NAI					
NAI					
NAI					

Briefly state specific information to be sought that will substantiate each indication.

Specific information needs become the basis for orders and requests to collect information.

(List all available units that can be employed in the collection of required information.)

Place an "X" under each unit that can acquire the specific information sought. Circle the "X" under the unit actually assigned collection action.

CLASSIFICATION

Figure D-1. Standard collection plan format with sample entries.

PIR and IR	INDICATORS	SIR	COLLECTION AGENCIES	PLACE and TIME to REPORT	REMARKS
	INSTRUCTIONS				
List PIR and IR. Leave sufficient space to list indicators for each PIR and in IR column 2.	List indicators that will satisfy each PIR.	Then, if necessary, list specific information required to satisfy the indicator. Key requirements to NAI on the event template if possible. These requirements form the basis for specific orders and requests.	Place an "X" under each agency that can collect the required information. Circle the "X" when an agency has been selected and tasked.	Place may be a headquarters or unit. Time may be specific, periodic, or as obtained.	Include means of reporting; for example, via spot report format. Include established communications; for example, multichannel, frequency modulated, RATT, or state "by SOP" if SOP criteria applies for responding to collection requirements.
	EXAMPLE				
Where and in what strengths are threat forces?	Discovery trails within the AO.	Report increased border crossing vic 5D47-5042 to Seine River.			

Figure D-2. Instructions for filling out the major parts of a standard collection plan format.

PIR

- ○ Where and in what strengths are insurgent forces in the AO?
- ○ Where and how is the threat applying the elements of power (military, informational, economic, and political) in the AO?
- ○ Where is there a lack of military or political indicators in the AO?
- ○ Will the population in the target area be supportive, hostile, or neutral toward friendly operations?
- ○ What type of surface- to- air capability does the threat have?

IR

- ○ What is the strength of popular support for the threat?
- ○ How, where, when, and by whom will the threat be resupplied and reinforced?
- ○ What reactions will nonbelligerent third parties have toward friendly operations?
- ○ What are the friendly, threat, and nonbelligerent third- party organizations in the AO?

Figure D-3. Some examples of LIC PIR and IR.

DETERMINE POTENTIAL INDICATORS

Second, determine what activities in, or characteristics of, the operational area will answer the PIR and IR. This procedure is called determining indicators. An indicator is any positive or negative evidence of threat activity or any characteristic of the operational area that points toward threat capabilities, vulnerabilities, or intentions.

The ability to read indicators (including deception indicators) contributes to the success of friendly operations, since indicator analysis is the basis for your recommendations to the commander for a specific COA.

Potential indicators are written and analyzed to determine if they can answer any of the established PIR and IR. All indicators that answer one or several PIR or IR are prioritized. Any indicator that does not answer PIR or IR is deleted. This is a very important step.

The resulting list of indicators forms the basis for collection tasks. By knowing what indicators satisfy PIR and IR—and the most likely methods and places of finding them—you can determine specific collection tasks and assign them to your collection resources.

CMOs need a thorough knowledge of the threat, the characteristics of the AO and the general capabilities of collection assets before they can translate the commander's PIR and IR into indicators. This includes a detailed knowledge of the—

- Threat organization, equipment, and doctrine.
- Biographical data on major personalities.
- Present and past performance of units and organizations.
- Terrain and weather constraints.
- Patterns of current operations.
- Degree of popular support.

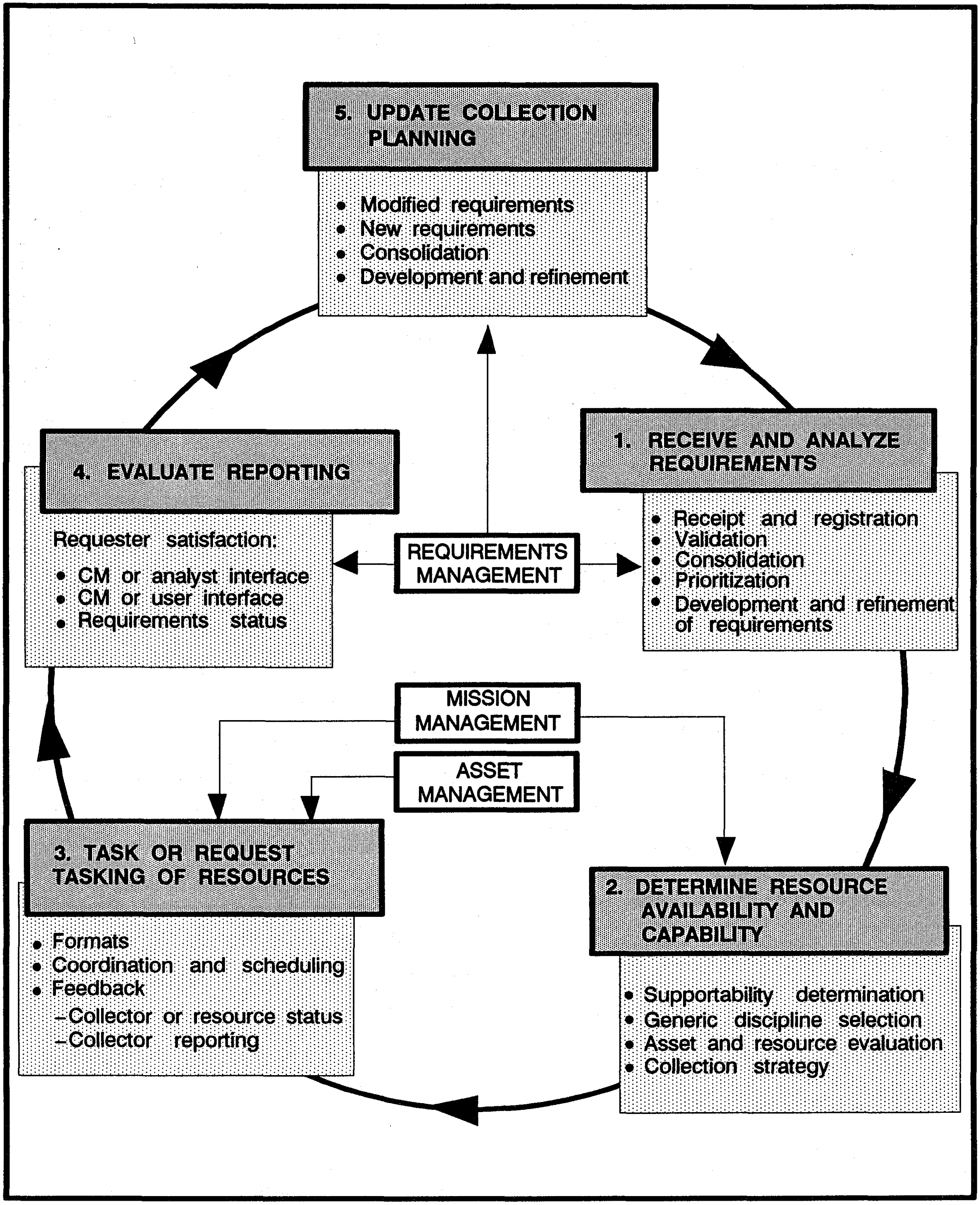

5. UPDATE COLLECTION PLANNING
• Modified requirements
• New requirements
• Consolidation
• Development and refinement
1. RECEIVE AND ANALYZE REQUIREMENTS
• Receipt and registration
• Validation
• Consolidation
• Prioritization
• Development and refinement of requirements
REQUIREMENTS MANAGEMENT
4. EVALUATE REPORTING
Requester satisfaction:
• CM or analyst interface
• CM or user interface
• Requirements status
MISSION MANAGEMENT
ASSET MANAGEMENT
3. TASK OR REQUEST TASKING OF RESOURCES
• Formats
• Coordination and scheduling
• Feedback
–Collector or resource status
–Collector reporting
2. DETERMINE RESOURCE AVAILABILITY AND CAPABILITY
• Supportability determination
• Generic discipline selection
• Asset and resource evaluation
• Collection strategy

Figure D-4. Collection management process.

PIR

1. Where and in what strengths are the insurgent forces in the AO?
2. Will insurgent forces attack US forces; if so, where, when, and in what strength?
3. Where can the insurgent forces conduct main force operations; if so, when and in what strength?
4. Where, how, and in what strength are insurgent forces air defense capable ?
5. Where are the supply and training bases of insurgent forces ?

IR

A. How strong is popular support for the insurgents ?

B. How, where, and by whom will the insurgent forces be resupplied.

C. Where are the infiltration and exfiltration routes ?

D. What are the names and numbers of internal and external organizations supporting the insurgent forces ?

E. Will third- world countries react to US forces conducting military operations; if so, how ?

Figure D-5. Examples of prioritized dispersed battlefield collection PIR and IR.

CMOs must also understand the circumstances and support required for a particular indicator to occur. These include but are not limited to a detailed knowledge of the—

- Amount and availability of support required for a particular action and activity.
- Normal doctrinal activity or disposition.
- Activity required for a particular COA.
- Actions within threat capabilities and limitations.
- Characteristics of foreign commanders.
- Possibility or practicality of operations.
- Collection characteristics.
- Identification of target characteristics.

Established patterns also can be used to determine indicators. Often these existing patterns link a particular event or activity to probable COAs. Sometimes, they can even be used to determine when and where that activity might occur. Patterns help to decide—

- Where to look.
- When to look.
- What to look for.

Indicator Examples

Indicators can be broken into three categories:

- Immediate threat indicators.

- Preparatory indicators.
- Secondary indicators.

All three categories appear at strategic, operational, and tactical levels.

Immediate Threat Indicators. As the name implies, these are indicators of threat activities that are in progress or, better yet, about to happen. They are developed by analyzing threat tactics, movements, activities, and final preparations. This includes indicators for imminent nonviolent acts such as—

- Demonstrations.
- Sit-ins.
- Drug harvesting, processing, and transport.

These are some examples of immediate threat indicators for an attack:

- Increased threat movement towards possible objective.
- Increased threat infiltration into staging areas within 12 to 24 hours' walk from possible objective.
- Reports of cache recovery near possible objective.
- Heavily armed reconnaissance.

The following are some examples of immediate threat indicators for a violent demonstration—all of which show an imminent threat:

- Presence of known or suspected agitators in schools or public gatherings.
- Stockpiling of rocks, homemade weapons, gasoline bombs, and material that can be used for building barricades.
- Presence of threat-oriented media at places of public gatherings.

Preparatory Indicators. These are activities which a threat has to complete prior to executing a COA. They are developed by analyzing all the intelligence, planning, training, and logistical activity that the threat has to undertake in order to successfully carry out a COA.

For an attack, these could include—

- Lightly armed reconnaissance elements that avoid or break contact quickly.
- Stepped-up training.
- Construction of mock-ups.
- Stockpiling supplies in base areas and near potential objectives.

For street demonstrations, these could be—

- Pro-threat political meetings prior to a national holiday or observance.
- Posting of banners and other media announcing mass meetings or rallies.
- Low-level incidents designed to create discontent among the population.

Preparatory indicators may also show up in the I&W system as strategic indicators. These can manifest themselves as diplomatic or material support from other countries both in and outside the region. Some examples are—

- Regional powers making political statements in support of the threat.
- Pro-threat countries breaking UN or other world body-sponsored embargoes or blockades.
- Overt or covert arms shipments.

Secondary Indicators. Secondary indicators reflect threat activity on the civilian populace. They are developed by analyzing the interrelationship between tactical level preparatory indicators as well as by evaluating their effects on the civilian population, economy, and commodities. For example, if the threat has long-range plans for a large-scale offensive, there will be some preparatory indicators such as logistics, training, and others.

However, there may also be some more subtle secondary indicators such as reported shortages and large purchases of food, medicine, hardware, and other seemingly innocuous or non-lethal material.

Secondary indicators can also appear in other intangible ways, such as attitudes, fears, and reactions among the civilian population. Some examples are—

- Locals who refuse to talk to authorities.
- Drops in school attendance.
- Drop in attendance at festivities, dances, and other entertainments.

Another way to develop indicators is to study past threat activity and patterns. Although this can be extremely useful, we must consider the threat's ability to alter or change its modus operandi. This is an important thing to remember when analyzing indicators.

Indicator Worksheet

Figure D-6 shows a sample format to aid you in determining indicators. The breakdown of the indicator worksheet is as follows—

- The far left column is the indicator number (**IND NO**). It is used as a reference point. Each line is labeled to quickly orient analysts.
- The next column is **INDICATOR**. All potential indicators are written and analyzed to determine if they answer any PIR or IR.
- The third column is the **PIR NUMBER AND IR LETTER**. The ASPS records the PIR number and IR letter that can be answered by the corresponding indicator. For example, indicator 1 may provide information regarding PIR 1 and 5 and IR A, B, and C. Your CMO inserts 1 and 5 and A, B, and C in the appropriate block. If an indicator fails to support any PIR or IR, it is quickly replaced.
- The fourth column is the **INDICATOR PRIORITY**. In this column each indicator is prioritized.

CMOs determine which indicator answers the most important PIR and IR and ranks them accordingly.

For example:

- Indicator 1 answers PIR 1 and 5 and IR A, B, and C.
- Indicator 2 answers PIR 1, 2, and 5 and IR B and C.
- Indicator 3 answers PIR 1, 2, and IR A, B, D, and E.

After ranking by your CMO, indicator 1 would be the 17th priority, 2 the second, and 3 the third priority.

Prioritization Matrix

The following steps determine the priority of a large number of indicators or SIR. Figure D-7 is an example of a prioritization matrix.

Step 1. Mark PIR and IR. On graph paper, mark your PIR and IR down the left column. Allocate the weighted value of each PIR and IR (in brackets next to the PIR and IR). You can set the value of each PIR and IR by counting the number of PIR and IR and then giving the highest PIR the highest number and each successive PIR and IR a lower number (as shown in Figure D-7).

Alternately, you can place a greater weighting on individual PIR and IR to accurately reflect the relative importance of each PIR and IR. Doing this, as you will see, reduces conflicts within the matrix. You determine the value of each PIR and IR.

Step 2. Mark Indicator or SIR. Mark the indicator or SIR numbers across the top row.

Step 3. Use Indicator Worksheet. Using the dispersed battlefield indicator worksheet, place an X in the appropriate position within the matrix to indicate which PIR, IR, indicator, or SIR it answers.

Step 4. Use Weighted Values. Using the weighted value allocated to each PIR and IR, add the total value of each indicator or SIR. This will give an overall weighting for each indicator or SIR.

Step 5. Determine Priorities. The indicators or SIR with the highest weighted values have the highest priority. Those with lower weighted values have lower priorities. In cases where two or more indicators or SIR have the same weighted value, discriminate which has the highest priority.

DETERMINE SIR

In the third step, the ASPS analyzes the prioritized indicators and target characteristics to determine the SIR. SIR are the basic questions that need to be answered to confirm or deny the validity of an indicator.

For example, the first PIR asks where and in what strength are the insurgent forces in the AO (see Figure D-5). Some indicators that may assist in answering this requirement are—

- Locations of threat base camps.
- Locations of threat cache sites.
- Establishment of new and unexplained agricultural areas or recently cleared fields.
- Size and location of threat cells, groups, and units.
- Unexplained weapons firing or explosions in the countryside.

All the above indicators can assist in answering the first PIR. These indicators are now analyzed to develop SIR. Some examples of SIR for the indicator locations of threat cache sites could be—

IND NO	INDICATOR	PIR NO IR LTR	INDICATOR PRIORITY
1	Locations of threat base camps	1,5,A,B,C	17
2	Locations of threat cache sites	1,2,5,B,C	2
3	Degree of insurgent popular support	1,2,A,B,D,E	3
4	Establishment of new unexplained agricultural areas, or recently cleared fields	1,3,5,B	12
5	Size and location of threat forces	1,2,3,5,B	1
6	Unexplained weapons firing or explosions in the country side	1,5	20
7	Threat reconnaissance activity	2,C	27
8	Attitude of local populace toward government and threat forces	1,2,A,B	5
9	Threat propaganda efforts	2,A,D,E	26
10	Disappearance of populace from previously populated areas	1,2	9
11	Avoidance of certain areas by the populace	1,2	10
12	Equipment found in threat cache sites	1,3,4,5, A,B,C,D	11
13	Unexplained trails	1,5,C	19
14	Threat use of air defense weapons or small arms against aircraft	1,4	13
15	Significant changes in threat TTP	2,3,A,D	25
16	Sabotage attempts against supply depots, ammo supply points, ammo facilities, and LOC	1,2	8
17	Significant movement of civilians and refugees	1,A,C	22
18	Location and type of threat indirect fire		
19	Names and number of internal organizations supporting threat	1,5,A,B,D	18
20	Names and number of external organizations supporting threat	1,5,A,B,D,E	15
21	Failure of police or information nets to report correctly	A,D	32
22	Attacks on communications sites		
23	Damage to roads, airfields, and helipads in the operational area	1,3	14

Figure D-6. Dispersed battlefield indicator worksheet.

INDICATORS or SIR / PIR	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1 (10)	x	x	x	x	x	x		x		x	x	x	x	x		x	x		x	x			x
2 (9)		x	x		x		x	x	x	x	x				x	x							
3 (8)				x	x							x			x								x
4 (7)												x		x									
5 (6)	x	x		x	x	x						x	x						x	x			
A (5)	x		x					x	x			x			x		x		x	x	x		
B (4)	x	x	x	x	x			x				x							x	x			
C (3)	x	x					x					x	x				x						
D (2)			x						x			x			x				x	x	x		
E (1)			x						x											x			
TOTALS	28	32	31	28	37	16	12	28	17	19	19	45	19	17	24	19	18	0	27	28	7	0	18
RANK ORDER	5*	3	4	5*	2	11	12	5*	10*	8*	8*	1	8*	10*	7	8*	9*	-	6	5*	13	-	9*

* TIED SCORE: Resolved by analyst.

Figure D-7. Prioritization matrix.

- Report any signs of digging in area Gold.
- Report contents of all caches discovered in area Gold.
- Report any information concerning insurgent cache techniques and procedures.
- Examine and report any unexplained dead foliage.

Accurate determination of indicators and SIR is essential for effective collection management. Knowing where, when, and what to look for helps in selecting what to look with.

This process maximizes the use of limited collection assets against an array of collection targets. After indicators and SIR are prepared, the ASPS passes them to the CM&D section for asset tasking.

The CMO prioritizes the SIR and tasks appropriate sources to answer them. The list of taskings for each source also should be prioritized. All of this can be completed in this step. The dispersed battlefield collection plan format provides the CMO with an effective format to organize and monitor this task.

An example of a completed collection plan using the dispersed battlefield collection plan format is at Figure D-8.

The far left column of the format is **SIR NUMBER.** It is used as a reference point. Each line is labeled numerically to quickly orient personnel to the SIR on the worksheet.

The next column is **TIME.** List the start and stop times the corresponding SIR should confirm or deny a particular SIR. These SIR may be extremely time sensitive, such as reporting a threat force leaving its post to

LINEAR BATTLEFIELD COLLECTION PLAN UNIT: 1 BN 9SFG(A)						AGENCIES AND AGENCY COLLECTION PRIORITY																
SIR NO.	TIME		SPECIFIC INFORMATION REQUIREMENTS	PIR/ IR NO	SIR PRI	GRP MI DET	SOT-A (1)	SOT-A (2)	SOT-A (3)	CITM	B930	A931	A933	A934	4th POG	96th CA	TASO-SC ISE	SOC J2	HN police	HN 1st BDE	HN 2d BDE	Other HN Agencies
		NAI				ALL	TWO	FIVE	SIX	RED-A Green-A	ALL	RED	BLACK	GREEN	ALL	ALL	ALL	ALL	ALL	RED	BLACK GREEN	ALL
1	INDEF	ALL	Report location, quantity and type of unexplained firing in the area	1,5	20		3 * 5	3 * 5	3 * 5							9 * 1			13 * 2	11 * 3	11 * 4	
2	INDEF	ALL	Report any presence of mines, booby traps and obstacles etc, in the area	1,5	21							8 * 1	8 * 2	8 * 3		10 * 4			14 * 5	12 * 6	12 * 7	
3	INDEF	ALL	Report locations of suspected nongovernment training sites and the approx No. of personnel the site can support	1,5,B,C	15							6 * 3	6 * 4	6 * 5				3 * 1	10 * 3			
4	INDEF	ALL	Report sighting of groups of strangers in and around the area	1,2,5,B,C	5					2 * 3						4 * 2			3 * 1			
5	INDEF	ALL	Report areas showing significant signs of activity but few if any inhabitants	1,5	22					8 * 1		9 * 3	9 * 4	9 * 5					15 * 2	13 * 6	13 * 7	
6	INDEF	ALL	Report the number, size, equipment, composition, route and time of suspected insurgents in the area	1,3,4,5, B,C	10		2 * 6	2 * 7	2 * 8			4 * 3	4 * 4	4 * 5		6 * 9				6 * 1	6 * 2	
7	INDEF	ALL	Report insurgent recruitment tactics, techniques and procedures and their effectiveness	1,A,B,D	23										3 * 1	11 * 2			16 * 3			
8	INDEF	ALL	Report information obtained from EPWs and civilians on insurgent locations, probable COAs, activities, strengths and cache sites	1,2,3,4,5, A,B,C,D	1	1 * 1						1 * 4	1 * 5	1 * 6		1 * 3			1 * 2			
9	INDEF	ALL	Report the establishment of new and unexplained agricultural areas or recently cleared fields	1,3,5,B	11											7 * 3	2 * 2	1 * 1				
10	INDEF	ALL	Report location and contents of confirmed or suspected cache sites	1,3,4,5, A,B,C,D	9							3 * 2	3 * 3	3 * 4		5 * 5			7 * 1	5 * 6	5 * 7	
11	INDEF	ALL	Report signs of suspected digging or areas of dead or unusual foliage	1,5,B	18	6 * 3											4 * 2	5 * 1		10 * 4	10 * 5	
12	INDEF	ALL	Report latenight or otherwise unusual moving of boxes/equipment into a residence or business	1,5,B	19					7 * 2									12 * 1			
13	INDEF	ALL	Report large numbers of personnel visiting a particular residence	1,5,B,D	17					6 * 2									11 * 1			
14	INDEF	ALL	Report connections with political parties, labor unions, schools, churches, etc.	5,A,B,C,D	26	8 * 1									5 * 2	13 * 3		19 * 4	16 * 5	16 * 6		
15	INDEF	ALL	Report increased domestic/foreign media coverage of insurgent activities and insurgent sensitivities to public attitudes and reactions	1,5,A,D,E	14	5 * 1					2 * 3							9 * 2				
16	INDEF	ALL	Report propaganda effort's (indicate, type, targets, location, time encountered, theme and effectiveness)	1,2,3,D,E	2	2 * 3						2 * 4	2 * 5	2 * 6	1 * 1	2 * 2			1 * 7	1 * 8		
17	INDEF	ALL	Report the use of new words, phrases or symbols in the area	1,2,4,A,D	4					1 * 1					2 * 3	3 * 2		2 * 4	3 * 5	3 * 6		
18	INDEF	ALL	Report sabotage attempts against supply depots, ASPs, commo facilities or LOC.	1,2	8	4 * 4												6 * 1	4 * 2	4 * 3		
19	INDEF	ALL	Rpt location and contents of thefts that could support activities (bulk food, clothing boots, weapons and road taxes)	1,2,B	7					4 * 2								5 * 1				
20	INDEF	ALL	Rpt significant movements of civilians & refugees, to include the avoidance of certain areas	1,2,5,A	6	3 * 3				3 * 4							1 * 2		4 * 1			
21	INDEF	ALL	Report the use of air defense weapons or small arms fire at aircraft to include the type and locations of weapon	1,4,D	13							5 * 5	5 * 6	5 * 7				2 * 4		8 * 2	8 * 3	HN AF 1 * 1
22	INDEF	ALL	Rpt damage to roads, airfields, & other structures	1,3	12					5 * 5						8 * 2			8 * 1	7 * 3	7 * 4	
23	INDEF	ALL	Report unexplained trails or increased activity on established roads, trails, rivers or streams	1,5,B,C	16							7 * 3	7 * 4	7 * 5			3 * 2	4 * 1		9 * 6	9 * 7	
24	INDEF	ALL	Report unusual, public gatherings, strikes, riots, or demonstrations	A	28	9 * 4				10 * 3					7 * 5	15 * 2						
25	INDEF	ALL	Rpt any significant changes in tactics, techniques, or procedures	2,3,A,D	24	7 * 3					3 * 4				4 * 2	12 * 1			17 * 6	14 * 7	14 * 8	
26	INDEF	ALL	Report any confirmed or suspected recon activity	2,C	25							10 * 2	10 * 3	10 * 4					18 * 1	15 * 5	15 * 6	
27	INDEF	ALL	Rpt lack of cooperation from local authorities	A,D	27					9 * 1					6 * 3	14 * 2			20 * 4			
28	INDEF	ALL	Rpt any radio traffic or EW activity	1,2	3		1 * 1	1 * 2	1 * 3		1 * 4									2 * 5	2 * 6	

Figure D-8. Dispersed battlefield collection plan format.

reinforce a target. The indicator may remain in effect throughout the entire operation, such as the local populace avoiding a specified area.

The third column is NAI. NAI can be shown vertically or horizontally on the chart. The NAI listed in the vertical NAI column indicates where the SIR should be observed. An NAI may pertain to one or more SIR or vice versa. List the NAIs that each particular source is responsible for in the horizontal NAI column. A CI team may be responsible for only one NAI while an IMINT source may cover several NAIs.

The fourth column is **SIR DESCRIPTION.** In this column the CM&D section lists the SIR they believe will confirm or deny particular indicators and which help to answer one or more PIR and IR. It is common to develop several SIR from one indicator or for each SIR to provide information on several indicators and PIR and IR.

The next column is **PIR AND IR NUMBER.** Record the PIR number and IR letter that can be answered by the SIR in this column.

The next column is **SIR PRIORITY.** In this column each SIR is prioritized. The CMO determines which SIR answer the most important PIR and IR and rates them accordingly.

The next column is **AGENCIES AND AGENCY COLLECTION PRIORITY.** Across the top of this section all organic and supporting collection agencies are listed. In the blocks below agencies, their respective NAIs are listed.

Before a particular agency or unit is selected to collect on a SIR, the CMO determines what assets are available and capable of collecting the information he needs. This includes assets in organic, supporting, and higher collection agencies.

To do this, the CMO needs to know the capabilities and availability of each asset. These include factors such as—

- Frequency ranges for intercept radios.
- Aircraft mission durations.
- Number of flights.
- Mobility.
- Linguistic capabilities.

This information is essential to determine which asset or agency is capable of collecting information to answer SIR. DDI 2660-3139-YR has information to answer SIR and profile system capabilities. HN or HUMINT resource capabilities must be obtained from the parent organization. Figure D-9 shows a capability and requirement correlation chart.

After determining asset capability and availability, the CMO places a check in the small square located in the lower left corner of the block that corresponds to the SIR that a particular agency or asset is capable and available to answer. Next, he determines which agency or asset can best answer the SIR and prioritizes them.

To do this, he considers the location, range, and threat to the collector, as well as other mission requirements. This is shown on the worksheet by placing the appropriate number in the small square located in the right corner of the block.

For example, the CM&D section determines that the CI team, CA unit, and HN LEA are capable of answering SIR 4 - Report sighting of groups of strangers in and around the area (see Figure D-8).

The CMO places an asterisk in the square located in the lower left corner of the block that corresponds to that particular SIR and each of the three capable agencies. After further consideration, he determines that HN LEA can best answer the SIR, followed by the CA unit, then the CI team. He then puts 1 in the square located in the lower right corner of the block that corresponds to SIR 4 and the HN LEA; 2 in the CA unit's block, and 3 in the CI team's block.

THE TASKING LIST

In the fourth and final step, the CM&D section prepares an easy-to-read prioritized tasking list for each collection agency. To do this, he lists the SIR each agency is tasked with and prioritizes them by the SIR priority column.

For example, in Figure D-8, the support operations team-Alpha (SOT-A) (1) is tasked with SIR 1, 6, and 28. SIR 1 has a SIR priority of 20; SIR 6, a priority of 10; and SIR 28, a priority of 3. This means the CMO must provide the SOT-A (1) with a prioritized tasking list as follows:

1 — Report time, frequency, and location of insurgent radio traffic or EW activity (SIR 28).

2 — Report the number, size, equipment, composition, route, and time of suspected insurgent patrols in the area (SIR 6).

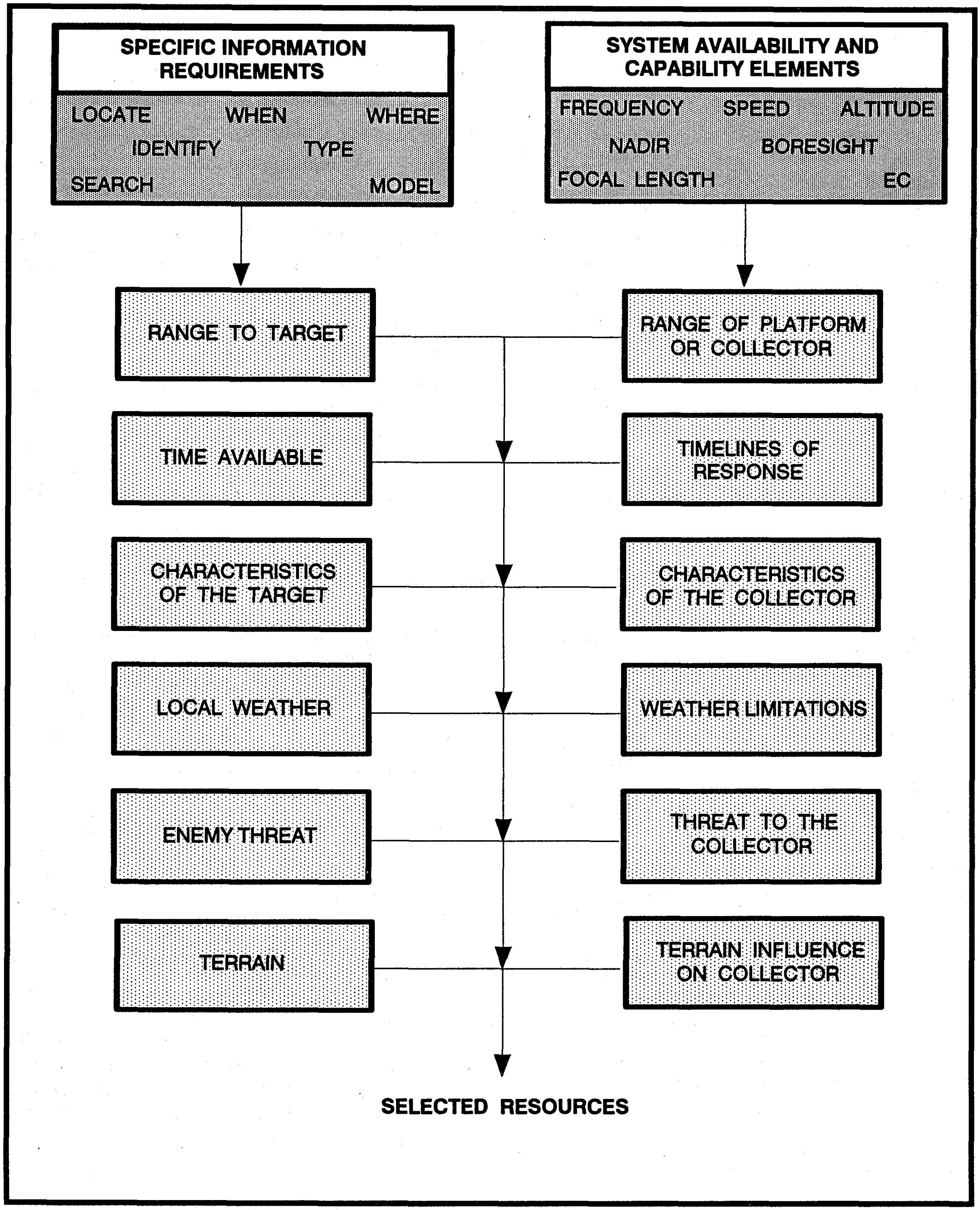


Figure D-9. Capability and requirement correlation chart.

3 — Report the location, quantity, and type of unexplained firings in the area (SIR 1).

Other Considerations

The only exception to this procedure is when the CMO tasks interrogators. They need verbatim PIR and IR in addition to the indicators or SIR containing specific intelligence or combat information requirements.

Interrogators need this information because their primary source of information and intelligence comes from people who have different levels of understanding and background. This means interrogators must tailor their questions so that the subject can understand what is being asked. Often, interrogators must ask a subject several different questions, all seemingly unrelated to the other, before the subject understands and can answer the question.

For example, suppose the CM&D tasks interrogators to "... report instances of dead foliage." This SIR is specific. If the subject is not native to the area, they may not have noticed dead foliage.

However, if the interrogator knows the larger PIR is to "... locate insurgent supply caches," he can rephrase or ask different questions to secure this information. By knowing the larger question, the interrogator is able to quickly secure the information or intelligence the commander needs and spot report it back immediately.

A Sample of the Process

If the commander's PIR and IR demand to know if the enemy will attack, focus on those enemy activities and preparations which will confirm or deny the enemy's capabilities and probable COA.

Look first for immediate threat indicators. Immediate threat indicators must be given a higher priority and quickly turned into specific IR and tasked out to collectors.

While this is happening, look for preparatory and secondary indicators to turn into specific IR.

Consider the following scenario: Suppose a PIR was, "What is the location of drug processing plants?" Some immediate threat indicators would be—

- Presence of waste in streams and rivers flowing from isolated areas.
- Presence of smoke in isolated areas.
- Unexplained presence of people (armed and unarmed) in unpopulated areas.

The above examples tend to show that activity is about to happen or is already in progress. Some preparatory indicators would be—

- Purchases or movements of precursor chemicals.
- Recruitment of unemployed workers.
- Purchases of building supplies.

Secondary indicators would be—

- Unexplained affluence among the populace.
- Drop in the number of locals that frequent bars or taverns.

For the above indicators, your SIR should look something like this:

- Report abnormal discoloration in streams and rivers in XX areas.
- Report purchases and movements of precursor chemicals in XX areas.
- Report drops in unskilled manpower pools in XX areas.
- Report sales of construction material to local builders or property owners in the XX valley area.
- Report sightings of smoke in isolated areas in the XX valley area.
- Report changes in business patterns in taverns, bars, and other entertainment establishments in the XX district.
- Report unexplained home improvements or new construction in XX barrio.
- Report unexplained appearance of high-value household goods and luxury items in XX barrio.

The above sample SIR are all specific as to what you want to know and where you want the assets to look for it.

You may have to translate your SIR for specific agencies or intelligence disciplines. For example, for a radio intercept unit, a SIR for information on the location of a training camp may read, "Report location of emitters in XX areas" or "Report increased volume of radio traffic." For IMINT, this same SIR could read, "Report unusual foot movement or location of running tracks, mock ups, in XX barrio, YY province."

Rules for Indicator Analysis

Once you have developed your indicators and tasked the appropriate agencies and sources, you must analyze the results. You must evaluate the results of your SIR and adjust them if necessary. This is a continual process.

There are several basic rules in indicator analysis:

- Always consider all possible threat COAs when developing indicators.
- Always consider all available indicators and current intelligence before making a determination as to their significance.
- Never attempt to predict current or future threat activity based solely on past threat activity.
- Always look at every possible explanation or meaning for each individual indicator. Local cultural factors may often hold the key.
- Do not forget using investigative technology to detect indicators. A simple water test can determine, for example, if the water discoloration is due to drug-processing chemicals or some natural or industrial pollutant.
- Do not allow past success, failure, or inaccuracy in your predictive analysis to become the driving factor in indicator selection and analysis. Treat each situation without any preconceived ideas about the worth of specific indicators.

THE INTELLIGENCE SYNCHRONIZATION MATRIX

The purpose of this matrix is to focus all collection, production, and dissemination requirements on the commander's PIR and IR. After the OPLAN is well developed and the BOS synchronization matrix is available, you can begin to assemble your matrix.

As shown in Figure D-10, the intelligence synchronization matrix has three parts:

- Friendly decision points.
- Time-sequenced and pre-planned PIR.
- Synchronization of resources.

The first part graphically shows the key times in the battle when critical friendly events are expected to occur. If you need more time lines because, for example, your division has three maneuver brigades, you can add a third time line.

The second part represents time-sequenced and pre-planned PIR. Pre-planned PIR are what the commander estimates he will need to know as the battle progresses and when he will need to know it.

As PIR are answered, or as their timeliness diminish, the pre-planned PIR replace them. This allows for no more than three or four PIR to be collected against at a given time but permits advanced planning to occur. The G2 or S2, G3 or S3, and the commander develop these together. After they are established, the commander's staff, primarily the S2 and S3 staff, backplan the collection, production, and dissemination efforts to answer the PIR.

The third part of this matrix is a collection schedule. It shows the planned coverage times for collectors available to the headquarters constructing the matrix.

The commander's time requirements for getting answers to his PIR dictate the amount of collection time available to the CMO. He selects the assets capable of answering PIR. While the matrix shows you what is available for collection, it does not show specific collection taskings or requests. This comes from the collection plan. Specific assets are listed in the lower right corner of the matrix. (You get them from your collection plan.)

This matrix does not replace existing templates, overlays, or planning techniques. It does combine the key points of the DST, R&S plan, collection plan, and the OPLAN into one consolidated graphic.

The intelligence synchronization matrix is intended to be a flexible document. It combines the key points of other planning tools on a single graphic the commander can use as a quick reference to see—

- Where he estimates he should be.
- When he should be there.
- Who or what he needs to get there.

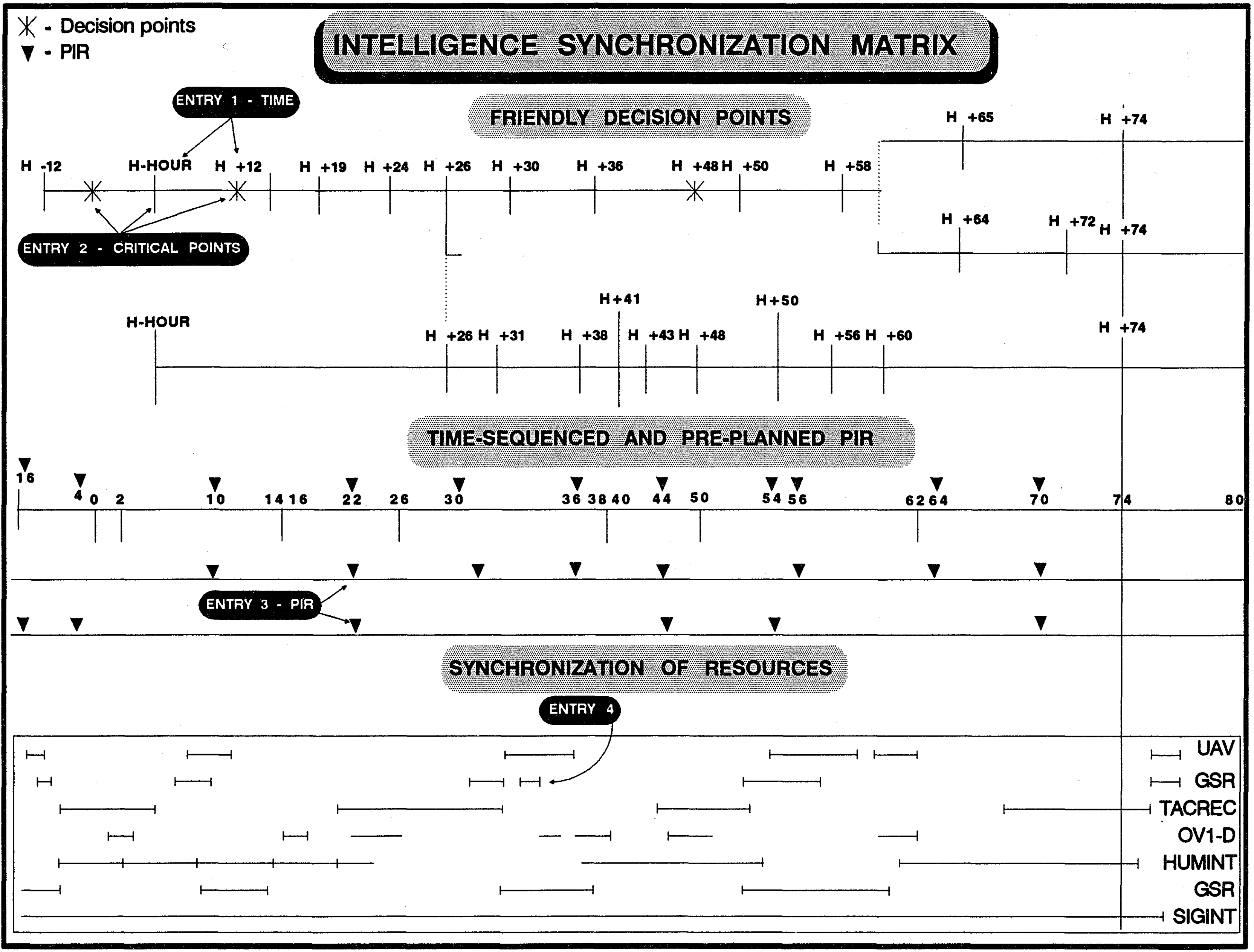


Figure D-10. Intelligence synchronization matrix.

APPENDIX E
REQUIREMENTS, SOURCES, AND AGENCIES

This appendix covers the intelligence requirements for LIC by operational category. It looks at available sources and agencies which can fulfill those needs.

The four operational categories of LIC are—

- Supporting insurgencies and counterinsurgencies.
- Combatting terrorism.
- PKO.
- PCO.

These transcend the operational continuum of—

- Peacetime engagement.
- Hostilities short of war.
- War.

The ever-changing political and military realities of today require us to be prepared to fight in any place on the globe, and at any or all of the conditions of the operational continuum. Figure E-1 shows this relationship.

In all military operations the commander identifies his PIR and IR based on METT-T factors. However, the diversity of LIC missions demands that IEW support be more visionary and proactive in identifying potential dangers before, during, and after hostilities.

INFORMATIONAL CATEGORIES

In broad terms, LIC information requirements are placed into five basic categories:

- Political.
- Economic and social.
- Geographic and environmental.
- Military and security.
- Threat.

Since each of these categories interact, it is important to view each of them as an interdependent part of the whole.

REQUIREMENTS FOR SUPPORT TO AN INSURGENCY OR COUNTERINSURGENCY

IEW support for insurgency and counterinsurgency is similar. But there are enough differences to justify a separate look at each.

INSURGENCY

This is half of the first operational category. It involves supporting foreign political and military entities engaged in pro-democracy struggles within their own borders.

When deemed appropriate by the NCA, US forces can be tasked to provide training, materiel, and intelligence support to pro-western insurgents. Although this mission would probably be assigned to SOF, conventional forces may also participate in a limited support role.

To assist in determining the intelligence requirements for this operational category, mentally put yourself in the place of the insurgent.

Political

Political questions include—

- Is the insurgency legitimate?
- What portion of the population is politically supportive of the insurgents?
- What are the political issues which fueled the pro-western insurgency?
- What existing political organizations share political views with the insurgents?
- What is the position of neighboring countries and other regional powers vis-a-vis US support to the insurgency?

Economic and Social

Economic and social questions include—

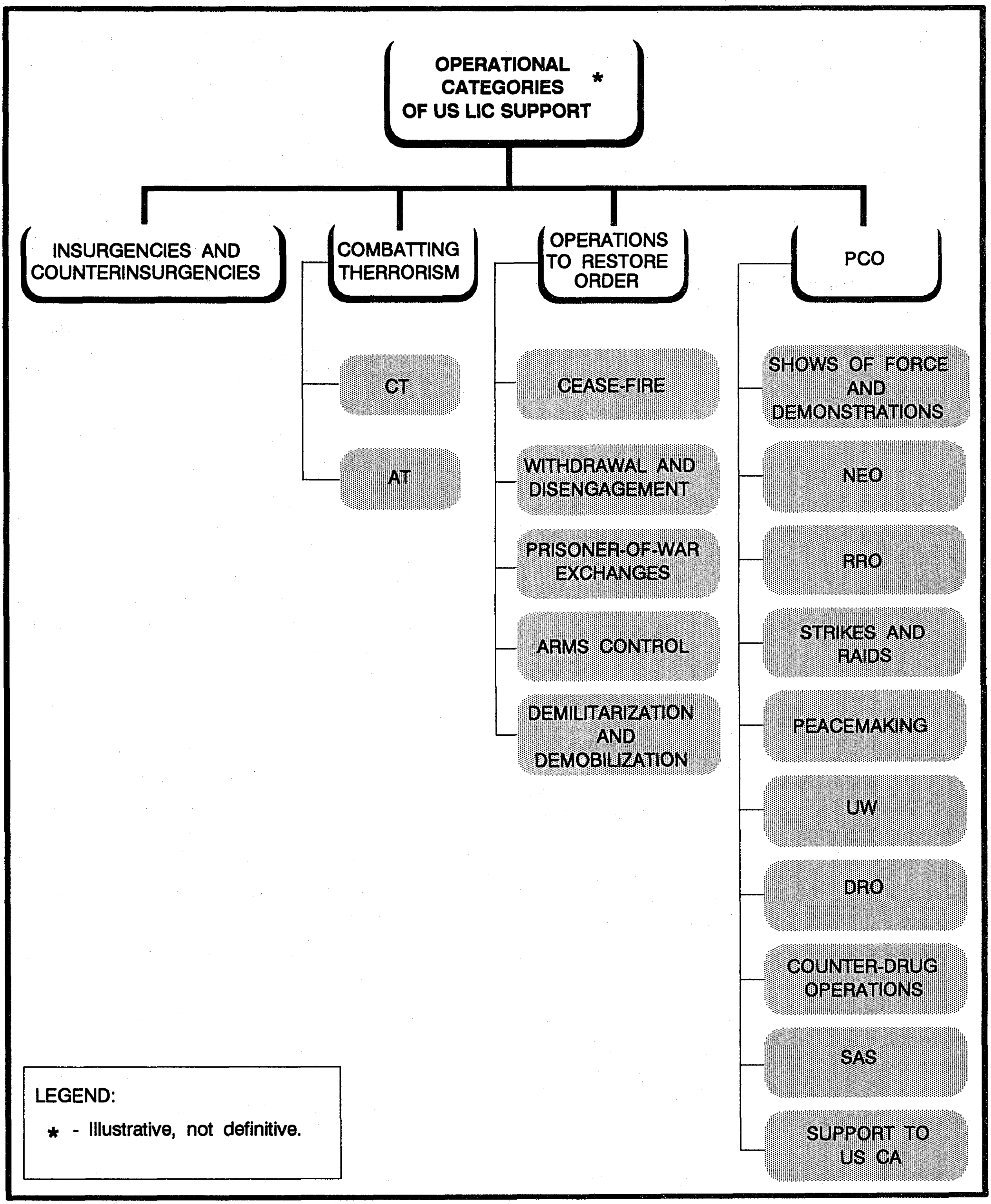

OPERATIONAL CATEGORIES OF US LIC SUPPORT *
INSURGENCIES AND COUNTERINSURGENCIES
COMBATTING THERRORISM
OPERATIONS TO RESTORE ORDER
PCO
CT
AT
CEASE-FIRE
WITHDRAWAL AND DISENGAGEMENT
PRISONER-OF-WAR EXCHANGES
ARMS CONTROL
DEMILITARIZATION AND DEMOBILIZATION
SHOWS OF FORCE AND DEMONSTRATIONS
NEO
RRO
STRIKES AND RAIDS
PEACEMAKING
UW
DRO
COUNTER-DRUG OPERATIONS
SAS
SUPPORT TO US CA
LEGEND:
* - Illustrative, not definitive.

Figure E-1. US support to LICs.

- What economic factors influenced the outbreak of the insurgency?
- What are the government's economic choke points?
- Can the insurgents weaken the government by attacking economic targets without alienating the civilian population?
- How long can the government finance its counterinsurgency campaign?
- What ethnic, religious, cultural, and other sociological divisions exist within the country?
- Which of these social categories are hostile to the government?
- Can the insurgents exploit these divisions?

Geographic and Environmental

This intelligence requirement includes a detailed study of the country's terrain and climate much as is done in conventional warfare. In fact, if the government employs conventional forces against the insurgents, then all the usual terrain and weather factors apply.

Military and Security

In certain cases, a neighboring country may either openly or covertly allow the insurgents to use their territory as sanctuary, training, and staging areas. For example, Pakistan often allowed Afghanistan rebel activity in Pakistan. In these cases, we need information pertaining to the degree or level of support activity a neighboring country will allow or provide the insurgents.

What segment of the military supports the insurgency? Will the military engage any military force (neighboring government or rebel) crossing the border? This can also include an inward evaluation of the supported insurgency. How well trained are they? Are their tactics effective?

Threat

In a support to an insurgency role, the threat is the government force and their allies. Traditional OB factors are prominent in the data base. If the government has conventional warfighting capabilities, then IPB for enemy conventional operations will be necessary.

COUNTERINSURGENCY

This is the other half of this operational category. We could find ourselves involved in a counterinsurgency effort as part of a FID program in support of a HN. In this case, our involvement primarily would be advisory in nature. However, we could also become directly involved if the HN requests US combat troops and the request is approved by the NCA.

In either case, we will require detailed knowledge of the AO and the existing military and political situation. Of course, we ask the usual questions: What are threat capabilities and immediate intentions? What are threat strengths, weaknesses, and how can they be exploited?

But we also must be aware of weaknesses in the HN society, political base, and administrative machinery which allows for insurgent development. Therefore, understanding the threat goes far beyond identifying military capabilities. It must include understanding the political, economic, and sociological factors which made the existence of an insurgency possible in the first place.

Counterinsurgency data base building is essential at all levels beginning with basic intelligence data. Your basic intelligence data should answer two prime questions: Do you know your enemy? Do you know yourself? We need to look at these requirements in more detail.

Political

Does the HN truly recognize it has an insurgent problem? This is critical. If they do not, you could have a big problem trying to implement counterinsurgency policy. Your questions should include:

- How do the political structure, laws, and regulations of the HN support or hinder counterinsurgency operations?
- What are the HN's national policies (foreign and domestic)?
- What are the significant political groups?
- What biographic data is available on key political figures?
- Where, and by whom, were major leaders taught?
- Where did they go to college or university?

Economic and Social

What is the status of the country's commerce and industry?

Industries. Who owns them and where are they located?

Agriculture and Land Ownership. What agricultural products are grown; what percent of land is owned by what percent of the population?

Labor. How is the labor force organized and into what categories? What is the status of economic organizations, activity, and development?

Foreign Interchange. Look at foreign trade, treaties, exchange, investment, and aid. Who do they trade with? Who is providing aid and in what form? Who has large investments in the country? What treaties do they have and what are they about?

Natural Resources. What are the surpluses and shortages? What is imported, at what cost, and in what amounts?

Communications. How advanced is the communication systems? How widespread? What is the percent of population with televisions, radios, and newspapers? Who owns the different media systems and what are their political leanings?

Culture. What is the country's social structure and the characteristics of the people? How about customs and manners; number of languages and dialects; identity of minorities or tribes?

Religion. What religions are being practiced? What is the percent of population in each? Are there hostile rivalries?

Education. What is the literacy rate; education program; number of higher education facilities?

Arts and Sciences. How advanced is their science? What kinds of arts, music, and dance are established?

Public Information and Assistance. What information is available and to what extent is assistance provided? Who owns the media?

Census Data. Collect all that is available. What are the popular opinions and attitudes in the HN? What are the locations, attitudes, and opinions of refugees, evacuees, or DPs?

Health and Welfare. Do sanitation and hygiene facilities meet the needs of the population? If not, what is needed to bring them to acceptable standards? Is there a public welfare program in operation and what is the scope of its responsibility? What social problems, related to health, are contributing to the insurgency?

Geographic and Environmental

All standard military weather and terrain requirements such as surface configurations and land features, drainage, and vegetation exist in LIC. However, counterinsurgency operations require detailed analysis of population-related key terrain and other nonstandard terrain factors. These are discussed in Chapter 3 and Appendix H. MC&G may be scarce or not available and will have to be augmented by foreign or commercial tourist maps. Up-to-date imagery can be an asset to your geographic intelligence by displaying changes in vegetation, roads, villages, and fields.

Military and Security

When conducting counterinsurgency in support of a HN, we need information on the government and the armed forces. On the government, we must look at how it addresses and responds to problems and issues identified during the study of the country's political, social, and economic posture. Is the government implementing reforms? Is it structured and committed to meet the needs of the people?

For the armed forces, some areas that you will probably gather information on are—

- **Capabilities.** Who is responsible for providing internal security and what are their capabilities? What are their manpower resources and their ability to replace personnel?
- **Command and staff.** What is their doctrine, and what does it allow and restrict them from doing? What is the structure of their armed forces, both conventional and unconventional? How does structure affect operational capabilities?
- **Attitudes.** What percent of the armed forces can be considered loyal to the HN; who is not, why and where are they? What status does a soldier enjoy in the society and how does it differ between officer and enlisted?
- **Traditions.** What traditions does the armed forces uphold and do they favor or hinder the insurgent's plan? What are the feelings of soldiers towards the civilian population? Do these feelings hinder the counterinsurgency effort?

- **Organization.** How are national level agencies, regular armed forces, and unconventional forces organized? What are their equipment and level of training?
- **Biographies.** Collect data on senior military leaders to discover where they received their education and their military training. Determine their political leanings, if any. What are their attitudes towards insurgents and population? How much military experience and level of training do key military leaders have? All of this will give you an insight on how those individuals intend to deal with insurgent activity and their relationship to the government in power.

Threat

Your knowledge and understanding of the threat will, of course, better enable you to defeat him. Here, in a counterinsurgency, that information is usually more detailed than that found in a conventional engagement.

Your data needs include—

- **Leadership.** Who are the leaders? What is his or her importance? Are they associated with any certain class? What is their ideological commitment and philosophy? Where, when, and on what were they trained? What are their immediate, near term, and final objectives? Are there similarities to other insurgencies?
- **Organization.** Are they divided into covert and overt operations? Typically, the covert information you are interested in includes how extensive is the threat shadow government? How is the C^3 system set up, and how effective is it? From whom, to what extent, and how are they getting passive and active support? What techniques do they use when recruiting; when is it done and by whom? What are the strengths and weaknesses of the insurgency that need to be targeted or exploited?
- **Overt information.** What loyal political parties exist? What roles do propaganda and recruiting play? How important are overt operations to the overall plan of the insurgency? What are their vulnerabilities that can be exploited?
- **Ideology.** What are the central values and beliefs of the insurgents? Who are target groups and what is the insurgent's ideological appeal to these groups? How important is ideology to the insurgent movement? Are there conflicting ideologies?
- **External support.** This can come in several different forms—moral, political, sanctuary, economic, and training material. For each of these you need to consider its importance to the insurgent movement, the source, and the methods or means of delivery.
- **Timing.** What phase is the insurgency in? Does it follow a timetable? Does the insurgent strategy require a quick victory?
- **Tactics.** Is this terrorism, an insurgency, guerrilla action, or civil war?
- **Other capabilities.** What are threat intelligence and security capabilities? Do they employ violent and nonviolent means?

REQUIREMENTS FOR COMBATTING TERRORISM

Combatting terrorism divides itself into two halves: CT and AT. Defining terminology commonly used in discussing terrorism and its associated activities is substantially more complex than you might at first think. See AR 525-13 for defining common terminology.

COUNTERTERRORISM

CT is the offensive half of the combatting terrorism operational continuum. Although the intelligence requirements for CT are similar to those for counterinsurgency, the offensive nature of these missions requires target specific information. This includes layout of terrorist camps, complexes, buildings, habits, traits, and tactics.

Here are the broad requirements:

- What are the terrorist organization, equipment, and tactics?
- Are the terrorists supported or affiliated with international terrorist movements?
- Will terrorists directly attack US interests and personnel?

Terrorists have no overt or legal representation and do not usually employ large numbers of combatants. We must remember that while insurgents use terrorism as a tactic, pure terrorists cannot, by definition, engage in guerrilla warfare or a war of movement. Here are important questions you need to ask in a CT environment:

- **Political.** What are the underlying political motivations of the terrorists? What legal political parties or movements have similar motivations? Do the terrorists have direct ties to an insurgent organization?
- **Economic and social.** Does the HN have unpopular economic policies? Is the HN economy vulnerable to terrorist attack, and, if so, what are key economic targets? What are the economic needs of the terrorist group? Who provides the terrorist group economic aid? What existing social problems contribute to the terrorist cause? What segments of society support the terrorists?
- **Geographic and environmental.** Considerations are similar to those found in support to insurgency or counterinsurgency. Additionally, refine these considerations to apply in a MOUT environment.
- **Military and security.** Although CT missions may be unilateral, some may involve HN forces. Therefore, we need to know if the HN forces are organized, trained, equipped, and have the will for CT missions.
- **Threat.** Already defined.

ANTITERRORISM

AT is the defensive aspect of combatting terrorism and encompasses all measures used to reduce the vulnerability of personnel, dependents, facilities, and equipment to terrorist attack. It requires a study of all the factors listed above in CT, but the focus is on prevention and defense. Both US and HN measures are considered.

REQUIREMENTS FOR PEACEKEEPING AND PEACETIME CONTINGENCY OPERATIONS

Before looking at the requirements for these operational categories, we must realize that they both present a wide range of challenges to the IEW system. Both may involve the insertion of US forces in between or against the full range of military threats. US forces deploying on these missions may have to perform IPB in conventional or unconventional environments. We need to look at both categories separately.

PEACEKEEPING OPERATIONS

Here are some examples of the kinds of questions asked in PKO:

- **Political.** US forces performing these types of missions require detailed knowledge of the political and military aspects of the conflict between the cobelligerents. Many of the diplomatic rules that govern PKO limit our intelligence collection efforts.
- **Economic and social.** US forces must understand what the economic factors of the conflict are. Is the war over food or other resources? What about the economic and social conditions of the populace in the buffer zone? Are there deep-seated ethnic hatreds or conflicts between people living in and around the buffer zone? What are social or religious taboos within the populace?
- **Geographic and environmental.** The scope of this information will depend on the type of conflict or level of war. Whether the original conflict was a conventional or guerrilla war will affect the level of detail employed.
- **Military and security.**
  - Although these missions require neutrality and are not in support of a HN, certain parallels exist. The presence of US peacekeepers will be under the auspices of the governing world organization (UN, The Organization of American States [OAS], and others).
  - The legal jurisdiction of the territory on which US peacekeepers are deployed will be as determined by the world body. However, third-party countries may provide bases or staging areas for the US peacekeeping force. We must understand, for instance, if the third-party host country has sympathies for one of the belligerents. If so, how far are they willing to support them? Could HN forces pose a threat to US forces? Are the HN forces

capable of providing adequate security for US forces?

- **Threat.** Even in PKO, you must understand the full military capabilities of the cobelligerents. This includes all OB factors and previous combat history in the area. US peacekeepers must be prepared for the possibility that they may be caught in the middle of renewed hostilities or come under attack from terrorists or armed civilians.

PEACETIME CONTINGENCY OPERATIONS

This operational category is by far the most diverse and demanding on the IEW system. It includes, but is not limited to—

- Shows of force.
- NEO.
- Strikes and raids.
- Operations to restore order.
- UW.
- DRO.
- Counter-drug operations.
- Security assistance programs.
- Support to US civil authorities.

These operations can occur at any time and at any place on the globe. Listing all the requirements for these missions would be impractical. As one example, though, we will discuss counter-drug requirements.

Counter-drug operations can fall under the heading of SAS, MTTs, intelligence sharing, or DOD support to drug interdiction. If carried out within US borders, it then falls under the heading of support to US civil authorities.

Currently, US policy is that we will not conduct direct combat operations against drug traffickers. However, we will support HN forces with intelligence, CSS, and training.

Counter-drug operations are similar to counterinsurgency operations—both in the manner in which the US supports the HN and in the tactics employed by the drug traffickers. In fact, most of the major insurgent groups in Latin America today are *narco-guerrillas.* Therefore, many of the intelligence requirements for counter-drug operations are the same as for counterinsurgency operations. Doctrinally, counter-drug operations fall under the LIC operational category of PCO. Counter-drug intelligence requirements are discussed in the PCO portion of this appendix.

As with the previous missions, we can apply the five basic intelligence categories to counter-drug operations with some minor variations:

- **Political.** What are HN political issues regarding US counter-drug assistance? Do the majority of the people support their government's counter-drug policy? What is the political sentiment on extradition of HN nationals to the US?
- **Economic and social.** What natural or preexisting social divisions make a segment of society more susceptible to the allures of the drug trade? What social groups are already taking part in the drug trade? What economic factors are pushing the population toward the drug trade? Does the economy offer reasonable alternatives? Are there signs of unexplained affluence among certain groups or in certain areas?
- **Geographic and environmental.** Where in the country are the climate and terrain factors favorable to the cultivation of drugs? When are the growing and harvest seasons? Where is the terrain concealment and cover, availability of water, and transport favorable to establishing processing plants? What natural and manmade LOC are available to the drug traffickers? What areas of the country are populated by pro-drug, anti-drug, or neutral segments which can influence drug trafficking? This includes manpower for harvest, transportation, and protection.
- **Military and security.** Is the HN security and military committed to the war on drugs? Are they trained and organized to carry out the mission? Can they react to US-provided or derived intelligence.
- **Threat.** What is the nature of the drug threat? Are they narco-guerrillas—that is, do they use drugs to finance their insurgency? Are they purely drug runners in it just for the money? What is their organization, tactics, weapons, level of training? What is their transportation capability? Where do the drug traffickers get precursor

chemicals? Do they have cross-border connections with other drug organizations or guerrillas?

SOURCES AND AGENCIES

Current intelligence is comprehensive, all-source data that is derived from both tactical and strategic sources. When combined with basic intelligence, it forms your operational data base and can identify planning refinements, additional training needs, operational requirements, and intelligence gaps.

DIA publishes daily and periodic reports on current intelligence developments. Also, US Unified Commands publish periodic intelligence summaries, especially during a regional crisis. Finally, the DA Office of the Deputy Chief of Staff for Intelligence issues a daily, worldwide, electronically transmitted intelligence summary (INTSUM) at a collateral classification level.

BASIC INTELLIGENCE SOURCES

Here are some of the basic sources that you can use to fill intelligence gaps in support of LIC operational missions. National products yield a great deal of the information needed and can be found in national and classified products such as estimates, surveys, area handbooks, periodic studies, and reports. Some of these are obtained by submitting a statement of intelligence interest (SII) through channels.

The Register of Intelligence Products (RIP), published by DIA, is a comprehensive list of products that assists you in completing your SII. Gaps or shortcomings in your information may be filled by going to unclassified sources such as educational institutions, financial institutions, and businesses.

Open sources such as weekly news magazines, encyclopedias, maps and geodetic surveys, wire services, and network television news can provide NRT local information to augment classified current intelligence reporting.

Informal Sources

An informal source is an individual or group that works outside the official structure but can provide invaluable information. They can include, but are not limited to, individual troops, general population, teachers, farmers, merchants, bar or pub owners, community leaders, organizers, and socialites.

These examples are all pertinent to operations inside the HN or the target area. Therefore, given the luxury of a cooperative HN, local HUMINT collection would be the most effective. However, PCO in which US forces are inserted without the consent of, or in direct opposition to, the local government will require unilateral collection.

Agencies

An agency is an organization designed to collect intelligence or information or perform other official functions in service to the government. These include, but are not limited to, tactical units, LEAs, intelligence and security units, health organizations, public welfare agencies, educational institutions, and government economic, legal, and agricultural agencies. The following list is not all-inclusive:

Federal Level:

- **CIA.** Strategic intelligence on full range of political, economic, social, and military topics.
- NSA. Strategic and tactical SIGINT.

Department of Defense:

- **DIA.** Strategic and operational intelligence with a focus on military matters.
- **National Military Intelligence Center (NMIC).** I&W, current intelligence.
- **Joint Tactical Intelligence Center (JTIC).** All-source analysis of information and intelligence gathered by DOD and non-DOD agencies, to include host government. JTIC produces tactical support packages (TSPs) for specific targets. Although the focus is primarily South American CI and counter-drug missions, it also supports purely conventional operations.
- **The Central America Joint Tactical Intelligence Center (CAJTIC)**—out of which JTIC evolved—is a subelement of JTIC with a focus on counterinsurgency operations.
- **Counter-drug JTFs 4, 5, and 6.** The JTFs are the counter-drug intelligence and operations center for United States Atlantic Command (LANTCOM) (Caribbean, Atlantic); Pacific Command (PACOM) (Pacific); and United States Army Forces Command (FORSCOM) (US-Mexico border, located at Ft Bliss, TX). They consist of personnel from each of the armed forces, the US Coast Guard, and US Customs.
- **Defense Medical Intelligence Agency.** Information on global medical phenomena, situations, and trends.

- **Defense Mapping Agency (DMA).** Global MC&G products.
- **Specified Commands, Global Unified Commands, Regional Unified Commands Joint Intelligence Directorate (J2).** The J2 oversees the Joint Reconnaissance Center (JRC), which manages all theater R&S (collection assets). The JRC also coordinates support from national level assets.
- **The Joint Intelligence Center (JIC).** This is a new name for an old concept. The name has been used before as a theater all-source intelligence center. Operation DESERT STORM proved the value of top-down intelligence where intelligence products were funneled through the JIC to theater army and down to the corps. Operation DESERT STORM gave the concept formal acceptance—Central Command (CENTCOM) and PACOM now have JICs.
- **Theater Special Operations Command (TSOC).** This command supports the theater commander by coordinating all intelligence requirements for in-theater SOF. Many LIC-related intelligence requirements can be met by this organization and its supporting IEW infrastructure.

Department of the Army:

- **INSCOM.** Various EAC intelligence products.
- **USAIA.** Operational and tactical intelligence imagery.
- **ITAC.** Threat analysis on full spectrum of military and terrorist threat.
- **MI brigades (EAC).** See Appendix A.
- **Army component commands of unified and specified command G2.** US Army South, Allied Forces, Central Europe (AFCENT), others.
- **Corps G2s.**

In addition to the theater army G2, MI brigades (EAC), and the Corps G2 and its MI brigade, there are other standard and nonstandard entities which exist at this level.

Theater Army Special Operations Support Command (TASOSC) is a functional command subordinate to the theater army. Under the TASOSC, the TASOSC ISE provides theater ARSOF with CM&D, target development, and intelligence liaison with other Army and theater IEW assets.

The US country team consists of principal representatives of the US departments and agencies working within a specific country. The team is headed by the Chief of Mission (usually an ambassador) and, therefore, is under DOS control.

The TAFT is a TDA-type organization with no set size, structure, or mission. Each individually tailored mission is to coordinate all US civilian and military activities in support of the host government. Military representatives on the country team include the Defense Attache, the individual service attaches, and the Chief of the SAO. These are excellent sources.

TATs are nonstandard organizations which support selected country teams in Latin America with real-time intelligence analysis. The mission and the situation in a country will determine the TAT's organization and function. As the focal point for fused tactical intelligence support from national, theater, and local assets, TATs are capable of funneling intelligence support to the host government through the country team. TATs can support counterinsurgency, counter-drug, and other LIC missions.

Non-DOD Agencies: Non-DOD agencies play an important role in the nonmilitary aspects of LIC. In CONUS, they can assist MACOMs with broad informational categories. Many agencies are also present in the host countries and are part of the US country team. Following are some significant non-DOD agencies:

- **Office of the National Drug Control Policy (ONDCP).** The national drug coordinator recommends anti-drug policy to the President. Based on input from other agencies, the ONDCP publishes the annual National Drug Strategy under the President's signature. ONDCP is a coordinating staff and has no control over any of the agencies employed in counter-drug operations.
- **DOS.** This is the lead agency for US foreign policy. With the exception of some combat situations where the theater or JTF CINC is in control, DOS (through the US Ambassador), has authority over all US activities in a host country. The DOS, both in CONUS and OCONUS, can provide current intelligence and information on the full range of informational categories.

- **USAID.** This is a major agency under DOS and is in charge of implementing US economic policies and programs in friendly nations. Although its focus is economic development, it has access to the full range of informational categories.
- **FBI.** This is the lead agency for domestic and international terrorist threat in the US. It investigates terrorist bombings and attacks on US citizens and facilities and conducts domestic narcotics operations.
- **DEA.** This is the lead US Government agency for drug interdiction (a role shared, in practice, with the US Customs Service). Aside from a managerial staff, DEA maintains two distinct career fields: drug enforcement agents and intelligence analysts. Agents operate in many locations in the US and in US embassies. Analysts process drug-related tactical and operational information at major field offices and operational and strategic information at DEA headquarters.
- **US Customs Service.** By virtue of its responsibility for inspection of goods coming into the US, the Customs Service shares responsibility for drug interdiction with the DEA. US Customs Service, by congressional declaration, is the lead agency for research and development of counter-drug technology.
- **INS and Border Patrol.** Until recently, neither the INS nor the Border Patrol was significantly chartered to conduct drug interdiction missions. However, the close association between illegal immigration and drug smuggling resulted in both agencies involved in drug seizures. The US Border Patrol has been responsible for some of the largest total annual seizures of drugs—even though it is not specifically tasked with that mission.
- **US Coast Guard (USCG), DOT.** The USCG works extensively with DOD, US Customs Service, and DEA in the seizure of illegal drugs in US and, under certain circumstances, international waters. USCG Law Enforcement Detachments (LEDETs) are frequently used aboard US Navy vessels to perform seizures and arrests on the high seas.
- **El Paso Intelligence Center (EPIC).** This center includes personnel from a number of US Government agencies under the supervision of DEA. EPIC personnel perform analysis and dissemination of counter-drug intelligence.

HN Agencies: These are normally the best sources of information. However, usually the user has to be in-country and have good working relationships with the HN officials. While this is possible, we must remember that these agencies are not under our control and may not always be willing to divert resources to support our requests.

- **HN cabinet level offices.** Economic, social, education, and others can provide basic information.
- **Other HN offices and departments.** Medical, census, labor, agriculture, communications, public works, and utilities.
- **HN defense and security offices.** Central and regional level, to include regional intelligence centers.
- **HN regional level departments.** Economic and social data on specific regions and areas of the country.

HN RICs or area coordination centers (ACCs) belong to the HN and are all-source, multi-agency intelligence centers located at the host country tactical level. Their mission is to coordinate and analyze all intelligence activities within their AO.

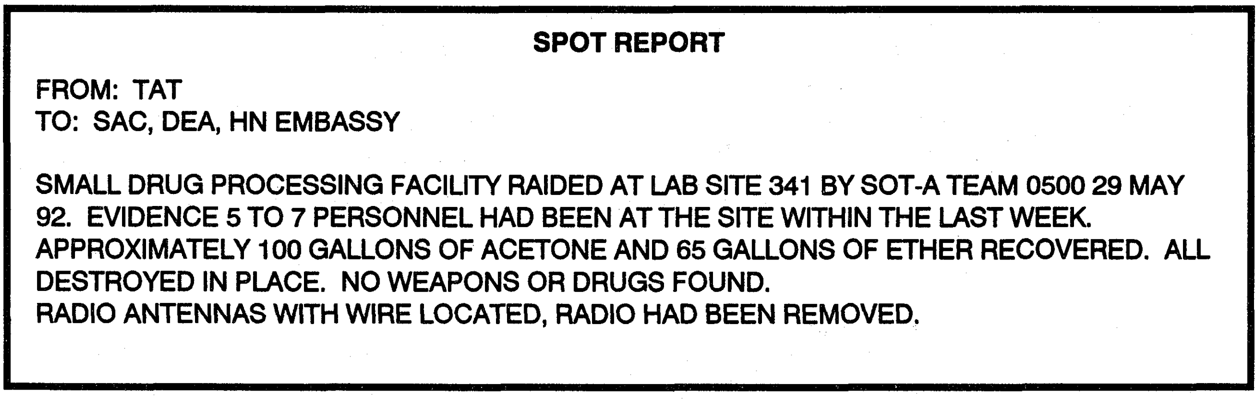
RICs and ACCs support military and paramilitary forces with all-source intelligence, and coordinate with local nonmilitary counterinsurgency, counter-drug, or IDAD activities. In the case of El Salvador, US advisors were present at the RIC to provide training and advice. In the Philippines, where they are known as ACCs, there are no US military advisors present.

APPENDIX F
REPORT FORMATS

This appendix provides a brief description of the most common intelligence-related formats, including those formats used to pass information of immediate potential intelligence value from one echelon to another.

SPOT REPORT

The SALUTE mnemonic requires users to report enemy size, activity, location, unit (or uniform), time, and equipment. Figure F-1 shows a spot report using a narrative format.



SPOT REPORT

FROM: TAT
TO: SAC, DEA, HN EMBASSY

SMALL DRUG PROCESSING FACILITY RAIDED AT LAB SITE 341 BY SOT-A TEAM 0500 29 MAY 92. EVIDENCE 5 TO 7 PERSONNEL HAD BEEN AT THE SITE WITHIN THE LAST WEEK. APPROXIMATELY 100 GALLONS OF ACETONE AND 65 GALLONS OF ETHER RECOVERED. ALL DESTROYED IN PLACE. NO WEAPONS OR DRUGS FOUND.
RADIO ANTENNAS WITH WIRE LOCATED, RADIO HAD BEEN REMOVED.

Figure F-1. Spot report in narrative format.

INTELLIGENCE ESTIMATE

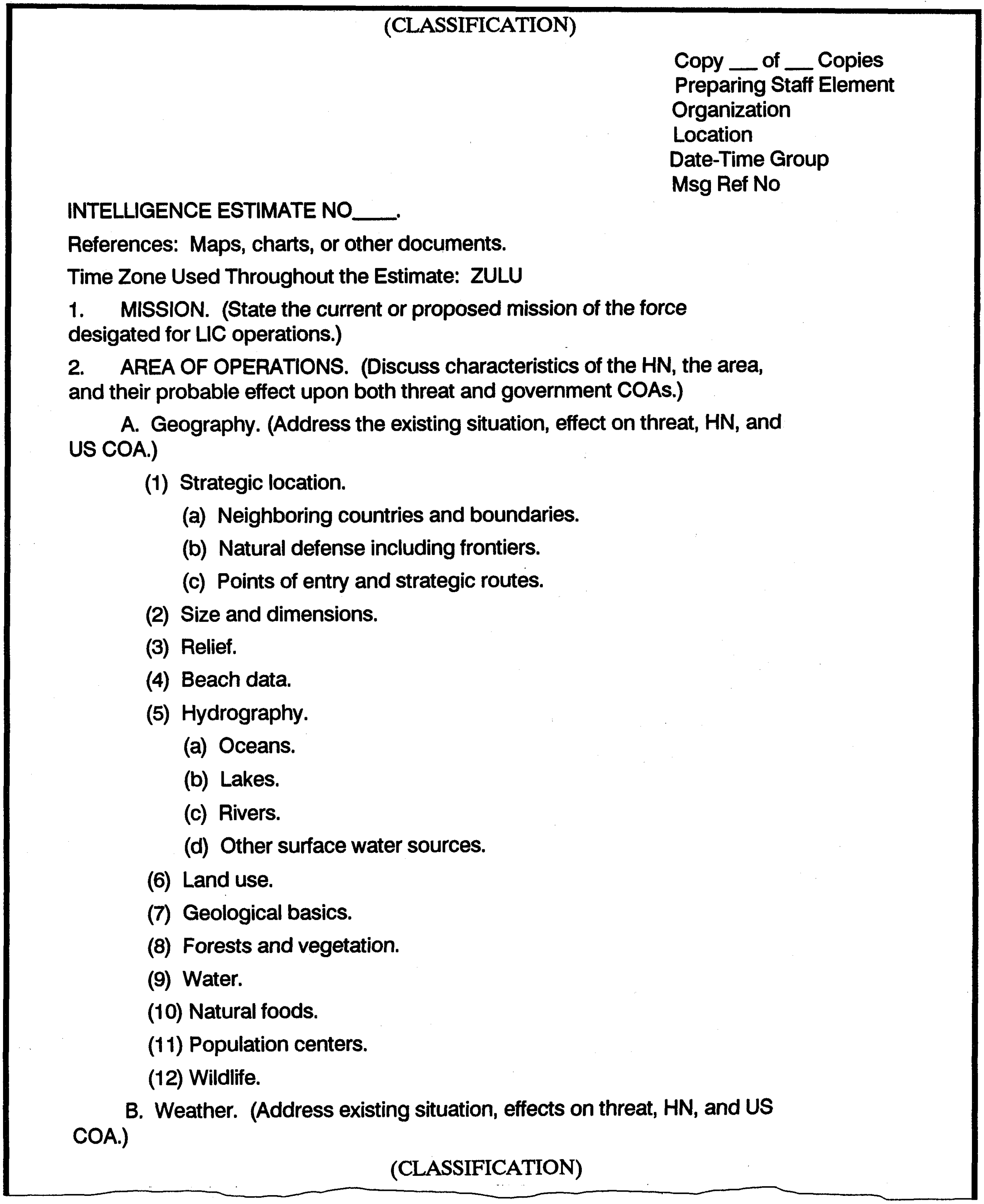
The intelligence estimate consists of seven paragraphs. The first paragraph is a restatement of the mission. The remaining paragraphs outline an analysis of the battlefield area based on—

- IPB.
- An estimate of enemy strengths, capabilities, and limitations.
- The S2 or G2 conclusions about the total effects of the AO on friendly COAs, COAs most likely to be adopted by the enemy, and exploitable enemy vulnerabilities.

Figure F-2 shows an intelligence estimate used in LIC missions. This format will have applications to the battlefield operations.

Figure F-3 is an example of an MDCI annex, which is used as the dissemination tool for CI analysis reporting.

Examples of imagery reports are in TC 34-55. Make sure you find out the types of reports that will be provided by your support unit.



(CLASSIFICATION)

Copy ___ of ___ Copies
Preparing Staff Element
Organization
Location
Date-Time Group
Msg Ref No

INTELLIGENCE ESTIMATE NO____.

References: Maps, charts, or other documents.

Time Zone Used Throughout the Estimate: ZULU

1. MISSION. (State the current or proposed mission of the force desigated for LIC operations.)

2. AREA OF OPERATIONS. (Discuss characteristics of the HN, the area, and their probable effect upon both threat and government COAs.)

A. Geography. (Address the existing situation, effect on threat, HN, and US COA.)

(1) Strategic location.

(a) Neighboring countries and boundaries.

(b) Natural defense including frontiers.

(c) Points of entry and strategic routes.

(2) Size and dimensions.

(3) Relief.

(4) Beach data.

(5) Hydrography.

(a) Oceans.

(b) Lakes.

(c) Rivers.

(d) Other surface water sources.

(6) Land use.

(7) Geological basics.

(8) Forests and vegetation.

(9) Water.

(10) Natural foods.

(11) Population centers.

(12) Wildlife.

B. Weather. (Address existing situation, effects on threat, HN, and US COA.)

(CLASSIFICATION)

Figure F-2. Intelligence estimate for LIC.

(CLASSIFICATION)

(1) Temperature.

(2) Precipitation.

(3) Wind (direction and velocity).

(4) Light data.

(5) Seasonal effect of weather on terrain and visibility.

C. Demographics.

(1) History.

(2) Ethnic.

(3) Languages.

(4) Social system.

(5) Education.

(6) Living conditions.

(7) Cultures.

(8) Religions.

(9) Taboos.

(10) Grievances.

(11) Psychology (behavior patterns and motivating factors).

D. Politics. (Address existing situation, effect on threat, HN, and US COA.)

(1) National government.

(a) Structure.

(b) International orientation.

(c) Degree of popular support.

(2) Political parties.

(3) Foreign dependence or alliances.

(4) Controls and restrictions.

(5) Laws (civil and religious).

(6) Grievances.

E. Economics. (Address existing situation, effect on threat, HN, and US COA.)

(1) Current value of money, wage scales.

(2) Financial structure: To include national and international banking system.

(3) Foreign dependence.

(a) Assistance programs.

(b) In-country business.

(CLASSIFICATION)

Figure F-2. Intelligence estimate for LIC (continued).

(CLASSIFICATION)

(c) Trade agreements.

(4) Agriculture and domestic food supply.

(5) Natural resources and degree of self-sufficiency.

(6) Industry.

(a) Types (base and main industries).

(b) Production levels.

(c) Consumer demands.

(d) Unions.

(7) Black market and illicit trades (drugs, weapons).

(8) Technology.

(a) Capabilities.

(b) Expertise.

(9) Foreign trade.

(a) Type.

(b) Level.

(c) Transportation.

(10) Fuels and power.

(a) Locations.

(b) Quality.

(c) Production system.

(11) Mass communications.

(a) Telecommunications.

- Telephone.
- Telegraph.
- Television.
- Radio.

(b) Microwave systems.

(c) Satellite and laser systems.

(12) Transportation.

(a) Railroads.

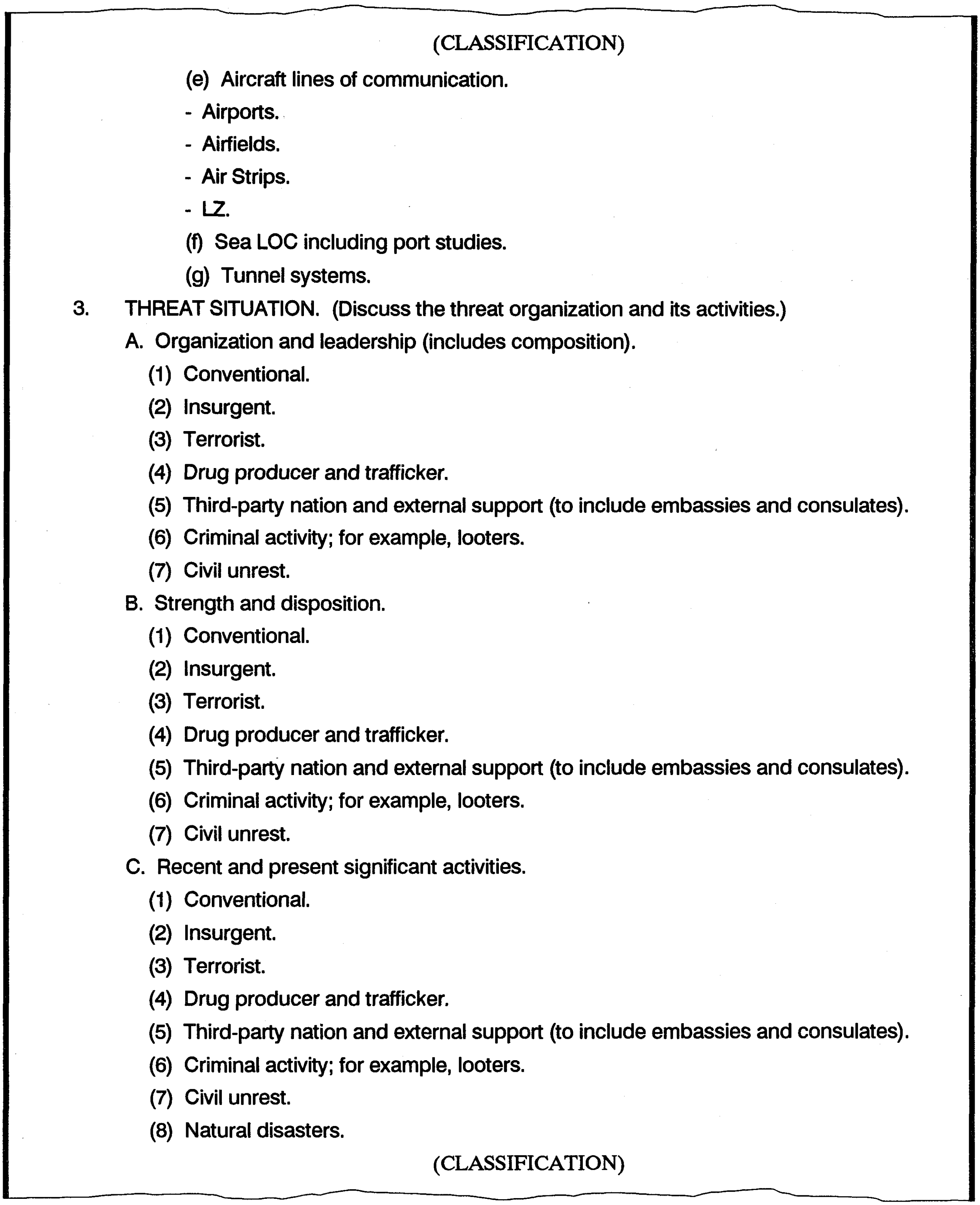
(b) Highways and roads.

(c) Trails and paths.

(d) Waterways and canals.

(CLASSIFICATION)

Figure F-2. Intelligence estimate for LIC (continued).



(CLASSIFICATION)

(e) Aircraft lines of communication.

- Airports.
- Airfields.
- Air Strips.
- LZ.

(f) Sea LOC including port studies.

(g) Tunnel systems.

3. THREAT SITUATION. (Discuss the threat organization and its activities.)

A. Organization and leadership (includes composition).

(1) Conventional.

(2) Insurgent.

(3) Terrorist.

(4) Drug producer and trafficker.

(5) Third-party nation and external support (to include embassies and consulates).

(6) Criminal activity; for example, looters.

(7) Civil unrest.

B. Strength and disposition.

(1) Conventional.

(2) Insurgent.

(3) Terrorist.

(4) Drug producer and trafficker.

(5) Third-party nation and external support (to include embassies and consulates).

(6) Criminal activity; for example, looters.

(7) Civil unrest.

C. Recent and present significant activities.

(1) Conventional.

(2) Insurgent.

(3) Terrorist.

(4) Drug producer and trafficker.

(5) Third-party nation and external support (to include embassies and consulates).

(6) Criminal activity; for example, looters.

(7) Civil unrest.

(8) Natural disasters.

(CLASSIFICATION)

Figure F-2. Intelligence estimate for LIC (continued).

(CLASSIFICATION)

D. Strengths and weaknesses.

(1) Conventional.

(2) Insurgent.

(3) Terrorist.

(4) Drug producer and trafficker.

(5) Third-party nation and external support (to include embassies and consulates).

(6) Criminal activity; for example, looters.

(7) Civil unrest.

4. THREAT CAPABILITIES. (List current insurgent capabilities and discuss them in regard to probability of adoption.)

A. Enumeration. (For each capability, include what, where, when, and how for each capability.)

(1) Basic capabilities.

(a) Conventional.

(b) Insurgent.

(c) Terrorist.

(d) Drug producer and trafficker.

(e) Third-party nation and external support (to include embassies and consulates).

(f) Criminal activity; for example, looters.

(g) Civil unrest.

(h) Natural disasters.

(2) Supporting capabilities. (Include intelligence, security, recruitment, organization, training, finance, and logistics.)

(a) Conventional.

(b) Insurgent.

(c) Terrorist.

(d) Drug producer and trafficker.

(e) Third-party nation and external support (to include embassies and consulates).

(f) Criminal activity; for example, looters.

(g) Civil unrest.

(h) Natural disasters.

B. Analysis and discussion. (Include all evidence supporting or rejecting the adoption of each capability.)

(CLASSIFICATION)

Figure F-2. Intelligence estimate for LIC (continued).

(CLASSIFICATION)

5. HN SECURITY.

A. Situation (as defined in paragraphs 3A, B, and C).

(1) Public order and internal security.

(2) Armed forces.

(3) External support and dependency.

B. Capabilities (as defined in paragraph 4A).

(1) Public order and internal security.

(2) Armed forces.

(3) External support and dependency.

C. Analysis and discussion. (Include all evidence supporting or rejecting the adoption of each capability.)

6. FRIENDLY AND NEUTRAL THIRD-PARTY.

A. Situation (as defined in paragraphs 3A, B, and C).

(1) Embassies and consulates.

(2) Military.

(3) Business interests.

B. Capabilities (as defined in paragraph 4A).

(1) Embassies and consulates.

(2) Military.

(3) Business interests.

C. Analysis and discussion. (Include all evidence supporting or rejecting the adoption of each capability.)

7. CONCLUSIONS. (Draw conclusions from the content of the preceding paragraphs and furnish a basis for selection of COAs to accomplish the assigned mission.

A. Effects of the operational environment. (State the total effect of the AO upon COAs.)

B. Probable threat COAs. (List probable threat COAs in order of relative probability of adoption.)

C. Threat vulnerabilities. (List exploitable threat vulnerabilities.)

/s/ ____________________
G2 or S2
(Commander if distributed
outside headquarters)

ANNEXES:

Distribution: (Only if distributed.)

Authentication: (G2 or S2 authenticates if commander signs.)

(CLASSIFICATION)

Figure F-2. Intelligence estimate for LIC (continued).

(CLASSIFICATION)

Headquarters
Place
Date, Time, and Zone

ANNEX____(MDCI) TO INTELLIGENCE ESTIMATE NO:____

References: MDCI Annex to AAO, MDCI Threat Assessment, and other IPB documents, maps, and charts.

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

2. FOREIGN INTELLIGENCE AND SECURITY SERVICE CAPABILITIES: Discuss the threat intelligence cycle, HUMINT, IMINT, SIGINT, and Levels I and II capabilities including C^3, organization, equipment, personnel, and doctrine. (Current situation and recent and significant activities.)

A. Ground R&S (visual observation, patrols, ground radar, infrared surveillance, unattended ground sensors).

B. Aerial R&S (intrusion flights, standoff flights, sensors, reconnaissance satellites).

C. SIGINT (airborne and ground-based communications and electronic intercept and direction finding).

D. Level I threat (espionage and subversion; controlled agents, SAEDA, propaganda, terrorism, and politics).

E. Level II threat (unconventional forces and sabotage operations; economic and military targets).

F. Guerrillas and insurgents.

G. CI.

H. Other (line crossers, refugees, EPWs, detainees, open sources of information.)

3. FRIENDLY VULNERABILITIES AND COUNTERMEASURES: Describe EEFI for each COA and respective vulnerability and identify proposed countermeasures.

4. CHARACTERISTICS OF THE LIC AO:

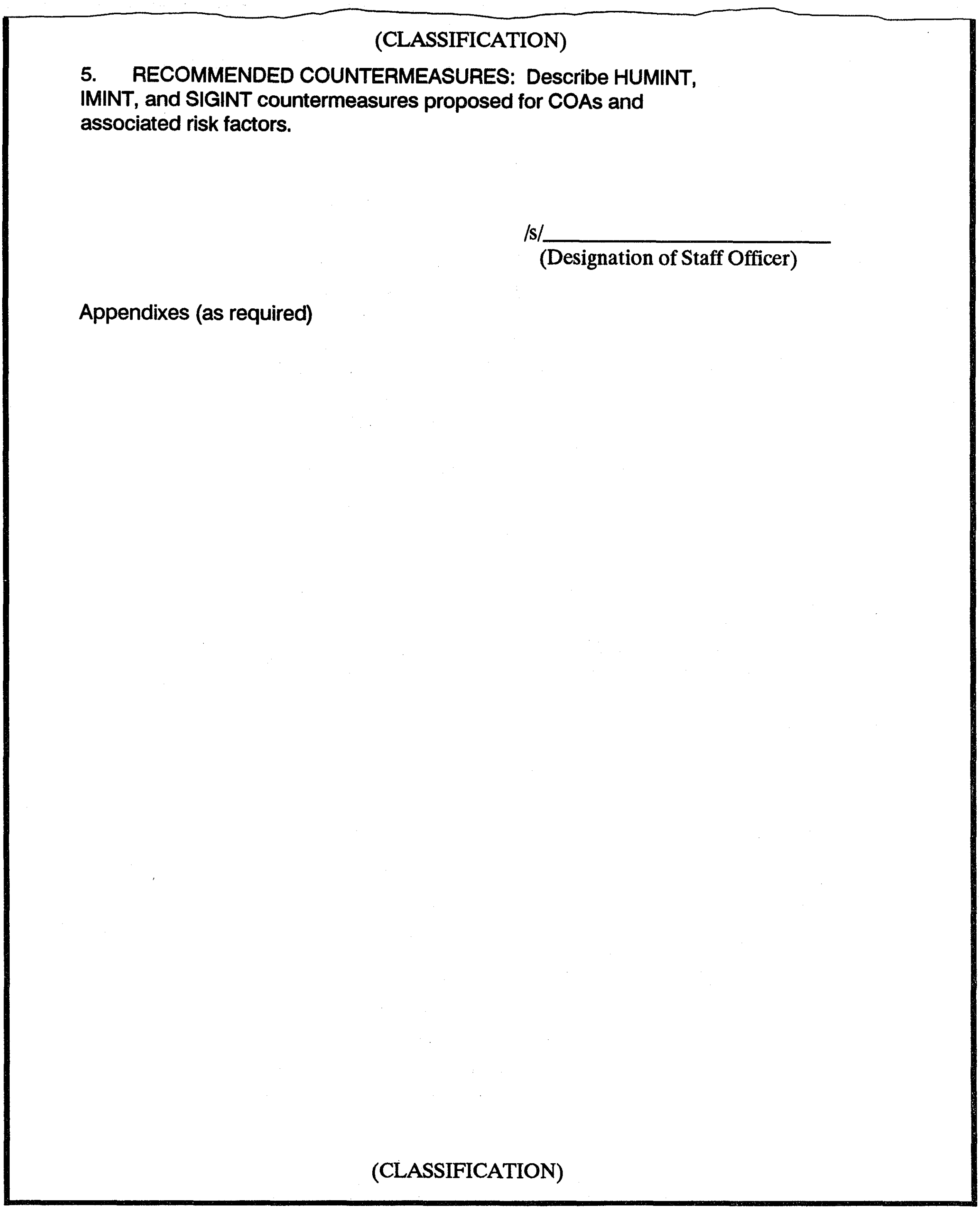
A. Weather. Evaluate the effects of weather on threat collection and Levels I and II capabilities, friendly vulnerabilities, and countermeasures.

B. Terrain. Evaluate the effects of terrain on threat collection and Levels I and II capabilities, friendly vulnerabilities, and countermeasures.

C. Other characteristics. Evaluate the effects of political, economic, demographic, and transportation on the threat collection and Levels I and II capabilities, friendly vulnerabilities, and countermeasures.

(CLASSIFICATION)

Figure F-3. MDCI annex.



(CLASSIFICATION)

5. RECOMMENDED COUNTERMEASURES: Describe HUMINT, IMINT, and SIGINT countermeasures proposed for COAs and associated risk factors.

/s/________________________
(Designation of Staff Officer)

Appendixes (as required)

(CLASSIFICATION)

Figure F-3. MDCI annex (continued).

APPENDIX G
LOW-INTENSITY CONFLICT INTELLIGENCE PREPARATION OF THE BATTLEFIELD GRAPHICS

During the evaluation process, you begin to identify the location of the threat. You do this by producing and fusing various templates or overlays to assist in the analysis. This appendix describes the overlays and templates used in the IPB process and provides examples of how each is used.

TERRAIN OVERLAYS

We produce five basic terrain overlays in LIC: population status, concealment and cover, logistics sustainability, key facilities and targets, and LOC. These overlays are heavily dependent on new data. You receive new information, develop new intelligence, and post it to the overlays.

POPULATION STATUS OVERLAY

As we have said before, population is the *key terrain* in all LIC operations. Population provides both support and security to the threat and represents the only terrain feature which must be seized, controlled, or defended. For example, the failure of an insurgent offensive in San Salvador, El Salvador, in November 1989, was a result of the insurgent's inability to mobilize the urban population against the government. This not only cost the insurgents the offensive but also severely undercut the credibility of their claim to represent the people's will.

The generic population status overlay geographically represents the sectors of the population that are pro-government, anti-government, and neutral in the built-up areas as well as the country's interior. Figure G-1 shows a population status overlay. This graphic may also display education, religion, ethnic, or economical aspects of the population.

A more refined product in a MOUT environment displays the exact homes and work places of key military, civilian, or subversive personnel as well as their relatives. In this instance, use large-scale maps or imagery to accurately plot the information by marking rooftops of buildings.

Such a refined product should be cross-referenced to OB files such as personality, faction, and organization. This graphic also assists the commander with his view of the battlefield and mission planning. This is also a good tool for prospecting for key nodes in built-up areas and factoring in the possibility of collateral damage to population and property.

This tool is also valuable in counter-drugs operations when used to show the quarters and work locations of known or suspected participants.

CONCEALMENT AND COVER OVERLAY

This product remains fairly constant throughout all facets of LIC; it graphically depicts the availability, density, type, and location of subversive concealment and cover. It should depict concealment and cover from the ground as well as from the air. See Figure G-2 for an example of this overlay.

In areas of frequent aerial attack or observation, overhead concealment and cover is important in selecting base camps, logistical bases, or drug laboratories. Surface configuration primarily determines cover. Here, cover includes caves and constructed features such as buildings, mine shafts, bunkers, tunnels, and fighting positions.

Vegetation is the primary feature that provides concealment. Some vegetation may provide concealment from both aerial and ground observation while other types will only provide concealment from the air or ground.

For example, picture a grove of cottonwood trees; bushy at the top and nothing below. This would prevent observation from the air but would allow observation from the ground. Conversely, tall saw grass or elephant grass would not permit observation from the ground. But from the air, trails and stop points would be observable.

The canopy closure overlay is critical in determining areas that offer concealment from aerial observation and is incorporated here. This is important when you are operating in an AO that is a tropical rain forest.

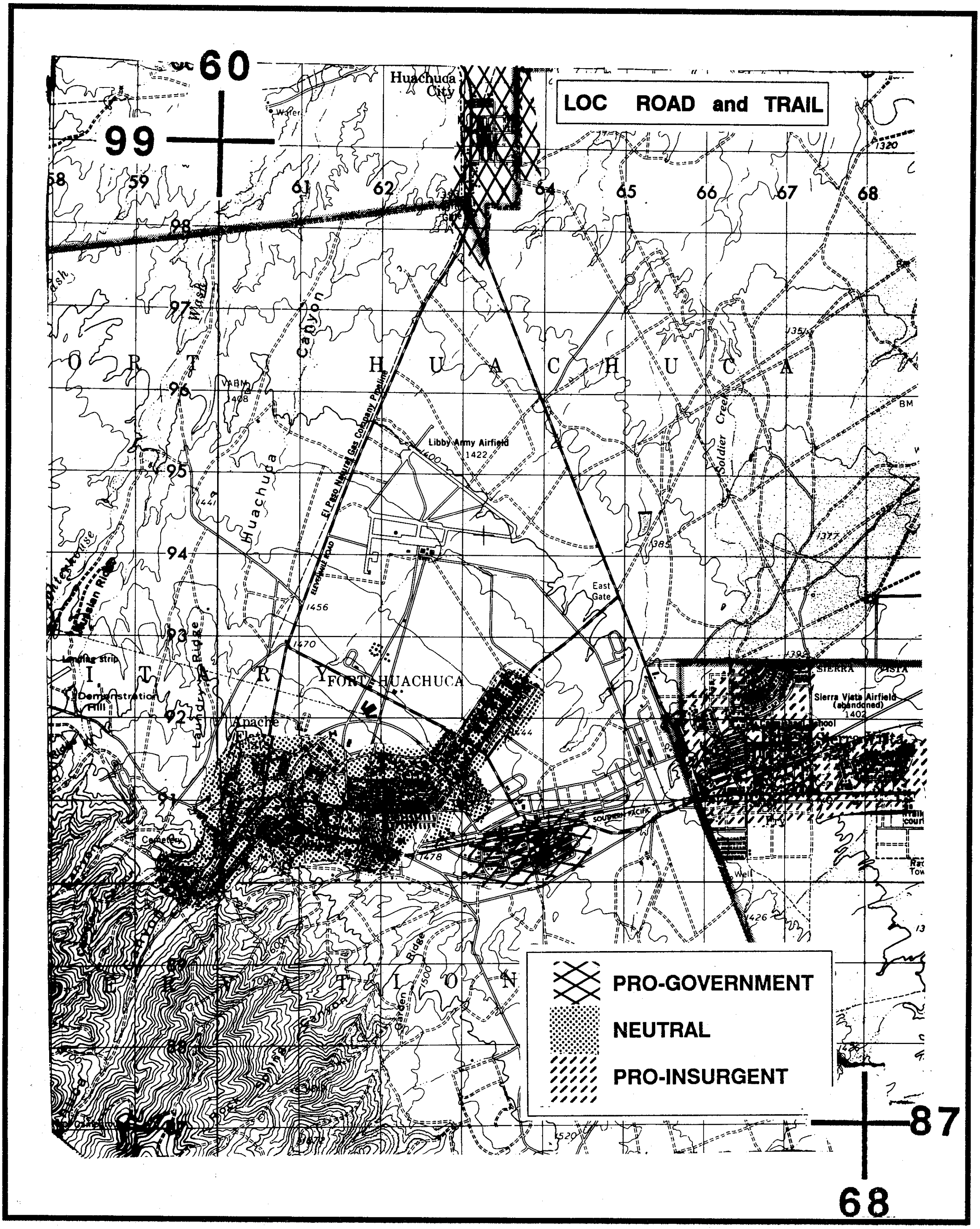


Figure G-1. Population status overlay.

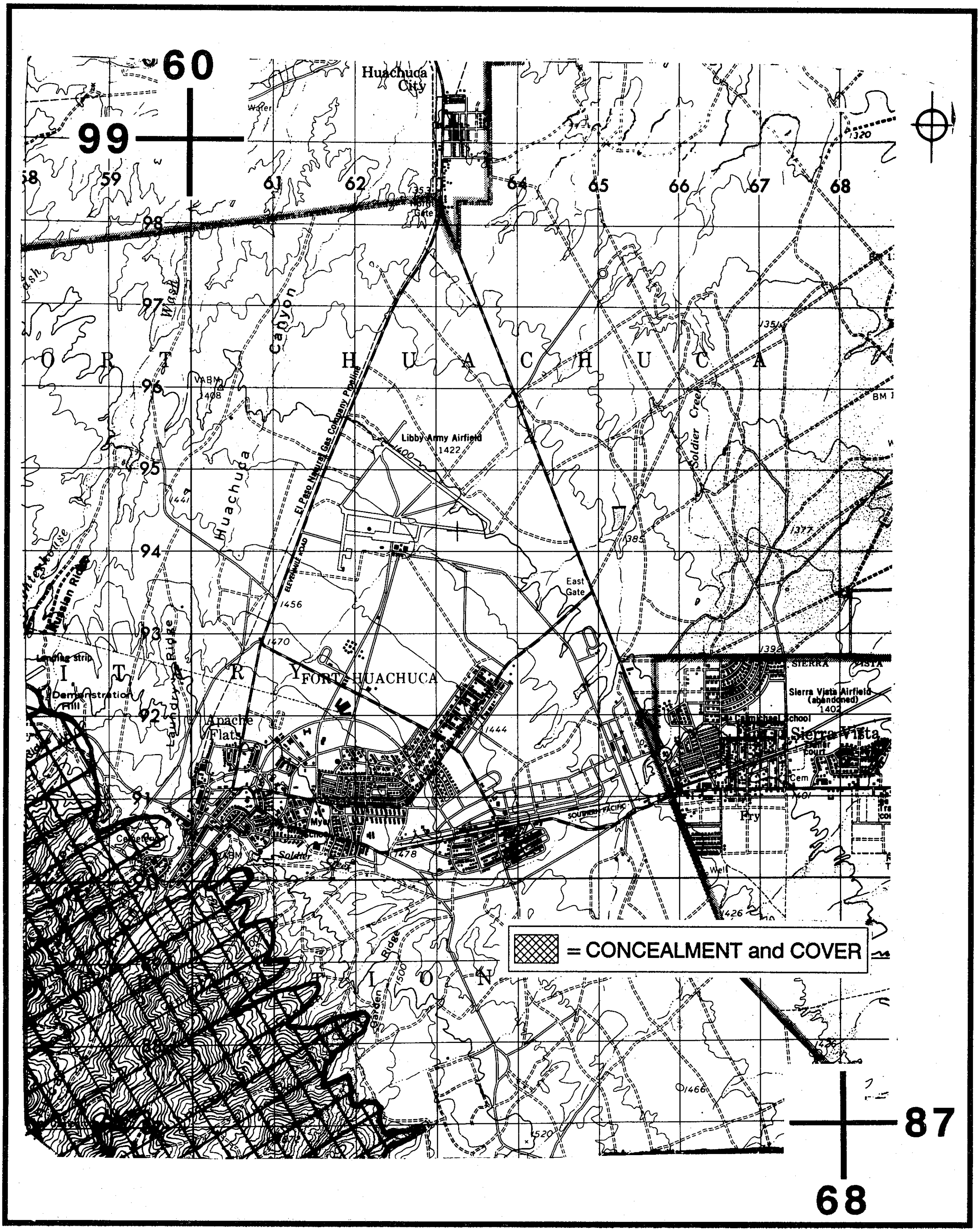


Figure G-2. Concealment and cover overlay.

In MOUT, it is obvious that the city itself provides concealment and cover to the subversive. To isolate probable locations or areas in use, begin with data from the population status overlay. Aside from locating quarters and work places of these individuals and their family members, begin identifying safe houses as well. Combine these locations with known rally points and meeting places and you have a good start on a concealment and cover overlay for MOUT operations.

LOGISTICS SUSTAINABILITY OVERLAY

In LIC missions, the subversives always require supply and resupply. As in conventional warfare the supply or logistics base is a key threat location. Here, though, we are more interested with the availability or sources of goods and services.

If the group is operating away from a built-up area, look at farms, orchards, growing seasons, and water sources. In a built-up area, focus on supermarkets, food warehouses, pharmacies, hospitals, clinics, and doctors' residences.

There are also unique applications for this overlay; in counter-drugs you want to identify the locations of suppliers of processing chemicals. In counterinsurgency you may need to locate businesses that sell PVC tubing that can be used in making mines and booby traps.

In PKO you may need to identify retail or wholesale outlets that sell printing materials that could be used for PSYOP products. The key to this function originates from your BAE: Know the subversive, his requirements, and the availability and location of his needs. Figure G-3 is an example of a logistics sustainability overlay.

KEY FACILITIES AND TARGETS OVERLAY

This product, formerly known as the trap overlay, shows the location of possible threat targets within your AO. Targets include banks, bridges, electric power grids, oil refineries, HN and US military installations, key residences, and places of employment of HN and US personnel. Figure G-4 is an example of a key facilities and target overlay.

This overlay requires refinement on some locations such as airfields and military installations. In these instances you have to determine what facilities at these locations are most susceptible to attack based on subversive capabilities and desires. For example, if the goal is to disrupt air traffic at an airfield, the control tower and fuel storage tanks would become lucrative targets as important as the runway itself. Direct mortar fire on runways cause minimal damage compared to that inflicted upon fuel storage tanks.

This type of information is significant to the commander and his planners, as well as to internal security and CI personnel. Discovering an indigenous worker pacing off the distance between a guard tower to the fuel storage area is a valuable indicator of threat intentions.

There are other instances when this overlay is extremely important, such as during a nation-building operation or a DRO when you may face lawlessness, pilfering, or looting. This overlay is a good tool for identifying those locations that are most likely to be struck by such activities: grocery, clothing, or appliance stores and supporting warehouses.

LINES OF COMMUNICATION OVERLAY

This seasonal tool, formerly known as the road and trail overlay, highlights roads, trails, railways, airfields, and major waterways in the AO. Carefully compare recent aerial imagery and map products to ensure updating new LOC to the final product.

If you are operating in a tropical rain forest region with a dense canopy, fresh-cut ground trails will not be observable from the air and will require specific map-tracking debriefings of US or HN patrols. This often proves to be a valuable indicator of potential threat activity.

For example, if a specific trail is freshly cut by unknown individuals once a month, pattern analysis may reveal that at about the same time the trail is cleared each month there has been some type of major action conducted by the threat force.

Therefore, this trail could be one of several LOC for the threat force to move into the area. This lets the commander determine where he will attempt to interdict the next threat push.

Graphically represent waterways by displaying width, depth, velocity, navigability, and fording sites.

In MOUT operations it is important to develop a product that depicts both sewage and storm drainage systems. Another valuable product in MOUT is a depiction of public transportation routes (bus and subway) with timetables. Generally, these products should already exist and be readily available from the HN. Figure G-5 is an example of LOC overlays.

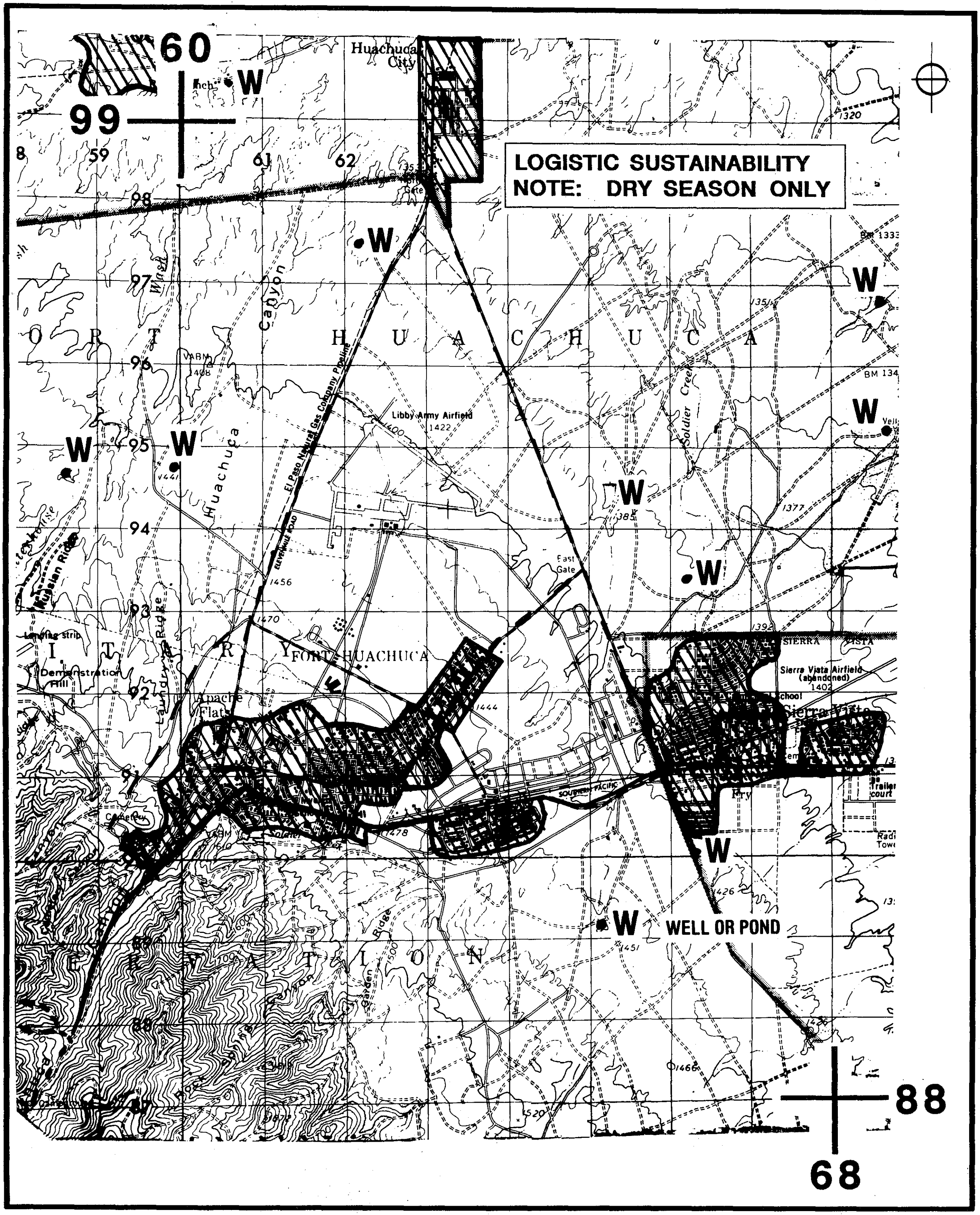


Figure G-3. Logistics sustainability overlay.

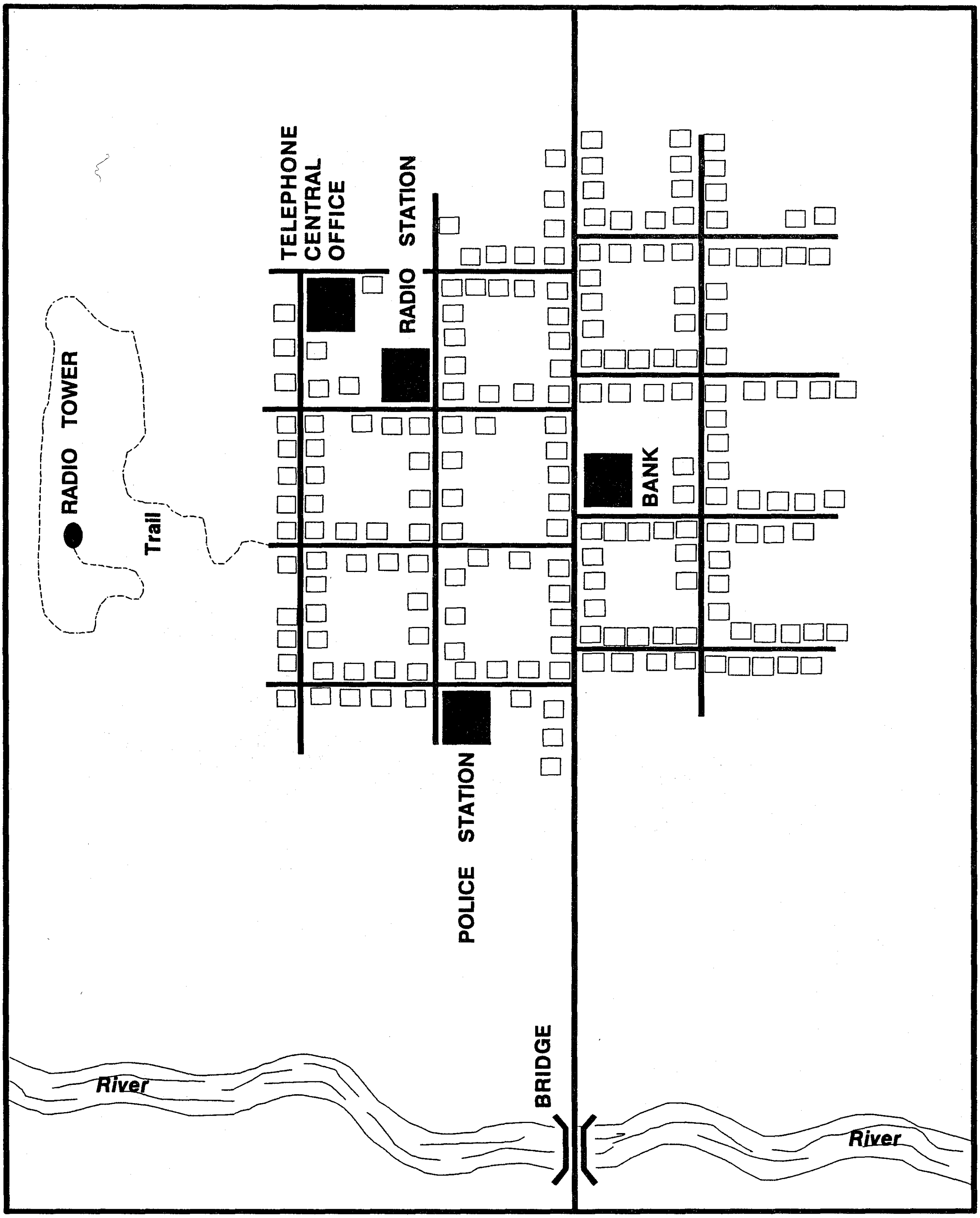


Figure G-4. Key facilities and target overlay.

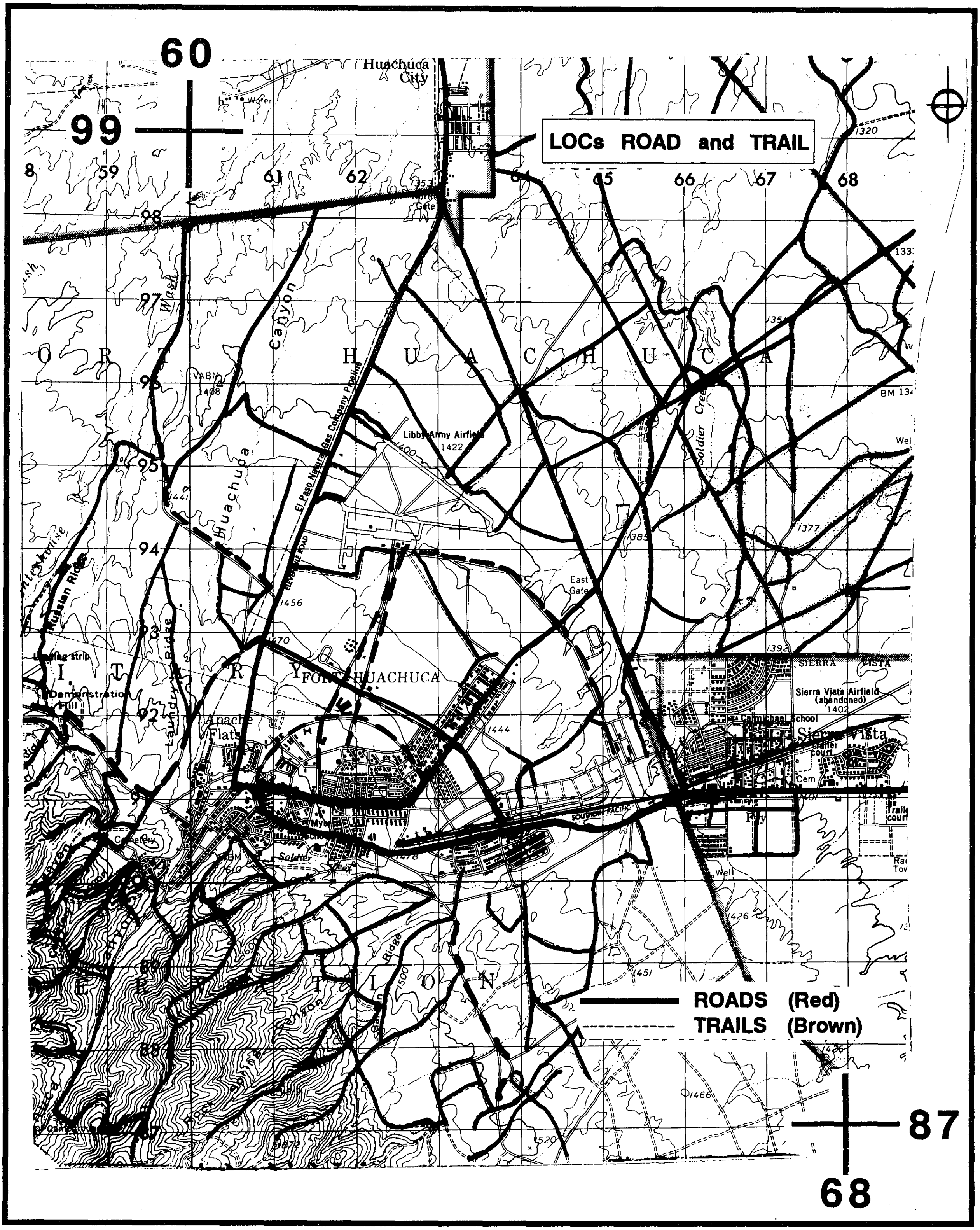


Figure G-5. LOC overlay.

OTHER OVERLAYS AND TEMPLATES

While the previous overlays are the most significant, there are others that you need to know about. They tend toward narrow focus and greater detail than the previous ones.

HOST NATION GOVERNMENT AND MILITARY OVERLAYS

These overlays depict the disposition of key personnel (homes and work locations), organizations, facilities, and key nodes of the HN. They are useful in any LIC mission, but are critical in nation-building or DRO. Locations recommended for inclusion are—

- Key personnel and leaders' homes and work places, their immediate relatives, and the routes taken to and from work.
- Military installations, LEA, and fire departments.
- Public utilities such as telephone, power, garbage dumps, sewage treatment plants. Add water purification facilities, including the locations of business offices and substations.
- Radio, television, newspaper, and printing facilities to include transmitters and repeater sites.
- Embassies and consulates.
- Universities and secondary schools.
- Hospitals, clinics, Red Cross, and Red Crescent facilities.
- Religious facilities (churches, synagogues, mosques).
- Banks.
- Public markets.
- Cultural centers and tourist points of interest.
- Judicial, executive, and administrative centers.

NONBELLIGERENT THIRD-PARTY OVERLAYS

These overlays are used for the same purpose as those described for HN. They are beneficial in NEO missions. Consider the value of these overlays during Operation JUST CAUSE when forces were searching for General Manuel Noriega. Had all nonbelligerent locations been depicted, and fused with the SITMAP, perhaps someone would have *seen* the Vatican's Papal Nuncia.

WEATHER OVERLAY

Weather analysis or templating in LIC does not differ a great deal from that conducted during the standard process.

Weather effects on observation and fields of fire, camouflage, helicopter LZs, and LOS for radio and radar equipment still apply.

A thorough knowledge of regional climatic conditions, as well as the usual evaluation of short duration weather forecasts, is needed to determine the effects of weather on unit mission.

In the areas of great seasonal climatic change, terrain intelligence produced during one season may be practically useless in others. Therefore, weather effects, based on observed or forecast weather and terrain analysis must be fused and continuously updated. Weather effects on systems, operations, and personnel are detailed in Chapter 3 and FM 34-81-1.

SITUATION TEMPLATE

You use situation templates to show how threat, friendly, and nonbelligerent third-party forces might operate and communicate within constraints imposed by meteorological conditions and geography. The situation template is basically a doctrinal template with terrain and weather constraints applied.

It is used to identify critical threat, friendly, and nonbelligerent activities and locations. It provides a basis for situation and target development and HVT analysis. A situation template is a visualization of what a particular force might do at a certain time and place. In a counterinsurgency operation, this template might be substituted for a target analysis overlay.

EVENT TEMPLATE

Event templates show locations where critical events and activities are expected to occur and where significant targets and opportunities will appear. You use these templates to predict time-related events within critical areas. They provide—

- A basis for CM.
- Threat, HN, and third-party COAs.
- HVT locations and tracking.

They depict NAIs; the events, the sequence of activities, and relationships that should occur for each

COA. The SOF SIO in FID, for example, attempts to identify significant actions the insurgents may take, such as—

- Engage in nationwide economic sabotage.
- Assassinate mayors in contested regions.
- Negotiate with the government.

As the forces are templated, critical areas become apparent, significant events and activities will occur, and targets and opportunities will appear. Figure G-6 shows insurgent planning for an operation. These NAIs are points or areas where human activity or lack of activity will confirm or deny a particular COA.

Events within NAIs can be analyzed for indicators in which intelligence and target acquisition resources can be directed to look. NAIs and SIR are incorporated into the collection plan.

You may have to correlate types of events with historical or insurgent commemorative dates; for example, identify a historical or commemorative day or time frame during which the insurgents are likely to be active. You then identify the types of training, logistics, intelligence, and tactics the insurgents would likely employ.

One insurgent COA may be to seize a small district capital on a national holiday and hold it for 24 hours. The hope is to trigger an anti-government insurrection among the inhabitants. Insurgent planning for such operations require—

- Detailed HUMINT.
- Deception.
- Psychological preparation of the populace.
- Pre-attack surveillance.

Specialized assault teams in the opening stage of the assault should identify and target selected key nodes, such as—

- Police stations.
- Military garrison headquarters.
- Government radio and television stations.
- Telephone exchanges.
- Power plants.
- Fuel depots.

To do all of this, the insurgents require—

- A battalion-sized assault force.
- Direct and indirect fires.
- Possibly antiaircraft weapons.
- Propaganda teams.
- Population screening and control.

Therefore, the insurgents must designate assembly areas and routes to the objective. These insurgent activities can be observed by establishing NAIs and TAIs. Figure G-7 is an example of a TAI within a NAI.

DECISION SUPPORT TEMPLATE

You use the DST to show decision points keyed to significant events and activities. The DST is the intelligence estimate in graphic form. It does not dictate decisions to the friendly commander, but rather identifies critical events and human activities relative to time and location that may require tactical or operational decisions by that commander.

DSTs identify where and when targets can be attacked or other opportunities exploited to support the commander's mission concept.

A TAI is an area or point along an infiltration or maneuver corridor (MC) where friendly interdiction of threat forces will cause them to change their plans. Examples of TAIs include key bridges, road junctions, checkpoints, DZs and LZs, known fording sites, and assembly areas. TAIs which are essential to the uninterrupted progress of threat forces are HVTs.

The identification of a TAI is a joint effort between the intelligence and operations staffs. In LIC, population groups can be TAIs for targeting by PSYOP, civil-military operations, and other nonlethal means.

Decision points are those operational events that require tactical or operational decisions. They are geographical and chronological points where the commander must make a decision in order to retain the initiative. Decision points can be NAIs or TAIs.

Decisions must be made early so they can be implemented in time, but they cannot be made until there are indications that particular events will occur and their locations accurately fixed. Decision points are determined by comparing times required to implement decisions, doctrinal movement rates (adjusted to

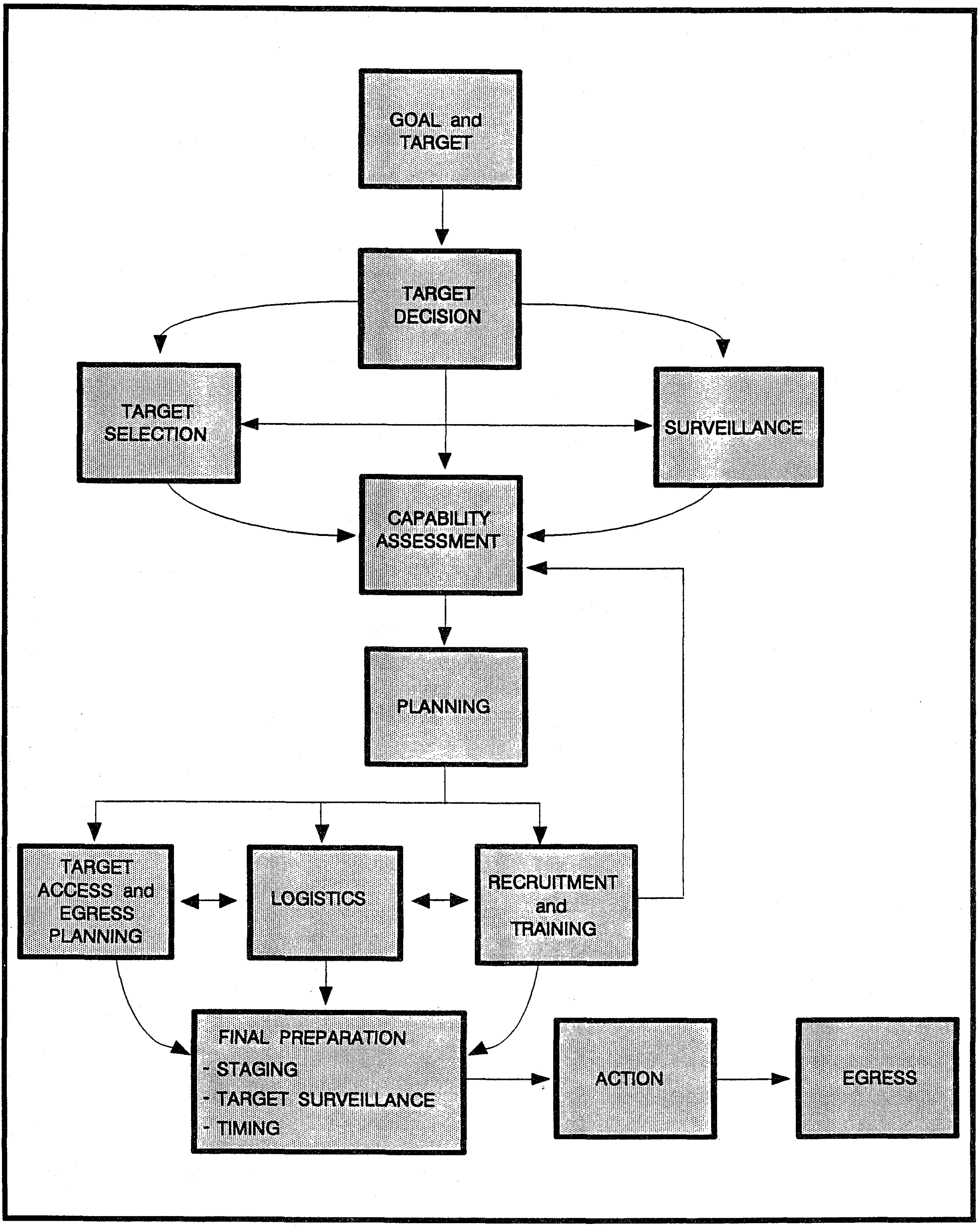


Figure G-6. Insurgent incident steps, drawn as an equivalent event template.

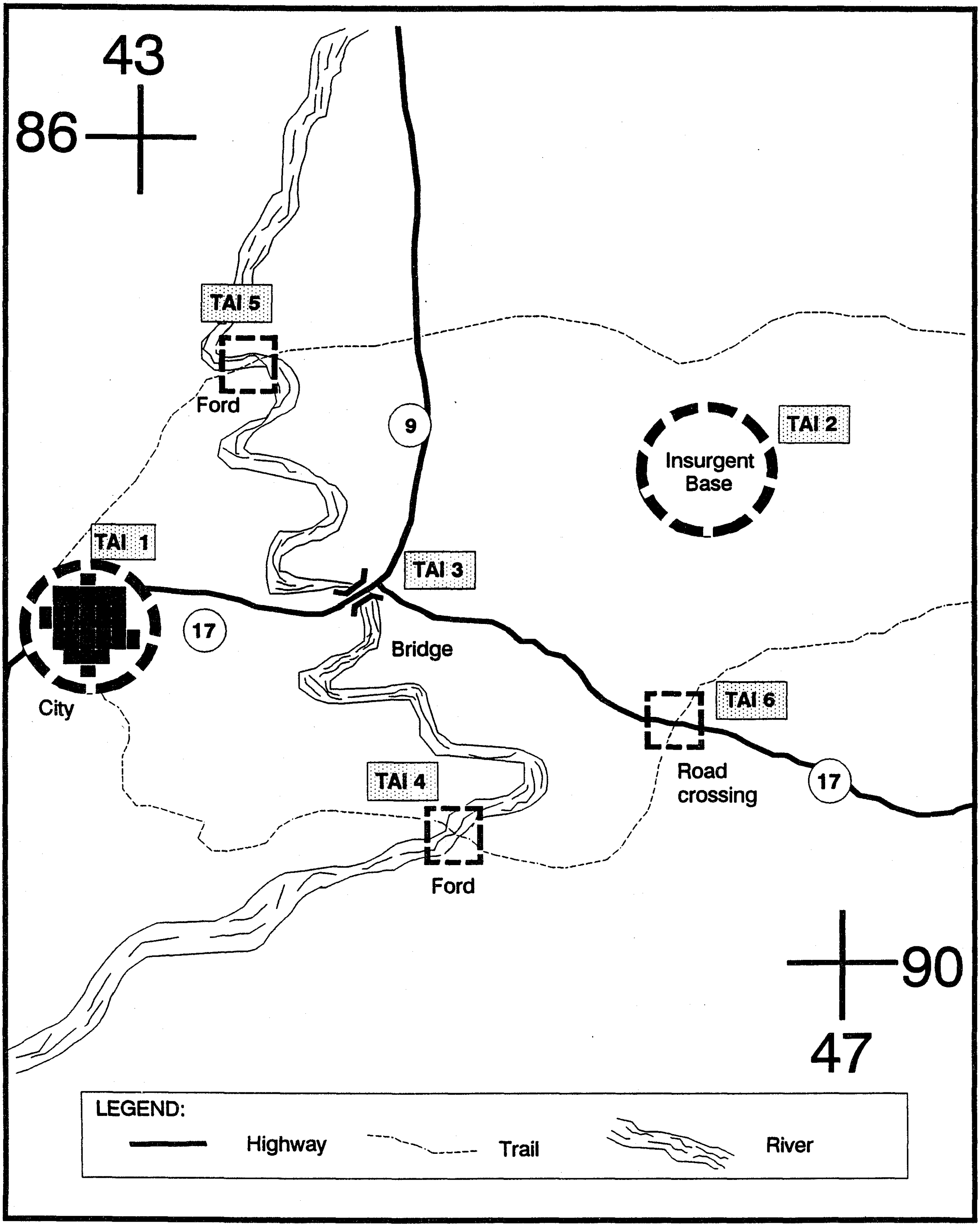


Figure G-7. TAI within an NAI.

compensate for the effects of weather conditions, terrain, and human action on mobility), and distances.

For example, if it requires 2 hours to implement a friendly decision, the decision must be made while the threat force is at least 2 hours from the TAI where the event will occur.

Time phase lines (TPLs) are based on threat doctrine, pattern, and trend analysis. They help to determine where the threat, friendly, or nonbelligerent third-party force will be and what it will look like. TPLs are drawn across an assembly area or MC to illustrate potential threat advance at doctrinal or historical rates, as modified by terrain and weather conditions. TPLs project where a particular force is expected to be at any given time.

THREAT INTEGRATION TEMPLATES

You may also produce a combination of locally produced standard and nonstandard templates during the threat integration step.

REACTIVE SITUATIONAL TEMPLATE

In counterinsurgency missions, the reactive doctrinal template, a kind of doctrinal template, becomes the reactive situational template (RST) when applied to the actual terrain in the operational environment. The RST shows uses of TPLs to forecast where the insurgents are likely to be in reaction to friendly actions. Figure G-8 is an example of an RST.

REACTIVE EVENT TEMPLATE

The RST becomes the reaction event template when you add NAIs and TAIs. Figure G-9 shows an example of a reactive event template.

REACTIVE DECISION SUPPORT TEMPLATE

This template is the reactive event template that has TAIs and decision points added. For example, in counterinsurgency decision points indicate when reaction and blocking forces would be inserted into the TAI. Or in counter-drugs, the decision points would indicate the shipment of the drug or precursor element. Figure G-10 is an example of a reactive decision support template.

NONCOMBATANT EVACUATION OPERATION EVENT TEMPLATE

The event template for NEO should portray any event that pertains to—

- The safety of US citizens in the country.
- Movements of threat forces.
- Status of all other parties involved in the operation.

The event template should depict the location, number, and status of all potential COAs, NAIs, TAIs, and decision points. NAIs will be potential assembly areas for evacuation to take place, likely choke points on roads, and possible locations of critical installations.

DISASTER RELIEF OVERLAY

Overlays for disaster relief include locations of critical facilities. Also important is the location of key people (within the national, state, and local governments) who can reestablish law and order, get government functioning again, and stabilize the situation. Formats outlined above can be tailored for this overlay.

DISPLACED PERSONS OVERLAY

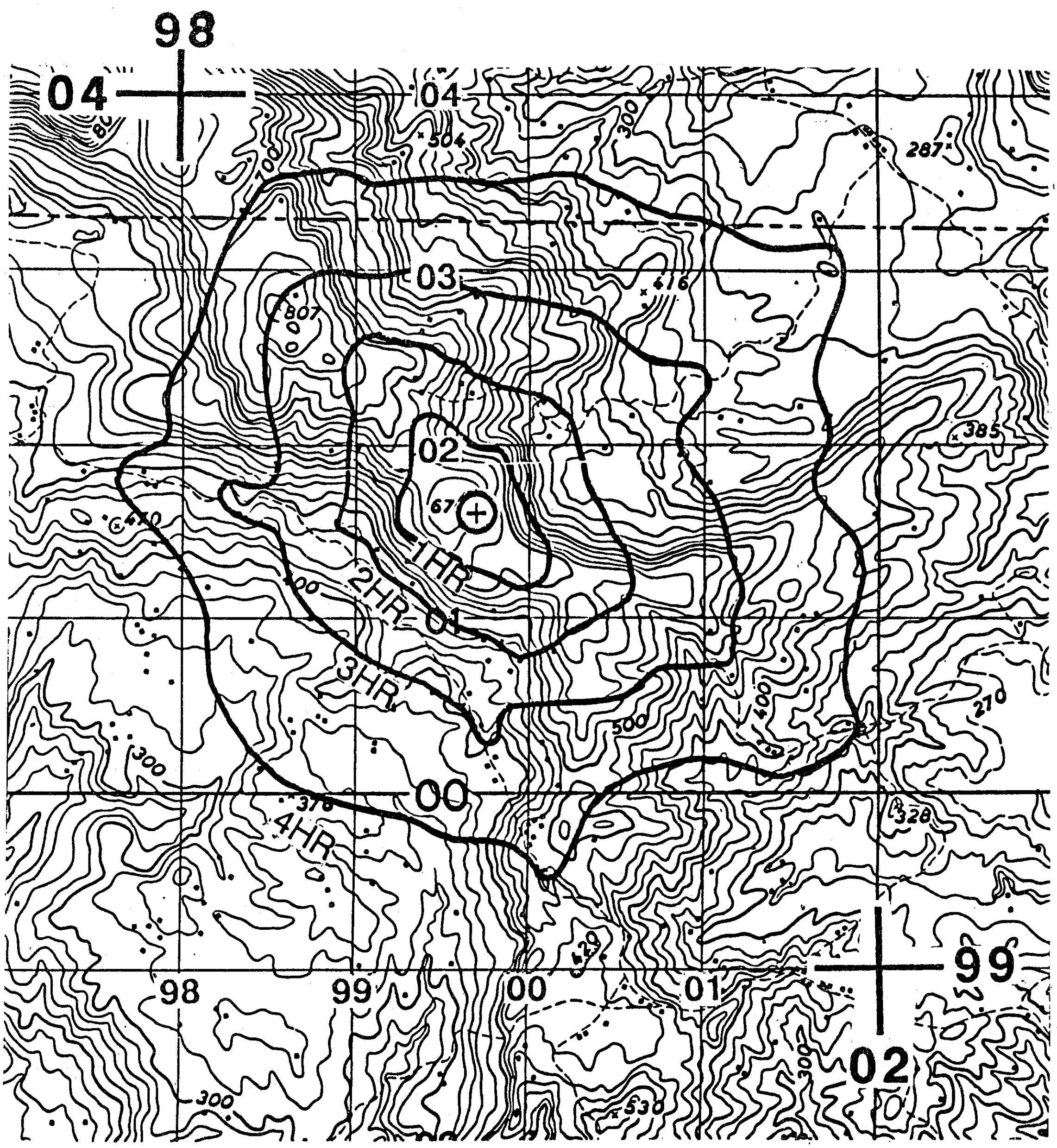
Graphic overlays for DP operations would include information on the—

- Location of existing and potential camps.
- Migratory routes which DPs take or will potentially take.
- LOC to get to the sites.
- Destinations.

Critical installations and facilities are also templated and analyzed for potential use. Again, adapt a previously shown format to display this overlay.

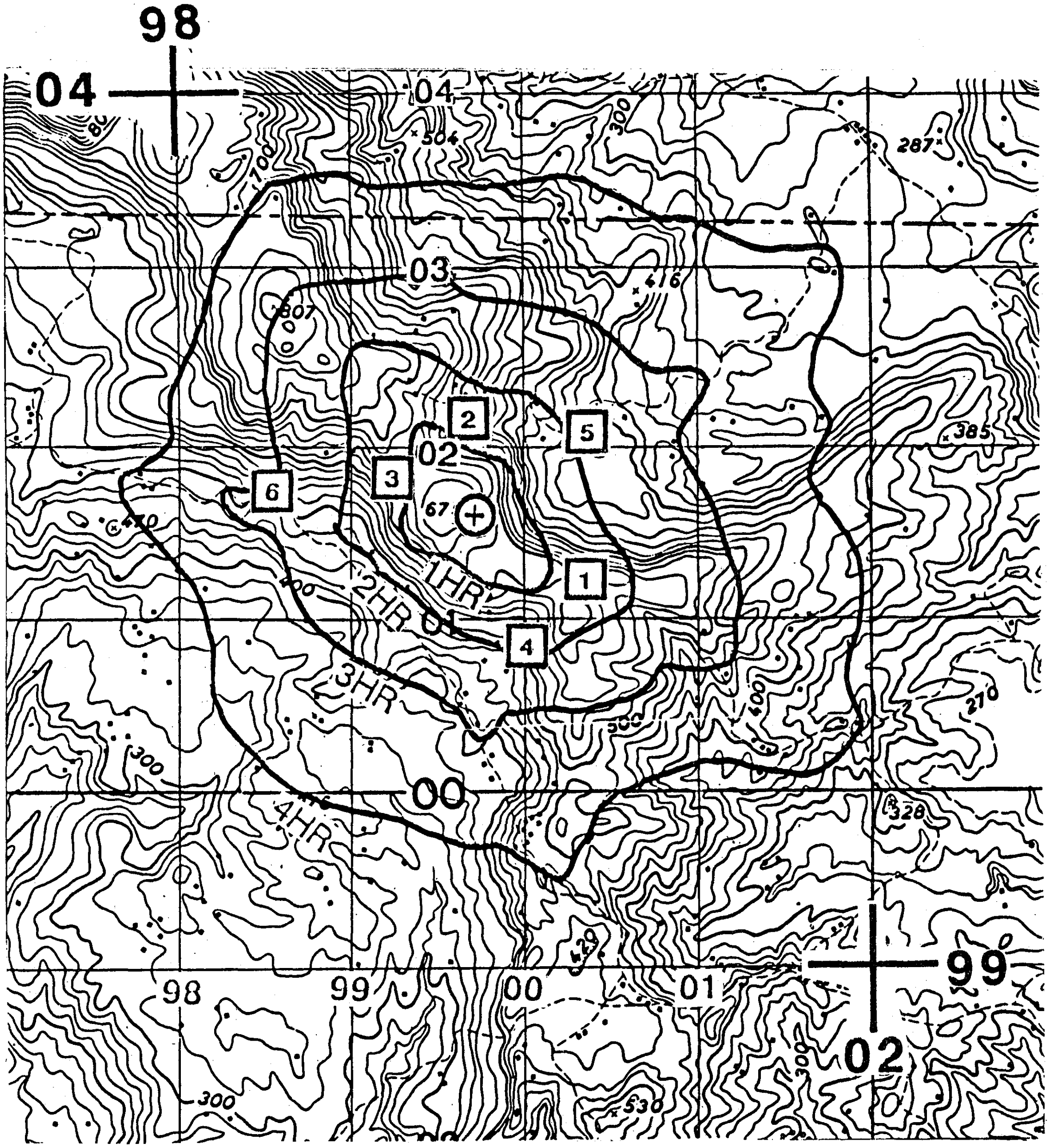
TARGET AREA REPLICAS

Whether LIC is being conducted in a rural or an urban environment, a key technique in destroying the enemy while not alienating the population is the surgical application of force. The entire planning effort for surgical assaults is greatly enhanced when you portray the specific battle area in detail.



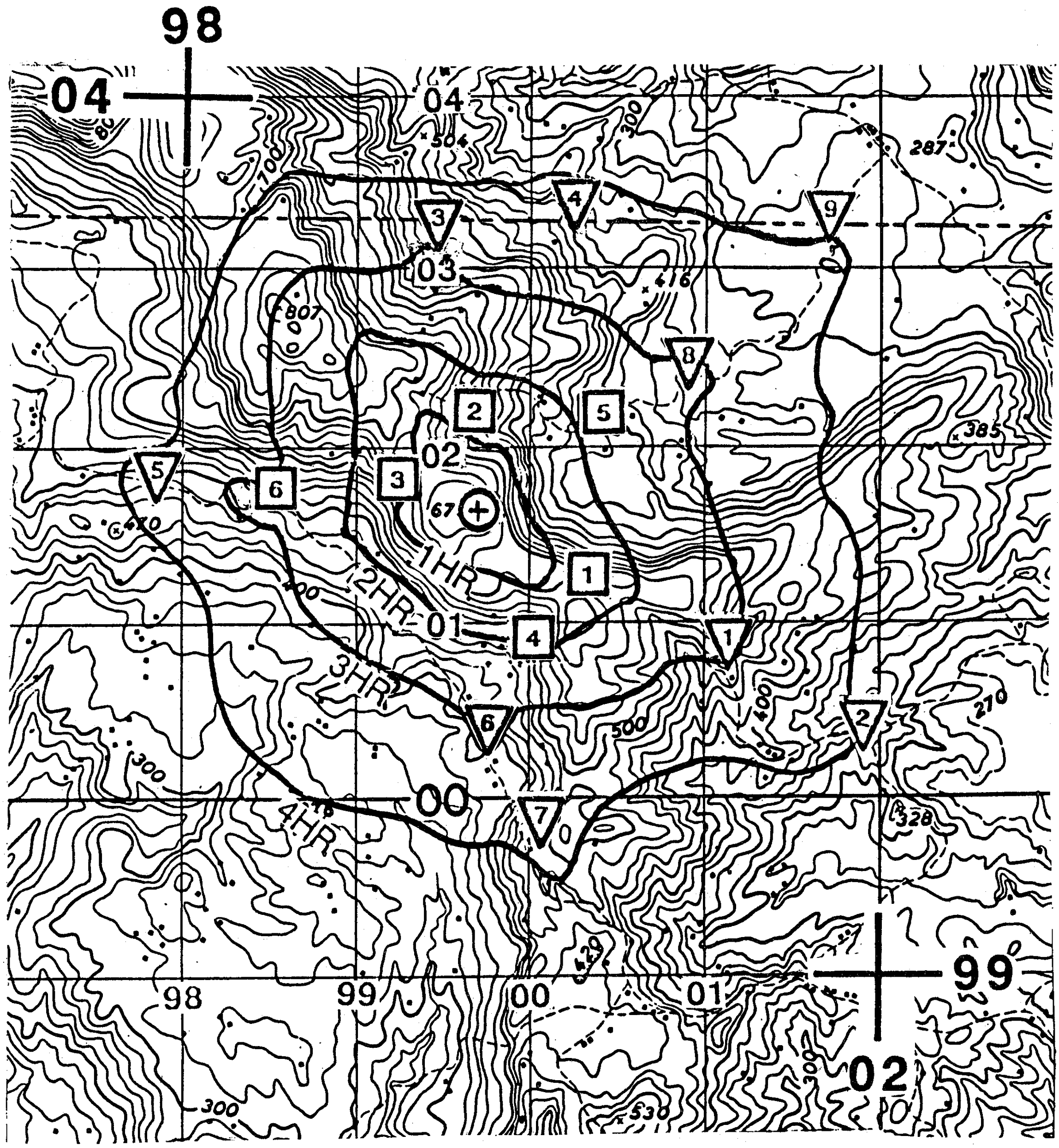
LEGEND: HR - Hour

Figure G-8. Reactive situational template for counterinsurgency operations.



LEGEND:
HR - Hour
No. - NAI

Figure G-9. Reactive event template for counterinsurgency operations.



LEGEND: HR - Hour ▽ - TAI □ - NAI

Figure G-10. Reactive decision support template for counterinsurgency operations.

Map scales of 1:50,000, as well as 1:12,500 city graphics, are usually inadequate for surgical planning and target identification.

Target area replicas (TARs) are a combination of the standard terrain model or sand table, with the addition of cultural features (buildings and vertical obstructions) at an appropriate scale for planning. TARs are as much a function of IPB as traditional overlays.

The process is imagery intensive and can be done over months, time permitting. You could do a TAR in hours with some loss of detail. All aspect imagery is required (stereo is ideal) for a fully detailed TAR; however, less than all aspect coverage is enough to begin.

Other aspects can be filled in later based on debriefing or reconnaissance reports. The level of detail depicted is usually a function of the target, mission, and possible schemes of maneuver.

Construction methods vary with the time, materials, and personnel resources available. TARs which are produced at one echelon and intended for dissemination to subordinate units must be built to survive transport. Locally produced TARs need not be moved and can be constructed more simply. In any event, all efforts should be made to have the TAR ready by COA development.

SCALE

If the target consists of a small complex of buildings—and infiltration points are not an issue—scales between 1:300 and 1:500 work well in depicting windows, doors, construction, and terrain features.

Larger targets (such as airfields, sections of a town to be cordoned and searched, or a target plus a distant infiltration point) require a smaller scale, varying between 1:800 up to 1:8,000.

AREA OF COVERAGE

The mission dictates the coverage required. On some missions where helicopter or parachute infiltration is followed by a ground approach, the model should cover the infiltration points, the most likely approaches, as well as the target itself.

Should the scale turn out to be too small for detailed coverage of the target itself, construct another, more detailed TAR of just the target.

Disposition of nearby hostile forces may require coverage of that unit's most likely avenue of approach. In any event, the target does not have to be in the center of the TAR.

SKILLS REQUIRED

IA are useful in TAR construction because they can read out the cultural details and provide measurements (particularly on the vertical plane). Topographic specialists often can conduct some imagery interpretation and work well with scale.

When necessary, anyone who can convert actual distances to a given scale can construct a TAR. Often, TARs that are rapidly constructed at the local level are built by untrained personnel using only eyeball proportions.

PORTABLE SAND TABLE METHOD

The fastest and easiest method of TAR construction involves a simple kit. Build a shallow, rectangular box with a hinged top. Inside the box, keep—

- An entrenching tool.
- A sturdy cloth bag suitable for carrying dirt and sand.
- Straight edge and ruler.
- Six quarts (or more) of mixed color lichen (used to represent vegetation and readily available at hobby shops).
- Various color paints, markers, and pencils.
- Several sharp hobby knives.
- Several sheets of white posterboard.
- Tongue depressors or popsicle sticks.
- Scrap balsa wood.
- Pins and thumbtacks.
- String.
- Thin dowels or cheap bamboo skewers and toothpicks.
- Large sheets of butcher block or tracing paper.
- A roll of acetate.
- White glue.
- A plastic spray bottle (for water).
- Hair spray.

After roughly establishing the desired scale and area to be covered, template the rectangular shape of your box onto the topographic map with a piece of acetate. Trace all the contours, roads, buildings, and power and treelines (include grid lines for reference).

If a viewgraph machine is available, project the traced image through the acetate onto a sheet of butcher block or tracing paper exactly the size of your rectangular box. Make sure that the projection is not at an oblique. Move the projector back and forth until the projected tracing exactly covers your pre-cut paper. Transfer the tracing onto your paper.

If a viewgraph machine is not available, sketch the tracing directly onto your paper by eye. This paper (now called the blueprint or sketch) should be tacked onto the lid of the box and will serve as the blueprint for TAR construction.

Place dirt or sand (remove rocks and twigs) into the cloth bag and place it in the box. Tack string across the box exactly where the grid lines are located on your blueprint or sketch. Spray the dirt with water until it will stay together while being shaped. Using acetate strips, draw vertical distance scales and tack these to the inside four corners of the box.

If you desire, a vertical exaggeration factor (often in the neighborhood of 1:4) can make terrain features stand out (do not let the dirt and sand level exceed the height of the box). Shape the dirt and sand with the tongue depressor, based on the contours depicted on the blueprint or sketch.

Use the vertical scales in the corners of the box to determine dirt and sand height. Spraypaint the terrain green (or brown or whatever the prevailing ground cover color).

Trace the roads, rivers, streams, and ponds from your blueprint sketch onto pieces of tracing paper. Cut these features out and color or paint them appropriately. In a hurry, colored pieces of string can substitute for painted paper. Place these carefully onto the dirt, using the terrain features and the grid lines for reference.

Place lichen to represent vegetation where required. On very large-scale TARs, individual trees are represented by placing a piece of lichen on a cut bamboo skewer or toothpick.

While this is being done, other personnel check the available imagery to add detail. First efforts are on the horizontal plane to update the blueprint or sketch with significant features not shown on the map. These include, but are not limited to—

- New roads or trails.
- Changes in treelines.
- Individual trees (depending on scale).
- Outlines of buildings.
- Defensive positions.
- Powerlines, poles, and the like.

The next, and perhaps hardest, step is detailed, scale sketches of buildings. These should be transferred, each view flat, onto the thick posterboard, complete with windows and doors. The posterboard is then cut and assembled with glue to form the buildings.

Paint can be applied if you have a feel for what the actual colors are on the buildings. Place the buildings onto the dirt in their correct locations.

Finally, search the imagery for additional vertical obstructions, which should be scaled, constructed, and placed appropriately on the TAR. With moist dirt, the box may be moved as necessary. If you want the dirt to stay together for an extended period, spray it liberally with hair spray.

TAR CONSTRUCTION FOR TRANSPORT

Building a TAR for transport to another unit involves a similar method, but with different materials. This process usually takes more time and supplies. Essentially, the blueprint or sketch plus cultural feature construction are the same.

Instead of using a box with dirt and sand, a baseboard of plywood is used with the ground contours built up with clay, layers of cut cardboard glued together, or plaster of paris (or any combination). Linear features such as roads and streams are painted onto the finished terrain, while buildings and vertical obstructions are glued in.

If the TAR will be too big for safe transport, it should be constructed on separate, smaller rectangular baseboards which can be placed together for display. Often, a protective box or covering is necessary to ensure the TAR arrives safely.

APPENDIX H

IMAGERY INTELLIGENCE SUPPORT TO LOW-INTENSITY CONFLICT

This appendix provides information that intelligence personnel must consider if imagery intelligence is to be used advantageously in LIC.

IMINT is the product of imagery analysis collected, classified, and evaluated for military use. IMINT is obtained from the analysis of imagery from photographic (optical), radar, and infrared sensor systems carried on ground, airborne, or orbital platforms.

The focus of imagery collection in LIC depends on the mission in which the unit is involved. In other words, the commander's PIR and IR drive the collection effort. See TC 34-55 for information on IMINT.

IAs are responsible for exploiting imagery from various sensors. Imagery can be hard copy (paper or film), or soft copy (graphics displayed on a monitor). IAs also generate reports and other imagery-derived products for dissemination to requesting units.

These products include, but are not limited to—

- Annotated prints.
- Overlays and graphics.
- Studies.

IAs examine the imagery to detect, recognize, identify, and locate objects and activities. They then analyze and deduce the significance of these indicators in a given area. Indicators differ from one geographic region to another, and by operational category.

For example, training facilities used by some insurgent groups in Central America are different from those used by a terrorist organization in the Middle East. The first facility is very basic and usually found in remote areas. The second is often a secure facility with modern equipment.

Indicators also change over time, as targeted groups alter their modes of operation to prevent detection or can afford to update their facilities. Chapters 5 through 8 discuss some possible imagery indicators or signatures for each operational category.

IMINT has varying degrees of usefulness in LIC operations. Long-term surveillance over the AO and AI is necessary to gain baseline imagery. Acquisition of this type of coverage is usually the responsibility of national or theater assets.

This and later imagery coverage is studied initially by IAs from units at these echelons, but is also sent to the unit in the AO for further analysis. This in-depth, long-term analytical effort forms a baseline for further study and intelligence estimates. New information is passed to units assigned to or deploying into the AO.

Imagery is not always a timely source of information. Camera film needs to be offloaded from the aircraft upon return to base and is processed and printed before analysis and reporting.

Imagery data that is downlinked from the sensor platform to a ground station can be analyzed and reported more quickly.

However, historical coverage of the target area is used for mission planning. This older film coverage may be the only imagery available early on. Keep in mind any significant changes in the target, such as new structures, roads, or other features, that may affect the operation.

IAs often conduct comparative analysis. This is the analysis of imagery of the same area, or target, taken at different times to detect significant changes.

Analysis of imagery coverage over the long term can provide invaluable intelligence on insurgent patterns of deployment and operations. Imagery of a target taken by different sensors within a similar time frame can also be compared for indications of camouflage, concealment, and deception measures.

ADVANTAGES AND DISADVANTAGES OF IMAGERY INTELLIGENCE

ADVANTAGES

IAs produce highly accurate and detailed intelligence. Results are influenced by the factors discussed below.

Imaging Sensor Used

Different imaging sensors produce images which require different interpretation or analytical skills. It is easier to understand an image produced by an optical system than one produced by a radar system.

Optical imagery from cameras provides specific target information such as equipment type and facility layout. Radar imagery assists in the detection of activity.

Imaging sensors can be deceived. The enemy may be able to hide equipment or operations from optical sensors, but not from infrared sensors.

Equipment and Facilities

IAs rely on photographic facilities for processing and reproducing film and prints. The equipment used to look at the film ranges from small, portable, tabletop light tables—some with low power optic accessories—to 800-pound units with powerful optics, cameras, and monitors.

Equipment needed for the downlink of data from the sensor to the analyst may be available. For example, the ground station module (GSM) is capable of receiving radar data in NRT from the Joint Surveillance Target Attack Radar System (Joint STARS) airborne platform, thus expediting the analysis process.

Time Available to Analyze Reports

IAs meet certain timelines for report writing and release. For example, the reconnaissance exploitation report is based on a pilot debriefing and limited analysis of the imagery. Release of the report to the communications center must be within 45 minutes.

However, accuracy in report writing must not be sacrificed for speed, although there are times when the information in a delayed report is no longer valuable. Reports are discussed in this appendix and samples are in TC 34-55.

Ability, Knowledge, and Expertise of Imagery Analysts

IAs must be trained to recognize indicators and their significance for each operational category and geographic area. Senior IAs are responsible for training their teams.

Weather and Climate

Weather conditions can affect the sensor and the platform. Certain conditions can affect the quality of the imagery and even prevent the platform from flying. For example, both optical and radar imagery quality is degraded under rainy conditions, and airborne platforms cannot operate in extreme rainy conditions.

Other weather conditions such as clouds, fog, or snow can also obscure the target. You should be aware of the impact of weather and climate-related conditions on imagery collection when operating in various areas of the world.

Weather may prevent the completion of a mission, or even prevent the aircraft from taking off. The aircraft may take off in good weather but encounter cloudy conditions over the target.

Forecasted weather conditions, altitude, time of day, and local climatic conditions are used to determine whether the aircraft will fly. For example, the aircraft may not be able to take off at high altitudes because of insufficient air density.

Thunderstorms and turbulence will affect radar, while rain and poor visibility will affect optical and infrared missions, to some degree.

Imagery of Inaccessible Areas

Perhaps the most important military advantage of imagery is that sensors can collect information over otherwise inaccessible areas. This capability is platform dependent. Imagery is a permanent record of the target and can be studied over time for various purposes by different users.

DISADVANTAGES

Imagery also has disadvantages. The fine details of a target cannot always be detected. This can be a function of scale or image quality. Imagery cannot always answer the commander's PIR.

Information about the materials used in the construction of a wall may not be available from the inspection of imagery because the scale is too small. The mission may have to be flown again to obtain a more appropriate scale, or another sensor used.

The analytical efforts of IA are limited to the area imaged on the film. For example: Mission requirements cannot be satisfied if the target area was not imaged. Incomplete coverage can result from sensor or platform malfunctions, inaccurate target coordinates, and poor mission planning.

IMAGERY INTELLIGENCE IN LOW-INTENSITY CONFLICT AS PART OF MULTIDISCIPLINE INTELLIGENCE

Multidiscipline intelligence is the use of all the intelligence disciplines in a combined, mutually supporting effort to answer your commander's PIR and IR. It is applied at all levels of the IEW mission. Collection, planning, and reporting are discussed below.

No single intelligence discipline continuously provides all the answers. IMINT is not a standalone discipline. Imagery collection systems are subject to deception. Additional confirmation of information by another discipline increases the probability of the imagery being validated. Information from the other disciplines is analyzed to deny or confirm information collected by any one discipline.

Target information gathered by one collection means is used to trigger collection by other systems. For example, a number of weapons caches were detected and correctly identified on imagery during Operation JUST CAUSE as a result of cueing from HUMINT.

COLLECTION

Requests for coverage are submitted when intelligence gaps are identified. Approval of imagery collection is most dependent on the justification requirement.

Justification

Proposed missions must be fully justified by the requesting unit. The requestor must state how imagery is able to answer the commander's PIR, and the effect on the mission if the target is not imaged. For example, an optical imaging system is not suitable for collection against activity that typically occurs during darkness. In this case, a request for an infrared or radar sensor is fully justifiable.

There are many intelligence agencies competing for the use of IMINT assets. Your strong justification can ensure your unit's collection requirements are validated and approved.

For example, Air Force assets support the ground commander. But the Air Force has its own mission requirements, and they must justify their missions too. This justification is the most important part of the request for imagery collection, and your poorly worded request may not be approved by the validating authority.

Approval

The approval process can take up to 1 month for national and theater assets. Time-sensitive requests can be approved in less time. This process involves the review of multiple requests by many elements in the intelligence community before final approval is made.

Requests for imagery collection are submitted through review and validation channels using the accepted DIA formatted message. Corps is usually the lowest level from which this particular format is sent. Instructions for completing it are in DIAM 58-5(S).

The approval process for the use of tactical assets is shorter. Tasking is submitted for either preplanned or immediate requests. Preplanned requests are submitted for routine requirements 24 hours in advance. Immediate requirements are urgent needs when the imagery is vital to the mission. Tactical aircraft can usually react to an immediate request within 4 hours.

Although procedures for requesting imagery collection and exploitation support are standardized, each operational theater may have slightly different SOPs. You need to find out what assets are available and the procedures used to task them.

Be aware that your next higher unit may disapprove your request because another asset is able to collect the same information and already has been tasked. Missions are normally not flown if the requested information is available, or if the request duplicates an upcoming mission or one in progress.

Cost

Imagery collection is expensive from the standpoint of collection, processing, and especially dissemination. Regular maintenance of sensors and platforms is required, and there can be unexpected equipment malfunctions. Aircraft and crew must have downtime after a prescribed number of flight hours. Film processing and reproduction are also costly.

Host Nation Approval

Collection by airborne platforms depends on whether the HN allows US assets to use its airspace and conduct aerial imagery operations.

PLANNING

The objective of IMINT collection planning is to ensure the collection of information required to answer the commander's PIR and IR. Careful planning leads to the coordination of all the intelligence discipline resources into one collection effort.

Personnel involved in planning need to anticipate imagery and imagery product requirements which may be needed to support future operations. Intelligence production sections (ASPS and CIAS) can provide information on the current situation and thus guide collection planning.

REPORTING

Reports, prints, overlays, and intelligence documents are tools that you can use to support and accomplish your mission.

Imagery reports are in standardized formats that speed the information to the requesting unit. Some reports are written in free text format, while others are formatted for electronic data processing input. All reports have a specified time limit imposed. This ensures the timely release of information to the requesting unit.

Information collected by imaging sensors is perishable and must be passed within the prescribed time. Reports must be accurate. Poor analysis and reporting could ultimately endanger soldiers' lives. Make sure IA reports are checked by supervisors for accuracy before releasing to the communications center.

Imagery products include prints, overlays, terrain maps, and imagery-based intelligence documents. Prints and overlays are easily understood means of presenting information to the requestor. Prints are usually annotated to highlight specific areas or items of interest. Basic information is included, such as target title, location, date of coverage, and classification.

A photographic laboratory is required for film processing and reproduction of prints. Prints are often needed for mission and operational planning. If you need prints for data bases and mission planning, give the producing unit sufficient lead time.

The photographic reproduction process is lengthy. It includes the selection of imagery, production of multiple copies, and annotation of the prints. Arrangements for the delivery of final products should also be made.

Terrain imagery is used to update existing maps or provide supplemental information on areas with poor map coverage. US forces may be assigned to areas of the world with limited map coverage.

Current imagery was used to provide mapping information for Operation URGENT FURY. Basic topographic map coverage for the mission area was either unavailable or was not at a usable scale.

SENSOR USES, CAPABILITIES, AND LIMITATIONS

This section provides information on the uses, capabilities, and limitations of imagery sensor systems. General capabilities and limitations of airborne platforms are mentioned, where applicable. Further information on sensor and platform characteristics are in TC 34-55 and DDI-2600-3139-YR (S/NF).

OPTICAL (PHOTOGRAPHY)

A single camera, or combination of cameras, can be used to ensure complete coverage of the target. Basic aerial camera positions are vertical, oblique, and panoramic.

Capabilities

Vertical coverage provides an overhead view of the target and allows for accurate interpretation and analysis of the imagery. Imagery from vertical coverage can be used to make mosaics because the photographic scale is constant. A mosaic is an assembly of overlapping photographs which you match to form a continuous photographic *map* of the target area.

Oblique coverage provides a sloping view which helps see targets in tree lines or vehicle storage sheds. Such targets might not be picked up on vertical coverage. Oblique coverage shows targets with depth, distance, and perspective, just as they would appear to the naked eye.

Panoramic coverage provides a combination of vertical and oblique views of the target area.

Limitations

Still camera systems are not capable of inflight processing or providing inflight readouts. The aircraft must return to base to offload the film for processing. Imagery must then be analyzed before it can be used to provide intelligence. The time required to process and conduct analysis of the imagery must be factored into dissemination time.

An aircraft with a vertical camera system must pass directly over the target. This implies penetration of threat airspace and greater platform exposure.

An aircraft with an oblique camera system may operate in a semi-standoff mode or may penetrate enemy airspace and fly close to the target. An aircraft with a panoramic camera system has a greater standoff capability. The characteristics of the cameras determine how close to the target the aircraft must fly.

INFRARED

Infrared sensor systems detect heat energy reflected or radiated from manmade objects on the ground and the terrain.

Capabilities

Infrared is a passive system. The quality of imagery nearly equals that of photography. Infrared systems perform well at night.

Limitations

Infrared missions can be flown at any time of day or night. It is least sensitive during crossover or transition periods when targets and background have about the same temperature. Crossover occurs approximately 1 to 1-1/2 hours after sunrise and sunset.

Smoke, light rain, fog, and light vegetation can prevent optical target acquisition, but pose a lesser limitation for infrared. However, heavy rain, heavy fog, snow, cloud cover, and dense vegetation defeat the system's ability to detect temperature differences.

Some infrared sensor systems require the aircraft to pass over the target. This exposes the platform to enemy air defenses. Other systems, such as forward looking infrared (FLIR), provide a greater standoff capability. Older infrared systems lack a data transmission capability.

MULTISPECTRAL IMAGERY

MSI is used to enhance a data base by providing broad area coverage. MSI is a map-like product from satellites. Some MSI systems are part of commercial industry and, as a result, coverage may be difficult to obtain.

There are two principal civil satellite imaging systems. LANDSAT, operated by Earth Observation Satellite Company (EOSAT), has a 30-meter resolution and images in 7 spectral bands.

The French-owned Systeme Probatoire d'Observation de La Terre (SPOT) has a spatial resolution of 10 meters panchromatic and 20 meters color, and images in 3 spectral bands. SPOT also has a stereo-imaging capability. These parameters are adequate for detecting enemy activities such as clearing fields for training, agriculture, LZs and strips, map updating, basic mapping, vegetation, and soil typing.

RADAR

Imaging radar systems are used to detect moving and fixed targets. Newer systems can detect and classify targets by size and general type. Radar sensors are used for large area surveillance missions or LOC monitoring.

Capabilities

Radar sensors have near all-weather capability and are equally effective day or night. The standoff capability places airborne platforms out of range of enemy forward air defenses. Radar data can be data-linked in NRT to ground data terminals.

Limitations

Radar sensors are active systems and are susceptible to ECM. Sensor performance is affected by heavy rain and thunderstorms. Radar shadows can mask targets. These are areas not illuminated by the radar beam due to terrain or other obstacles.

VISUAL RECONNAISSANCE

Aircrews contribute to the collection effort by reporting visually observed threat force activities and facilities.

Capabilities

Visual reconnaissance can be a timely means of information collection. Aircrews are trained to perform visual reconnaissance, and their observations are used with the analysis of imagery in reports.

Limitations

Weather conditions can prevent full observation of the target area. Fatigue also plays a role in visual acuity and observation skills.

PLATFORMS

Most platforms used to carry imagery sensor systems are either airborne or orbital. Some are designed to carry more than one sensor at a time. For example, the RF-4C carries both optical and infrared camera systems.

New systems are constantly being developed. These include radar sensor systems installed in balloons. The balloon is either land or boat-tethered and can monitor land, air, or sea targets.

Unmanned aerial vehicle (UAV) systems are small, remotely piloted vehicles. They are equipped with different sensor packages and have data-link capability.

CONCLUSION

IMINT is a major contributor to the overall intelligence effort. Imagery collection provides intelligence, reference information, and planning support. IMINT collection is not always timely due to sensor and platform limitations. However, historical coverage and comparative analysis provide valuable information.

APPENDIX I

INTERROGATION SUPPORT TO LOW-INTENSITY CONFLICT

This appendix describes the conduct of interrogations in support of LIC operations. The principles and techniques of interrogation (FM 34-52) apply to LIC operations.

Applications will be modified to meet local conditions. However, because of the unique aspects of LIC operations, this appendix provides some additional guidelines.

Intelligence interrogations play a large role in identifying insurgencies in their early phases. Such information might include—

- Intentions.
- Attitudes.
- Capabilities.
- Limitations.
- Underground organization.
- Support systems.

LIMITATIONS TO UNITED STATES ASSISTANCE

US participation in interrogations during LIC operations is generally limited by the HN and US-HN SOFA. Normally, the interrogator is asked to advise, assist, and train HN personnel who are members of the armed forces, paramilitary forces, LEA, and other security agencies (FM 100-20/AFP 3-20).

The interrogator may also provide intelligence interrogation support to committed US or allied forces during LIC operations. This will require close coordination.

Coordination problems can be avoided by US interrogators working with HN interrogators. Advantages include the HN language fluency and their detailed knowledge of the area.

LIC intelligence requirements demand detailed familiarity with threat military, political, and front organizations and the environment in which they operate.

The interrogator must understand and appreciate the insurgency; its objectives, history, successes, and failures. This sensitivity is needed on a general countrywide basis and specifically within the interrogator's own AO.

Therefore, it is essential that the interrogator understands the importance that the insurgents place on the accomplishment of political objectives as distinct from military successes.

Interrogator effectiveness may be measured by the ability to apply appropriate interrogation techniques to the source's personality. In LIC a full range of interrogation techniques are needed because of the many types of interrogations encountered.

ADVISOR AND INTERROGATOR RELATIONSHIPS

US Army interrogators may be assigned to a HN to assist in developing interrogation capabilities of HN forces.

FM 100-20/AFP 3-20 contains detailed information on advisor duties, techniques, and procedures. However, the relationship of the advisor to HN interrogators needs mentioning and is discussed below.

ADVISOR QUALIFICATIONS

Advisors must be senior interrogators with an extensive intelligence background. They require area orientation, language fluency, and the ability to work with HN personnel. They—

- Establish a working relationship with HN counterparts through development of mutual respect and confidence.
- Provide advice for effective collection through interrogation.
- Assist in establishing combined interrogation centers.

- Provide on-the-job training for HN interrogators.
- Assist in establishing necessary file systems to support interrogation operations.
- Keep in contact with all units participating in the combined interrogation center.
- Keep the Army SIO informed on operations and activities within your area.
- Provide financial support, as authorized, for interrogation operations to your counterpart.
- Coordinate with other US intelligence advisors.

COUNTERPART RELATIONSHIP

Advisor accomplishments depend upon the relationship established with their counterpart. This relationship is influenced by the personalities of each. Ideally, this relationship should develop as your counterpart's knowledge of the area merges with your professionalism.

Before providing advice to your counterpart, observe the operation of the unit and become familiar with the area and the local situation. For convenience, your office should be adjacent to that of your counterpart. However, do not interfere with the routine administrative duties that must be accomplished by the counterpart.

Above all, remember that yours is an advisory role and not as supervisor or commander. Advise one counterpart rather than individuals within the unit. This is important, for advising individuals could result in advice which is contrary to the orders of the counterpart.

In reality, advice is totally accepted only when the counterpart is convinced that the advice is sound and appropriate to the situation.

If brutality is observed, do not participate; quickly remove yourself and any other US personnel from the scene. Local theater policies and directives normally assign other specified actions in these situations.

These policies and directives may include advising the counterpart of the undesirability of the action and reporting the incident to the US chain of command. Comply with any theater (or other command) policies and directives.

ADVISOR OPERATIONS

Emphasize that development of a combined interrogation effort is important to successful operations. This merged capability is gained by uniting the interrogation resources of all intelligence forces (except tactical) within a specific geographic AOR (that is, national, province, district).

Most likely, in many host countries, interrogation responsibilities will be assigned as follows:

- Civilian LEA—suspects and insurgent political cadre.
- Military interrogators—captured military insurgents and those military insurgents who have defected to the HN government.
- Indigenous military CI—insurgent infiltrators and deserters from HN forces.

As the advisor, you must aim at the working-level integration of both US and HN interrogators to achieve economy of force and unity of effort. Often your task will be complicated by strong HN personalities. But if harmonious working relationships are established with those key personalities, you can succeed.

As the interrogator, you will establish liaison with US advisors working with HN tactical forces. These advisors can inform you of captured insurgents. You and the tactical unit advisor, working together, can ensure effective interrogation. Further, both of you can help to achieve the required coordination between HN tactical units and area forces.

The status of insurgents in LIC differs from that of recognized belligerents, and interrogations will be wider ranging.

LEGAL STATUS OF INSURGENTS

EPW interrogations are conducted in support of wartime military operations and are governed by the Geneva Conventions Relative to the Treatment of Prisoners of War of August 12, 1949 (GPW), and FM 27-10.

However, insurgents seeking to overthrow an established government do not hold legal status as belligerents. Since their activities are clandestine or covert, those operating in this context avoid involvement with HN LEA and military security forces. Insurgents taken into custody by HN security forces may not be protected by the GPW, Article 3.

Insurgents will be subject to the internal security laws of the HN concerning subversion and lawlessness. Action of US forces will be governed by US-HN SOFA and GPW, Article 3.

POPULATION

In LIC the population becomes the prime target. As a result, the population is a principal source of intelligence. This population will be composed of friendly, hostile, and completely indifferent elements. In dealing with these population segments and insurgents, consider the desires of the HN.

There is a basic need to gain the support of the population in order to deprive the insurgents of their primary sources of support. This need places a burden upon the interrogator to learn more about the people. Study their—

- Customs and taboos (by ethnic groups, if appropriate).
- Distrust and fear of foreigners.
- Fear of insurgent reprisal.
- Philosophy or outlook on life.
- Political, economic, and social institutions.

Since CI elements have the mission of countersubversion, they have the primary job of identifying insurgent operations in the population.

INSURGENT VULNERABILITY TO INTERROGATION

Individual insurgents lack many of the usual psychological supports for resisting interrogation. Often they are in conflict with their own people; perhaps of the same ethnic group, religion, environment, or even family. Further, the insurgent has no legal status as an EPW and realizes he may be viewed as a common criminal.

The insurgent often expects to receive harsh and brutal treatment after capture. If he does not receive this harsh treatment, the psychological effect may make him useful. In addition, the shock of capture will increase his vulnerability. As a consequence, the individual insurgent may rationalize cooperation as his best chance for survival.

Although insurgents lack conventional psychological support, interrogators should realize that other support may exist. Indoctrinations using such techniques as self and group criticism can give insurgents a strong group identification and a fanatical belief in the cause.

Insurgent activity is vulnerable to mass screening of the populace. Since insurgent operations need the support of the people, members of the population inevitably learn the identities and activities of the insurgents. With many people knowing him, the insurgent's identity is detectable by mass screening and interrogation programs.

Success of such programs may be enhanced by the insurgent's previously committed acts of terror, tax collection, and forced recruitment, which will have angered some of the population.

HANDLING OF INSURGENT CAPTIVES AND SUSPECTS

Insurgency is identified as a condition resulting from a revolt or insurrection against a constituted government which falls short of civil war. It is not usually an international conflict and is not a recognized belligerency.

Insurgent captives are not guaranteed full protection under the Geneva Conventions. However, GPW, Article 3, requires that insurgent captives be humanely treated and forbids violence to life and person; in particular murder, mutilation, cruel treatment, and torture.

It further forbids commitment of outrages upon personal dignity, taking of hostages, passing of sentences, and execution without prior judgment by a regularly constituted court.

Humane treatment of insurgent captives should extend far beyond compliance with Article 3, if for no other reason than to make them more susceptible to interrogation.

The insurgent is trained to expect brutal treatment upon capture. If, contrary to what he has been led to believe, this mistreatment does not happen, he may become psychologically softened for interrogation. Furthermore, brutality by either capturing troops or friendly interrogators will reduce defections and serve as grist for insurgent propaganda mills.

Care must be taken in handling unidentified suspects, for their degree of sympathy with the insurgency is not known. Improper handling of such persons may foster sympathies for the insurgency or induce them to remain passive at a time when the HN requires active support from its citizens.

INSURGENT METHODS OF RESISTANCE

Recognizing vulnerability to interrogation, the insurgent counters by—

- Keeping his forces ignorant of future operations, unit designations, and true names of leaders.
- Assigning multiple designations to units, frequently changing them, and using aliases for names of leaders.
- Hiring informants to watch and report on the people and committing reprisals against those who provide information to the government.
- Instructing his forces to remain silent upon capture for a given period. This time delay tends to decrease the value of the information which is ultimately revealed.
- Providing plausible cover stories to hide true information.
- Indoctrinating his forces with ideological training.
- Publicizing cases where captives have been killed or mistreated by capturing forces.
- Screening his recruits carefully.
- Using cellular structure to restrict knowledge of personnel and operations.

COMMON CHARACTERISTICS AND KNOWLEDGEABILITY OF SOURCES

The characteristics and knowledge of interrogation sources vary widely based upon position, status, and mission of the insurgent in his organization. Appraisal of these factors, coupled with his own knowledge of the source and the organization to which he belongs, will assist in quickly evaluating the source's potential.

Interrogation sources vary and include the main and local combatants, militia, political cadre, sympathizers, and defectors. They may be young or old, male or female, educated or illiterate. General characteristics and knowledgeability of the more common types are discussed below.

MAIN AND LOCAL FORCES

The main force combatant is the best indoctrinated, trained, led, disciplined, and equipped of all insurgent forces. They will know more, but may be inclined to reveal less, than a local force insurgent or a member of the village militia. When properly interrogated, however, they can be expected to be a fruitful source of information on—

- Their unit and its personnel.
- Current and past military operations.
- Supply and base areas.
- Status of training and morale.
- Information on higher, lower, and adjacent units.
- Routes of infiltration and exfiltration.
- Tactics and general information on the AO.

In short, they may be likened to the more conventional enemy prisoner of war (EPW) and will be knowledgeable on topics akin to that type of individual. They will differ, however, in that their knowledge of units other than their own will be far less than that of the conventional EPW.

The local force insurgent soldier (the second component of the insurgent regular armed forces) will be almost as valuable as the main force soldier. His knowledge will depend primarily upon the methods of operation used by the insurgent movement.

MILITIA

Compared to the main and local force insurgent, the local village militia member is often poorly trained, disciplined, and equipped. While he is not likely to be a profitable source of information on regular force units, his native familiarity with the area in which he operates makes him a valuable source for—

- Local terrain.
- Insurgent infrastructure.

- Food and weapons caches.
- LOC and logistics.
- Intelligence operations.
- OB information on his own unit.

When cooperative, he can be used to identify local insurgent sympathizers within his area.

POLITICAL CADRE

This individual is a profitable source for information on the makeup and operation of the insurgent's political structure. At the lowest level (hamlet and village), he normally wears two hats: one as the political leader, the other as the commander of the militia.

At higher levels the individual is more political in orientation and can provide information on cell members, front organizations, sympathizers, and nets. He is also knowledgeable on the military units within his area, their LOC and methods of communications, and future plans and operations of political and military organizations.

SYMPATHIZER

This individual may be a sympathizer in fact or because of other circumstances such as blackmail, terror, or relatives being held hostage.

In any event, if skillfully interrogated, the sympathizer can become the most fruitful source of information on one of the greatest and most perplexing questions of insurgency: "How do you tell the difference between friend and foe?"

The sympathizer coerced into assisting the insurgent is, of course, the most useful type of individual, but care must be taken to protect him after he has revealed useful information.

DEFECTORS

These individuals are perhaps the best source of information available during LIC. They are usually cooperative and easily susceptible to direct approach interrogation techniques.

The most important feature of interrogating defectors is the capability to exploit physically the individual who voluntarily agrees to accompany friendly personnel into tactical operations areas.

The primary methods of exploiting defectors are as—

- Tactical guides and advisors.
- Informants.
- Aides in interrogation and document analysis.
- Advisors on enemy agent net modus operandi.

It should be noted, however, that some of these techniques involve personal danger for the defector and, for that reason, he should be provided appropriate protective equipment. Coercion cannot be used to induce his cooperation.

INTERROGATION SCREENING TECHNIQUES

Screening insurgent captives and suspects is the key to productive interrogation. Screening is a twofold operation. It is conducted to—

- Identify insurgents, or their sympathizers, in the population.
- Find the most knowledgeable individuals for interrogation.

Techniques for accomplishing these functions are varied and depend mainly upon the imagination and ingenuity of screening personnel. For this reason, only the most resourceful interrogators should be selected as screeners. Examples of successful screening aids and techniques are discussed below.

LOCAL LEADER

The local leader—whether a government official, religious personage, teacher, or village elder—is a useful screening assistant. This individual knows the people, their habits, and activities. He knows the legitimate resident from the stranger and can often point out insurgents and their sympathizers in his area.

However, since the local leader is vulnerable to insurgent terror or reprisals, his overt use in screening may be sometimes limited. When employed in an overt capacity, he will always require protection later.

The fact that a man is a constituted local leader should never be viewed as prima facie evidence of loyalty to the HN government. A leader may be secretly or tacitly supporting the insurgency or may, for personal political reasons, discredit political rivals with false accusations.

INSURGENT CAPTIVE

The insurgent captive can be used as a *finger man* in a police-type lineup, and is excellent help in mass screenings. As the entire population of a community files past, the captive points out those individuals loyal to the insurgency. A police mug file is a useful variant of this technique; here, the captive reviews photographs taken from family registries.

INFORMANT TECHNIQUE

This technique involves planting a friendly *mole* among a group of suspects or captives. The mole acts out the role of an insurgent sympathizer to gain confidence of the group and to learn the identity of the true insurgents and their leaders.

INTERROGATION OF ILLITERATES

Interrogating illiterate sources requires special questioning techniques. The interrogator is after facts. Eliciting data from illiterates, such as sizes or numbers, are often difficult. The interrogator must agree on common terminology with his source so he can communicate and obtain the information desired. For example:

- He can use a system of holding up fingers on his hands, marking on a piece of paper, or using matchsticks, pieces of wood, or other materials to determine numerical facts.
- He can determine types of weapons by using photographs or drawings of weapons from which the source can make a comparison with what he actually saw.
- He can use pieces of materials or color charts to describe colors.
- He can determine direction of movement by the location of the sun, stars, or landmarks familiar to the source.
- He can determine time by the position of the sun, locating a traveled route and then computing how rapidly the source walked, or finding out how often he stopped and how many meals he ate.

These methods are examples of common terminology or reference points which an interrogator employs. Additionally, knowledge of the specific habits of the populace and of the area allows the interrogator to select a definite term of reference. Further information on interrogation operations are in FM 34-52.

APPENDIX J

S2 CHECKLIST FOR COUNTERINSURGENCY OPERATIONS

LIC operations include support to insurgency and counterinsurgency operations. However, because conventional US Army forces normally do not provide this support, insurgency operations are not addressed. This checklist is a guide to the S2 and is not all inclusive.

COUNTERINSURGENCY OPERATIONS

Facts and Assumptions

DEFINE THE BATTLEFIELD

- AI. Consider—
  - Strategic locations; neighboring countries, boundaries, and frontiers.
  - The use of coastal waterways.
  - Third-country support for the insurgency.
- Realms of activity.
  - Analyze HN population, government, military, demographics, and threat.
  - Evaluate political structure, economics, foreign policy and relations, and policies on military use.

DESCRIBE THE BATTLEFIELD

In addition to OCOKA, consider that—

- Terrain dictates points of entry, infiltration and exfiltration routes, and C^2 for operations.
- Weather affects the availability of food supply to insurgents. Floods may limit cache sites. Drastic changes in weather may limit usefulness of terrain intelligence.
- Migration and settlement patterns will help indicate which areas are becoming pro-government or pro-insurgent.
- Both friendly and threat COAs will be influenced accordingly.
- Economics may affect the insurgent's ability to conduct operations. A lack of money may result in the theft of equipment.
- Economics may also influence the populace's political leaning. This could contribute to a rise or fall in insurgent capability to conduct offensive operations.

DESCRIBE THE THREAT

- Include personalities in your OB analysis. Identify leaders, trainers, recruiters, staff members, and logistics personnel. Develop doctrinal templates based on observed operating procedures.
- In describing personalities, look at the functional specialty of each individual. The number of trainers for a specific weapon might indicate the type of tactics or readiness due to time and the number of personnel trained.
- Consider the types of weapons the insurgent has at his disposal. Sophisticated weaponry is an indicator of external support and the capability to attack more sophisticated or well-protected targets.
- Consider unit organization. It takes insurgent organizations longer than conventional units to train for major attacks. This is because larger insurgent units require more planning and training time; large training areas; and fast, effective, and secure communications. These are capabilities that are difficult to acquire.
- Analyze movement patterns. They may coincide with logistics or operational activities.
- Consider where the insurgent lives and works. He may be located near key terrain such as major LOC, agricultural areas, or government installations.

DEVELOP ENEMY COAs

- Threat COAs on the objective might include—
  - Attacks and raids on military installations or other HN facilities.
  - Attacks on public utilities and installations or other forms of economic sabotage.
  - Kidnappings and assassination of public officials.
  - PSYOP directed against the population (intimidation, propaganda).
  - Ambushes of HN or US convoys.
  - Evasion from friendly troops.
- To determine the most likely insurgent COAs, template the best locations for potential insurgent attacks, sabotage, raids, and roadblocks. Use the key facilities and targets overlay.
- Template insurgent activity near the objective to include—
  - Movement around objectives (infiltration and exfiltration routes).
  - Assembly points, rally points, and staging areas.
  - Surveillance positions.
- Template insurgent activity away from their objective areas to include—
  - Locations of known and suspected base camps.
  - Locations of known and suspected training areas.

- Centers of pro-insurgent population (villages, political areas), areas of guerilla influence, residences of insurgent leadership, and key sympathizers (for surveillance and movement).

- Template insurgent support functions to include—
  - Logistic routes and transshipment hubs.
  - Cache sites, water sources, agricultural areas, POL storage and production areas (government and commercial).
  - Locations of communications equipment (commercial establishments for purchase or theft and government installations for theft).

Analyze Mission
Develop COAs
Analyze COAs
Recommand COA

ANALYZE MISSION

There are no intelligence considerations that are unique in counterinsurgency operations.

DEVELOP COAs

Planners must consider operations against all types of insurgent activity:

- Operations on the objective.
- Activities near the objective.
- Activities away from the objective.
- Support functions.

ANALYZE COAs

- During wargaming you or the S5 (CA officer) should roleplay the population in addition to the insurgents.
- Wargame the collapse of key planning assumptions.
- Wargame the ability of insurgents to surprise friendly forces.

RECOMMEND A COA

Politics and population are more important than terrain.

Write OPORD

PIR

- Consider including the verification of planning assumptions into the PIR.
- Once CI and interrogation teams establish themselves in an AO, the number of PIR and IR they can handle are fairly large. Do not undertask them.

COLLECTION PLAN

The nature of insurgent activities may cause a considerable amount of collection assets to be dedicated to support friendly operations, verify planning assumptions, and prevent surprise.

Supervise
Execution

COLLECT

Collection focuses on HUMINT and MDCI assessment but IMINT, SIGINT, and EW also contribute. Task—

- HUMINT to exploit sources of information regarding insurgent logistic support, potential insurgent targets and objectives, and identification of insurgent supporters.
- IMINT to track insurgent disposition, update existing MC&G, and locate training facilities and base camps. Use Remotely Monitored Battlefield Sensor System (REMBASS) on likely infiltration and exfiltration lanes.
- SIGINT and EW to intercept, identify, and locate insurgents and to develop or verify data needed for jamming and deception.
- MDCI to provide threat assessments, friendly vulnerability assessments, and security A&A. MDCI also conducts liaison, collection operations, and community (search and cordon) intelligence operations.

PROCESS

- Use pattern analysis to verify or refute indicators of key insurgent activity.
- Use a coordinates register to keep track of insurgent activity in key areas over a period of time.
- To determine which insurgent personalities contact each other, use an association matrix.
- Use an activities matrix to help you connect individuals to organizations, events, and activities other than people.
- Use a time event chart to show a chronological record of individual or group activities (who did what that contributed to a particular event). This will help develop doctrinal templates for these groups.
- Combine these charts to show the linkages between the insurgent and his events.

DISSEMINATE

- The complex nature of counterinsurgency operations usually makes the written INTSUM a better tool than the graphic one.
- The slower pace of counterinsurgency operations enables you to conduct more face-to-face intelligence briefings, which are usually preferred.

APPENDIX K
S2 CHECKLIST FOR COMBATTING TERRORISM

Combatting terrorism consists of AT (defensive measures) and CT (offensive measures). This checklist describes intelligence considerations for a unit conducting AT operations. CT is not discussed here because most conventional Army units will not engage in such activities.

ANTITERRORISM OPERATIONS

Facts and Assumptions

DEFINE THE BATTLEFIELD

- AI. Consider—
  - — Known terrorist activity.
  - — Terrorist activities in nations that sponsor terrorist groups.
  - — International and national support to the terrorists; for example, moral, physical, and financial support.
  - — If US presence, or potential presence, by itself could be a catalyst for terrorist activity.
  - — The identity of recent worldwide anti-US terrorist activity, or any intent to conduct such activity.
- Realms of activity.
  - — Identify the demographic issues that make a protected area (unit, facility, organization, installation, personnel) attractive to terrorists.
  - — Identify any time constraints that might limit the availability of a target.
  - — Coordinate with supporting MP and MI activities while preparing initial threat analyses and updates.

DESCRIBE THE BATTLEFIELD

- Demographics.
  - — What demographic issues (economics, politics, propaganda) make a target attractive to terrorists?
  - — How do these demographic issues shape terrorist COAs? For example, the political grievances of a terrorist organization might make some targets more attractive than others. Religious convictions might cause terrorists to reject assassinations in favor of kidnappings.
- Targets and routes.
  - — Identify the susceptibility of targets (installations or personnel) to terrorists.
  - — Identify infiltration routes and avenues of approach.

DESCRIBE THE THREAT

- Determine the type of terrorist groups you might face. Are they state supported? Are they nonstate supported? Are they state directed?
- Identify which terrorist groups are present, thought to be present, or have access to your AO.
- Conduct OB analysis for each group to include:
  - Organization and cellular composition.
  - Internal discipline.
  - Long- and short-range goals.
  - Dedication (willingness to kill or die for the cause).
  - Religious, political, and ethnic affiliations of the groups.
  - The identity of leaders, trainers, opportunists, and idealists.
  - Group skills and specialties of each organization (for example, sniping, demolition, air and water operations, electronic surveillance, and tunneling).
- Describe the preferred tactics of each organization. These might include assassination, arson, bombing, hijacking, hostage taking, kidnapping, maiming, raids, seizure, sabotage, hoaxes, or chemical and biological weapons. Consider international writings on terrorist or insurgent operations; for example, Mao, Che Guavara.
- Describe or template demonstrated terrorist activity over a period of time in the AO.

DEVELOP ENEMY COAs

- Identify likely terrorist targets within the protected entity by matching friendly vulnerabilities against terrorist capabilities and objectives.
- Template terrorist actions on likely objectives within the protected entity. Remember that the choice of tactics is often related to the amount of desire for attention.
- Template terrorist activities near the objective (assembly areas, movement to the objective site, surveillance, escape routes).
- Template or describe the supporting functions for terrorism (training, logistics, C^3I, finance). During antiterrorism operations these activities may provide warnings of coming attacks.

Analyze Mission
Develop COAs
Analyze COAs
Recommend COA

MISSION ANALYSIS

While it is impossible to establish 100 percent deterrence against all possible terrorist attacks, the level of local deterrence needs to be well defined in order to focus the intelligence effort.

DEVELOP COAs

- Typical COAs include—
  - The establishment of a guard or security force.

- — An increase in information, personnel, and physical security measures.
- — Random personnel, equipment, and vehicle checks.
- — An increase in intelligence operations to provide early warning.
- — The establishment of a quick reaction force.
- — A terrorism awareness education program.

- You must determine that each COA actually deters the local threat to the level specified during mission analysis.
- You should also identify those measures which deter the local threat beyond the specified level.

ANALYZE COAs

- During wargaming you should roleplay the terrorists against the unified countermeasures effort.
- Each COA should be evaluated for unit cost weighed against increased deterrence.

Write OPORD

PIR

- PIR and IR that support AT will be almost exclusively dedicated to early warning.
- AT operations are usually conducted concurrently with other operations. Command judgment is required to prioritize the AT PIR and IR against other requirements.

COLLECTION PLAN

- Indicators and NAIs should be established near known or suspected terrorists sites, along infiltration routes into a protected area, and near vulnerable HVTs.
- Consult the staff judge advocate (SJA) for legal restrictions prior to executing the collection plan.

Supervise Execution

COLLECT

- HUMINT provides information on terrorist organizations, capabilities, tactics, and targets.
- IMINT provides information pertaining to installation vulnerabilities. IMINT may also provide imagery of terrorist training facilities and other operational imagery to units actively involved in CT operations.
- SIGINT may provide locational data on terrorists once an event is underway (hostage location).
- MDCI helps determine friendly vulnerabilities and possible terrorist surveillance of those weaknesses.
- Use all sources to provide information on terrorist groups. Consult—
  - — Open information sources such as news media and private sector publications.
  - — Military and civilian LEAs.

  - Governmental information, intelligence, and investigative agencies.
  - Informal local sources such as soldiers, family members, and civil employees.
- Provide terrorism threat awareness training and briefings to all personnel and family members as required. This increases spontaneous reporting.

PROCESS

- Time event charts predict the order of events leading to a terrorist event. This will help produce new doctrinal templates.
- Association and activities matrices help determine operational capabilities of individual terrorists and their associated groups.
- Association matrices show which personalities associate with each other. This provides an idea of cell size and the overall organization of the group.
- Link diagrams show the cellular structure of the organization.

DISSEMINATE

Agencies responsible for coordinating antiterrorist activities must have immediate communications with collection agencies and the executors of all unit countermeasures.

APPENDIX L

S2 CHECKLIST FOR PEACEKEEPING OPERATIONS

As outlined in Joint Publication 3-07.3, "Intelligence" is not conducted during PKO. Instead, there will be an information section.

PEACEKEEPING OPERATIONS

Facts and Assumptions

DEFINE THE BATTLEFIELD

- AI. Identify and locate all outside influences on the operation. Consider political groups, media, and third-nation support to the belligerents.
- Realms of activity.
  - — Identify the legal mandate, geographic boundaries, and other limitations upon both peacekeepers and belligerents.
  - — Identify pertinent demographic and economic issues. These might include living conditions, religious beliefs, cultural distinctions, allocation of wealth, political grievances, social status, or political affiliations.
  - — Identify the best and worst case timeline of the operation.

DESCRIBE THE BATTLEFIELD

- Demographics.
  - — What are the root causes of the conflict? Analyze this from the perspective of both belligerents.
  - — What would cause or caused each side to agree to peace?
  - — Are there any new issues that have increased tensions since peace was initiated?
  - — How committed is each belligerent to keeping the peace? How much trust and faith do the belligerents have in each other to keep the peace?
  - — How capable is each belligerent to keep the peace? Can the leadership which negotiated the peace enforce discipline throughout the belligerent parties?
  - — How do these factors affect the COA of each belligerent? How do they affect COAs available to the peacekeeping force?
  - — Analyze these questions relative to each of the pertinent demographic factors identified during Define the Battlefield Phase (standard of living, culture, religion, politics).
- Legal. What legitimate COAs are available to the belligerents and the peacekeeping force? How likely is each belligerent to obey these laws?

- Terrain.
  - Does terrain impact military operations? Conduct terrain analysis. Identify good infiltration lanes, engagement areas, defensive positions, attack routes, and staging areas.
  - Does terrain lend itself to PKO? Can the peacekeepers see and be seen? If so, the belligerents may be less likely to violate the peace. If necessary, where can the peacekeeping force establish blocking positions to blunt possible violations of the peace?
  - Identify terrain that allows all belligerents equal access to the peacekeepers.
  - Analyze terrain for current disposition of belligerent forces.
- Weather.
  - Analyze weather affects such as visibility for all parties including the peacekeepers.
  - Consider weather impact on mobility and trafficability. (See FM 34-81-1.)
  - Weather may affect participation at demonstrations and other gatherings.
- Other. Identify and analyze government, military, and agency support available to the peacekeeping force.

DESCRIBE THE BELLIGERENTS

- Identify all factions involved in the PKO. Which are likely to violate the peace and why?
- What is the political organization and military OB for each of the belligerent groups? Who are the key personnel that control the rank and file of each faction?
- Identify the political and religious beliefs that directly affect or influence the conduct of belligerents.
- Identify belligerent tactics for offense and defense. Use this as the basis for doctrinal templates.
- Identify local support to all belligerents.

DETERMINE ENEMY COAs

- Template or describe the actions of the belligerents that would violate the peace. Border crossings, entering demilitarized zones, and initiation of hostilities are examples of violations.
- Template or describe the actions associated with violations of the peace; occupation of assembly areas, training, C^3I, and logistics.
- Template or describe the response of belligerents to violations of the peace.
- Template or describe the reactions of all belligerents to US actions within the AO and AI.

- Identify possible reactions of the belligerents to the whole peacekeeping mission. Consider acts of terrorism.
  - — How will the local populace react to the COAs?
  - — How will the HN government and military react to the COAs?

Analyze Mission
Develop COAs
Analyze COAs
Recommend COA

ANALYZE MISSION

There are no intelligence considerations that are unique to mission analysis in PKO.

DEVELOP COAs

All peacekeeper COAs should be impartial from the belligerent's perspective.

ANALYZE COAs

- During wargaming the executive officer or you should designate individuals to roleplay each of the belligerents.
- All of the situation templates identified above should be wargamed.
- Wargame terrorist actions and other activities where the belligerents could reasonably avoid claiming responsibility.

RECOMMEND A COA

The perspectives of both belligerents should be heavily weighted as decision criteria.

Write OPORD

PIR

These will be almost exclusively I&W of possible violations by either belligerent. They should focus on force protection.

COLLECTION PLAN

Conventional indicators and NAIs will help analyze overt violations of the peace. Indicators for terrorist actions will be more unconventional.

Supervise
Execution

COLLECT

- When tasking collectors, ask the following questions:
  - — Will you have to rely on higher headquarters?
  - — Can any element of the peacekeeping force answer the requirement?
  - — Does the desired information already exist in an analytical data base?
- After asking the preceding questions, consider the following:
  - — HUMINT may be the only source of information you have. Observer and patrol reporting will give I&W of hostilities among the belligerents.
  - — Ensure all PKO observers are trained to submit complete incident reports. Refer to the incident report checklist described in the **Show of Force Operations** section of Appendix M.
  - — SIGINT and IMINT support may not be available.
- Use MDCI to protect the peacekeeper. Its role is force protection.

- Use outside sources to gather information. Actual sources and types of information may be directed by diplomatic authorities (for example, the UN, other multinational organizations, and news media).

PROCESS

- Use coordinate registers, intelligence workbooks, and OB files to record activities of belligerents in key areas.
- In addition to the standard objective analysis, you may have to analyze reports from the following perspectives:
  - Belligerent parties.
  - Civilian population.
  - Terrorist groups.
- Integrate data base information by layering incident overlays over a specific period of time.

DISSEMINATE

- Develop fast and effective means of disseminating your processed information to consumers.
- Keep in mind that the S2's consumers are his commander, the multinational force commander and, ultimately, the parties to the conflict.

APPENDIX M
S2 CHECKLIST FOR PEACETIME CONTINGENCY OPERATIONS

This appendix contains S2 checklists that pertain to the following PCO:

- Counter-drug operations.
- NEO.
- Operations to restore order.
- Show of force operations.

Other PCO such as UW, strikes and raids, RRO, and arms control are not discussed because the majority of Army units will never plan for these operations.

These checklists contain items that are unique to LIC operations but are not all inclusive. They support the development of your operational planning.

COUNTER-DRUG OPERATIONS

Facts and Assumptions

DEFINE THE BATTLEFIELD

- AI. Consider both air and ground AIs. Questions include—
  - — Where do precursor elements originate?
  - — How and where do they enter the HN and the AO?
- Realms of activity. Consider local economic conditions, effectiveness of HN military, LEAs, and the nature of the HN government.

DESCRIBE THE BATTLEFIELD

- Consider that MC&G coverage of your AO and AI may be lacking.
- Identify agricultural areas for drug crops and growing seasons.
- Consider HN hydrography necessary to support the drug crop.
- Consider terrain and weather in relation to production, growth, and movement cycles of drug crops.
- Identify routes and techniques available to traffickers for infiltration by air, ground, and sea.
- Identify exfiltration routes (including transshipment points) and techniques for air, land, and water movement.
- Identify likely storage areas for drug shipments awaiting transit.
- Identify physical conditions and operational procedures such as customs inspection stations, amount of vehicle traffic across the border, or movement choke points that affect trafficking.

DESCRIBE THE ENEMY

- Consider the structure of the drug organization:
  - — Look at family relationships.

  - Identify key personnel (leaders, logisticians, security specialists, and chemists).

- Consider security elements and methods of production, concealment, and transportation.
- Identify narcoterrorist groups, their tactics and procedures.
- Consider support that the local government cannot or will not give to the local populace.
- Consider the threat use of force tactics such as blackmail, kidnapping, threats of violence to gain support, and control populace and the government.

DETERMINE THREAT COAs

- Template or describe the activities of drug producers in the AO and AI.
- Template or describe production activities such as logistics, security, and training.
- Template or describe the specific actions of the traffickers through the AO and AI. This includes storage areas, drying areas, surface and air routes to include airstrip analysis, ports, and types of vehicles or animals used by the traffickers.
- Template trafficker and producer actions upon confrontation. Include legal evasion.
- Template or describe the support activities associated with trafficking in the AO and AI. Include finances, front organizations, civic actions, and money laundering.
- Template the security procedures and procedures to avoid detection for the above templates.

Analyze Mission
Develop COAs
Analyze COAs
Recommend COA

ANALYZE MISSION

There are no intelligence considerations that are unique to mission analyses in counter-drug operations.

DEVELOP COAs

- Planners must consider operations against all types of threat activities, including—
  - Producing.
  - Trafficking.
  - Support activities.
  - Security measures.
- The SJA will validate each friendly COA against HN, US, and international laws.

ANALYZE COAs

- During wargaming, you should roleplay producers, traffickers, support, and security personnel.

- The S5 should roleplay the local populace.
- The S2 ensures that trafficker and producer actions (when confronted) are wargamed in detail.

RECOMMEND A COA

You should consider politics, HN legal system, and profit motive as more important than weather or terrain.

Write OPORD

PIR

Since producers and traffickers strive to avoid detection, all PIR can be dedicated to support unit operations instead of verifying planning assumptions and preventing surprise.

COLLECTION PLAN

You need to allocate a significant number of indicators for each NAI. For example, the surveillance of the back entrance of a trafficking safe house by one person might include distinctly different indicators to confirm or deny the—

- Presence of the drug shipment.
- Presence of key trafficking personnel.
- Presence of money.
- Presence of incriminating documentation and a destruction plan.
- Presence of weapons and other security measures.
- Escape and evasion procedures.
- Traffickers' actions upon confrontation.

Supervise Execution

COLLECT

Political relations and pre-mission agreements with the HN will dictate the quantity and type of assets available to you.

- HUMINT observes, elicits, and exploits material and documents to gain information on drug traffickers.
- IMINT aids in identifying illicit crops, production facilities, LOC, and transshipment points.
- SIGINT identifies transshipment points, logistics activity, and movement of drugs.
- MDCI tells you how your unit looks to the threat. It keys on the balance between mission goals and the scope, intensity, and nature of friendly operations.

PROCESS

- Use target folders to organize data. These folders include—
  - — Locational data.
  - — Historical drug trafficking routes to and from the target.
  - — Identified defensive positions.

- Physical characteristics of known structures.
- Observed antenna configurations with photographs or sketches.
- Coordinates register of recent activity.
- Confirmed data about this target.

- Using pattern analysis based on the results of past raids may reveal changes in movement patterns, front companies, and laboratory locations.
- Use link analysis to show association between types of supplies; who orders them, and the intended user.

DISSEMINATE

- Take advantage of the slower pace of counter-drug operations to brief key personnel face-to-face.
- Organize INTSUMs and other intelligence reports by target areas. Group the target areas using the flow of drugs through country. An example report might be structured as follows:
  - Ground infiltration lanes into country.
  - Sea infiltration lanes into country.
  - Air routes into country.
  - Transshipment points.
  - Support activities in country.
  - Ground, sea, and air routes out of country.
- Encourage the SJA to write a report for each INTSUM.

NONCOMBATANT EVACUATION OPERATIONS

Facts and Assumptions

DEFINE THE BATTLEFIELD

- AI.
  - Within the nation where NEO will be conducted, identify and locate all groups that might influence operations.
  - Check which countries might accept evacuees?
  - Which countries are likely to assist or hinder the operation?
- Realms of activity.
  - Identify whether evacuation is expected to be permissive, semi-permissive, or non-permissive.
  - Identify the operational time sensitivities.
  - Identify the root cause of the situation that has prompted the NEO. Consider the political, social, economic, legal, and religious situations. In general, look at the government, military, and population.

DESCRIBE THE BATTLEFIELD

- The SJA should identify all legal issues that impact on the NEO.
- Identify local political issues that shape friendly COAs. Learn if—
  - Hostile groups oppose the evacuation of noncombatants?
  - This source of irritation might be minimized?
  - There are areas where anti-evacuation sentiment is the strongest?
  - There are identified areas where sympathy for the evacuation is strongest?
- Identify the logistics infrastructure that might support NEO. Choose—
  - Consolidation points that are secure from attack and well equipped with power, water, restrooms, and heat. Consider football and soccer stadiums, gymnasiums, auditoriums, large halls, and recreation centers.
  - Evacuation routes that are fast and secure.
  - A secure means of transportation for evacuees. Consider the local transport system.
  - Available sources of food and potable water for evacuees.
  - Communications systems that can support evacuation operations. Analyze the ability of isolated evacuees to contact evacuation authorities.
- Map the location of key facilities to include foreign embassies, military installations, hospitals, police stations, and government buildings.
- Conduct a standard OCOKA terrain analysis to—
  - Identify probable locations for ambushes of NEO vehicles. Within urban areas, look at major thoroughfares and public transportation.
  - Identify infiltration routes and assembly areas for enemy attacks on consolidation points of evacuees.
  - Identify places suited for anti-US demonstrations and their relative position to NEO sites and US installations.
- Weather. Analyze the effect of weather upon—
  - Adverse groups. Dedicated insurgents prefer inclement weather while casual demonstrators do not.
  - Evacuation operations. Will sudden rain, cold, or extreme heat require changing evacuation facilities or evacuation transportation?

DESCRIBE THE ENEMY

- Identify all groups that might intentionally interfere with NEO. Consider HN LEA, military, political groups, religious factions, and the general population. Focus on hostile groups such as insurgents, terrorists, and radical extremists.

- Using a population, conduct an OB analysis for each of these potentially hostile groups:
  - — Disposition. Where do hostile groups live and gather in relation to NEO objectives? For example: neighborhoods near embassies, US citizen population centers, or US businesses.
  - — Composition and strength. How are these groups organized? What kind of weapons do they possess?
  - — Tactics. What resistance methods and techniques can these groups employ against the evacuation? Consider attacks, raids, ambushes, snipings, bombings, hijackings, hostage taking, kidnapping, and demonstrations.
- Identify all groups that might unintentionally interfere with the NEO. Consider groups such as students, labor unions, demonstrators, rioters, HN forces, and criminal elements.
- Conduct OB analysis on the adverse groups also. Identify their goals and objectives as well as their position towards the evacuation operation. Focus on the methods of resistance and techniques employed to achieve these objectives. How would they interfere with the NEO?
- Consider threat influence on the logistics infrastructure. Look for the control of workers such as bus drivers, dock workers, police, food service personnel, and labor groups.

DETERMINE THREAT COAs

- Use the key facilities and targets overlay to identify the most likely points of interference for US NEO.
- Template intentional interference with NEO by hostile groups at each likely interference site. Consider terrorist actions, ambushes, delays at checkpoints, demonstrations, raids on consolidation points, and sniping. Determine alternative routes or COA at these points.
- Identify unintentional interference with the NEO by wild card groups and template this activity (riots, criminal activity, and arson).
- Template or describe the support functions for groups that would interfere with NEO (planning, C^3I, weapons, ammunition, food, water, shelter, and training).
- Template threat influence on local transportation systems (control of workers such as bus drivers, dock workers, police, and labor groups).

Analyze Mission
Develop COAs
Analyze COAs
Recommend COA

ANALYZE MISSION

There are no intelligence considerations that are unique to mission analysis in NEO.

DEVELOP COAs

You ensure that each COA considers taking maximum advantage of the HN logistics infrastructure, if available. You should also ensure that each COA optimizes the available security measures.

ANALYZE COAs

During wargaming you role play both intentionally and unintentionally hostile adverse groups.

Write OPORD

PIR

Intelligence requirements during NEO usually focus on gaining advance warning of activities by hostile or unintentionally adverse groups that would interfere with evacuation.

COLLECTION PLAN

- NAIs and indicators for hostile groups are similar to those that support counterinsurgency and antiterrorist operations.
- NAIs and indicators for the unintentionally adverse groups are usually simple to identify and collect against. This is because these groups are overt and usually advertise their planned activities.

Supervise Execution

COLLECT

- Use HUMINT to identify the threat infrastructure. Activities include liaison, interrogations, and debriefing.
- Use IMINT for target coverage of LOC, airfield, and evacuation points.
- Use SIGINT to provide a means of assessing threat reaction to NEO. It also helps pinpoint areas of threat activity.
- Use MDCI to—
  - — Gauge hostile reaction to NEO.
  - — Provide threat assessment to the NEO force.
  - — Perform liaison with other US agencies in the HN and, when possible, with HN intelligence, security, and LEAs.
- These activities refine the key facilities and targets overlay.

PROCESS

- Use a population status overlay to identify the areas most likely to harbor people who would interfere with NEO operations.
- Use a coordinates register to record activities around key routes and consolidation points.
- Use an intelligence workbook and OB files to record information about potentially hostile and adverse groups.
- Use activities and association matrices to identify which key individuals are actively interfering with evacuation.
- Use the LOC and key facilities and targets overlays to determine where interference will occur.
- The reliability and credibility of each report will need to be evaluated in detail. NEO operations generally occur in chaotic environments where false rumors are often presented as fact. HN personnel may use reports for personal vendettas.

DISSEMINATE

Develop a fast, effective means of disseminating intelligence to consumers.

- Consider physical collocation of the quick reaction force and decision makers.
- Also consider electronic collocation via the operations and intelligence net.

OPERATIONS TO RESTORE ORDER

Facts and Assumptions

DEFINE THE BATTLEFIELD

- AI.
  - Identify third-nation support for any of the belligerent parties.
  - Identify outside influences such as world organizations, news media, and others.
- Realms of activity. Almost every demographic topic (religion, politics, ethnic differences) will have to be considered in peacemaking operations.

DESCRIBE THE BATTLEFIELD

- Legal. Identify the legal limits of friendly use of force in the AO. What COAs does this allow for, and under what conditions?
- Demographics.
  - A comprehensive and continuing demographic study is required to support peacemaking operations. The symptoms, causes, and aggravations of the conflict should be defined in terms of all demographic factors.
  - Obstacles to resolutions should be identified and studied in detail.
  - Identify how demographics allow for, encourage, and discourage belligerent COAs. For example, a historical feud between two religious sects might designate certain monuments or other icons as key terrain.
- COAs. Also identify which friendly COAs will be tolerated, encouraged, or discouraged. Consider the balance of the forces in the area.
- Terrain.
  - Conduct OCOKA analysis to determine where terrain imparts both offensive and defensive operations for all belligerents.
  - Identify the terrain which is best suited for police action to support friendly patrols. Use population status, LOC, logistic sustainability, and key facility and target overlays to do this.

DESCRIBE THE ENEMY

- Fully identify all belligerent groups. If the relationship between two groups is in question, consider them separately even if their political objectives are the same.
- What is the relationship of each group to every other allied, neutral, or hostile group?
- What is the political organization of each group? What are the political objectives of each group? How strong are each of their convictions?
- How much discipline can the leadership of each group expect from their followers? How likely are rank and file members to violate a truce negotiated by their leaders?
- Fully identify the military capability of each group. Start with traditional OB factors to develop doctrinal templates.
- What friendly COAs would induce the belligerents to obey the law? Some options to consider are—
  - — Show of force.
  - — Defensive measures for key facilities, police patrols, and cordon and search operations.
  - — Designating territorial boundaries.
  - — Establishing demilitarized zones.

DETERMINE ENEMY COAs

- Template or describe the belligerent actions (raids, ambushes, occupation of contested areas) that prevent peace or other desired end states.
- Template or describe the supporting functions associated with the belligerent actions of the warring groups such as massing at assembly areas, logistics, finance, and C^3I.
- Template or describe the responses of belligerent groups to US actions within the AO and AI. Consider terrorist actions.

Analize Mission
Develop COAs
Analyze COAs
Recommend COA

ANALYZE MISSION

- Precisely define the desired end state.
- Designate the resolution of each military contention as implied tasks.
- Designate the resolution of the most decisive military conflicts as mission-essential tasks.
- Identify the political, religious, economic, and other demographic areas of contention as limitations to friendly operations.

DEVELOP COAs

For each COA you should identify the suitability, feasibility, and acceptability for that COA in terms of the—

- Probability of inducing the cessation of military actions by all parties.
- Probability that the US will retain neutrality within the conflict.

- Likelihood that the leadership of each party can keep the forced peace within its faction.
- Ability of US forces to make peace. (Can they do it indefinitely?)
- Estimate the demographic and military situation that would follow withdrawal of US forces (and the collapse of any negotiated agreements).

ANALYZE COAs

- During wargaming you should roleplay each of the belligerent parties.
- Wargame the interaction of belligerents to each other and to US forces upon the initiation of the friendly COA.
- Wargame all potential incidents in terms of the suitability, feasibility, and acceptability factors listed above.

RECOMMEND A COA

The decision criteria will vary drastically with each peacemaking operation.

Write OPORD

PIR

The PIR will have to be custom designed for each peacemaking operation. There are no typical PIR or IR.

COLLECTION PLAN

- Indicators and NAIs will have to be double or triple redundant due to the irreversible nature of operations during peacemaking. Analytical mistakes may result in major setbacks.
- Indicators and NAIs may have to be proven to a court-of-law standard before friendly action can be taken.

Supervise Execution

COLLECT

- Use HUMINT to identify and neutralize the threat infrastructure. It does this by filling gaps in your commander's intelligence requirements and by concentrating on identifying and analyzing the potential threat.
- Use IMINT to determine the disposition of threat forces. IMINT can provide data concerning defenses or new structures. IMINT also shows changes in LOC and target coverage (observation) for key military areas, installations, and main government centers.
- Use SIGINT to identify and locate threat groups and determine changes in communications levels.
- Use MDCI to assess friendly vulnerability to all types of threat; conduct joint liaison; and contribute to mission analysis through investigations, operations, collection, analysis, and production.
- All soldiers must use the incident report checklist described in **Show of Force Operations** below.

PROCESS

- An intelligence workbook and OB files should be kept on each of the belligerent factions.

- Use association and activities matrices to further determine the loyalties and relationships of key personnel.
- Use event diagrams and link analysis to develop doctrinal templates for each faction.
- A coordinates register should be maintained for each critical area.
- Color code the SITMAP for the standard incidents within the crisis. For example, allocate different colors to raids, ambushes, sniping, assassinations, arson, vandalism, and terrorism.
- Use pattern analysis to identify indicators associated with each of these standard incidents.

DISSEMINATE

Dissemination techniques will have to be custom made for each peacemaking operation. There are no rules of thumb.

SHOW OF FORCE OPERATIONS

Facts and Assumptions

DEFINE THE BATTLEFIELD

- AO. Define the boundaries for the maneuver of US forces relative to both HN and target nation.
- AI.
  - — Expand the AI to include all military, paramilitary, or other organizations that might interact with friendly forces.
  - — Identify those nations which influence or are influenced by events in the AO.
- Realms of activity.
  - — The psychology of all key decision makers will need to be studied in detail. This is probably the dominant consideration for show of force operations.
  - — Identify the legal parameters that bind the activities of the HN, target nation, and US forces in the region. This includes treaties, international law, SOFA, and ROE restrictions.
  - — Identify the moral issues that affect the activities of the nation involved.
  - — Identify the scope of pertinent political issues within the region. For example: Do the actions of local politicians affect mission success or should friendly concern be confined to politicians at the national level?
  - — Which economic issues influence the crisis?

DESCRIBE THE BATTLEFIELD

- Psychological. What is the psychological environment in which key decision makers find themselves? Is the key leadership secure, or is there a legitimate threat to their power base? How would compliance with US desires affect their positions?
- Legal. Identify the—
  - — Terrain that is legitimate for use by US forces.
  - — Legal restrictions that affect friendly terrain use and COAs.
- Moral. What friendly actions would be encouraged, tolerated, discouraged, and not tolerated by—
  - — US public opinion? (Consider actions that are legally correct but morally suspect.)
  - — The international community?
- Political.
  - — How does the regional political situation (HN, target nation, and neighboring states) affect friendly COAs?
  - — How does the world political situation affect friendly COAs?
  - — How does the political situation affect target COAs?
- Economic.
  - — How does the economic situation in the region affect friendly COAs? Would a particular friendly action unduly interfere with a vital economic function such as farming?
  - — How does the economic situation affect target COAs?
- Terrain.
  - — Which terrain best lends itself to the show of force operations being considered? For example, does the terrain allow for observation of (and by) the target audience?
  - — Consider that the show of force could escalate to war. Conduct a standard OCOKA analysis to determine that terrain which best supports offensive and defensive operations.
- Weather. Remember to evaluate the impact of weather upon any PSYOP actions.

DESCRIBE THE ENEMY

- Decision makers. Develop a psychological profile of the key target decision makers. Include—
  - — Personal objectives, goals, concerns, values, and perspectives of each individual. Are there any support bases, material possessions, official positions, ranks, titles, privileges, or relationships that individuals value over the good of their country?

- Current position, attitude, opinions, and views of each individual towards the contentious issues.
- Decision-making procedures for each individual. Determine the influence of emotion and logic as the individual deliberates. When does each individual actively seek information? When do they allow information to come to them?
- The ability of each individual to access information. Do decision makers get complete, honest, and unbiased information? Are the decision makers surrounded by cowards or sycophants who would withhold or change information for personal reasons?
- Other psychological aspects that affect decision making, to include ability to objectively reason; ability to compare long-term and short-term gain; ability to calculate risks; and courage to take risks.
- Doctrinal templates. What do the key decision makers usually do when confronted with similar situations?

- Target nation. What friendly COAs would increase or decrease popular support for target decision makers?
  - Is the target nation prepared for escalation to war?
  - Conduct traditional OB analysis and develop doctrinal templates in case the crisis escalates to war.
  - Carefully identify the willingness of the target nation military to fight. Do they believe they can successfully fight US forces should the crisis escalate? What friendly actions would help the US gain moral ascendancy over the target nation military?

DETERMINE ENEMY COAs

- Template or describe the possible decision-making processes of key target leaders. What are the crux elements of each individual's position? What are likely and unlikely leveraging forces that would lead to desired and undesired decisions?
- Template or describe enemy actions to be influenced. Describe the key elements that would lead to the implementation of desired actions or the cessation of nondesired actions.
- Template or describe enemy support functions associated with both desired and nondesired actions; for example, movement, C^3I, rehearsals, and propaganda.
- Template or describe enemy reactions to friendly actions. For example: Will they fight? Will they comply? Will they resort to legal or political recourse?
- Consider illegal threat actions for which the target nation does not need to claim responsibility. Terrorism and agitation of HN are examples.

Analyze Mission
Develop COAs
Analyze COAs
Recommend COA

ANALYZE MISSION

- Carefully specify the perception that the show of force should register. Typical perceptions include—

  - Capability. Convince the target nation that they will lose should the crisis escalate to hostilities.
  - Willingness or resolve. Convince the target nation that friendly forces will likely be committed if the target nation does not comply.
- Carefully specify the target audience for each of the desired perceptions described above. Typical audiences will include—
  - Decision makers (for the compliance actions).
  - Sources of support for decision makers; for example, population, military, wealthy families, and religious groups.
- In most show of force operations, it is desirable to overwhelm the armed forces of the target nation with demonstrations. In other words, friendly forces must gain *moral ascendancy* over the armed forces of the target nation. The target audience for this perception should be the entire armed forces—from private to CINC.
- If the results of the above analysis are not already *specified* tasks, they should be considered *implied* tasks. The registration of perceptions (willingness or capability) upon key personnel are usually mission-essential tasks in show of force operations.

DEVELOP COAs

The friendly force should always prepare contingency plans for hostilities in the event that the show of force fails. These plans should demonstrate the—

- Willingness of the friendly force to conduct precombat activities that can be collected against by target nation intelligence sources. These activities might include rehearsals, lock-downs, issue of ammunition, crash training programs, readiness measures, and practice alerts.
- Capability that friendly force can conduct displays of combat equipment, firepower demonstrations, and training demonstrations of difficult tasks openly.

ANALYZE COAs

- For perceptions to be registered, you should roleplay the target audience as well as the target nation intelligence services that can collect against friendly actions.
- Wargame target nation reactions to friendly actions. The psychological reactions of key decision makers should be wargamed in detail.
- What friendly COAs would influence target decision makers to comply.
- Events that would lead to the escalation to hostilities should be wargamed in detail. The SJA should be involved in this wargaming to determine the moral, legal, and political status of both sides during escalation.

RECOMMEND A COA

- The psychology of key decision makers should be heavily weighted as a decision criteria.

- The ability of friendly collection assets to verify or deny the target audience awareness of friendly operations should be considered as one of the decision criteria.

Write OPORD

PIR

Intelligence questions for show of force operations will usually include:

- Has the appropriate perception registered upon the target audience?
- Has the target nation complied with desired actions?
- Has the target nation elected to escalate to war either intentionally or unintentionally?

COLLECTION PLAN

Indicators and NAIs for the registration of perceptions are difficult to effectively collect against. The analyst should generate a large number of indicators to validate analytical conclusions. The indicators should be double or triple redundant.

Supervise Execution

COLLECT

— HUMINT is the best collection source to determine how the target audience perceives friendly operations.

— IMINT can provide disposition, strength, and composition of target nation forces. It can also provide valuable information about support functions to include status of LOC, bridges, airfields, ports, and border areas.

— SIGINT helps to gain insight into the target nation's immediate reactions to friendly operations.

— MDCI provides intelligence on threat targeting of friendly forces.

— All collection sources should be utilized to provide I&W of target nation operations.

— Every incident reported during show of force operations should be rigorously followed up. Every soldier should be trained to report the following aspects of any incident with identified or suspected forces of the target nation. This list goes well beyond the standard SALUTE format:

□ What is the short title of the suspicious activity? (Possible enemy surveillance, possible terrorist activity, combat patrol by target nation, possible probe of friendly perimeter.)

□ When did you first identify suspect activity? Could you determine where the suspect personnel came from?

□ How many personnel were involved in the suspect activity? What did each person do during the entire time of observation? Were they armed? What were they wearing? Did the personnel have any other equipment?

□ Did the suspect personnel say anything during the incident? With whom did they interact?

- □ Where did the incident occur? Submit a sketch map showing the locations of all suspect personnel during the incident.
- □ What time did the incident occur? How long did the incident last?
- □ In which direction did the suspect personnel leave?
- □ Did any other friendly personnel observe the incident? HN forces? Local population?

- The unit should consider sending cameras or video equipment with patrols to document incidents.

PROCESS

- Use an intelligence workbook to analyze incidents during show of force operations. The titles of the subsections might include target nation—
  - Decision makers.
  - Intelligence services.
  - Covert activities.
  - Military readiness.
  - Army.
  - Navy.
  - Air Force.
  - Legal activities.
  - Propaganda.
- A coordinates register should be used to record events that occur in key areas (such as contested lands or border areas along likely invasion routes).
- The evaluation step of processing (pertinence, reliability, credibility) requires extra attention.
- Analytic conclusions reached during show of force operations are often subjective. Additionally, unit analysts are very prone to group think, and other biases, when analyzing the psychology behind events. Before the force commander acts, he should explain the action he is about to take and the analysis that supports that action to his higher commander.

DISSEMINATE

- The intelligence situation for show of force operations is usually so subtle and complex that few personnel outside the concerned headquarters are likely to have any expertise in the area. Since a large number of key friendly personnel need and want to understand the situation, you should develop a standard presentation that gives visitors to the AO a quick and effective picture of the intelligence situation.
- Written INTSUMs and intelligence reports are the norm for show of force operations.

The following operations, although PCO, are addressed in general terms because they generally do not involve interaction with hostile forces.

HUMANITARIAN ASSISTANCE AND DISASTER RELIEF OPERATIONS

These operations usually take the form of economic and logistic assistance.

- Determine the present and potential extent of the disaster (additional floods, earthquakes, mudslides, DPs). Through analysis, predict which population sectors will require assistance and determine the type.
- Consider weather and the environment as potential threats:
  - Weather will impact your ability to conduct relief operations. For example, if the target of a relief effort is a village isolated by mudslides or another natural disaster, inclement weather may limit or curtail air and ground operations to the site.
  - The environment may pose threats to the health of both mission and HN personnel in the forms of waterborne diseases, spoiled or contaminated foodstuffs, and other environmental hazards.
- Use non-DOD assets and HN resources to fill voids in map coverage of your AO.
- Use MDCI for force protection. It provides you with vulnerability assessments and will assess all threats whether actual or potential.

SUPPORT TO DOMESTIC CIVIL AUTHORITY

This type of support includes activities conducted by military forces in support of federal and state officials.

- The battlefield in this type of operation may be created by emergency situations such as domestic unrest, threats to federal property including firefighting, illegal immigration, and drug trafficking.
- Intelligence support to this type of operation is conducted under and limited by the Posse Comitatus Act and other laws and regulations to include AR 381-10 and AR 381-20.
- In planning, it is advisable to defer to the expertise of the organization being supported.

SECURITY ASSISTANCE SURGES

These operations occur when a friendly or allied nation faces an imminent threat. Assistance can take the form of logistical support, additional combat systems, or training.

- The battlefield in this type of operation includes the air AI and AO plus delivery points in the HN. Consider the threat to friendly aircraft in the form of surveillance from third-party nations. Hostile threat on the ground concerns surveillance and threats to physical security.
- Use HUMINT throughout the operation to deny the enemy knowledge of the operation.
- MDCI assesses all threat intelligence activities to deny the threat knowledge of the operation and its intent.

GLOSSARY

Section I. ACRONYMS AND ABBREVIATIONS

A

A&A	advice and assistance
AAO	analysis of the area of operations
AAR	after-action report
AASLT	air assault
abn	airborne
AC	Active Component
ACC	area coordination center
ACR	armored cavalry regiment
ADP	automated data processing
AE	aerial exploitation
AFCENT	Allied Forces, Central Europe
AHFEWS	Army HF EW System
AI	area of interest
ammo	ammunition
AO	area of operation
AOR	area of responsibility
appl	application
ARL	aerial reconnaissance low
ARNG	Army National Guard
ARSOF	Army Special Operations Forces
AS	aerial surveillance
aslt	assault
ASP	ammunition supply point
ASPS	all-source production section
AT	antiterrorism
ATF	Bureau of Alcohol, Tobacco, and Firearms
avn	aviation

B

BAE	battlefield area evaluation
BDA	battle damage assessment
bde	brigade
BFA	battlefield functional area
BICC	battlefield information coordination center
bn	battalion
BOS	battlefield operating system

C

C^2	command and control
C^3	command, control, and communications
C^3CM	command, control, and communications countermeasures
C^3I	command, control, communications, and intelligence
C&J	collection and jamming
C-E	communications-electronics
CA	civil affairs
CAJTIC	Central America Joint Tactical Intelligence Center
cbt	combat
CD	counter-drug
CE	counterespionage
CED	captured enemy document
CEM	captured enemy materiel
CENTCOM	Central Command
CESO	communications-electronic staff officer
CG	Commanding General
char	characteristic
CI	counterintelligence
CIA	Central Intelligence Agency
CIAS	counterintelligence analysis section
CID	Criminal Investigation Division
CINC	Commander in Chief
CJTIC	Central America Joint Tactical Intelligence Center
CM	collection management
CM&D	collection management and dissemination
CM-O	countermeasure option
CMO	collection management officer
co	company
COA	course of action
coll	collection
COMINT	communications intelligence
COMMZ	communications zone
COMSEC	communications security
CONUS	continental United States
comm	communications
cmd	command
CMS	countermeasures past success
cntrl	control
CP	command post
CPX	command post exercise
CS	combat support
CSS	combat service support
CT	counterterrorism
CUCV	commercial utility cargo vehicle

D

DA	Department of the Army
DASH	Drone Antisubmarine Helicopter
DEA	Drug Enforcement Administration
demo	demonstration
dept	department
det	detachment
DF	direction finding
DIA	Defense Intelligence Agency
dist	distinguishing
div	division
DMA	Defense Mapping Agency
DOB	date of birth
DOC	Department of Commerce
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DP	displaced person
DRO	disaster relief operations
DS	direct support
DSM	decision support matrix
DST	decision support template
DTOC	division tactical operations center
DZ	drop zone

E

E-O	electro-optical
EAC	echelons above corps
EACIC	echelons above corps intelligence center
EC	electronic combat
ECB	echelons corps and below
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
ed	education
EDPP	Evolutionary Democratic Popular Party
EEFI	essential elements of friendly information
ELINT	electronic intelligence
EOSAT	Earth Observation Satellite Company
EP	electronic protection
EPDS	Electronic Processing and Dissemination System
EPIC	El Paso Intelligence Center
EPW	enemy prisoner of war
ES	electronic warfare support
ESAF	El Salvador Air Force
ESD	engine shut down
ESM	electronic warfare support measures
etc	and so forth
ETUT	Enhanced Tactical Users Terminal
EW	electronic warfare
EWR	early warning radar

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FID	foreign internal defense
FIS	foreign intelligence and security service
FISINT	foreign instrumentation signals intelligence
FLIR	forward looking infrared
flt	flight
FM	from
FMLN	Frente Farabundo Marti de la Liberacion Nacional
FORSCOM	United States Army Forces Command
FRAGO	fragmentary order
FSB	forward staging base
FSLN	Frente Sandinista Liberacion Nacional
FTX	field training exercise
fwd	forward

G

G	generator
G2	Assistant Chief of Staff (Intelligence)
G3	Assistant Chief of Staff (Operations and Plans)
gen	general
GCI	ground-controlled intercept
gp	group
GPW	Geneva Conventions Relative to the Treatment of Prisoners of War of August 12, 1949
GS	general support
GSM	ground station module
GSR	ground surveillance radar

H

H	hours
HF	high frequency
HHC	headquarters and headquarters company
HHD	headquarters and headquarters detachment

HHOC	headquarters, headquarters and operations company
HHSC	headquarters, headquarters service company
HIC	high-intensity conflict
HMMWV	high mobility multipurpose wheeled vehicle
HN	host nation
HPT	high-payoff target
HQ	headquarters
hr	hour
HUMINT	human intelligence
HVT	high-value target
hvy	heavy

I

I&E	interrogation and exploitation
I&S	intelligence and surveillance
I&W	indications and warning
IA	imagery analyst
IAW	in accordance with
ID	identification
IDAD	internal defense and development
IES	Imagery Exploitation System
IEW	intelligence and electronic warfare
IEWSO	intelligence and electronic warfare support officer
IMINT	imagery intelligence
indef	indefinite
inf	infantry
info	information
INFOSEC	information security
INS	Immigration and Naturalization Service
INSCOM	US Army Intelligence and Security Command
intel	intelligence
INTSUM	intelligence summary
IPB	intelligence preparation of the battlefield
IPT	intelligence preparation of the theater
IR	information requirements
IRS	Internal Revenue Service
ISB	initial staging base
ISE	intelligence support element
ITAC	intelligence threat analysis center
IVA	insurgent vulnerability assessment

J

J2	Joint Intelligence Directorate
JIC	Joint Intelligence Center
JOG	joint operations graphic
Joint STARS	Joint Surveillance Target Attack Radar System
JRC	Joint Reconnaissance Center
JSOA	Joint Special Operations Area
JTF	joint task force
JTIC	Joint Tactical Intelligence Center
JTTP	joint tactics, techniques, and procedures

K

km	kilometer

L

lab	laboratory
LANDSAT	topographic satellite
LANTCOM	United States Atlantic Command
LEA	law enforcement agency
LEDET	Law Enforcement Detachment
LI	low intensity
LIC	low-intensity conflict
LLSO	low-level source operations
LLVI	low-level voice intercept
LN	local national
LOB	line of bearing
LOC	lines of communication
LOI	letter of instruction
LOS	line-of-sight
LRS	long-range surveillance
LRSO	long-range surveillance operations
LT	light
LTR	letter
LZ	landing zone

M

m	meter
MACOM	major Army command
MASINT	measurement and signature intelligence
MC	maneuver corridor
MC&G	mapping, charting, and geodesy
MCOO	modified combined obstacle overlay
MCS	master control station
MDCI	multidiscipline counterintelligence
MED	manipulative electronic deception
METL	mission-essential task list
METT-T	mission, enemy, terrain, troops, and time available
MI	military intelligence
MIBLI	military intelligence battalion, low

	intensity
MIC	mid-intensity conflict
MIJI	meaconing, intrusion, jamming, and interference
mil	military
MOUT	military operations in urban terrain
MP	military police
msg	message
MSI	multispectral imagery
MTOE	modified tables of organization and equipment
MTT	mobile training team

N

NA	not applicable
NADIR	navigational direction radar
NAI	named area of interest
NBC	nuclear, biological, and chemical
NCA	National Command Authorities
NEO	noncombatant evacuation operations
NET	not earlier than
NIC	national intelligence center
NIS	national intelligence survey
NLT	not later than
NMIC	National Military Intelligence Center
NO	number
noncomms	noncommunications
NRT	near-real-time
NSA	National Security Agency

O

OAS	The Organization of American States
OB	order of battle
OBE	overcome by events
OCOKA	observation and fields of fire, concealment and cover, obstacles, key terrain, avenues of approach, and mobility corridors
OCONUS	outside continental United States
ODA	operating detachment alpha
OFCO	offensive counterintelligence operations
ONDCP	Office of the National Drug Control Policy
OP	observation post
op	operations
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security
org	organization
OSI	Office of Special Investigations (USAF)

P

PACOM	Pacific Command
PAO	public affairs officer
PCO	peacetime contingency operations
pers	personnel
photo	photograph
PIR	priority intelligence requirements
PLF	Popular Liberation Front
PL	phase line
plt	platoon
PKO	peacekeeping operations
PMO	provost marshal's office
POG	psychological operations group
POL	petroleum, oils, and lubricants
proc	processing
PSA	post-strike assessment
PSI	personnel security investigation
PSYOP	phsycological operations
pub	public
PVC	polyvinyl chloride (plastic)

R

R&S	reconnaissance and surveillance
RATT	radio teletype
RC	Reserve Components
RDF	radio direction finding
ref	reference
REMBASS	Remotely Monitored Battlefield Sensor System
RF	risk factor
RIC	regional intelligence center
RIP	Register of Intelligence Products
ROE	rules of engagement
RRO	rescue and recovery operations
RST	reactive situational template

S

S2	Intelligence Officer
S3	Operations and Training Officer
S5	Civil Affairs Officer
SAC	senior Army commander
SAEDA	Subversion and Espionage Directed Against the US Army
SALUTE	size, activity, location, unit, time, equipment (spot report format)
SAM	surface-to-air missile
SAO	security assistance office
SAP	special access program

SAS	security assistance surges
SASS	Small Airborne Surveillance System
scty	security
Sec	section
Sep	September
SF	special forces
SIGINT	signals intelligence
SIGSEC	signals security
SII	statement of intelligence interest
SIO	senior intelligence officer
SIR	specific information requirements
SITMAP	situation map
SJA	staff judge advocate
SLAR	side-looking airborne radar
SOA	special operations aircraft
SOC	Special Operations Command
SOF	special operations forces
SOFA	Status of Forces Agreement
SOI	signal operating instructions
SOP	standing operating procedure
SOT-A	support operations team-Alpha
SPOT	Systeme Probatoire d'Observation de La Terre (France)
spt	support
SSI	statement of intelligence interest
SSO	special security officer
STANAG	standardization agreement
stks	strikes
SUPIR	supplemental programmed interpretation report
survl	surveillance
SWO	staff weather officer

T

TACJAM	tactical jamming
TACREC	tactical reconnaissance
TAFT	training assistance field team
TAI	target area of interest
TAREX	target exploitation
TASOSC	Theater Army Special Operations Support Command
TAR	target area replica
TAT	tactical analysis team
TDA	tables of distribution and allowance
TE	tactical exploitation
TECHINT	technical intelligence
TF	task force
tng	training
TOC	tactical operations center
TOE	tables of organization and equipment
TOR	terms of reference
TRAFFICJAM	traffic jamming
TSOC	Theater Special Operations Command
TSP	tactical support package
TPL	time phase line
TTP	tactics, techniques, and procedures
TV	television
TVA	target value analysis

U

UAV	unmanned aerial vehicle
UHF	ultra high frequency
ULF	United Liberation Front
UN	United Nations
US	United States
USAIA	United States Army Intelligence Agency
USACIDC	US Army Criminal Investigation Command
USAID	US Agency for International Development
USCG	United States Coast Guard
UW	unconventional warfare
UWO	unconventional warfare operations

V

V	vulnerability
veh	vehicle
VHF	very high frequency
vic	vicinity

W

w	with
WARM	wartime reserve mode
wpn	weapon

Section II. DEFINITIONS

Antiterrorism

Defensive measures used to reduce the vulnerability of personnel, their dependents, facilities, and equipment to terrorist acts (Joint Pub 1-02 and DOD Directive 0-2000.12).

Battle damage assessment

A timely and accurate all-source analysis of the results of a military operation in terms of damage and impact on enemy combat effectiveness. (See strategic, operational, and tactical BDA.)

Combatting terrorism

Actions, including AT and CT taken to oppose terrorism throughout the entire threat spectrum (Joint Pub 1-02 and FM 100-20/AFP 3-20).

Counterterrorism

Offensive measures taken to prevent, deter, and respond to terrorism. See also antiterrorism; terrorism (Joint Pub 1-02). Also offensive measures taken to respond to a terrorist act, including the gathering of information and threat analysis in support of these measurers.

Crisis management team

A team found at a MACOM or installation level. This team is concerned with plans, procedures, techniques, policies, and controls for dealing with terrorism, special threats or other major disruptions occurring on Government installations and facilities. It considers all aspects of the incident and establishes contact with the Emergency Operations Center.

Extremism

The quality or state of being extreme or the advocacy of extreme political measures; radicalism.

Fundamentalism

A movement or attitude stressing strict and literal adherence to a set of basic principles.

High-risk personnel

Personnel that, by their grade, assignment, symbolic value, or relative isolation, are more likely to be attractive or accessible terrorist targets.

Hostage

A person held as a pledge that certain terms or agreements will be kept. (The taking of hostages is forbidden under the GPW, 1949) (Joint Pub 1-02.) Also any person held against their will as security for the performance or nonperformance of specific actions.

Ideology

A systematic body of concepts, especially about human life or culture, a manner or the content of thinking characteristic of an individual, group, or culture, or the integrated assertions, theories, and aims that constitute a sociopolitical program.

Insurgency

An organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict (Joint Pub 1-02).

International terrorism

Terrorism transcending national boundaries in the carrying out of the act, the purpose of the act, the nationalities of the victims, or the resolution of the incident. Acts are usually designed to attract wide publicity to focus attention on the existence, cause, or demands of the terrorists.

Major disruptions

Acts, threats, or attempts to commit such acts as kidnapping, extortion, bombings, hijackings, ambushing, major weapons thefts, arson, assassination, and hostage taking on a military installation. These acts that have a potential for widespread publicity require special response, tactics, and management.

Morality
A doctrine or system of moral conduct, particular moral principles or rule of conduct, conformity to ideals of right human conduct, or moral conduct; virtue.

Non-state supported terrorism
A terrorist group that operates autonomously, receiving no significant support from any government. For example, Italy's Red Brigades (FM 100-37).

Operational BDA
At the operational level, BDA measures the results of a strike or series of strikes; it estimates the remaining combat effectiveness of enemy forces and support facilities within a predetermined theater or AO.

Peacekeeping operations
Military operations conducted with the consent of the belligerent parties to a conflict, to maintain a negotiated truce and to facilitate diplomatic resolution of a conflict between the belligerents (FM 100-20/AFP 3-20).

Peacemaking operations
A type of peacetime contingency operation intended to establish or restore peace and order through the use of force (FM 100-20/AFP 3-20).

Peacetime contingency operations
Politically sensitive military operations normally characterized by the short-term, rapid projection or employment of forces in conditions short of war (FM 100-20/AFP 3-20).

Special reaction team
A specially trained team of military and security personnel armed and equipped to isolate, contain, gather information for, and, if necessary, neutralize a special threat.

Special threat
Any situation involving a sniper, barricaded criminal, or hostage taker or any terrorist incident that requires special responses or reactions, manpower management, training, and equipment.

Strategic BDA
Estimates a threat nation's ability to conduct or support warfare, and assists the NCA in measuring the effectiveness of military operations supporting our national policy objectives.

State-sponsored (or state-directed) terrorism
A terrorist group that operates as an agent of a government, receiving substantial intelligence, logistics, and operational support. In some instances, terrorist organizations have become *de facto* extensions of the sponsoring government. State sponsorship, by definition, includes the lesser situation of state support (FM 100-37).

State-supported terrorism
A terrorist group that generally operates independently but receives support from one or more governments. Support may include financing, training, equipment (including arms and explosives), issue of documentation (passports, visas, passes), furnishing operational intelligence, and furnishing a base of operations. Governments which support terrorist groups (as opposed to those which sponsor terrorist groups) are generally able to disclaim responsibility for the group's activities (plausible tenability).

Tactical BDA
Determines if the commander's targeting objectives were achieved within a limited AO.

Terrorism
The calculated use or use of violence or threat of violence to inculate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological (DOD Directive 0-2000.12 and JCS Pub 1-02). Also, the unlawful use or threatened use of force or violence against individuals or

property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives. See also antiterrorism; combatting terrorism; counterterrorism. Terrorism involves a criminal act that is often symbolic in nature and intended to influence an audience beyond the immediate victims. (A CIA working definition: A method of combat where the victim of violence is not the actual target of the attack.)

Terrorist group

A political, religious, or ideological oriented group which uses terrorism as its prime mode of operations.

REFERENCES

SOURCES USED

These are the sources quoted or paraphrased in this publication.

Joint and Multiservice Publications

FM 34-81. *Weather Support for Army Tactical Operations*. AFM 105-4. 31 August 1989.

JCS Publication 3-07.3. *Joint Tactics, Techniques, and Procedures for Peacekeeping Operations*. April 1992.

Army Publications

FM 19-30. *Physical Security.* 1 March 1979.

FM 27-10. *The Law of Land Warfare.* 18 July 1956.

FM 34-1. *Intelligence and Electronic Warfare Operations.* 2 July 1987.

FM 34-2. *Collection Management.* 20 October 1990.

FM 34-3. *Intelligence Analysis.* 15 March 1990.

FM 34-10-7. *Quickfix Operations.* 30 September 1991.

FM 34-36. *Special Operations Forces Intelligence and Electronic Warfare Operations.* 30 September 1991.

FM 34-37. *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations.* 15 January 1991.

(C)FM 34-40-3. *Tactical Signals Intelligence (SIGINT) Analysis Operations* (U). 21 May 1991.

FM 34-40-7. *Communications Jamming Handbook.* 23 November 1992.

FM 34-52. *Intelligence Interrogation.* 28 September 1992.

FM 34-60. *Counterintelligence.* 5 February 1990.

(S)FM 34-60A. *Counterintelligence Operations* (U). 6 June 1989.

FM 34-81-1. *Battlefield Weather Effects.* December 1992.

FM 34-130. *Intelligence Preparation of the Battlefield.* 23 May 1989.

(S/NF) DIAM 58-5. *Imagery Requirements* (U). 1 March 1986.

(S/NF DIAM 58-13. *Defense Human Resources Intelligence Collection Procedures* (U). 28 March 1988.

(S/NF) DDI 2660-3139-YR. *DIA-Directive for General MI Capabilities Handbook* (U).

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

AR 190-52. *Countering Terrorism and Other Major Disruptions on Military Installations.* 15 July 1983.

AR 380-5. *Department of the Army Information Security Program.* 25 February 1988.

AR 380-67. *Department of the Army Personnel Security Program.* 9 September 1988.

AR 381-10. *US Army Intelligence Activities.* 1 July 1984.

AR 381-12. *Subversion and Espionage Directed Against US Army (SAEDA).* 1 July 1981.

AR 381-20. *US Army Counterintelligence Activities.* 26 September 1986.

(S)AR 381-47. *US Army Offensive Counterespionage Operations* (U). *30 July 1992.*

(S)AR 381-100. *US Army Human Intelligence Collection Program* (U). 15 May 1980.

AR 525-13. *Army Terrorism Counteraction Program.* 12 August 1992.

(S)TC 34-5. *Human Intelligence Operations* (U). 3 October 1988.

FM 6-20-10. *Tactics, Techniques, and Procedures for the Targeting Process.* 29 March 1990.
FM 100-20. *Military Operations in Low Intensity Conflict.* AFP 3-20. 5 December 1990.
FM 100-37. *Terrorism Counteraction.* 24 July 1987.

READINGS RECOMMENDED

These readings contain relevant supplemental information.

FM 71-100. *Division Operations.* 16 June 1990.
(S)FM 90-2A. *Electronic Deception* (U). 12 June 1989.
FM 100-37. *Terrorism Counteraction.* 24 July 1987.
FM 101-5. *Staff Organization and Operations.* 25 May 1984.

TC 34-55. *Imagery Intelligence.* 3 October 1988.

Joint Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms (Incorporating the NATO and IADB Dictionaries).* 1 December 1989.
Joint Pub 3-0. *Doctrine for Unified and Joint Operations.* January 1990.
Joint Pub 3-07. *Doctrine for Unified and Joint Operations In Low-Intensity Conflict*. October 1990.

(FOUO)DODD 0-2000.12. *Department of Defense Terrorism Program*, 27 August 1990.

(S/NF)DCID 5/1. *Espionage and Counterintelligence Activities Abroad* (U). 19 December 1984.

Geneva Conventions Relative to the Treatment of Prisoners of War (GPW) of 12 August 1949.

INDEX

A

analysis in LIC, 4-1
- biases, 4-4
- mission, 4-13
- nature of government, 4-16
- nature of society, 4-13
- risk factors, 4-2
- techniques, 4-5
- threat model, 4-2
- user requirements, 4-1

area handbooks, 1-6

B

battle damage assessment, 2-3
- levels. See glossary.
- post strike assessment, 2-3

battlefield area evaluation (BAE), 3-2

battlefield operating system (BOS)
- as a combat multiplier, 2-1

C

collection plan formats, D-1
- collection management process, D-5
- examples of LIC PIR and IR, D-4
- prioritization matrix, D-8, D-10
- synchronization matrix, D-15

combatting terrorism, 1-5
- antiterrorism, 1-5
- counterterrorism, 1-5
- LIC category, 1-3
- S2 checklist, Appendix K

concealment and cover overlay, G-1, G-3

counterinsurgency, 1-3
- definition, 1-4
- LIC category, 1-3
- S2 checklist, Appendix J
- US forces activities in, 1-4

counterintelligence
- counterinsurgency support, 5-7
- IEW support to, 5-1
- insurgency support, 5-4
- intelligence operations, 5-11
- security A&A, 5-8
- tactical operations, 5-12

D

decision support template, G-9

defensive EW
- preventive techniques, B-1

disaster relief overlay, G-12

dispersed battlefield collection plan format, D-1

displaced persons overlay, G-12

E

echelons above corps
- MI Brigade capability, A-1

event template, G-9

H

HN government and military overlays, G-8

I

I&W. See IEW functions.

IEW architecture
- HN assets, 2-8
- non-DOD assets, 2-6, 2-7
- US assets, 2-6
- US sources within HN, 2-8

IEW assets. See IEW architecture.

IEW functions
- BDA and PSA, 2-3
- force protection (CI and OPSEC), 2-4
- I&W, 2-2
- IPB, 2-2
- situation development, 2-2
- target development, 2-3

IEW support to insurgency and counterinsurgency
- CI, 5-4
- HUMINT, 5-1
- IMINT, 5-2
- SIGINT, 5-3

imagery intelligence (IMINT)
- advantages and disadvantages, H-2
- as part of MDCI, H-3
- in support of PCO, 8-2
- phases, 5-2
- support to LIC, H-1

imagery sensor systems, H-4
- airborne and orbital platforms, H-6

insurgency, 1-3
- common elements, 1-3
- definition, 1-3
- LIC category, 1-3
- types of operations in, 1-3

insurgency phases, 3-11

intelligence cycle, 2-4

intelligence preparation of the battlefield (IPB)

area of interest and area of operations, 2-2
commander's mission, 3-1
terrain analysis, 3-5
threat evaluation, 3-9
threat integration, 3-16
weather analysis, 3-8

intelligence requirements for LIC
informational categories, E-1
operational categories, 1-3, E-1

intelligence support to PKO
mission and functions, 7-1

interrogation support
handling insurgents, I-3
limitations, I-1
screening techniques, I-5

K

key facilities and target overlay, G-4, G-6

L

letter of instruction (LOI), 1-6

LIC
fundamentals, 1-1
imperatives, 1-2
influences, 1-1
operational categories, 1-1, 1-3, E-1

link analysis. See analysis in LIC.
activities matrix, 4-6, 4-10
association matrix, 4-6, 4-9
link diagram, 4-6
time event chart sample, 4-6, 4-11

LOC overlay, G-4, G-7

logistics sustainability overlay, G-4, G-5

M

MDCI support responsibilities, C-1

N

nonbelligerent third-party overlays, G-8

noncombatant evaluation operation event template, G-12

O

OCOKA factors, 3-5, 3-6

offensive EW
ES and EC, B-1

operational categories. See LIC.

P

pattern analysis. See analysis in LIC.
coordinate register, 4-6, 4-7
hot file, 4-5
personality card, 4-6, 4-8

peacekeeping operations (PKO), 1-5
S2 checklist, Appendix L

peacetime contingency operations (PCO), 1-6
continuum, 1-7
IEW support to, 8-1
S2 checklist, Appendix M

physical security, 5-10

population status overlay, G-1, G-2

R

reactive decision support template, G-12, G-15

reactive event template, G-12, G-14

reactive situational template, G-12, G-13

reports
Spot Report, F-1
Intelligence Estimate, F-1

restrictive areas. See physical security.

S

signals intelligence (SIGINT)
in support of PCO, 8-3
phases, 5-3, 5-4

situation template, G-8

standard collection plan format, D-1

T

tactical EW equipment, B-1

target area replicas (TARs), G-16

target areas of interest
categories, 3-17

target development
HPT, 2-3
HVT, 2-3

target value analysis, 3-17

terms of reference (TOR), 1-5

terrain overlays, G-1 through G-7

threat evaluation
development, 3-9 through 3-16
evaluation and production, 3-16

threat integration templates, G-12 through G-15

training, 3-13

W

weather effects, 3-8, G-8

weather overlay, G-8

FM 34-7
18 MAY 1993

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:

Milton H. Hamilton
MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army
03693

DISTRIBUTION:

Active Army, USAR, and ARNG: To be distributed in accordance with DA Form 12-11E, requirements for FM 34-7, Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations (Qty rqr block no. 5104).

*U.S. Government Printing Office: 1993 — 728-027/60136