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 counterinsurgent 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.

**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 (LA). 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.

SIGNS 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 C3 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 C3 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 C3 and logistics activities.

In the offense, EW measures include the exploitation, disruption, and deception of threat command, control, communications, and intelligence (C3I) 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 C3 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, 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 maybe 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. C3 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 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.
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.

Insurgences 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.
- C³ system.
- All-source collection capabilities.
- Third-country intelligence and security IDAD support.
- CI capabilities and countermeasure.
- 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\'I. 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 database 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 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.
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.
- C3.
- 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 380-6Z. 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.
- Countersabversion.
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 maybe 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.

LEGEND:
- Movement direction
- Security elements
- Search elements
- Buildings
- Sweep elements
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 sopor 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.