MCWP 2-14
(Coordinating Draft -- 7 Oct 98)

COUNTERINTELLIGENCE

U.S. Marine Corps

PCN ??? ?????? ??

MCWP 2-14, *COUNTERINTELLIGENCE*

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

__ ___ 1998

FOREWORD

Marine Corps Doctrinal Publication 2, *Intelligence*, and Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations*, provide the doctrine and higher order tactics, techniques, and procedures for intelligence operations. MCWP 2-14, *Counterintelligence,* complements and expands upon this information by detailing doctrine, tactics, techniques, and procedures for the conduct of counterintelligence operations in support of the Marine Air-Ground Task Force (MAGTF). The primary target audience of this publication is intelligence personnel responsible for the planning and execution of counterintelligence operations. Personnel who provide support to counterintelligence or who use the results from these operations should also read this publication.

MCWP 2-14 describes aspects of counterintelligence operations including doctrinal fundamentals, equipment, command and control, communications and information systems support, planning, execution, security, and training. MCWP 2-14 provides the information needed by Marines to understand, plan, and execute counterintelligence operations in support of the Marine Air-Ground Task Force across the spectrum of conflict.

MCWP 2-14 supersedes FMFM 3-25, *Counterintelligence*, dated 22 September 1992.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

JOHN E. RHODES
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: ??? ?????? ??

MCWP 2-14, *Counterintelligence*

Table of Contents

CHAPTER 1

DOCTRINAL FUNDAMENTALS

1001. Introduction. Intelligence strives to accomplish **two** objectives. **First**, it *provides accurate, timely, and relevant knowledge about the enemy (or potential enemy) and the surrounding environment.* In other words, the primary objective of intelligence is to support decision making by reducing uncertainty about the hostile situation to a reasonable level—recognizing, of course, that the fog of war renders anything close to absolute certainty impossible. The **second** intelligence objective is that it *assists in protecting friendly forces through counterintelligence.* Counterintelligence includes both active and passive measures intended to deny the enemy valuable information about the friendly situation. Counterintelligence also includes activities related to countering hostile espionage, subversion, and terrorism. Counterintelligence directly supports force protection operations by helping the commander deny intelligence to the enemy and plan appropriate security measures. The two intelligence objectives demonstrate that intelligence possesses either positive—or exploitative—and protective elements. It uncovers conditions that can be exploited and simultaneously provides warning of enemy actions. Intelligence thus provides the basis for our own actions, both offensive and defensive. Identifying, planning, and implementing MAGTF counterintelligence operations and measures are the main focus of this publication.

1002. Objective. Counterintelligence (CI) is the intelligence function that is concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion, or terrorism. The objective of CI is to enhance command security by denying an adversary information that might be used to conduct effective operations against friendly forces and to protect the command by identifying and neutralizing espionage, sabotage, subversion, or terrorism efforts. CI provides critical intelligence support to command force protection efforts by helping identify potential threats, threat capabilities and planned intentions to friendly operations while helping deceive the adversary as to friendly capabilities, vulnerabilities and intentions. Physical security reduces our vulnerability. Operations security reduces our exposure. Combating terrorism efforts combine to make us a less lucrative target. In so doing, CI increases uncertainty for the enemy, thereby making a significant contribution to the success of friendly operations. CI also identifies friendly vulnerabilities, evaluates security measures, and assists with implementing appropriate security plans. The integration of intelligence, CI and operations culminates in a cohesive unit force protection program.

> Counterintelligence -- Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Jt

1003. Basis for CI Activities

a. Hostile objectives. Adversaries can be expected to use every available means to thwart or otherwise impede our forces with his efforts directed towards intelligence, espionage, sabotage, subversion, and terrorism operations. Hostile intelligence collection activities are directed toward obtaining detailed knowledge of our forces and their capabilities, limitations, centers of gravity, vulnerabilities, intentions, and probable courses of action. These activities also obtain information concerning the area of operations, including weather, terrain, and hydrography.

b. Adversarial advantage. Adversary knowledge of friendly operations will enable him to concentrate his efforts. His efforts are on preparing the objective for defense, attacking friendly staging areas, and disrupting the operation through espionage, sabotage, terrorism, and subversive activities. Accordingly, CI is essential to the security of our forces—commencing with routine garrison operations, to the inception of planning and until the operation is completed—in order to deny the enemy any advantage and manipulate his understanding of us.

(1) Hostile Espionage Activities. Foreign intelligence services must be estimated with being at least as effective as our own. An adversary should always be given the benefit of the doubt in assessing his capabilities in collecting information and producing intelligence on friendly operations. Foreign intelligence services do not normally develop vital intelligence by obtaining one all-revealing fact. Rather, most of their worthwhile intelligence is the product of the assembly, comparison, and interpretation of many small and seemingly insignificant items of information.

(2) Enemy Sabotage Activities. Sabotage is an act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources. Immediately prior to the outbreak of hostilities, during combat, and even during military operations other than war (MOOTW) the enemy can be expected to employ sabotage techniques to disrupt friendly operations.

(3) Subversive Activities. Subversive activities are designed and conducted to undermine the authority of friendly forces and/or that of the local government in order to disrupt friendly activities or to gain aid, comfort, and moral support for the cause of the enemy or hostile force or group. Subversive activity can be directed against individuals, groups, organizations, or entire populations. Frequently, subversive activity supports, conceals, or provides a favorable environment for espionage, sabotage, and terrorist operations. Subversion is an action designed to undermine the military, economic, psychological, political strength or morale of a regime.

(4) Terrorist Activities. Terrorist activities are often extreme. Any personality, organization, or installation of political or military significance could be a potential terrorist target. Terrorists have become adept in the calculated and systematic use of violence or threat of violence in pursuit of their political or ideological goals. Although the tactics and modus operandi of terrorists may vary from group

to group, the techniques they employ to dramatize their goals through fear, intimidation, and coercion are similar.

Security -- Measures taken by a military unit, an activity, or an installation to protect itself against all acts designed to, or which may, impair its effectiveness. (Joint Pub 1-02).

1004. Concepts of CI and Force Protection

a. Historical Services Perspectives. CI has had a long history of being a "stovepipe" discipline. The four Services each perceive and execute CI differently.

(1) Navy and Air Force. The Navy's Naval Criminal Investigative Service (NCIS) and the Air Force's Office of Special Investigations (0SI) have traditionally viewed CI with a strategic focus drawn from their perspectives as, primarily, law enforcement organizations. NCIS is mainly a civilian investigative organization with a chain of command directly from the Secretary of the Navy to the Director, NCIS. The Director of Naval Intelligence (DNI), however, has policy and oversight responsibilities for Navy CI. CI activities of NCIS are funded from the Foreign Counterintelligence Program (FCIP). OSI is a field operating agency of the Air Force. Policy and programmatic oversight rests with the Secretary of the Air Force Office of the Inspector General, not the Director of Intelligence. CI activities of OSI are also funded from the FCIP. Like NCIS, there is no programmatic provision in OSI for Tactical Intelligence and Related Activities (TIARA) funding or resources.

(2) Marine Corps and the Army. The Army and Marine Corps maintain CI as a component of their intelligence staffs. The Marine Corps CI orientation is entirely tactical, with funding exclusively within the Navy Department's budget for TIARA. The Army emphasizes both strategic and tactical CI and, thus, CI is supported by a mixture of FCIP and TIARA resources.

(3) Joint. Because of these differences in emphasis and support for CI, during the development of joint CI doctrine, the issue arose as to whether CI should fall under the staff cognizance of intelligence or operations. Doctrinal evolution has placed the CI of the combatant commands and JTFs command under the J2.

b. Joint Operations and CI. In exercising command and control of CI, different rules also apply. In peacetime and times other than the execution of an NCA-approved OPLAN, Service CI elements are under the command or operational control of their Service (in the case of the Navy and Air Force) or operating forces headquarters. Under execution of an NCA-approved OPLAN, however, the commanders exercise command and control of CI elements organic to or supporting their commands. There are, however, continuous requirements for keeping the commanders informed of any CI activities within their areas of interest.

c. CI and Intelligence. CI, like all intelligence matters, is a command responsibility. In preparing for operations, all units must develop a CI plan and implement appropriate CI measures to protect themselves from potential threats. CI is integrated into the overall intelligence effort to identify and counter an adversary's intelligence efforts. Failure to adequately plan for and implement CI operations and measures may result in serious damage to the MAGTF. Continuing attention to CI and effective

intelligence and operations integration is thus required at all levels of command, from the MAGTF commander through the individual Marine.

d. CI and Force Protection. Force protection is a responsibility of command. An operations function, force protection is under the staff cognizance of the unit operations officer. CI is a significant contributor to the command's overall force protection effort. Security is a matter of vulnerability and threat assessment in conjunction with effective risk management. CI helps identify the hostile intelligence threat, assists in determining friendly vulnerabilities to it, and aids with the development of friendly measures that can lessen or negate these. The commander weighs the importance of intelligence and CI to be used as a tool in risk management. Marine Corps CI elements provide unique force protection capabilities through both active and passive CI measures and human resource intelligence (HUMINT) support. Often times, CI elements can provide unique intelligence support to the commander's estimate of the situation and situation development (e.g., providing an assessment of the *'mood'* of the area of operations, allowing us to feel the pulse of an incident as it develops). CI also provides critical support to the command's overall intelligence efforts by providing indications and warning (I&W) of potential attack and support to targeting and combat assessment efforts.

> **Force Protection** -- A security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, CI, and other security programs. (Joint Pub 1-02)

1005. MAGTF Counterintelligence Operations—Overview.

a. Responsibilities. CI, like all intelligence matters, is a command responsibility. In preparing for operations, all units must develop a CI plan and implement appropriate CI measures to protect themselves from potential threats. The unit intelligence officer plans, implements, and supervises the CI effort for the commander. The G-2/S-2 may have access to or request support from MAGTF CI units and specialists to assist in developing CI estimates and plans. All members of the command are involved in executing the CI plan and implementing appropriate CI measures. Key participants in this process and their specific responsibilities are:

- Unit security manager (generally the chief of staff or executive officer)—overall integration and effectiveness of unit security practices
- G-3/S-3—force protection, operations security (OPSEC), counterreconnaissance, and deception.
- G-6/S-6—communications and information systems security
- G-1/S-1—information and personnel security
- Headquarters commandant—physical security of unit command post and echelons

b. CI Process. The CI process at all levels is conducted by using a standard methodology that consists of three steps: developing a CI estimate, conducting a CI survey, and developing the CI plan. Figure 1-1 summarizes the CI process.

(1) The CI Estimate. The CI estimate details the capabilities and limitations of hostile intelligence, subversive, and terrorist organizations that could carry out actions against friendly units and facilities or against individuals, groups, or locations of concern to our forces, such as the local population or civilian organizations operating in the area. It also provides an estimate of possible and probable COAs that these threat organizations will adopt. Intelligence and CI analysts of the MAGTF CE and CI/HUMINT company will normally prepare a comprehensive CI estimate that addresses threats to the MARFOR or MAGTF by using an IPB methodology that is focused on CI factors and the CI threat. However, each level of command must conduct its own evaluation to determine which of the adversary's capabilities identified in the MAGTF CI estimate represent a threat to their particular unit. The CI estimate must be updated on a regular basis, and the revised estimate or appropriate CI warning reports must be disseminated to all units involved in the operation.

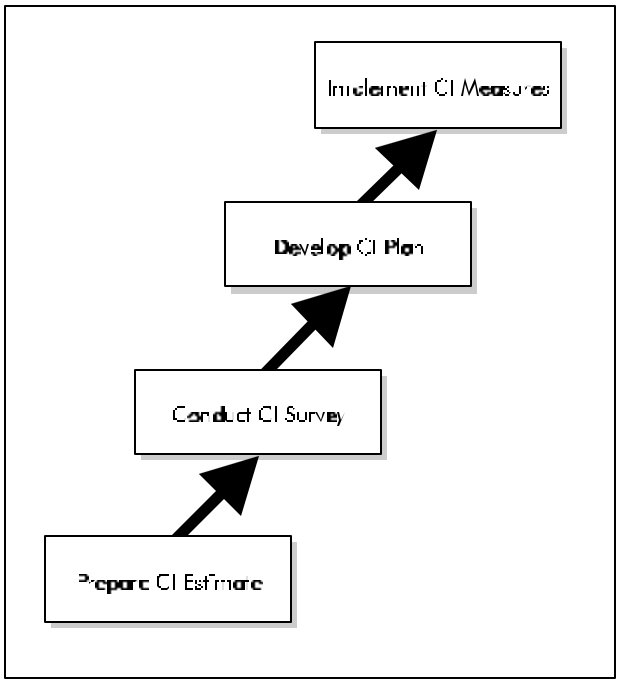


Figure 1-1. The Counterintelligence Process

(2) The CI Survey. The CI survey assesses a unit's security posture against the threats detailed in the CI estimate. The CI survey should identify vulnerabilities to specific hostile intelligence, espionage, sabotage, subversion, or terrorist capabilities and provide recommendations on how to eliminate or minimize these vulnerabilities. The survey should be as detailed as possible. During the planning phase of an operation, it may be possible to do a formal, written survey. CI specialists from the CI/HUMINT company may be available to assist in this effort. In a time-compressed situation, the survey will likely

result from a brief discussion between the appropriate intelligence, operations, communications, and security personnel. In either case, it is critical that the survey look forward in both space and time to support the development of the CI measures necessary to protect the unit as it carries out successive phases of the operation; that is, the survey makes recommendations to improve the CI posture of the command both now and in the future.

(3) The CI Plan. The CI plan details the activities and operations that the command will use to counter the CI threat. It includes procedures for detecting and monitoring the activities of hostile intelligence and terrorist organizations and directs the implementation of active and passive measures that are intended to protect the force from these activities. The CI plan is based on the threats identified in the CI estimate and the vulnerabilities detected by the CI survey. The MAGTF staff CI officer normally prepares a detailed, comprehensive CI plan that addresses the entire MAGTF and is integrated with CI plans of the JTF and other pertinent forces. Included in the MAGTF CI plan are details of the employment of dedicated CI capabilities and the conduct of specialized CI operations intended to detect and neutralize or eliminate specific CI threats. Plans of subordinate MAGTF elements closely follow the MAGTF plan, normally adding only security measures that are applicable to their specific units. As with all plans, CI plans must be continually updated to ensure that they are current and support both ongoing and future operations.

c. CI Execution. CI analysis develops threat assessments that can assist decision makers in determining the threat posed to their plans, strategies, resources, programs, operations and systems by foreign intelligence activity. An understanding of the interest and capability of adversarial intelligence organizations to collect information on evolving U.S. technologies is critical to developing appropriate countermeasures. CI personnel can readily obtain information from other national intelligence and security organizations because of its unique liaison arrangements. That capability not only supports the analytical efforts of the national agencies and intelligence centers, but also can give an added dimension to I&W. One of the most highly effective tools of the CI collection activity is the CI Force Protection Source Operation (CFSO), which has been used with great effectiveness in recently deployed JTFs. The CFSO provides the commander with a collection and production capability to protect his force without resorting to complex national coordination procedures. The role of CI is even greater as U.S. military operations increasingly rely upon cooperation and support of our allies. CI personnel can assess the capabilities, effectiveness, organization and methods of operation of foreign intelligence services as well as the effectiveness of their security procedures and, thus, their ability to support or to detract from the U.S. effort.

1006. Counterintelligence Measures. CI measures encompass a broad range of both active and passive measures designed to protect against the CI threat. There are two general categories of CI measures: active and passive.

a. Active Measures. Active CI measures are those designed to neutralize the multi-discipline intelligence effort (all disciplines used to collect intelligence such as human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT)) and hostile efforts toward sabotage, subversion, and terrorism. Active CI measures include, but are not limited to counterespionage,

countersabotage, countersubversion, counterterrorism, counter-reconnaissance, concealment, and deception operations. Active CI measures vary with the mission and capabilities of the unit. Complex active CI measures such as counterespionage operations, counterterrorism operations, screening and interrogations, and defensive source operations are conducted only by CI personnel or other specialized organizations following the direction of the joint force and/or MAGTF commander

b. Passive Measures. Passive CI measures are those designed to conceal and deny information to the enemy, protect personnel from subversion and terrorism, and protect installations and material against sabotage. Measures include, but are not limited to, security of classified material, personnel security, physical security, security education, communications security, data security, electromagnetic emission security, censorship, camouflage, concealment, light, and security discipline. Passive measures are readily standardized in the unit's standing operating procedures (SOPS) regardless of the unit's mission.

c. Types of CI Measures. The three general CI measures are denial, detection, and deception. Frequently, the measures applied to accomplish one of these purposes contribute to the others.

(1) Denial Measures. Denial measures are applied to prevent the enemy from gaining access to classified and sensitive information, subverting personnel, and penetrating the physical security barriers established at command posts and echelons, facilities and installations. Counter-reconnaissance is one example of a denial measure that may be used.

(2) Detection Measures. Detection measures are used to expose and to neutralize enemy efforts directed toward intelligence collection, sabotage, subversion, and terrorism. MAGTF units detect or aid in the detection of these enemy efforts by collecting, analyzing, and reporting information on enemy activities that may indicate an intelligence effort, by establishing checkpoints to control the movement of personnel within or through their areas of responsibility, and by evacuations of possible enemy agents and materials to higher echelons for interrogation and exploitation. Other detection measures, usually accomplished by specialists, include document translation and analysis, screening, interrogation, and offensive and defensive CI activities.

(3) Deception Measures. Deception measures are used to mislead or otherwise confuse the enemy concerning our capabilities, centers of gravity, vulnerabilities, plans and intentions. Deception measures may include feints, ruses, demonstrations, and the provision of false information to the enemy. Control of deception operations should be at the highest level of command that is likely to be significantly affected by the enemy's reactions. Deception measures depend on effective command security for success. Special precautions must be taken to ensure that there is no leakage of friendly force information during the planning or execution of an operation. When enemy intelligence activities are identified, consideration must be given to the potential for using that activity in support of deception measures. The potential threat posed by the enemy must be weighed against the potential intelligence benefits of continued exploitation of the enemy's intelligence system versus its destruction or other degradation

1007. Counterintelligence Support to Operations. MAGTF CI support to operations normally is within one of the following two categories.

a. Support to Military Security. Military security encompasses all measures taken by a command to protect itself from sabotage, terrorism, and subversion, and to deny information to the enemy. In MAGTF units, it emphasizes protection of airfields and other major installations, and the defeat of hostile target acquisition efforts. Typical measures include operations security (OPSEC), counter-reconnaissance, countersigns, passwords, and restrictions on access to selected areas and installations.

(1) Support to Operations Security

(a) OPSEC is the functional responsibility of the operations officer (G-3/S-3). To be effective, OPSEC principles and concepts must be established and continuously proactive during the conduct of MOOTW as well as in combat environments. Commanders must determine what essential elements of friendly information (EEFI) and operations must be protected, what OPSEC measures to implement, when to implement them, and what level of risk they are willing to accept. Commanders, staffs, and individuals at all echelons of command are responsible for developing and implementing an effective OPSEC program.

(b) OPSEC denies the enemy prior knowledge of EEFI regarding command activities, plans, operations, strengths, vulnerabilities and intentions. The enemy collects this information through a variety of means—human, electronic, photographic, etc. To effectively counter this threat, commanders must have access to timely, reliable and accurate intelligence on enemy intelligence capabilities and operations.

(c) CI supports commanders' OPSEC programs by providing assessments of friendly vulnerabilities; briefings on enemy threats of espionage, sabotage, subversion, and terrorism; and assistance in establishing safeguards and countermeasures against these threats.

(2) Support to Information Security and C2 Protect. Information security (INFOSEC) is designed to protect sensitive information from exposure to potential release or compromise. The INFOSEC program includes a proper security classification determination being made in conjunction with applicable security regulations and the proper protection being afforded to the material throughout it life cycle. These measures included proper preparation, reproduction or manufacturing, storage, utilization and destruction. Failure to comply with required INFOSEC measures expose sensitive information to potential compromise. The rapid advancement of the microprocessor and the maturity of computer age technologies have presented a significant new area of exposure that leaves us particularly vulnerable. While these advances provide new capabilities and opportunities, they also create new vulnerabilities to be exploited. Information operations (IO) is the move to recognize the potential and the threats created by this trend. IO include actions taken to affect adversary information while defending one’s own information and information systems during both routine peacetime, MOOTW and combat operations. Command and control (C2) Protect are those defensive measures taken to detect and

prevent hostile efforts against our C2 and supporting communications and information systems. The ability to directly influence key decision-makers through the injection, disruption, manipulation or destruction of information and information means is a powerful tool in the advance of military objectives. Information system vulnerabilities include denial of service, information theft, information replacement or introduction of false data. Defensive measure to provide information assurance include use of secure networks, firewalls, encryption, anti-virus scans to detect malicious code, and proper systems administration to include aggressive auditing. Information protection comprises the authenticity, confidentiality, availability, integrity, and non-repudiation of information being handled by anyone involved with C2. It requires proper implementation of appropriate security features such as passwords, authentication, or other countermeasures. The criticality for CI in this area is the ability to identify the adversary's potential capability to exploit, deny, degrade or destroy friendly C2 before an attack in order to counter the attempt. The reporting and tracking of attempted and successful attacks will, through trend analysis assist in the development of countermeasures.

(3) Counter-reconnaissance. Of all the CI measures that are taken by a unit in combat, one of the most effective is counter-reconnaissance. Units may be assigned both reconnaissance and counter-reconnaissance responsibilities; these two activities complement each other and are inseparable. Good reconnaissance ensures a certain amount of security, and counter-reconnaissance provides a certain amount of reconnaissance information. However, a unit tasked with a reconnaissance mission is not ordinarily given a supplementary counter-reconnaissance mission as completing the counter-reconnaissance mission generally requires defeat of hostile reconnaissance elements, while the primary goal of reconnaissance is collection of information, not combat. Counter-reconnaissance can include the setting up of a defensive screen to deny enemy reconnaissance or an offensive screen designed to meet and destroy enemy reconnaissance in combat air operations. Counterair operations may be defined as counter-reconnaissance when counterair operations deny or reduce an enemy's capability for visual, photographic, or electromagnetic reconnaissance.

(a) Principles of Counter-reconnaissance. Counter-reconnaissance elements focus on friendly forces being screened. Hostile reconnaissance forces are destroyed or neutralized by combat, and friendly screening forces are echeloned in depth.

(b) Forms of Counter-reconnaissance. The defensive screen is protective. It is usually established behind natural obstacles. An offensive screen may be moving or stationary depending on the activities of the friendly force being screened. The offensive screen meets the enemy's reconnaissance forces and destroys them. The commander's adoption of a form of counter-reconnaissance screen depends on the situation, mission, weather, and terrain; thus the form of counter-reconnaissance screen adopted, need not reflect solely the tactical mission of the command. The fact that there are offensive and defensive screens does not imply a requirement for their employment only in support of a like tactical mission. An offensive screen may well be employed to support a tactical mission of defense, while an attack mission may be supported best by a defensive screen.

(4) Support to Embarkation Security. Embarkation security consists of the special application of military and civil security measures to the embarkation phase which include the movement

to the point of embarkation and the actual embarkation. Examples include the screening of civilians employed in the port or airfield, control of contact between troops and civilians, covering or removing tactical markings and other unit designations, and moving to the port or airfield under cover of darkness.

b. Support to Civil Security. Civil security operations include all the CI measures affecting the population of the area. Typical measures include security screening of civilian labor, imposing curfews and other circulation control measures, and the monitoring of suspect political groups. Civil security operations are generally conducted in coordination and in conjunction with law enforcement, civil affairs, and other appropriate agencies.

CHAPTER 2

COUNTERINTELLIGENCE FUNCTIONS AND SERVICES

"…Mogadishu has been one tough nut to crack… we are making steady and perceptible progress. From my perspective, one of the most encouraging outgrowths of our efforts in this socially, politically and geographically complex urban environment has been the **emergence of tactical HUMINT** as the driving force behind operations… in-by-9 out-by-5 service on priority intelligence requirements."

"… been directed against clearly defined targets – there have remarkably few dry holes. Spared the long unproductive walks in the sun sometimes associated with the Vietnam Conflict. The troops have remained alert, tactically disciplined and tightly focused. I believe this accounts, in some measure, for our low casualty rate."

"… it's refreshing to see things in their proper order – **INTELLIGENCE DRIVING OPERATIONS** … instead of operations driving intelligence."

MGen Wilhelm, USMC
Commander, Marine Forces-Somalia

2001. Counterintelligence Functions. There are four CI functions: CI operations; CI investigations; CI collection and reporting; and CI analysis, production, and dissemination. (See figure 2-1)

a. CI Operations. Offensive CI Operations (OFCO) are the employment of specialized CI techniques and procedures. They are directed against the espionage, sabotage, subversive and terrorism threat. These operations are planned, coordinated, and conducted by MAGTF CI personnel and include the following operations:

(1) Counterespionage Operations. These operations are designed to detect, destroy, neutralize, exploit, or prevent espionage activity. This is accomplished through the identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities.

(2) Countersubversion Operations. These operations are designed to detect, prevent, or neutralize the activities of subversive groups. Subversive activity is closely related to and frequently supports, conceals, or provides a favorable environment for espionage and sabotage operations. Based on this environment, the countersubversive mission may include offensive measures directed toward the origin of hostile subversive plans and policies.

Counterintelligence Function	Objectives
CI Operations	-- Determine foreign intentions -- Support tactical and strategic perception management operations -- Support all-source intelligence and other CI operations -- Support planning and military operations
CI Investigations	-- Detect, exploit, prevent, or neutralize espionage activities -- Detect and resolve incidents of foreign directed sabotage, subversion, sedition, terrorist activities, and assassinations -- Documents elements of proof for prosecutions -- Provide military commanders and policy makers with intelligence and information to use to eliminate security vulnerabilities and improve security postures
CI Collections and Reporting	-- Provide indications and warning of security threats to U.S. forces, facilities, and operations -- Provide intelligence on threats to forces to support planning and implementation of defensive or offensive countermeasures -- Respond to commander's priority intelligence requirements
CI Analysis, Production and Dissemination	-- Provide analysis and assessments of threats to U.S. forces, facilities, and operations -- Provide causal analysis of past events to identify vulnerabilities and risks -- Identify adversary organizations, personalities, and capabilities posing threats to forces, facilities, and operations

Figure 2-1. Objectives of CI Functions

(3) Countersabotage Operations. These operations require a comprehensive program to penetrate saboteur, partisan, or other dissident groups. The goal of the program is to determine sabotage plans and to identify saboteurs, method of operation, and specific targets and thus MAGTF force protection.

(4) Counterterrorism Operations. These operations are planned, coordinated, and conducted to detect, prevent, or neutralize terrorist groups or organizations by determining terrorist

plans or intentions. These operations are also employed to identify terrorists, methods of operation, and specific targets.

(5) Exploitation and Neutralization Operations. These operations are targeted against personalities, organizations, and installations of intelligence or CI interest, which must be seized, exploited, or protected. Screening and interrogations are operations designed to identify and apprehend enemy intelligence agents, subversives, terrorists, and saboteurs who attempt to infiltrate friendly lines and operations or conceal themselves among the population.

b. CI Investigations. CI investigations are investigations concerning personnel, security matters, espionage, sabotage, terrorism, and subversive activities (including defection). A CI investigation is a duly authorized, systematic, detailed examination/inquiry to uncover and report the facts of a matter. CI investigations fall under the jurisdiction of the Naval Criminal Investigative Service (NCIS). NCIS operates a worldwide organization in support of the Department of the Navy and holds exclusive investigative jurisdiction. These investigations are about matters involving actual, potential, or suspected espionage, sabotage, and subversion, including defection. During combat operations, the exclusive CI jurisdiction held by the NCIS in garrison is assigned to MAGTF commanders and executed by MAGTF CI elements under the staff cognizance of the unit intelligence officer. Such authority is subject only to legal considerations and restrictions, which may be imposed by the MAGTF commander or other higher authority. Additionally, MAGTF CI elements conduct investigation of friendly prisoners of war and persons missing (non-hostile) in action cases. The type of sensitive activities required in these investigations include collecting information of potential intelligence value on friendly personnel possibly in enemy hands (to include debriefings of returned POW/MIA, with emphasis on identifying, locating, and recovering additional personnel), and the collection of information that aids in identifying, locating, and recovering those friendly personnel known or suspected in enemy hands. Initial damage assessments relating to the possible compromise of operational and sensitive material must be included.

c. CI Collections and Reporting. CI collections and reporting are a significant force multiplier, which is intended to identify actual and potential threats to the command. Collections includes:

(1) Liaison. Coordination (within authorized jurisdictional limitations) conducted by CI elements with local intelligence, CI, security and law enforcement organizations/agencies, and civil affairs and psychological operations units where appropriate.

(2) CI Force Protection Source Operations (CFSO). CFSO are overt source collection activities of an expedient nature intended to identify threats to the command in support of the commander's force protection mission.

d. CI Analysis & Production. Limited initial analysis is conducted by MAGTF CI elements that originally collected and reported the information. Detailed analysis occurs as part of the MAGTF's all-source intelligence effort.

2002. Counterintelligence Services. CI services include CI surveys and vulnerability assessments, evaluations, inspections, training and technical services. They are conducted to enhance the security of the command against espionage, sabotage, subversion, and terrorism. Technical Surveillance Countermeasures (TSCM) involve the employment of services and techniques designed to locate, identify, and neutralize the effectiveness of hostile intelligence service's technical surveillance activity (see chapter 11).

2003. CI Support to the Strategic, Operational, and Tactical Levels of War

a. The levels of war form a hierarchy. Tactical engagements are components of battle, and battles are elements of a campaign. The campaign, in turn, is itself but one phase of a strategic design for gaining the objectives of policy. While a clear hierarchy exists, there are no sharp boundaries between levels. Rather, they merge and form a continuum. Consequently, a particular command echelon is not necessarily concerned with only one level of war. A commander's responsibilities within the hierarchy depend on the scale and nature of the operation and may shift up or down as the operation develops. (See MCDP 1-1, *Strategy*, and MCDP 1-2, *Campaigning*, for additional information on the levels of war.)

b. CI provides critical support to all three levels of war. (See figure 2-2) While certain activities may cross levels based on the environment and the nature of the threat, the levels and type of CI support remain fairly distinct. The distinctions are based on the supported commander's intelligence and CI requirements. If the support satisfies national interests and policy objectives, it is part of the strategic level CI support. When the objectives and requirements focus on the overall joint force and its operations and sustainment, CI support is at the operational level. Tactical CI support addresses the immediate needs of commanders, particularly maneuver commanders, conducting the battles and engagements, with CI support emphasizing force protection from proximate threats. This publication will focus predominantly on tactical CI support to MAGTF operations.

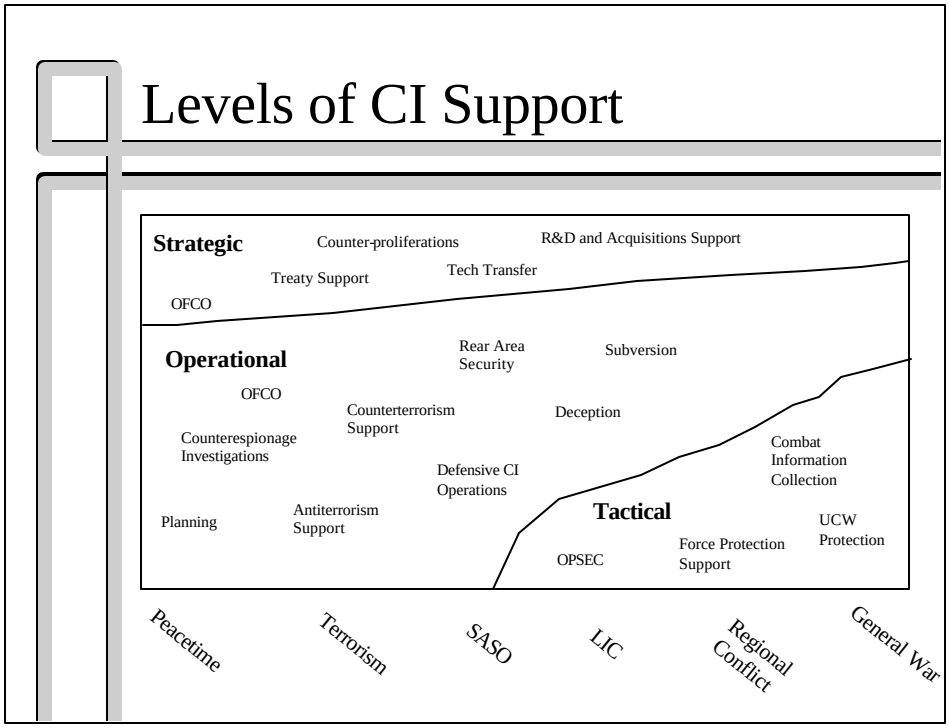


Figure 2-2. Levels of Counterintelligence Support

a. Strategic CI Support

(1) The strategic level focuses on national security objectives, and involves the National Command Authority (NCA), National Security Council, JCS, and Congress. The perspective is far more "macro" in looking at how the instrument of national power is used to satisfy the overarching national objectives, interests and policies. Marines support these programs independently and are fully integrated into these programs conducting CI Operations, often under the sponsorship of another service or national agencies.

(2) Strategic-level CI helps provides answers to the question, "What threats exist to the national interests and instruments of national power?" Strategic CI primarily supports national-level programs, satisfying requirements across the spectrum of potential combat. Strategic CI emphasizes systems protection, acquisition, proliferation, and strategic level Offensive CI Operations (OFCO). Although the above programs may also impact on the operational and tactical level, they are generally focused on addressing national-level requirements and support. The impact of these programs should be on national-level decision-making with direct linkages supporting combatant commands' strategies and initiatives. National-level agencies centrally manage and control strategic CI support, since the scope of these operations spans across geographic regions or service or organizational lines.

b. Operational CI Support

(1) The operational level looks at how to translate the national strategy and objectives into reality through the use of assigned forces. Although strategy, derived from national policies and objectives, defines the nature of the operations, the operational level is responsible for the specific implementation of those strategies. The operational level links strategic security objectives to the tactical decision making and the employment of forces. It is the level that wars are conducted. The operational level looks at the design, organization and integration of strategies, campaigns, and major operations. The operational-level commander is the principal supported commander at this level; JTF and MAGTF commanders also are key recipients of operational level CI support.

(2) Operational CI support, across the joint spectrum of potential employment, is probably the most daily active area of CI support. It has a major impact on the overall ability of commanders to conduct operations in support of national objectives. Operational CI focuses on threats to plans and operations, particularly within the context of the wider scope of the campaign, rather than the more specific scope of the tactical commander. Operational CI focuses on the question of "What are the threats to continuity and the ability to retain the tempo of overall operations?" Operational level CI emphasizes contingency planning, liaison, collections (including CFSO), counterespionage investigations, offensive and defensive CI operations, analysis, production and dissemination of threat related reporting. In contingencies and warfare, many operational CI activities focus on the rear areas, since that is where critical C2, logistics and other sustainment is located. The combatant command's joint intelligence center and the JTF joint intelligence support element are the principal planners and producers of operational CI support.

c. Tactical CI Support. The integration, sustainment, and protection of tactical level forces are of primary concern at this level. The perspective focuses on implementing or achieving national objectives through the use of tactical forces. To a great extent, the tactical level looks at the application of resources (means) applied to achieve national objectives (ends). Responsibility for fighting battles and engagements rests with tactical commanders. Tactical CI support emphasizes direct support to tactical commanders' intelligence and force protection requirements and operations through the identification, neutralization/destruction and potential exploitation of threats to maneuver forces through the collection of threat related information.

(1) Tactical CI is tailored to the needs of the MAGTF and subordinate commanders. MAGTF CI addresses the immediate and continuing need of the MAGTF and subordinate commanders for intelligence relating to all manner of threats posed against tactical or maneuver forces. CI conducts vulnerability assessments to look within at the command's overall security posture. CI provides threat assessments to evaluate the infrastructure, capabilities, and intentions of potential threats to the command. CI also provides commanders with assessments of the civil population within the area of operations, to include determining their response to the MAGTF presence and actions. The following provides typical examples of CI tactical support:

(a) Non-combatant Evacuation Operations. CI elements deploy to the embassy and other evacuation sites to coordinate and validate the screening of evacuees and assists at the evacuation site to ensure no one attempts to infiltrate with the evacuees.

(b) Peace Operations. CI helps identify and monitor the warring factions and possible third parties to determine potential threats to the peacekeeping/peace enforcement forces.

(c) Humanitarian and Disaster Relief. CI helps identify potential threats to the relief force, providers of aid and assistance, and aid recipients. Often the situation requiring assistance is caused by conflict and can flash with little warning.

(d) Psychological Operations. Psychological operations are normally an activity embedded within other operational activities. CI can assist in gauging the effectiveness of psychological operations and assist in special contingency planning.

(2) Due to the intelligence requirements of commanders in direct contact with adversaries and the indigenous forces, the line between CI and HUMINT at the tactical level is blurred almost beyond differentiation. Ground order of battle (GOB) intelligence is a key area of CI support and seeks to identify enemy forces, dispositions, capabilities, and vulnerabilities. In particular, the identification of threats posed against the MAGTF and the development of countermeasures are key areas CI supports. MAGTFs typically task organize CI and HUMINT elements into HUMINT exploitation teams (HET). HETs satisfy both CI and HUMINT requirements through the collection of threat information from all sources. The teams accomplish this through collection activities including CI force protection source operations (CFSO), liaison, interrogation, observation, and debriefings. Threat information in a contingency environment is highly perishable and may have limited utility to anyone other than forces in direct contact. The standard reporting vehicles are the CI Information Report and the CI SALUTE Report. In addition to this time-sensitive direct support, the MAGTF all-source fusion center (AFC) is the other key producer of tactical CI support.

2004. Garrison Support. The primary peacetime/garrison mission of CI activities is planning, preparing, and training to accomplish tactical CI functions. A secondary mission is to advise and assist commanders in the planning, coordinating, and implementing of command security and force protection efforts. See chapter 10 for additional information on garrison CI services.

CHAPTER 3

ORGANIZATION & RESPONSIBILITIES

3001. General. CI, like intelligence, supports the entire spectrum of the battlefield and all warfighting functions. Its effective integration within the intelligence effort requires a basic understanding of the national through tactical intelligence organizations. The commander, through his intelligence officer, depends on coordination and support from many organizations at all command echelons to satisfy his CI and operational requirements.

3002. Commander. *Intelligence and CI are inherent and essential command responsibilities* that require the personal involvement of the commander. Commanders at all command echelons are responsible for formulating CI plans and implementing CI measures. To do so, commanders must have a comprehensive understanding for the capabilities and limitations of CI—an understanding of concepts and theory, and an understanding of the practical capabilities, limitations and support requirements of his CI personnel, systems, procedures, operations and products. He must specify CI requirements, focus its efforts and operations, and provide any necessary guidance to ensure a timely and useful products and support. CI activities and measures help the commander shape the battlefield for a decisive action. CI measures support effective command security and force protection operations. While the intelligence officer advises on, plans and implements command CI activities, it is the commander who ultimately determines the meaning and effectiveness of the CI provided and how to use it. Additionally, the commander supervises the overall intelligence effort to ensure that the product is timely, relevant, and useful.

3003. Intelligence Officer. The commander directs the intelligence and CI effort. The intelligence officer manages these efforts for the commander, acting as the principal advisor on intelligence and CI and implementing activities that carry out the commander's responsibilities. *The intelligence officer is a full participant in the commander's decisionmaking process, ensuring that intelligence and CI are effectively used throughout the command during all phases of mission planning and execution.* His CI responsibilities parallel his basic intelligence responsibilities and include:

a. Facilitate understanding and use of CI in the planning and execution of operations.

b. Use CI support situation development and the commander's estimate of the situation through the identification of enemy capabilities, strengths, and vulnerabilities as well as opportunities and limitations presented by the environment.

c. Assist the commander in developing priority intelligence requirements and supporting CI requirements.

d. Ensure that the command's intelligence and CI requirements are received, understood, and acted on by organic and supporting intelligence assets as part of an integrated, all-source intelligence effort.

e. Supervise the integration of CI in the development and dissemination of all-source intelligence products that are tailored to the unit's mission and concept of operations.

f. Monitor the effectiveness of CI activities and the flow of intelligence and CI products throughout the command.

g. Provide necessary CI support to command security and force protection operations.

3004. Operations Officer. The operations officer is the commander's principal staff assistant in matters pertaining to organization, training and tactical operations. In addition to planning, coordinating and supervising the tactical employment of units, his principal responsibilities requiring CI support include:

a. Planning and coordinating command security (to include operations security and signal security).

b. Planning and coordinating command force protection operations.

c. Recommending missions and, with the intelligence officer, coordinating reconnaissance and counterreconnaissance operations.

d. Planning and coordinating electronic warfare and command and control warfare operations and activities (to include electronic protection and C2 protection).

3005. Individual Marines. All officers, staff noncommissioned officers, and NCOs—regardless of rank or military operations speciality—will ensure that the security of their unit is not compromised through comprehensive understanding of the unique security vulnerabilities of their operations and functions and the enforcement of necessary personnel, information, operations and electronic security measures.

3006. Marine Corps Counterintelligence Organization

a. CI within the Operating Forces

(1) CI/HUMINT Companies. Counterintelligence/HUMINT company (CI/HUMINT Co) are combat support elements organic to each Marine expeditionary forces (MEF) Headquarters Group. CI/HUMINT company is organized and equipped under the 4714 series tables of organization and equipment. As intelligence specialist teams, they are under the command of the MAGTF commander. The MAGTF commander exercises control through the Assistant Chief of Staff, G-2 to accomplish the CI/HUMINT mission. The Assistant Chief of Staff, G-2 exercises direction of the CI/HUMINT

company through the CIHO. The intelligence company commander, MEF headquarters group, exercises command, control, and supervision.

(a) Mission. The mission of the CI/HUMINT Co is to provide CI support and conduct CI and human resources intelligence (HUMINT) operations in support of the MEF, other MAGTFs, or other units as directed**.**

(b) Tasks

- Conduct tactical CI activities and operations, to include CI force protection source operations (CFSO), in support of MAGTF or Joint operations.
- Conduct screening, debriefing and interrogation of personnel of intelligence/CI interest.
- Direct and supervise intelligence activities conducted within the interrogation facility and the document and material exploitation facility.
- Perform CI and terrorism threat analysis and assist in the preparation of CI and intelligence studies, orders, estimates, and plans.
- Conduct low level source HUMINT operations.
- Collect and maintain information designed to identify, locate, and recover captured or missing personnel.
- Debrief friendly personnel recovered from EPW, hostage or detainee status.
- Translate and exploit captured documents.
- Assist in the conduct of tactical exploitation of captured material and equipment.
- Conduct limited CI investigations during combat or operations other than war.
- Conduct CI surveys and evaluations.
- Conduct TSCM operations.
- Maintain foreign area specialists who can provide sociological, economic, cultural and geo-political information about designated countries.

(c) Organization. Each MEF has one CI/HUMINT Company within the MEF headquarters group. A CI/HUMINT Company consists of a headquarters section, a CI platoon, an interrogator-translator (IT) platoon and three to five HUMINT exploitation teams (HETs). The CI platoon is organized into a platoon headquarters, four CI teams (CIT), and a Technical Surveillance Countermeasures (TSCM) team. The IT platoon is organized into a platoon headquarters and six IT teams (ITT). Figures 3-1 shows the organization of CI/HUMINT Co within I and II MEF; figure 3-2 shows the organization of III MEF's CI/HUMINT Co.

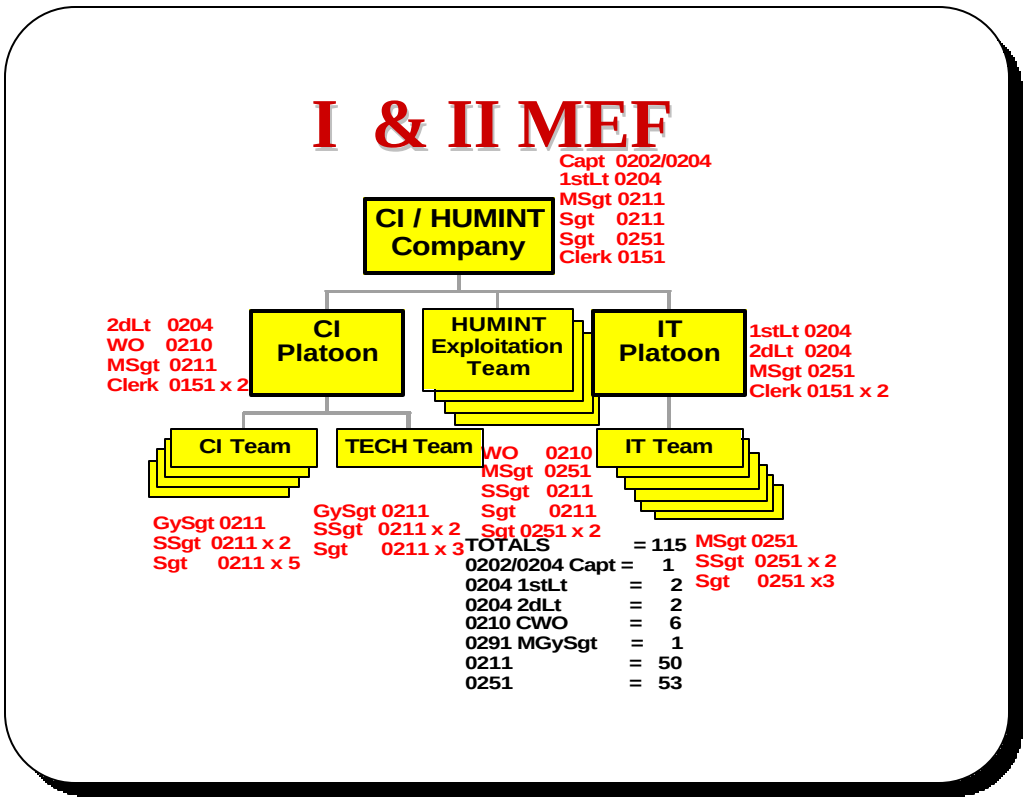


Figure 3-1. CI/HUMINT Company, I and II MEF

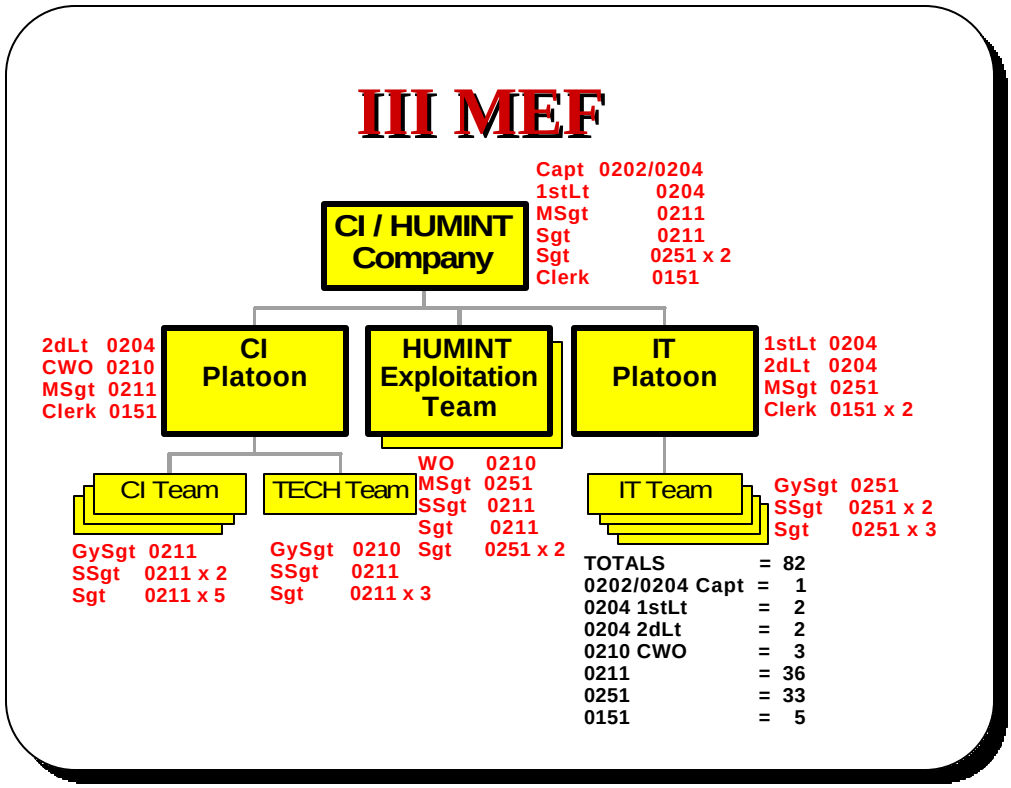


Figure 3-2. CI/HUMINT Company, III MEF

(d) Command and Control (C2) and Concept of Employment

- **Command and Control.** The CI/HUMINT Co commander exercises full command authority over his subordinate elements, less elements which have been detached under a particular task organization. The CI/HUMINT Co is under the direct operational control (OPCON) of the MAGTF commander. The MAGTF commander exercises OPCON through the MAGTF G/S-2. Tactical control or specified support relationships of CI/HUMINT elements may be provided to subordinate commanders of the MAGTF depending upon the situation. However, regardless of the MAGTF C2 and support relationships, technical control (TECHON) of all MAGTF CI/HUMINT Co elements will generally be retained by the MAGTF commander. Finally, the commanding officer, MEF headquarters group, exercises administrative control over the CI/HUMINT Co.

- **Concept of Employment.** The CI/HUMINT Co combines the MEF's CI and IT capabilities into one organization to provide unity of effort in CI and HUMINT operations and support to force protection. The company is employed in accordance with the concept of intelligence support, the CI plan, and the intelligence operations plan developed by the MAGTF G/S-2. The CI/HUMINT Co or task-organized HETs are usually employed in general support of the MAGTF. Subordinate elements of the company may be placed in general support of the MEF, placed in direct support of subordinate commands, or attached to subordinate elements. Additionally, a task-organized detachment will be provided to most subordinate MAGTFs and may be used to support joint

operations. In all cases other than GS, the degree of OPCON or TACON granted subordinate commanders over designated CI/HUMINT Co elements will be specified by the MAGTF commander.

(e) Administrative, Logistics and Other Support

- **Administrative**. CI/HUMINT Company and its subordinate units are not capable of self-administration. Administrative support is provided in by the parent MEF's Headquarters Battalion or other designated unit. Administrative support for HETs and CI/HUMINT Company detachments is provided by the supported unit.

- **Maintenance and Supply.** CI/HUMINT Company and its subordinate units are capable of first echelon maintenance support of organic equipment. All higher maintenance is provided from the parent MEF's headquarters group, other designated external units, or the supported unit.

- **Transportation.** CI/HUMINT has limited organic vehicular transportation support to support Company and subordinate units operations. External transportation support from the parent MEF's headquarters group, other designated unit or the supported unit is necessary to displace all company elements.

- **Selected Items of Equipment**[1]

TAMCN	Description	Nomenclature	Qty
A03809	Counterintelligence Equipment, Tech Surveillance		1
A0420	Comm System, Counterintelligence		8
A0890	Facsimile, Digital, Lightweight	AN/UXC-7	9
A1260	Navigation Set, Satellite (PLGR)	AN/PSN-11	25
A2030	Radio Set	AN/PRC-68A	2
A2065	Radio Set	AN/PRC-104B(V)	8
A2070	Radio Set	AN/PRC-119A	23
A2145	Radio Set	AN/VRC-46	5
A2167	Radio Set	AN/VRC-88A	20
D0850	Trailer, Cargo, 3/4-ton, 2-wheel	M-101A3	7
D1158	Truck, Utility, Cargo/Troop Carrier 1/4-ton, HMMWV	M-998	35

(2) HUMINT Exploitation Team (HET). As discussed above, HETs are part of the CI/HUMINT Co. The HET, apart from mission specific task organized elements, is the smallest element to deploy in support of a MAGTF and often serve as the basic building block for CI/HUMINT CO support to subordinate elements of the MAGTF. Specific elements and capabilities provided in the detachment will be based upon the mission of the supported unit, commander's intent, results of the

[1] T/Es for CI/HUMINT company had not been finalized by the time of publication of this manual. The items and quantities shown here were drawn from those designated for the ITP and the CITs in the T/Es for the intelligence companies as of 22 Oct 97. Refer to the current tables of equipment for accurate current information.

intelligence preparation of the battlespace, and the supported unit's concepts of operations and intelligence.

(a) Mission. HETs are used to support the MAGTF's focus of effort or other designated units, to exploit significant HUMINT or CI collection opportunities, or to provide tailored support to individual subordinate elements of the MAGTF, in particular elements which will be operating independently from the rest of the MAGTF (e.g., a HET is usually attached to the MEU(SOC) command element).

(b) Tasks

- Conduct offensive and defensive CI activities, including counterespionage, countersabotage, countersubversion, and counterterrorism, in support of tactical units.
- Conduct intelligence collection operations utilizing CFSO.
- Advise the commander concerning support to his force protection, OPSEC, deception, and security programs.
- Assist in the preparation of CI estimates and plans for areas of operations reflected by concept/operation plans.
- Maintain information and CI databases concerning personalities, organizations, installations, and incidents of CI interest in support of concept/operation plans.
- Collect and maintain information designed to identify, locate, and recover friendly personnel captured, mission (non-hostile), and missing in action.
- Conduct CI debriefings of friendly POWs who are returned to U.S. control.
- Conduct liaison with unit, JTF, other services, allied and host nation intelligence and local intelligence, CI, and law enforcement agencies as appropriate.
- Conduct CI investigations about espionage, sabotage, terrorism, subversion, and defection; and other special CI investigations, during combat operations per theater directives.
- Conduct debriefings/interrogation of known or suspected foreign intelligence personnel and agents taken prisoner.
- Maintain foreign language proficiency to support operations.

- Assist in Cl surveys/vulnerability assessments of commands and installations to determine the security measures necessary to protect against espionage, sabotage, subversion, terrorism, and unauthorized disclosure of, or access to, classified material.

- Debrief Marine Corps personnel detained/held hostage by foreign governments or terrorist organizations.

(c) Organization. HETs combine CI and IT personnel in a single unit to integrate CI and HUMINT collection capabilities in support of subordinate elements of the MAGTF. The HET normally consists of one CI officer, two CI enlisted specialists, and three enlisted interrogator/translators capable of planning and executing CI/HUMINT operations in support of the designated unit's intelligence and force protection requirements.

(d) Command and Control (C2) and Concept of Employment

- **Command and Control.** HETs are normally attached to the units they support, but may be placed in direct support. When attached they are OPCON to the supported commander, who exercises this via the unit intelligence officer. Finally, as discussed above, technical direction of HET operations generally will be retained by the MAGTF commander.

- **Concept of Employment.** HETs will be employed in accordance with the supported commander's concepts of intelligence and operations.

(3) Intelligence Section Staff Officers CI/HUMINT Responsibilities. The MAGTF G/S-2 section is the focus for MAGTF CI and HUMINT planning and management. Its principal C2 node is the command element's combat intelligence center (CIC). The CIC may consist of a number of subordinate elements depending upon the size of the MAGTF, operational requirements, and other

factors (see figure 3-3).[2]

Combat Intelligence Center (CIC) - intelligence operations center established within the MAGTF CP. Performs primary functions of the MAGTF intelligence section and includes the sub-elements listed below.

All-Source Fusion Center (AFC) - primary analysis and production element of the MAGTF. Processes and produces all-source intelligence products in response to requirements of the MAGTF.

Surveillance and Reconnaissance Center (SARC) - primary element for the supervision of MAGTF collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets.

Operations Control & Analysis Center (OCAC) - main node for the command and control of radio battalion SIGINT operations and the overall coordination of MAGTF SIGINT operations. Processes, analyzes, produces,

Figure 3-3. MAGTF G/S-2 Combat Intelligence Center and Subordinate Elements

Intelligence section and intelligence unit commanders/OICs SIGINT and related responsibilities and tasks include:

(a) Intelligence Operations Officer. The intelligence operations officer is responsible to the G/S-2 for the overall planning and execution of MAGTF all-source intelligence operations. Specific duties include:

- Planning and implementing a concept of intelligence operations based upon the mission, threat, commander's intent, and concept of operations.

- Developing, consolidating, validating and prioritizing recommended PIRs and IRs to support MAGTF planning and operations.

- Planning, developing, directing MAGTF intelligence collections, production and dissemination plans, to include the effective employment and integration of MAGTF multi-discipline intelligence, CI and reconnaissance operations.

[2] See MCWP 2-1, *Intelligence Operations*, for additional information on the CIC and its component parts.

- Coordinating and integrating MAGTF intelligence operations with other components, JTF, theater, and national intelligence operations.

- Evaluating and improving MAGTF intelligence operations.

(b) Counterintelligence/HUMINT Officer (CIHO)[3]. The CIHO is responsible to the G/S-2 (or the MAGTF intelligence operations officer) for the planning, direction and execution of MAGTF CI/HUMINT operations. Specified duties include:

- In conjunction with the intelligence operations officer, other intelligence section staff officer, the CI/HUMINT company commander, preparing MAGTF CI/HUMINT concept of operations, plans and orders; and directing, coordinating and managing organic and supporting CI/HUMINT operations.

- In conjunction with the collection management officer and CI/HUMINT Co planners, coordinating, planning, supervising, and assisting CI collection requirements and taskings for MAGTF operations.

- In coordination with the SARC OIC, CI/HUMINT Co commander, and G/S-3, coordinating the movement, operation and reporting of CI/HUMINT Co units.

- In conjunction with MAGTF AFC OIC, CI/HUMINT Co commander, coordinate MAGTF AFC analyst exchanges and production with CI/HUMINT analysts; develop CI/HUMINT reports, estimates and other products; and the integration of CI/HUMINT with all-source intelligence production.

- In coordination with the dissemination officer, planning for the timely reporting of CI/HUMINT-derived intelligence to MAGTF and external elements and the rapid handling of perishable CI/HUMINT information. This includes, in conjunction with the G/S-6 and subordinate units intelligence officers, the planning and coordination for special communications paths and operations.

- Assisting the intelligence operations officer with preparing and presenting intelligence briefings and reports as required.

- Serve as the principal point of contact between the command and NCIS in matters involving the investigation of actual, potential, or suspected espionage, sabotage, terrorism intelligence, and subversive activities, including defection, ensuring that information about these activities is reported promptly to the nearest NCIS representative. Informs the Criminal Investigation Division (CID) of the Provost Marshal Office (PMO) on criminal matters. These include those of a terrorist nature uncovered in the course of a CI investigation.

---

[3] In intelligence sections without a CIHO, a designated officer will generally be assigned to perform these tasks. If a HET or other CI/HUMINT Co element is attached, its senior CI/HUMINT officer will serve in this capacity.

- Maintain liaison with other Cl and HUMINT agencies.

- Monitor command Cl/HUMINT MOS training and provide advice and assistance for the maintenance of an effective program.

- Coordinates, on behalf of the G-2, with the G-3 for support to the command's force protection mission, including OPSEC, and deception.

- Maintain CI/HUMINT reference material for contingency planning and provides for further dissemination as appropriate.

- Conduct planning for the CI processing of friendly prisoners of war (POWs) who have been returned to friendly control.

- When a crisis action team is established in response to a terrorist or criminal situation, provide personnel to jointly man the CAT with CID, NCIS, and if required, civilian law enforcement agents.

- When the MAGTF CE is designated as a Joint Task Force headquarters, the CIHO may assume the role as the Task Force CI Coordinating Authority (TFCICA). (See Joint Pub 2-01.2, *JTTP for CI Support to Operations*.)

(c) Collection Management Officer (CMO). The CMO is responsible for formulating detailed intelligence collection requirements (ICR) and tasking and coordinating internal and external collection operations to satisfy these. The CMO receives PIRs and IRs from the intelligence operations officer, and then plans and manages the best methods to employ organic and supporting collection resources. Through coordination with the CIHO and CI/HUMINT Co commander, the CMO is responsible for the following CI/HUMINT-related tasks:

- Determination and coordination of the collection effort of PIRs/IRs that may be collected via CI resources.

- Determination of PIRs/IRs and preparation of requests for intelligence that are beyond organic capabilities and must be submitted to higher headquarters and external agencies for satisfaction.

(d) MAGTF All-Source Fusion Center OIC. The MAGTF AFC OIC has primary responsibility for managing and supervising the MAGTF's all-source intelligence processing, analytical and production. Key all-source and CI/HUMINT-related responsibilities include:

- Maintaining all-source automated intelligence databases, files, workbooks, country studies, planning imagery, mapping and topographic resources, and other references.

- Administrating, operating and maintaining intelligence processing and production systems, both GENSER and SCI (e.g., JDISS, IAS).

- Analyzing and fusing all-source intelligence into tailored products in response to stated or anticipated PIRs and IRs.

- Developing and maintaining current and future intelligence situational, threat and environmental assessment ,and target intelligence based upon all-source analysis, interpretation and integration.

- Direction and supervision of the MAGTF AFC's CI analytic team (CIAT). The CIAT normally consists of one CI officer and two CI specialists. Its principal tasks include:

  - CI analysis and integration within all-source intelligence production.

  - CI database development and management.

  - Production of CI estimates.

  - Maintenance of information on personalities, organizations, installations, and incidents of CI interest.

(e) Surveillance and Reconnaissance Center OIC. The SARC OIC is responsible for supervising the execution of the integrated organic, attached and direct support intelligence collection and reconnaissance operations. Specific CI/HUMINT-related responsibilities include:

- Maintaining the status of all ongoing intelligence collection operations, to include deployed CI/HUMINT Co elements. This status will include:

  - Mission, tasked ICRs and reporting criteria for collection elements.

  - Locations and times of all restricted fire areas and reconnaissance areas of operations.

  - C2 relationships with subordinate units, to include times of attachments.

  - Primary and alternate communications plans.

- Coordinating and monitoring organic and supporting CI/HUMINT and other intelligence elements operations.

- Conduct detailed planning and coordination with CI/HUMINT Co elements for CI/HUMINT collection. Ensure CI/HUMINT elements understand the collection plan and are able to carry out their responsibilities under the plan.

- Ensuring other MAGTF C2 nodes (e.g., the current operations center, the fire support coordination center, etc.) are apprised of ongoing intelligence, CI/HUMINT and reconnaissance operations.

- Receiving routine and time-sensitive intelligence and CI reports from deployed collection teams; cross-cueing amongst intelligence and CI collectors, as appropriate; and the rapid dissemination of intelligence and CI reports to MAGTF C2 nodes and others in accordance with intelligence reporting criteria.

(f) Dissemination Officer. The dissemination officer is responsible for the effective conduct of intelligence dissemination within the MAGTF. Specific CI/HUMINT-related responsibilities include:

- Developing intelligence dissemination operational plans and supporting architectures for both voice and data networked communications, and coordinating and integrating these with theater, joint force and MAGTF CIS and intelligence systems.

- Recommending intelligence dissemination priorities.

- Advising on and selecting dissemination means.

- Monitoring the flow of intelligence and CI throughout the MAGTF, ensuring that it is delivered to intended recipients in a timely fashion.

(4) Liaison

(a) CI requires extensive liaison to be effective during tactical operations. CI activities often closely parallel functions and responsibilities of other organizations and agencies and, in some cases, may overlap. Close and continuous liaison and coordination aids in the effectiveness of operations, the exchange of information, and in providing for mutual assistance.

(b) Policies and procedures for liaison and the coordination of CI activities are developed and promulgated at the MARFOR/MAGTF command echelons. Depending on the mission, area of operations and the type of CI activity, liaison and coordination is normally conducted by CI elements with local intelligence, CI, security and law enforcement organizations/agencies, and civil affairs and psychological operations units where appropriate. In all cases, liaison must be conducted within jurisdictional limitations imposed by higher authority.

b. Marine Corps CI Organizations within the Supporting Establishment. The Director of Intelligence is responsible to the Commandant of the Marine Corps for forming plans and policies pertaining to intelligence and CI within the Marine Corps. The Head, Cl/HUMINT Branch is the principal advisor to the Director of Intelligence for Cl/HUMINT matters. The Cl/HUMINT Branch performs the following functions:

(1) Prepares plans, policies, and directives, and formulates controlled CI/HUMINT missions.

(2) Coordinates with national-level Department of Defense (DOD) and non-DOD agencies on matters dealing with Cl and HUMINT.

(3) Acts as the CI military occupational specialty (MOS) sponsor (0204/0210/0211).

(4) Maintains staff cognizance over CI field units and staff management of training.

(5) Exercises staff responsibility for HUMINT resources and certain classified/special access programs.

(6) Coordinates with the NCIS in special investigations and operations.

(7) Conducts security reviews.

(8) Reviews reports from the field commands concerning security violations, loss of classified material, and compromises.

(9) Coordinates the release of information for foreign disclosure.

(10) Represents the Marine Corps on national level interagency CI committees and subcommittees.

3007. Naval Component Organization.

a. N-2 Intelligence Officer. While afloat, the N-2 coordinates activities of the attached NCIS agent to identify threats to the amphibious ready group (ARG). The N-2 coordinates vulnerability/threat assessments and other intelligence and CI support of ARG intelligence and force protection requirements for the ships. Close coordination between the MAGTF G/S-2 and the N-2 is required to ensure consolidation and dissemination of applicable threat related data for the formulation of the commander's estimate. Monitoring and rapid reporting of time sensitive information is critical for these deployed commanders as the situation develops. The critical role is the monitoring for indications and warning of impending attack during movement or the deployment of forces ashore. The ARG/MAGTF team continues this interactive relationship through the rapid collection, processing, production and dissemination of intelligence and CI in support of intelligence and force protection requirements.

b. Attached NCIS Agent. In conjunction with MAGTF CIHO and other CI elements, the NCIS agent afloat assists the command with the identification of threat and vulnerabilities of the ARG. As a special staff officer under the staff cognizance of N-2, the NCIS agent also has the responsibility for criminal investigation in conjunction with the ship's master-at-arms and the MAGTF criminal investigation division (CID) officer. During contingency operations, the NCIS agent serves as the principal planner and host for NCIS's surge capability via its Special Contingency Group (SCG). The SCG is a task organized group of specially trained NCIS agents prepared and equipped for deployment into tactical situations short of combat.

3008. Joint Counterintelligence Organization

a. CI Staff Officer (CISO). In accordance with DOD Dir 5240.10, *DOD CI Support to U&S Commands*, each combatant command has a special staff officer within the J-2 with staff cognizance for all CI activities within the theater. The CISO is the J-2's primary staff officer responsible for advising, planning and overseeing theater CI activities. Responsibilities include:

(1) Advise commander & J-2 on CI investigations, operations, collections and production activities affecting the command.

(2) Advise commander on counterdrug, OPSEC, counterterrorism and antiterrorism activities in the commands AOR.

(3) Coordinate CI support activities within combatant command's headquarters staff and with component organizations.

(4) Coordinate the combatant commander's CI requirements with pertinent U. S. CI organizations and U. S. country teams as required.

(5) Coordinate tasking of CI within AOR and area of interest upon implementation of NCA approved /directed action.

(6) Coordinate with the military services for integrated CI support to research and development and acquisition programs to protect sensitive or critical technologies.

(7) Ensure significant CI threat information developed within commander's AOR is forwarded to the J-2, other staff officers, and subordinate component commanders.

(8) Ensure CI support requirements are identified and satisfied during development of command intelligence architecture plans (CIAP).

(9) Ensure CI staffing and analytic and production support is integrated the combatant command's joint intelligence centers (JICs).

(10) Ensure CI collection, production and dissemination priorities are integrated into command's intelligence operations plans.

b. Task Force CI Coordinating Authority (TFCICA). The TFCICA is a JTF headquarters staff officer designated by the combatant commander as the executive agent for all CI activities within a JTF's area of responsibility (AOR). The TFCICA coordinates and deconflicts with the Defense HUMINT Service's representative to the JTF and the HUMINT Operations Cell (HOC). Together these two staff responsibilities combine to create the JTF headquarters J-2X, which has the task of coordinating and deconflicting all CI and HUMINT activity within the JTF AOR. This includes coordination with the U. S. country team and any external attachments and agencies conducting CI and HUMINT activity within the AOR.

3009. National Level Counterintelligence Support. The Defense Intelligence Agency (DIA) is critical in the planning and establishment of military CI activities. DIA is the principal DOD organization for CI analysis and production in support of DOD requirements. It focuses on hostile threat and foreign intelligence and security services, to include the development, population and maintenance of CI databases for personalities, organizations and installations (PO&I). PO&I files become the cornerstone of the CI activities planning and targeting, and guide all CI and HUMINT activities. DIA's Defense HUMINT Service (DHS) is the force provider for strategic HUMINT forces and capabilities. During operations, elements from DHS form a partnership within the supported JTF headquarter's J-2X element for the coordination and deconfliction of all HUMINT-source related collection activities.

CHAPTER 4

COUNTERINTELLIGENCE EMPLOYMENT

4001. Operational Environment. As forces are committed to an operation, the threat picture expands and situational awareness improves. As U. S. military involvement increases, existing threats remain and may increase while new threats may emerge. In a humanitarian operations and other military operations other than war (MOOTW), the criminal, terrorist, and espionage threats are generally the principal ones facing the MAGTF. These threats continue into the upper levels of conflict, with the addition of threats posed by irregular forces, special operations force, and finally, by large-scale conventional military forces.

Within MOOTW and in lesser levels of conflict where there may be no designated MAGTF or joint rear area, CI activities are directed at supporting force protection efforts by engaging with key civic leaders, existing intelligence and security structure, factional leaders and cooperative personnel, and allied forces. Threats are normally at the low to mid level. Threats at the higher levels of conflict normally involve conventional or unconventional force threats that require combat forces to counter. MAGTF CI elements conducts actions in support of these operations within the MAGTF area of operations and other assigned sectors as directed (e.g., the joint rear area (JRA)).

The primary operational environmental factor influencing MAGTF CI activities is political, vice physical. Accordingly, three basic political operational categories can be used to frame CI activities. These are:

- Permissive Environment -- An operational environment in which there are specific agreements that allow CI to conduct activities independently or in coordination with the host nation. In these environments, MAGTF CI activities and support to the security posture of the deployed forces are normally conducted in conjunction with the host nation, or the host nations has provided concurrence, either direct or tacit.

- Semi-Permissive Environment -- A operational environment in which there are either no in-place government organizations and/or laws, or where the government in power is not duly recognized by the U. S. or other international bodies. In situations of this type, the rules of engagement established by the JTF or multinational force commander is often the key variable as the host nation's civil, military and security agencies are frequently degraded or nonexistent (or may even be supporting threat forces). The rules of engagement of the deploying force primarily drive limitations and restrictions that may be placed on CI activities.

- Non-Permissive -- A non-permissive operational environment is one in which U. S. CI activities and contacts with the host nation are extremely limited, normally at the direction of the host nation. The situation in these countries may also place the US in a situation where the actions of the host nation or individuals in the host nation government may be inimical to those of the US government. In

most cases, the host government may severely curtail contacts, normally only through a single point of contact. In some cases, the information provided may be of questionable validity.

MAGTF CI personnel must be aware of the differences in each operational environment and be able to establish operations based on the mission, nature of the environment and threat conditions. Since much of the threat and vulnerability intelligence will be based on information provided by host nation or other sources, vulnerability assessments must be assessed and rapidly updated as necessary.

CI activities MAGTF commanders develop estimates of the situation, shape the battlefield and guide intelligence and force protection operations. The MAGTF commander focuses the CI effort by clearly identifying priority intelligence requirements, careful assignment of CI missions and tasks, and a clear statement of desired results. By orienting CI capabilities, the commander guides who or what are the CI targets and the nature and focus of operations (e.g., whether CI efforts will be designated primarily as defensive CI operations or offensive HUMINT operations).

4002. Employment of Counterintelligence Elements

a. Command and Control (C2) and Concept of Operations. The tactical concept of operations in depth governs C2 relationships and the execution of CI plans and operations. Specific CI concept of operations and C2 relationships will be established in either annex B (intelligence) to the operations order, fragmentary orders or other directive.

(1) General Support. CI elements normally operate in general support of the MAGTF. Operational control of CI elements by the force commander provides the commander with the means to meet the specific operational requirements of the entire MAGTF and other supported forces with his generally limited organic CI resources.

(2) Direct Support and Attachment. Situational and operational factors may require some CI elements to be either attached to or placed in direct support of MAGTF subordinate elements (e.g., during operations involving widely separated units in areas of dense population). Unit commanders employ CI personnel to satisfy their CI requirements or other mission specified by the MAGTF commander.

(3) Technical Direction. Regardless of the type C2 relationships established, the MAGTF commander will always retain technical direction authority over all MAGTF CI and supporting elements, which will be exercised by the G/S-2 via the CIHO.

b. Concept of Employment. MAGTF CI elements can be deployed on an area coverage concept or by unit assignment.

(1) Area Coverage

(a) Geographic Area of Responsibility. MAGTF CI elements employed under area coverage are assigned a specific geographic area of responsibility, under the operational control of the MAGTF commander. Under area coverage, CI support is provided to all commands located within the designated area. Such CI element continue to operate within the assigned area even though the tactical situation or supported units operating in the area may change.

(b) Continuity. Area coverage provides the greatest continuity of tactical CI operations. It allows MAGTF CI operations to focus on the enemy's intelligence organization and activities while remaining unfragmented and unrestricted by the tactical areas of responsibility assigned to supported units. It also allows MAGTF CI personnel to become familiar with the area, enemy intelligence organization and operations, and CI targets. Area coverage is particularly effective during MOOTW (e.g., counterinsurgency operations) where the threat forces often operate on political, vice military, boundaries.

(2) Unit Assignment. MAGTF CI elements employed on a unit assignment basis normally remain with designated supported units. They operate within that unit's area of responsibility under the specified C2 relationships. As tactical units displace, it is necessary for higher echelons to provide CI coverage for the areas vacated. Relief of an area can be accomplished by three methods - augmentation, leapfrog system, and relay system.

(a) Attachment. CI elements may be detached from the MAGTF CE and attached to subordinate commanders. This method provides CI support under the operational control of the commanders to which attached for employment against specific CI targets during the initial (and possibly subsequent) phase of an operation. It also prepares for subsequent transfer of areas of responsibility from subordinate units to MAGTF CE without loss of continuity. These CI elements generally operate under the operational control of the supported commander during the initial reduction of CI targets. The CI elements then remain in place as the unit advances, reverting to the operational control of the MAGTF commander (or other specified commander). By remaining in place, the CI element ensures continuous coverage regardless of tactical unit movements.

(b) Leapfrog System. This method is similar to the area coverage concept but on a smaller scale. Under the leapfrog system, MAGTF CI elements initially responsible for a specified area are detached from subordinate units and a new team attached as the operation progresses. The new CI element is attached sufficiently in advance to permit it to become thoroughly familiar with current operations within the area of responsibility. This method of relief permits the CI element familiar with the area, informants, and targets to remain and conduct more extensive operations, while continuing to provide necessary CI direct support to subordinate commanders.

(c) Relay System. This method requires MAGTF CI elements to be held in reserve. As the subordinate units advance, CI elements are dispatched forward to assume control of designated areas on a rotational basis.

c. CI Employment Considerations

(1) Characteristics of the AOR influence the nature and extent of MAGTF CI operations. The following factors influence CI task organization, C2 and resulting concepts of operations and support relationships.

- Historical/recent threat, espionage, sabotage, subversion or terrorism activities within the area of operations
- The population density.
- The cultural level of the country.
- The attitude of the people and political groups toward friendly and enemy forces.
- The people's susceptibility to enemy penetration (hostile intelligence threat) and propaganda.
- The stability of the local government, security and law enforcement.

(2) The number of MAGTF CI resources available, particularly HETs, is critical. Careful planning, awareness of CI operations throughout the joint AOR, and detailed intelligence and operations preparation are required. CI targets which require early reduction must be selected and the employment of MAGTF CI operations planned. Care must be taken to not overestimate CI element capabilities—this risks overextending and dispersing CI activity on many targets with limited effectiveness.

(3) During amphibious operations, the commander, landing force (CLF), assumes operational control over all assigned CI assets. Clear responsibility for CI operations must be assigned amongst MAGTF, naval and other supporting CI elements. CI investigations of a general support nature, particularly in rear areas, may be tasked to NCIS or other supporting CI elements. In such cases, jurisdiction must be clearly defined to optimize overall CI support.

d. Employment of MAGTF CE CI Elements

(1) MAGTF CE CI elements normally operate in the rear area conducting the following tasks:

- Overall MAGTF CI operational management and technical direction.
- Coordination and integration of MAGTF CI operations with JTF, multinational and other supporting CI operations.
- Conduct CFSO and HUMINT operations of a relatively long term nature.

- Provide assistance on military and civil security matters.

- Follow-up and complete CI tasks initiated by subordinate elements.

(2) MAGTF CE CI elements normally retain OPCON over technical surveillance countermeasures, CI inspections, and CI surveys for the entire MAGTF. If required, it also establishes and operates the MAGTF CI interrogation center.

e. Employment of CI Elements with the Ground Combat Element (GCE)

(1) Generally, the number of MAGTF CI elements employed in the GCE AOR is greater than in other areas. In combat or occupied areas, the enemy has more opportunities to penetrate the CI screen because of the constant contact of opposing ground forces and the presence of indigenous displaced populations. After the area has been cleared of the enemy, the CI element operating with the GCE is usually the first security unit to enter this area. They help determine initial requirements and establish initial security measures. Additionally, CI element with the GCE perform critical preparatory tasks for all subsequent CI and security operations. Prompt action by a CI element, particularly the rapid development and dissemination of intelligence based upon interrogations or exploitation of captured materials and documents, can be of substantial benefit to the GCE's operations and force protection efforts. CI elements must identify and secure :

- The most obvious CI targets.

- Agents left behind by the enemy for espionage and sabotage.

- Enemy collaborators.

- Key public buildings such as the seat of the local government, police stations and communication centers.

(2) The CI element focuses its operations on the GCE's distant and close areas, with responsibility for GCE rear area generally being coordinated with CI elements operating in general support of the MAGTF or those in direct support of the rear area operations commander. The CI elements operating with a division are generally deployed by task organizing multiple HETs. The HETs are responsible for the CI coverage of specific areas within the jurisdiction of the command. Each HET acts as an independent unit, but its activities are coordinated by the CI/HUMINT Company Commander or by one of the HET OICs.

(3) Time is of the essence during the assault phase of an operation. CI elements employed with attacking forces will generally limit their screening operation to identification and classification of civilians disguised as military personnel, enemy agents, and collaborators. If time permits, immediate tactical interrogation may be conducted of suspects. Normally, suspects will be passed to rear area,

intermediate detention facilities, ultimately arriving at the Joint Interrogation and Debriefing Center for more detailed interrogations and classification.

f. Employment of CI with the Aviation Combat Element (ACE)

(1) There is no significant difference in the mission of CI elements employed with either ground or air units. However, air units are normally characterized by a static situation. In air operations or an airborne movement, CI personnel are included in the tactical command echelon. They advise the commander on the control and security of sensitive areas, civilian control measures, and screening of local residents and transients. They also conduct security assessments of facilities in the vicinity as required.

(2) The ACE is often widely dispersed with elements operating from separate airfields. Since aircraft and support equipment are highly susceptible to damage and difficult to replace, aviation units are high priority targets for enemy saboteurs and terrorists. In many situations, ACE units employ large numbers of indigenous personnel in support roles, personnel who are a key target of enemy intelligence activities. Under such conditions, it may be necessary to provide HETs in direct support of ACE elements.

g. CI Support to the Combat Service Support Element (CSSE) and Rear Area Operations

(1) Within rear areas, the MAGTF CSSE (along with other MSE elements) is the principal organizations requiring CI support. While the CSSE's CI requirements are primarily concerned with military security, those of civil affairs elements generally deal with civil/military interaction and security of the populace. Despite the apparent differences of interest between their requirements, their CI problems are interrelated (e.g., a dissident civilian population hampering the efforts of MAGTF civil affairs elements attempting to establish effective administrative control in the area also disrupting logistics operations through sabotage, terrorism, and harassment attacks).

(2) MAGTF CE CI elements performing general support CI operations normally provide CI support to CSSE and other rear area operation elements. This includes support for installations and facilities dispersed through the combat service support areas. The number of team personnel supporting civil affairs units depends on the number of refugees to be identified in the area.

4003. Friendly Prisoners of War and Persons Missing (Non-hostile) and Missing in Action

a. Friendly personnel who are captured by the enemy can be a source of information through the compromise of documents, personal papers, or as the result of effective interrogation or coercion. It is a fundamental commander responsibility to take necessary steps to counter any possible disclosure that would affect the immediate tactical situation.

CI units are assigned responsibility for investigating and determining risks posed to MAGTF operations by friendly personnel who have or may have been captured, collecting information of

potential intelligence value on friendly personnel who may be under enemy control. They also collect intelligence information to aid in identifying, locating, and recovering captured friendly personnel. In addition, CI personnel conduct the intelligence and CI debriefings of friendly personnel who had been captured and then returned to friendly control.

b. When friendly personnel have been or may have been captured, the identifying commander will immediately notify their unit intelligence officer, who will then coordinate with the pertinent CI element to initiate the CI investigative process (see appendix E). The CI unit may be able to immediately provide information that could aid in the search and recovery efforts, such as routes to enemy detention centers, locations of possible holding areas, and enemy procedures for handling and evacuating prisoners. If appropriate, the CI element can also initiate immediate CI collection action, such as using CI sources to gain information for possible recovery or search and rescue operations.

c. If the search or recovery attempts are unsuccessful, the CI unit initiates an immediate investigation to gather basic identification data and to determine the circumstances surrounding the incident. The investigation is designed to:

(1) Provide information to aid in subsequently identifying and locating the individual.

(2) Assess the potential intelligence value to the enemy.

(3) Collect intelligence information that will be of value when evaluating future intelligence reports.

The investigation must be as thorough and detailed as possible and classified according to content. Every attempt is made to obtain recent photographs and handwriting samples of the captured Marine. A synopsis of the investigation, including a summary of the circumstances, is prepared on the CI report form. The completed basic identifying data form is attached as an enclosure to this report.

In the case of aircraft incidents, the investigation includes type of aircraft, location and sensitivity of classified equipment, bureau or registration number, call signs, and any aircraft distinguishing marks, such as insignia, etc. When feasible, the investigator should coordinate with the accident investigation team or aviation safety officer of the unit that experienced the loss.

d. The CI report, with the attached personnel data form, is distributed to the following commands:

(1) MAGTF CE.

(2) Individual's parent command (division, MAW, or Force Service Support Group (FSSG)).

(3) Each CI element in the AOR.

(4) Other appropriate headquarters (e.g., combatant commander, MARFOR headquarters, etc.).

(5) Commandant of the Marine Corps (Code C4I-CIC).

e. These reports are designed to aid follow-on CI operations. They do not replace normal G/S-1 casualty reporting procedures. When the CI report concerns a member of another Service assigned to a Marine Corps unit, a copy of the report is also provided to the appropriate component commander and Service headquarters. All subsequent pertinent information is distributed in the same manner as the initial CI report.

f. MAGTF personnel returned to friendly control after being detained by the enemy are debriefed by CI personnel. Normally, CI personnel supporting the unit that first gains custody of the individual conduct an initial debriefing to identify information of immediate tactical value and the locations of other friendly prisoners of war. As soon as possible, the returnee is evacuated to the MAGTF CE for further debriefing and subsequent evacuation to a formal debriefing site.

4004. Counterintelligence Support during Military Operations Other Than War (MOOTW). The CI operations previously discussed are generally applicable across the MOOTW, including non-combatant evacuation, peace, and humanitarian and disaster relief operations. CI activities during MOOTW require CI personnel to be thoroughly familiar with the nature of operation, to include its causes, characteristics, and peculiarities, and with the threat infrastructure directing and controlling efforts. Basic CI tasks are the denial of information to the threat force and the identification and neutralization of intelligence operations. A key aim of MOOTW is to restore internal security in the AOR, which requires a vigorous and highly coordinated CI effort. The nature of operation and the threat's covert methods of operation require the employment of a greater number of CI personnel than is generally required for conventional operations.

a. Jurisdiction. Effective CI operations require extensive coordination with the host country intelligence, CI, security, and law enforcement agencies. In such operations, MAGTF operations are normally covered by a status of forces agreement (SOFA). The SOFA may include limitations and restrictions concerning the investigation and apprehension of host country citizens or other operations matters.

b. MAGTF CI Employment

(1) The employment of CI elements during MOOTW is similar to that previously described. CI area coverage is generally used as it provides continuity of operations. Also, as the threat's intelligence operations usually have been are well established, area coverage allows MAGTF CI personnel to better understand and more effectively counter the threat.

(2) When assigning areas of responsibility, MAGTF CI elements ensure coverage overlaps to preclude gaps occurring between areas. Threat forces usually prefer to operate on the political or military boundaries where the assigned responsibilities of U.S. and allied forces may be vague and coordination is more difficult. CI elements employed through unit assignment are assigned responsibility

for the area of interest around specified unit's area of responsibility. Under the unit assignment concept, rear area CI elements assume responsibility for any gap in coverage that may develop.

c. Counterintelligence Measures and Operations

(1) The basic CI operations, techniques, and procedures previously are generally applicable during MOOTW. However, such operations generally require that both passive and active CI measures be increased and aggressively pursued to effectively counter the threat's advantages and capabilities.

(2) All MAGTF units must institute and continuously enforce CI and security measures to deny information to the threat force and to protect friendly units from sabotage. In coordination with host country authorities, emphasis is needed on security measures and checks of indigenous employees or other persons with access to MAGTF installations, facilities or command posts.

(3) A significant factor during MOOTW is population and resources control. The movement channels and patterns necessary for support, communications, and operations of insurgent forces are observed and controlled. Prior to implementing control measures, the population should be informed of the reasons for controls. Whenever possible, such controls should be performed and enforced by host country agencies.

(4) MAGTF CI elements must implement imaginative and highly aggressive special CI operations and HUMINT collection programs targeted against the threat's intelligence infrastructure and operational forces. The primary objective of special operations is the identification, location, and neutralization of specific members of the threat's infrastructure. A CI special operation consists of systematic intelligence collection and analysis with complete documentation concerning the activities of each targeted individual. This provides the host country with an account of the individual's illegal activities once the person is apprehended. Penetration of the infrastructure must be obtained at all levels possible—HUMINT operations are implemented to cover critical areas to identify and locate threat forces. Intelligence derived from HUMINT programs may also be useful in CI special operations.

(5) In MOOTW, cordon and search operations may be employed to ferret out the threat infrastructure. Ideally, a cadre of MAGTF CI personnel are assigned to each unit conducting the cordon and search operation in order to provide on scene exploitation and immediate reporting of threat related time-sensitive intelligence. These operations may also be employed to ferret out individual threat units that may use a community or area as cover for their activities or as a support base. Cordon and search operations should be conducted in conjunction with host country forces and organizations, with U. S. forces including CI units providing support, advice, and assistance for the entire operation. At a minimum, host country personnel should be part of the screening and sweep elements of any cordon and search operation. Sweep/screening is often conducted in conjunction with medical, civil affairs, and psychological operations programs (which are accomplished after the screening phase). Throughout the operation, care must be exercised to prevent an adverse psychological effect on the populace.

More details concerning the intelligence and CI applications of cordon and search operations are contained in Army FM 30-64A, CI Operations. Cordon and search operation basically consists of:

- Security forces which surround the area, usually at night, to prevent persons from leaving the area.
- A sweep element that escorts detained people to a collection point at first opportunity.
- Search elements that conduct detailed en-mass searches of the area.
- Screening elements to process and screen detainees for identification of known or suspected threat personnel.

CHAPTER 5

COMMUNICATIONS & INFORMATION SYSTEMS SUPPORT TO COUNTERINTELLIGENCE OPERATIONS[1]

5001. General. The MAGTF CI effort is heavily dependent upon a secure, reliable, and fast communication and information systems (CIS) support to receive JTF, other components, theater, and national CI and all-source intelligence and to transmit organically collected and produced CI product and reports. CIS are also required for the command and control of MAGTF and supporting CI units and their integration with multi-discipline intelligence operations. Every mission and situation is unique, requiring some modifications to the supporting CIS architecture to support MAGTF CI operations. Detailed planning and close coordination between the CI/HUMINT company/detachment CO/OICs, the MAGTF G/S-2 and G/S-6, and all pertinent operational and intelligence organizations is critical for establishing a reliable and effective CI CIS support.

5002. Basic CI CIS Requirements. Regardless of the size of the MAGTF CI/HUMINT forces, there are certain standing CI CIS requirements must be satisfied. These requirements are:

a. The capability to command and control subordinate units. Intelligence officers and CI/HUMINT element commanders/OICs must be capable of positive C2 of subordinate units and integration of its operations with broader MAGTF and external intelligence and operations C2. Traditionally single-channel radio (SCR) and record message traffic have been used to support C2 of MAGTF CI units. In semi-static situations, secure e-mail or telephone may be the method of choice, while in highly fluid or mobile scenarios, cellular, SATCOM, and VHF and HF radio may be used.

b. The ability to receive collected data and information from deployed CI elements. The CIS architecture must provide connectivity between organic and supporting CI/HUMINT elements (such as the HUMINT exploitation teams or CI liaison elements), CI analysis and production centers, and supported MAGTF operations and intelligence centers. Requirements include the capability to transmit collection files and reports digitally via fiber-optics, wire, or radio in formats (both voice and data) that are readily useable by the CI and all-source intelligence analysts.

c. The ability to provide intelligence to supported commanders. CI CIS requirements will be influenced by supported commanders' intents, concepts of operations and intelligence, command relationships, and standing PIRs and IRs. The CIS architecture must be capable of integrating CI/HUMINT element C2 and supporting CIS operations (to include special communications capabilities and channels unique to CI reporting) with the primary CIS channels used to by supported commanders.

---

[1] See MCWP 6-22, *Communications and Information Systems*, for a detailed review of MAGTF communications and information systems (CIS) and supporting tactics, techniques and procedures.

d. The ability to share CI products and reports with MAGTF all-source intelligence centers and with CI and all-source JTF, other components, theater, and national CI and intelligence centers. The traditional means for providing this capability are MAGTF general service secure record and voice communications. While these techniques continue to be used, they are rapidly becoming secondary in importance to the use of the Joint Worldwide Intelligence Communication System (JWICS), the Secret Internet Protocol Router Network (SIPRNET), and other CI unique CIS capabilities which allow participants to access each others CI products and databases and to immediately pull required data, intelligence and CI products.

5003. Command and Control

a. JTF. The joint force commander has operational control of all JTF CI elements. He exercises this authority via the JTF intelligence officer (J-2). Within the J-2, CI activities fall under the functional control of the Task Force CI Coordinating Authority (TFCICA) within the intelligence section's J-2X. All CI collection operations management, CI production and CI dissemination tasks are exercised by the TFCICA, to include source deconfliction with the Central Source Registry, reporting coordination and resource application. Other functional managers, such as the Defense HUMINT Service representative within the J-2X or the HUMINT Operations Cell (HOC), have direct tasking authority over their functional assets, requiring close coordination and planning amongst all to ensure effective JTF CI/HUMINT operations.

b. MAGTF

(1) The MAGTF commander has operational control of all MAGTF CI elements. He exercises this authority via the MAGTF intelligence officer. The intelligence officer's principal staff assistant responsible for planning, directing and managing organic and supporting CI operations is the Counterintelligence/HUMINT Officer (CIHO). At the CI unit level, the CI/HUMINT company commander/detachment OIC has command and operational control. Regardless of the C2 relationships and MAGTF CI concept of employment, technical control of all MAGTF CI/HUMINT company elements will generally be retained by the MAGTF commander.

(2) The following are the principal C2 nodes from which MAGTF CI operations are planned and directed:

(a) <u>MAGTF Command Element Combat Intelligence Center (G/S-2)</u>. CI elements are integrated within two key elements of the MAGTF CE combat intelligence center (CIC): the surveillance and reconnaissance center (SARC) and the all-source fusion center (AFC). Additionally, the MAGTF CIHO will integrate CI operations with those of the intelligence operations officer. The SARC is the primary element for the supervision of MAGTF collection operations and is responsible for the direction, coordination, and monitoring of intelligence collection operations conducted by organic, attached, and direct support collection assets. A CI/HUMINT element will be established within the SARC to monitor ongoing operations and to maintain designated CI radio nets. The AFC is the primary analysis and production element of the MAGTF, responsible for processing and producing

all-source intelligence products in response to MAGTF requirements. Various CI and interrogator-translator personnel are permanently assigned to the AFC to assist with its operations. Besides the CI nets established within the SARC, CI/HUMINT elements working within the CIC will have access to and use the full range of CIC CIS resources.

(b) CI/HUMINT Company HQ. Specialized CI and interrogator-translator platoons elements as well as task-organized HETs generally will be employed throughout the MAGTF. The CI/HUMINT company commander exercises full command authority over his subordinate elements, less elements which have been detached under a particular task organization. To support his operations, a CI/HUMINT company command posts generally will be established in the vicinity of the MAGTF CIC and using the full range of CIS supporting the CIC.

(c) Deployed CI/HUMINT Elements. CI/HUMINT elements will generally be deployed at many echelons and locations within the MAGTF. For example, significant elements may be either attached to or placed in direct support of GCE forces or the rear area operations commander. Likewise, CI/HUMINT elements may be employed at the MAGTF enemy prisoner of war (EPW) compound and other EPW collection points. The CIS used by these CI elements will be dependent upon the situation. Generally these elements will provide CIS resources to satisfy their organic C2 needs, while using the supported headquarter's CIS resources for broader requirements.

5004. CIS Support to MAGTF CI Operations

a. General. The CI CIS architecture for any given operation is dynamic. Key reference documentation with respect to a specific theater or MAGTF operation are:

(1) Combatant command, JTF and MAGTF CI/HUMINT plans developed for various OPLANs.

(2) MAGTF command element intelligence standing operating procedures and combatant commanders intelligence and CI/HUMINT tactics, techniques and procedures.

(3) Annexes B (intelligence), C (operations), J (command relationships), and K (communications and information systems) of the MAGTF and JTF OPORDs.

(4) The following parts of Annex B (Intelligence) to a MAGTF OPORD: Appendix 3 (Counterintelligence Operations); appendix 5 (Human Resources Intelligence Operations); and tab D (Intelligence Communications and Information Systems Plan) to appendix 10 (Intelligence Operations Plan).

b. Communications Systems. Information systems and supporting communications connectivity are evolving rapidly within the Marine Corps and other elements of the military. The following information provides typical key MAGTF CI communications requirements. The MAGTF mission, the nature of the threat, friendly concepts of operations and intelligence, supporting task organization and

command relationships, and extent of allied/multinational operations are the key factors influencing what specific CI communications are established during operations.

(1) Intelligence and CI/HUMINT Radio Nets. The following are radio nets typically established for either dedicated CI needs or are intelligence nets that CI elements may need to be stations on:

(a) MAGTF Intelligence (UHF-SATCOM/HF/VHF). Used for rapid reporting and dissemination of intelligence, collaborative planning of future MAGTF intelligence operations, and command and control of ongoing MAGTF intelligence and reconnaissance operations. Typical organizations/elements participating in this net include: the MAGTF CE; the GCE/ACE/CSSE headquarters; intelligence, CI and reconnaissance elements either attached to, OPCON to or supporting the MAGTF; and others as directed.

(b) GCE/ACE/CSSE Intelligence (HF/VHF). Used to provide rapid reporting and dissemination of intelligence, collaborative planning of future intelligence operations, and command and control of ongoing intelligence and reconnaissance operations. Typical organizations/elements participating in this net include: the GCE/ACE/CSSE headquarters; headquarters of their major subordinate units; intelligence, CI and reconnaissance elements either attached to, OPCON to or supporting the a MSE headquarters; and others as directed..

(c) Counterintelligence/Human Intelligence (HUMINT) Team(s) Command (HF/VHF). Used for command and control of counterintelligence teams, interrogator-translator teams, and HUMINT exploitation teams (HET) operations, and the coordination of counterintelligence/HUMINT administrative and logistic support. This net will also generally terminate in the MAGTF surveillance and reconnaissance center (SARC).

(d) Counterintelligence/HUMINT Reporting Net (VHF/HF). Used as a means for the rapid reporting of counterintelligence/HUMINT data to supported units. Participants generally include counterintelligence teams, interrogator-translator teams, and HET operations, the SARC, and the intelligence center of any supported units.

(2) CI/HUMINT Communications Equipment. CI elements require extensive communications support from the command to which they are attached. The command is responsible to provide frequency management, cryptographic materials system (CMS) control, and logistics support (e.g., batteries and maintenance). These requirements include secure dedicated and shared systems connectivity and are situationally dependent based upon employment method, terrain, distance and other factors. CI elements usually deploy with the following organic communications and information systems:

- SINGARS radios -- primarily to support CI element C2 and intelligence reporting.

- Motorola SABER radios -- principally to support internal CI element communications of an operational nature (e.g., surveillance or security).

c. Intelligence and CI/HUMINT Information Systems. The following are information systems and selected databases typically established for either dedicated CI needs or are multi-purpose intelligence systems that CI elements may either use or must interoperate with.

(1) Joint Deployable Intelligence Support System (JDISS). JDISS is an all-source automated intelligence tool that provides the backbone of intelligence connectivity amongst the national, theater, JTF headquarters, component commanders, and other intelligence organizations. JDISS employs a transportable workstation and communications suite that electronically extends a joint intelligence center to a JTF and other tactical users. Either SIPRNET or JWICS will provide the principal communications connectivity for JDISS.

(2) Intelligence Analysis System (IAS). IAS provides automated applications and other tools for all-source intelligence planning, management, analysis, production and dissemination. Various configurations of IAS will be organic to intelligence sections from the battalion/squadron through MAGTF CE levels.

(3) Defense Counterintelligence Information System (DCIIS). DCIIS is a DOD system which automates and standardizes CI functions at all command echelons. DCIIS contains standardized DOD forms (for CI investigations, collections, operations, and analysis & production) and shared CI databases. DCIIS also contains supplemental forms to satisfy tactical reporting requirements of Marine and Army CI elements. DCIIS is interoperable with JDISS and other intelligence systems. Communications connectivity is via SIPRNET.

(4) Defense Intelligence Threat Data System (DITDS). DITDS is available via JDISS, IAS and other intelligence systems. It contains the DOD CI/counter-terrorism/counter- proliferation databases and is principally used by CI analysts and production personnel. The system provides a number of analytical tools, such as automated and graphical link analysis hot-linked to the underlying reports, automatic time lining as well as access to various communications systems to support dissemination.

(5) Migration Defense Intelligence Threat Data System (MDITDS). The MDITDS is being developed to operate on the DCIIS to provide an automated production system for DODIIS Indications and Warning (I&W), counterintelligence, counterterrorism, and Arms Proliferation/Defense Industry communities. Many of the current intelligence/counterintelligence databases that reside on other systems will become resident within the MDITDS. Some of these include DITDS, SPHINX (DIA's CI database), CANNON LIGHT (U. S. Army CI database), BLOODHOUND (EUCOM CI database), Automated Intelligence Information Retrieval System (AIIRS), Automated Decision Making and Program Timeline (ADAPT), Defense Automated Warning System (DAWS), Sensitive Compartmented Automated Research Facility (SCARF), Terrorism Research & Analysis Program (TRAP), and many others.

(6) HUMINT Operational Communications Network (HOCNET). HOCNET is the umbrella name given to a collection of systems and applications currently operational or under development which support the Defense HUMINT Service (DHS) worldwide activities (i.e., Defense Attaché Worldwide Network (DAWN)).

(7) Special Operations Debriefing And Reporting System (SODARS). SODARS provides detailed mission debriefs and after-action reports from special operations forces (SOF). As SOF are often the first and perhaps only DOD force committed to an operation, they may provide invaluable intelligence and CI when developing pre-deployment threat assessments.

(8) AN/PYQ-3 CI/HUMINT Automated Tool Set (CHATS). CHATS consists of CIS hardware and software designed to meet the unique requirements of MAGTF CI/HUMINT elements. Operating up to the SECRET level and using the baseline DCIIS software suite, the system provides the capability to manage MAGTF CI assets and analyze information collected through CI investigations, interrogations, collection, and document exploitation. With CHATS, CI units may electronically store collected information in a local database, associate information with digital photography, and transmit/receive information over existing military and civilian communications. (See appendix B for additional information on CHATS.)

(9) Joint Collection Management Tool (JCMT). JCMT is the principal automated tool for all-source intelligence collection requirements management. It provides a capability for management, evaluation and direction of collection operations. Using DCIIS, CI collection requirements and taskings can be accessed from the JCMT.

(10) Community On Line Intelligence Support End User Management (COLISEUM) System. COLISEUM is the automated, DOD Intelligence Production Program (DODIPP) intelligence production requirements system that allows authorized users to directly submit multi-discipline intelligence production requirements to commanders and intelligence production centers. COLISEUM also tracks responses and provide status reports on validated production requirements.

d. Summary -- Counterintelligence Command and Control and Supporting Communications and Information Systems. Figure 5-1 depicts a notional MEF CI architecture, while figure 5-2 depicts key CI elements and supporting CIS within the MAGTF CE CIC. Together they emphasize three key aspects of MAGTF CI C2 and supporting CIS operations:

- The task organization and command/support relationships of MAGTF CI units -- CI/HUMINT company headquarters collocated with the MAGTF G/S-2. Although company elements normally operate in general support of the MAGTF, task-organized CI, interrogator-translator or HETs may be either attached to or placed in direct support of MAGTF subordinate units..

- Principal CI systems (e.g., CHATS) employed within and in support of the MAGTF.

- Communications connectivity -- the principal communications pathways and the level of security classification.

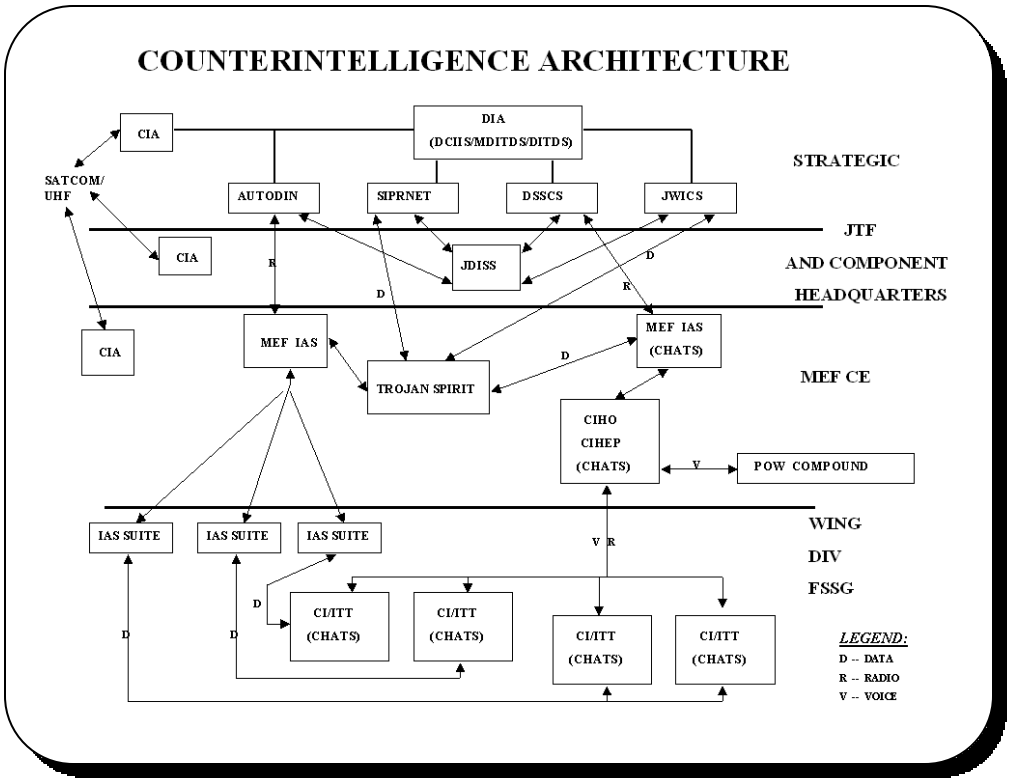


Figure 5-1. Counterintelligence Architecture

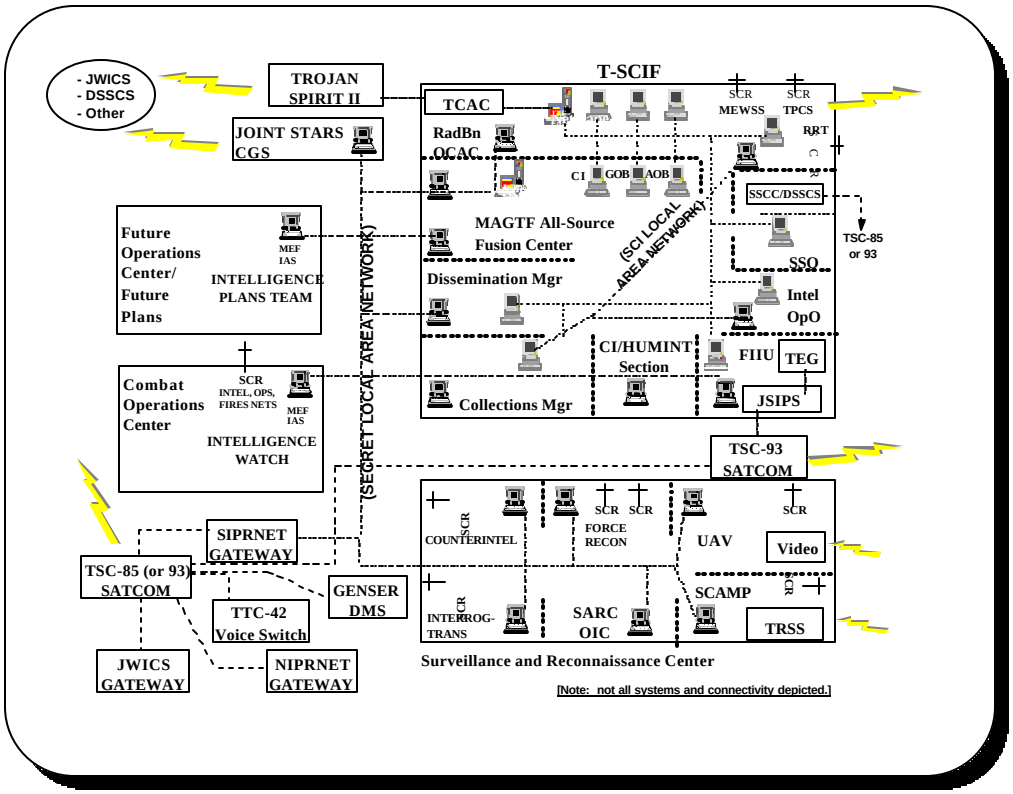


Figure 5-2. Counterintelligence Elements Within the MAGTF CE CIC

5005. CI CIS Planning Considerations. The following identifies key CIS requirements and planning considerations in support of MAGTF CI operations.

a. Ensure that the MAGTF CE, CI/HUMINT elements, and other MAGTF units are included in the distribution of CI/HUMINT-related address indicator groups to receive pertinent JTF, theater, & national intelligence and CI products.

b. Determine and coordinate radio nets requirements, supporting frequencies, and operational procedures in support of CI operations (external to MAGTF, internal MAGTF, intelligence broadcasts, retransmission sites, routine and time-sensitive operations, etc.).

c. Coordination of CI CIS activation and restoration priorities and supporting procedures.

d. CMS requirements for unique CI communications.

d. Determine and coordinate wire communications (to include telephones) in support of CI operations.

e. Establishment, operation and management of unique CI communications.

f. Determine and coordinate local and wide area networks and unique intelligence networks information systems requirements in support of CI operations (hardware, software, internet protocol addresses, etc.).

g. Integration of CI/HUMINT elements' CIS operations with those of other MAGTF and pertinent JTF and other components intelligence and reconnaissance units (mutual support, cueing, etc.).

h. Communications integration of CI/HUMINT elements employed in general support with collocated GCE, ACE, CSSE and other MAGTF elements (e.g., to provide time-sensitive reporting, coordination of maneuver, etc.).

i. Coordination of CI CIS and dissemination operations and procedures with allied and coalition forces.

CHAPTER 6

COUNTERINTELLIGENCE PLANNING

6001. Marine Corps Planning Process and Joint Planning Process Overview[1]

a. General. Planning is an act of preparing for future decisions in an uncertain and time-constrained environment. Whether it is done at the national or the battalion/squadron level, the key functions of planning are:

(1) Planning leads to a plan that directs and coordinates action.

(2) Planning develops a shared situational awareness.

(3) Planning generates expectations about how actions will evolve and how they will affect the desired outcome.

(4) Planning supports the exercise of initiative.

(5) Planning shapes the thinking of planners.

b. Marine Corps Planning Process (MCPP). The MCPP helps organize the thought processes of a commander and his staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps warfighting philosophy of maneuver warfare. It capitalizes on the principle of unity of effort and supports the establishment and maintenance of tempo. The MCPP steps can be as detailed or as abbreviated as time, staff resources, experience, and the situation permit. It applies to command and staff actions at all echelons. From the Marine Corps component headquarters to the battalion/squadron level, commanders and staff members must master the MCPP in order to be full participants in integrated planning. Additionally, the MCPP complements deliberate or crisis action planning (CAP) as outlined in the Joint Operation Planning and Execution System (JOPES).

The MCPP establishes procedures for analyzing a mission, developing and analyzing COAs against the threat, comparing friendly COAs against the commander's criteria and each other, selecting a COA, and preparing an OPORD for execution. The MCPP organizes the planning process into six manageable, logical steps. It provides the commander and his staff a means to organize their planning activities and transmit the plan to subordinates and subordinate commands. Through this process, all MAGTF levels of command can begin their planning effort with a common understanding of the mission and commander's guidance. The six integrated steps of this process are:

---

[1] MCWP 5-1, *Marine Corps Planning Process*, is now in development and will provide detailed doctrine and TTP regarding the MCPP. Jt Pub 5-00.2, *Joint Task Force Planning Guidance*, likewise provides detailed discussion of the joint planning processes.

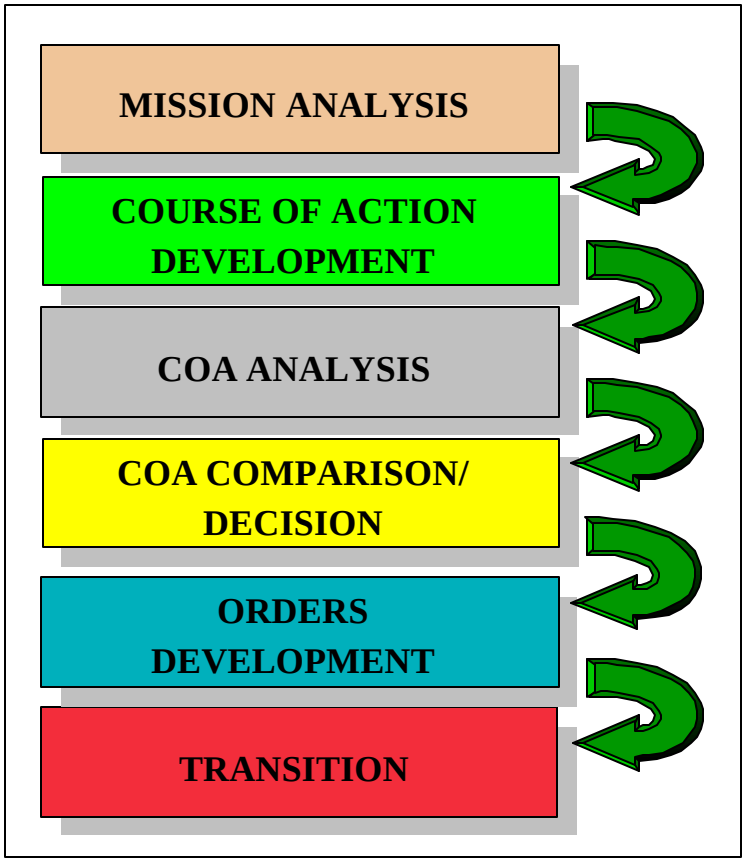


Figure 6-1. The Marine Corps Planning Process

(1) Mission Analysis. Mission analysis is the first step in planning. The purpose of mission analysis is to review and analyze orders, guidance, and other information provided by higher headquarters and produce a unit mission statement. Mission analysis drives the MCPP.

(2) COA Development. During COA development, the planners use the mission statement (which includes higher headquarters tasking and intent), commander's intent, and commander's planning guidance to develop several COAs. Each prospective COA is examined to ensure that it is suitable, feasible, different, acceptable, and complete with respect to the current and anticipated situation, the mission, and the commander's intent. In accordance with the commander's guidance, approved COAs are further developed in greater detail.

(3) COA Analysis. During COA analysis, each friendly COA is examined against selected threat COAs. COA analysis involves a detailed assessment of each COA as it pertains to the threat and the environment. COA analysis assists the planners in identifying strengths and weaknesses, associated risks, and asset shortfalls for each friendly COA. COA analysis will also identify branches

and potential sequels that may require additional planning. Short of actually executing the COA, COA analysis provides the most reliable basis for understanding and improving each COA.

(4) COA Comparison and Decision. In COA comparison and decision, the commander evaluates all friendly COAs—against established criteria, then against each other---and selects the COA that he deems most likely to accomplish the mission.

(5) Orders Development. During orders development, the staff takes the commander's COA decision, intent, and guidance, and develops orders to direct the actions of the unit. Orders serve as the principal means by which the commander expresses his decision, intent, and guidance.

(6) Transition. Transition is an orderly handover of a plan or order as it is passed to those tasked with execution of the operation. It provides those who will execute the plan or order with the situational awareness and rationale for key decisions necessary to ensure there is a coherent shift from planning to execution.

Interactions among various planning steps allow a concurrent, coordinated effort that maintains flexibility, makes efficient use of time available, and facilitates continuous information sharing.

c. Comparison of the MCPP and the Joint Planning Processes

(1) Joint Deliberate Planning**.** The deliberate planning process is used by the joint staff and commanders in chief (CINCs) to develop plans (OPLANs, CONPLANs, functional plans) in support of national strategy. The Joint Strategic Capabilities Plan (JSCP) apportions forces and resources for use during deliberate planning by the combatant commanders and their service component commanders. The figure below illustrates how the MCPP fits within and supports the joint deliberate planning process.

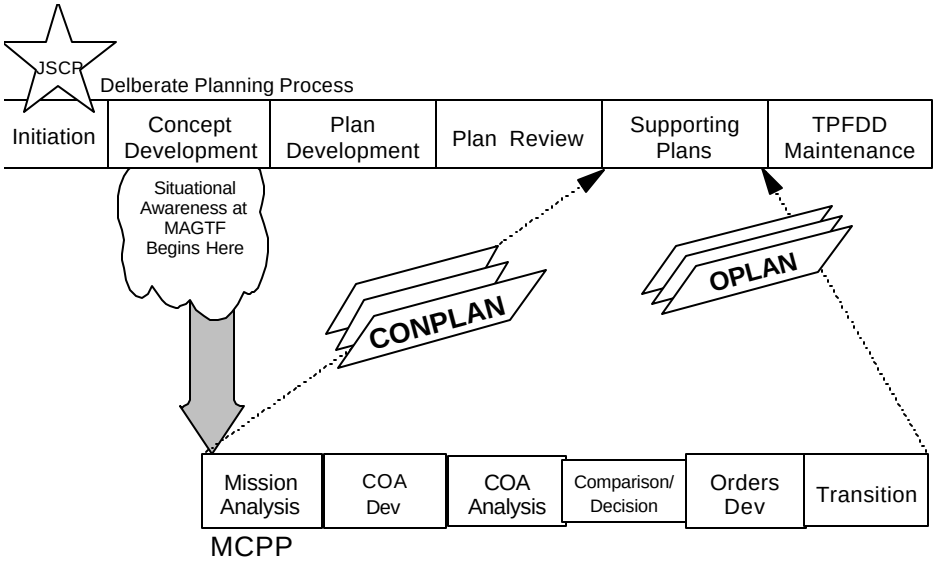


Figure 6-2. The MCPP and the Joint Deliberate Planning Process

(2) Crisis Action Planning (CAP). CAP is conducted in response to crises where national interests are threatened and a military response is being considered. In CAP, the time available for planning at the national level is reduced to as little as a few days. CAP procedures promote the logical, rapid flow of information and the timely preparation of campaign plans or OPORDs. The figure below illustrates how the MCPP fits within and supports the joint crisis action planning process.

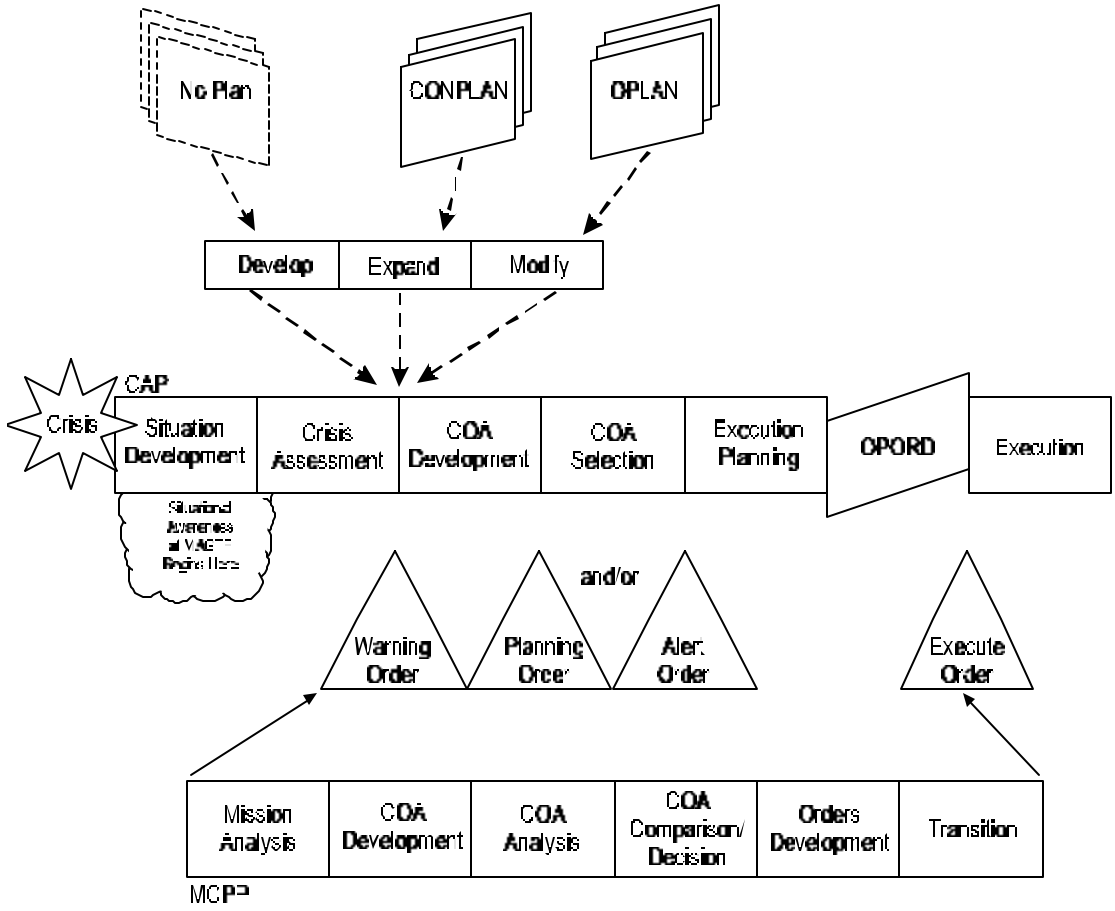


Figure 6-3. The MCPP and the Joint Crisis Action Planning Process

6002. Counterintelligence Planning

a. <u>Intelligence Planning</u>. CI planning and execution is conducted in concert with the six phases of the standard intelligence cycle. The first phase is planning and direction. It consists of those activities that identify pertinent intelligence requirements (IR) and provide the means for satisfying those requirements (see figure 6-4).[2] Intelligence planning and direction is a continuous function and a command responsibility. The commander directs the intelligence effort; the intelligence officer manages

[2] See chapter three of MCWP 2-1, *Intelligence Operations*, for comprehensive discussion of each phase of the intelligence cycle and the overall conduct of intelligence planning and direction.

this effort for the commander based on the intent, designation of priority intelligence requirements (PIR), and specific guidance provided during the planning process.

Figure 6-4. Functions of the Planning and Direction Phase

b. CI Planning -- General

(1) Focus. CI planning and subsequent operations are conducted in support of the MAGTF or designated subordinate commanders in order to both support the overall intelligence effort and to aid with force protection. Accordingly, CI must be planned in conjunction with the overall intelligence and force protection efforts. The commander must incorporate CI early in the planning process in order to formulate his estimate of the situation, identify the MAGTF's risks and security vulnerabilities, and begin shaping his overall operations and supporting intelligence and force protection operations.

(2) CI and HUMINT. CI also has to be considered with many other intelligence activities because of the mission of CI. HUMINT is the intelligence activity that has the most important connective tie to CI. CI and HUMINT work hand-in-hand because of the nature of their targets and the type of intelligence missions they perform: CI destroying the enemy intelligence effort and HUMINT collecting information about enemy activity. The differentiation and coordination required for the effective exploitation of human sources is critical, requiring integration of CI activities and HUMINT operations (e.g., interrogator/translator exploitation of enemy prisoners of war (EPW)). See DIAM 58-11, *DOD HUMINT Policies and Procedures*, and DIAM 58-12, *The DOD HUMINT Management System*, for additional information.

(3) CI Planning Responsibilities

(a) Intelligence Officer. Primary staff responsibility for CI operations planning lies with the G/S-2. Included in his responsibilities are:

- Preparation of integrated, multi-discipline intelligence and reconnaissance operations and supporting CI plans, orders, annexes, and appendices.

- Coordination with the G/S-3 to ensure that the planned CI effort will support the concept of operations and the scheme of maneuver; to ensure effective prioritization and integration of CI operations with MAGTF force protection operations; to ensure integration of CI operations with PSYOP, civil affairs, and military police activities; and to ensure effective integration of MAGTF CI elements with subordinate units' operations.

- Coordination with the G/S-6 officer for communication and information systems support to the CI elements, including circuits and networks access, frequency assignment, equipment, call signs, and support to special CI communications.

- Liaison with CI agencies and units external to the MAGTF, in particular the JTF J-2X.

- Coordination with the G/S-4 to ensure adequate logistics support of CI elements, in particular transportation and the maintenance of CI units' unique equipment.

(b) CI/HUMINT Officer (CIHO). The CIHO is responsible to the G/S-2 (or the MAGTF intelligence operations officer) for the planning, direction and execution of MAGTF CI operations. Specific duties include:

- In conjunction with other intelligence section staff officers and the CI/HUMINT company (Co) commander, prepare MAGTF CI plans and orders.

- In conjunction with the collection management officer and the CI/HUMINT Co planners, coordinate, plan, supervise, and assist CI collection requirements and taskings for MAGTF operations.

- In coordination with the SARC OIC, CI/HUMINT Co, and the G/S-3, coordinate the movement, operation and reporting of CI units.

- In conjunction with MAGTF AFC OIC and CI/HUMINT Co, coordinate MAGTF AFC analyst exchanges with CI analysts; and the integration of CI with all-source intelligence production.

- In coordination with the dissemination officer, plan for the timely reporting of CI-derived intelligence to MAGTF and external elements and the rapid handling of perishable CI information.

- In conjunction with the G/S-6, plan and coordinate CI special communications paths and operations.

(c) CI/HUMINT Company Commander. The CI/HUMINT Co commander is responsible for the effective conduct of MAGTF CI/HUMINT operations in support of the commander's intent and the operational and intelligence concept of operations. Specific CI tasks include:

- Plan and employ CI resources in response to the commander's intent, threat situation and the MAGTF G/S-2's guidance and direction and intelligence operations plan.

- Effect TECHON of MAGTF organic CI collection, processing and exploitation, production, and dissemination operations; and the effective coordination of MAGTF CI operations with JTF, other services, theater, national, and other Service CI agencies.

- Coordinate movement and operations of CI units with MAGTF staff elements and subordinate units commanders, ensuring that all element movements are coordinated with the current operations center, fire support coordination center and the SARC.

- Advise the G/S-2, CIHO, intelligence operations officer, MAGTF AFC OIC, collections officer, and dissemination officer on CI employment and its integration with JTF, theater, and national CI operations.

c. Coordination Considerations. The complexity of CI operations requires thorough coordination with all intelligence organizations. Detailed coordination ensures that CI operations are both focused upon intelligence priorities and are not duplicative. Constant coordination must be accomplished with the JTF and other component forces, combatant commander, and other supporting intelligence organizations to ensure that a coordinated, manageable and effective CI operations are conducted.

(1) CI Planning Considerations. Key considerations in planning CI operations include:

(a) Friendly Considerations. The CI operations effort must support and adapt to the commander's intent, concepts of intelligence and operations, and the supporting scheme of maneuver. Questions to answer include:

- What is the MAGTF area of operations (AO) and area of interest (AI)?

- What is the MAGTF concept of operations, task organization, main and supporting efforts?

- What is the task organization and command/support relationships amongst all MAGTF intelligence, CI and reconnaissance units? Can the friendly concept of operations be supported by CI elements operating in MAGTF general support, or are CI direct support/attachments to MAGTF subordinate units required?

- What are the standing PIRs and IRs? Which have been tasked to supporting CI units? What specific information is the commander most interested in (i.e., enemy air operations, enemy ground operations, friendly force protection, target BDA, or enemy future intentions)?

- What is the MAGTF force protection concept of operations? What are the standing EEFIs and their assessed priorities?

- What are the CI, intelligence and force protection concepts of operations of the JTF, other components and theater forces? How can external CI assets be best integrated and employed to support MAGTF operations?

(b) Enemy Considerations. Intelligence operations focus on the enemy. Prior to commencing MAGTF CI operations, we must learn as much as we can about the enemy. Key adversary information which must be considered when conducting CI planning include:

- What threat forces -- conventional, law enforcement/security, paramilitary, guerrilla, terrorist -- are within the MAGTF AO and AI? What are their centers of gravity and critical vulnerabilities? Is this a large enemy force organized along conventional military lines or a small, loosely knit guerrillas or unconventional military force? What are their sizes, composition, and tactics, techniques and procedures?

- Who are the key enemy military, security and civilian leaders? What and where are the enemy's critical nodes for command and control and what are their vulnerabilities? What security countermeasures do they employ to prevent CI exploitation of their operations? What are its command and control and CIS tactics, techniques and procedures?

- Who are the know enemy personalities engaged in intelligence, CI, security, police, terrorist, or political activities? Who are known or suspected collaborators and sympathizers, both within the populace as well as within other parties?

- What are the key installations and facilities used by enemy intelligence, espionage, sabotage, subversive and police organizations? What are the key communications, media, chemical, biological, utilities, and political installations and facilities?

- What are the national and local political parties or other groups known to have aims, beliefs, or ideologies contrary or in opposition to those of the U.S.? What are the student, police, military veterans, and similar groups known to be hostile to the U.S.?

6003. CI Planning and the Intelligence Cycle

a. General

(1) The intelligence cycle is a procedural framework for the development of mission-focused intelligence support. It is not an end in itself, nor should it be viewed as a rigid set of procedures that must be carried out in an identical manner on all occasions. Rather, the commander and the intelligence officer must consider each IR individually and apply the intelligence cycle in a manner that develops the required intelligence in the most effective way.

(2) The application of the intelligence cycle will vary with the phase of the planning cycle. In theory, a unique iteration of the intelligence cycle is carried out for each individual requirement. In practice, particularly during the planning phase, requirements are grouped together and satisfied through a single, concurrent intelligence development process that concurrently addresses CI requirements. During the planning phase, intelligence development is generally carried out through two major iterations of the intelligence cycle. The first primarily supports decision planning. Completion of this iteration of the intelligence cycle results in the preparation and use of basic intelligence and CI products—intelligence and CI estimates, supporting studies, and IPB analysis—that describe the battlespace and threat. These products form the basis for development and selection of MAGTF COAs. The second iteration of the intelligence cycle supports execution planning. It is an outgrowth of the selection of the COA and formulation of the concept of operations; the implementation of the intelligence collection, production and dissemination plan; refinement of IPB analysis, and the generation of mission-specific intelligence products and CI measures which are integrated with the concept of operations to support mission execution. During execution, requirements are satisfied on a more individualized basis. New requirements are usually generated in response to a specific operational need. Each requirement is unique and must be satisfied in a timely manner to facilitate rapid decisionmaking and the generation or maintenance of tempo (see figure 6-5).

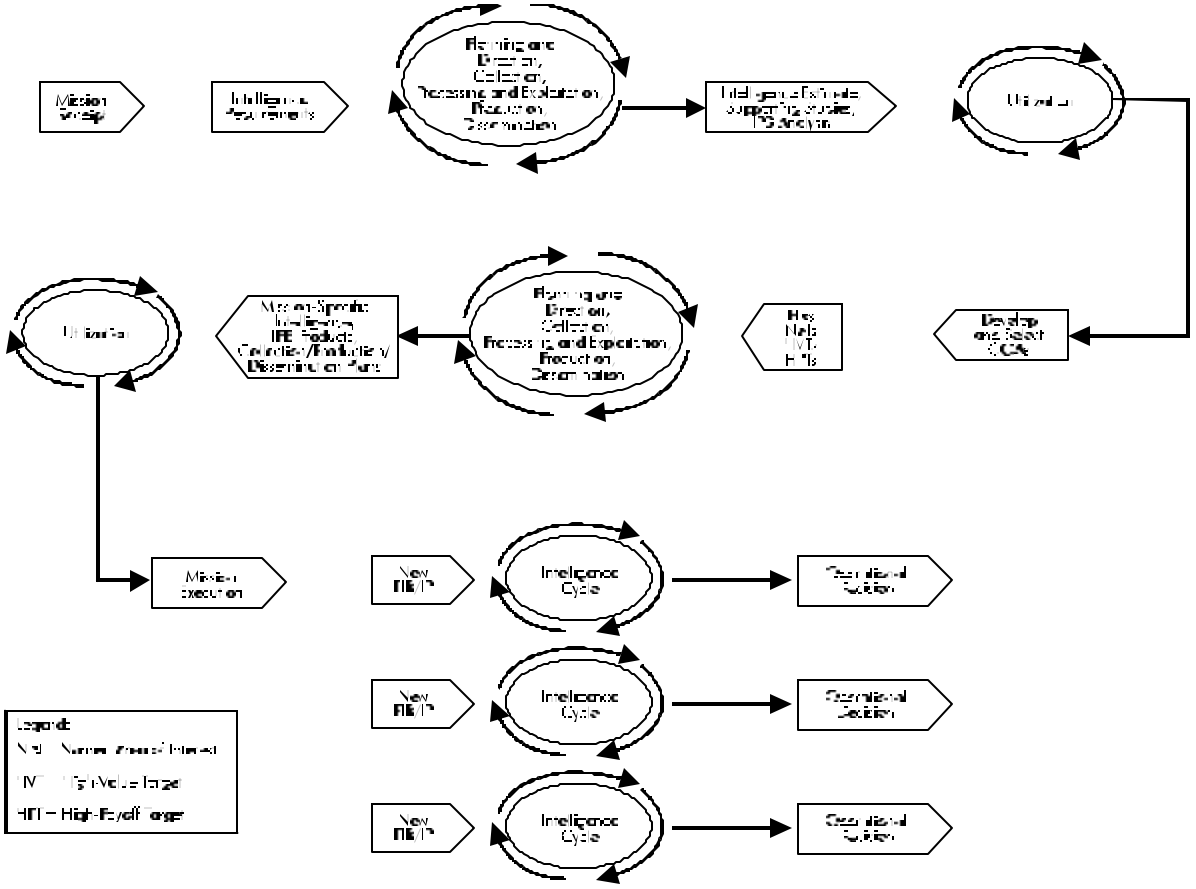


Figure 6-5. Application of the Intelligence Cycle

(3) The G-2/S-2 provides CI participation and assistance early in the planning phase of tactical operations. The commanders benefit from CI information given at this phase because it helps to formulate tactical plans and because CI/HUMINT operations, by their very nature, generally require more time than other intelligence disciplines to yield substantive results. CI also provides the commander with capabilities that are offered by no other discipline or technical system. CI is one of the tools that can help the commander anticipate the action of the enemy. Particular attention is directed to identifying friendly vulnerabilities to be exploited by hostile collections assets and to recommending specific CI measures.

(4) The CI effort focuses on the overall hostile intelligence collection, sabotage, terrorist, and subversive threat. The CI effort is also sufficiently flexible to adapt to the geographical environment, attitudes of the indigenous population, mission of the supported command, and changing emphasis by hostile intelligence, sabotage, terrorist, and subversive organizations.

b. <u>Planning the Activity</u>. The effectiveness of MAGTF CI operations depends largely on the planning preceding the operation. The CI staff officer, assisted by the CI/HUMINT Co commander or HET OIC, performs four separate functions in carrying out his planning responsibilities. First, he directs

the effort to collect information on the enemy's intelligence, sabotage, terrorism, and subversion capabilities, coordinating with the intelligence operations officer and collection manager to ensure CI collection requirements levied upon CI/HUMINT elements are realistic and within the capability of the CI elements and are integrated into the MAGTF's all-source intelligence collection plan. Second, in coordination with the AFC OIC and the G/S-3 force protection planners, he support the production of intelligence on the enemy's intelligence, sabotage, terrorism, and subversion capabilities, including clandestine and covert capabilities. Third, in coordination with the intelligence dissemination officer, he ensures the timely dissemination of CI products to all MAGTF units. Finally, he plans, recommends, and monitors CI measures throughout the entire command.

(1) CI Collection and Processing of Information. CI elements can collect both CI and combat intelligence information through the use of controlled HUMINT. In addition to its CI functions, an element may be assigned additional responsibility for combat intelligence collection. The area commander normally provides the procedures and authority governing the conduct of controlled HUMINT operations and certain offensive CI operations. These procedures are covered in detail in the classified addendum, DIAM 58-11 *DOD HUMINT Policies and Procedures*, DIAM 58-12 *DOD HUMINT Management System*, and theater collection plans. The determination of CI collection requirements follows the same process and procedures prescribed for other types of IRs (see MCWP 2-1, *MAGTF Intelligence Operations*, chapter 3). Especially pertinent to CI planning is information on the enemy's intelligence and reconnaissance capabilities and operations. Included are such matters as the hostile intelligence organization, means available to the enemy for the collection of information, and hostile sabotage, terrorism, and subversive agencies and capabilities.

(a) CI Collection Sources. CI sources of information include:

- **Casual Sources**. A casual source is one who, by social or professional position, has access to information of CI interest, usually on a continuing basis. Casual sources usually can be relied on to provide information which is routinely available to them. They are under no obligation to provide information. Casual sources include private citizens, such as retired officials or other prominent residents of an area. Members of private organizations also may furnish information of value.

- **Official Sources**. Official sources are liaison contacts. CI personnel conduct liaison with foreign and domestic CI intelligence, security, and law enforcement agencies to exchange information and obtain assistance. CI personnel are interested in investigative, operational, and threat information.

- **Recruited Sources**. Recruited sources include those who support CFSO and are by design, human source networks dispersed throughout the area of operations who can provide timely and pertinent force protection information

- **Refugees, Civilian Detainees and EPWs**. Refugees, civilian detainees, and EPWs are other sources of CI information. Interrogators normally conduct these collection operations, often with technical assistance from a CI agent. The key to identifying the source of valuable CI force

protection information is in analyzing the information being sought and predicting who, by virtue of their regular duties, would have regular, frequent, and unquestioned access to such information.

- **Open Sources.** Open source publications of all sorts (newspapers, magazines, etc.) and radio and television broadcasts are valuable sources of information of CI interest and information. When information is presented in a foreign language, linguist support is required for timely translation. Depending on the resources, this support can be provided by MAGTF interrogation personnel, allied personnel, or indigenous employees.

- **Documents**. Documents not openly available, such as adversary plans and reports, are exploited in much the same way as open source publications.

(b) Counterintelligence Targets. CI targets include personalities, organizations, and installations (PO&I) of intelligence or CI interest, which must be seized, exploited, neutralized or protected. The PO&I targeting triad forms the basis of CI activities. Incidents are also included within CI databases to conduct trend analysis of potential targets. DIA has the responsibility, in response to a validated requirement, to establish and maintain CI databases. Operational control of the database will pass to the Joint Task Force, once deployed. The AFC CIAT has the responsibility of establishing and maintaining CI databases for the MEF and will coordinate with the local collection elements to eliminate duplication of effort and maximize information sharing (within smaller MAGTFs, the CI/HUMINT Co detachment or HET performs this function).

Selecting and assigning targets is based on an assessment of the overall hostile threat, unit mission, commander's intent, designated PIRs and other IRs, and the overarching intelligence and force protection concepts of operations. The assessment considers both the immediate and estimated future threats to security. It normally is conducted at the MAGTF level where the resultant CI targets lists are also produced and which include any CI targets assigned by higher headquarters. Numerical priority designations are assigned to each target to emphasize the relative importance and value of the target. The designations also indicate the degree of security threat and urgency in neutralizing or exploiting the target. Priority designations established by higher headquarters are not altered; however, lower echelons may assign priorities to locally developed targets. CI targets are usually assigned priority designations according to the following criteria:

- **Priority One.** Priority One targets represent the greatest security threat to the MAGTF. They also possess the largest potential source of intelligence or CI information/material which must be exploited or neutralized as soon as possible.

- **Priority Two.** Priority Two targets are of lesser significance than priority one. They are to be taken under control after priority one targets have been neutralized or exploited.

- **Priority Three.** Priority Three targets are of lesser significance than priority one or two. They are to be neutralized or exploited as time and personnel permit.

1 Personalities. Except for well-known personalities, most persons of CI interest are identified and developed by CI units once operations have commenced. Personalities are divided into three categories. These categories comprise those persons who are a threat to security, whose intentions are unknown, and who can assist the intelligence and CI effort. For ease in identification, a color code indicates the categories.

- **DETAIN (Black) List.** An official CI listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of friendly forces (Joint Pub 1-02). The black list includes the following persons:

  - ➢ Known or suspected enemy or hostile espionage, sabotage, terrorist, political, and subversive individuals.

  - ➢ Known or suspected leaders and members of hostile paramilitary, partisan, or guerrilla groups.

  - ➢ Political leaders known or suspected to be hostile to the military and political objectives of the United States and/or an allied nation.

  - ➢ Known or suspected officials of enemy governments whose presence in the theater of operations poses a security threat to the U.S. Forces.

  - ➢ Known or suspected enemy collaborators and sympathizers whose presence in the theater of operations poses a security threat to the U.S. Forces.

  - ➢ Known enemy military or civilian personnel who have engaged in intelligence, CI, security, police, or political indoctrination activities among troops or civilians.

  - ➢ Other enemy personalities such as local political personalities, police chiefs, and heads of significant municipal and/or national departments or agencies.

- **OF INTEREST (Gray) List.** Gray lists, compiled or developed at all echelons of command, contain the identities and locations of those personalities whose inclinations and attitudes toward the political and military objectives of the United States are unknown. Regardless of their leanings, personalities may be on gray lists when known to possess information or particular skills required by friendly forces. They may be individuals whose political motivations require further exploration before they can be used effectively. Examples of individuals who may be included in this category are:

  - ➢ Potential or actual defectors from the hostile cause whose credibility has not been established.

➢ Individuals who have resisted, or are believed to have resisted the enemy government and who may be willing to cooperate with friendly forces, but whose credibility has not been established.

➢ Nuclear, biological, chemical and other scientists, and technicians suspected of having been engaged in enemy weapons of mass destruction and other programs against their will.

• **PROTECT (White) Lists.** White lists, compiled or developed at all echelons of command, contain the identities and locations of individuals in enemy controlled areas. These individuals are of intelligence or CI interest. They are expected to be able to provide information or assistance in the accumulation of intelligence data or in the exploitation of existing or new intelligence areas of interest. They are usually in accord with or favorably inclined toward U.S. policies. Their contributions are based on a voluntary and cooperative attitude. Decisions to place individuals on the white list may be affected by the combat situation, critical need for specialists in scientific fields, and such intelligence needs as are indicated from time to time. Examples of individuals included in this category are:

➢ Former political leaders of a hostile state deposed by the hostile political leaders.

➢ Intelligence agents employed by U.S. or Allied intelligence agencies

➢ Key civilians in areas of scientific research, to include faculty members of universities and staffs of industrial or national research facilities whose credibility have been established.

➢ Leaders of religious groups and other humanitarian groups.

➢ Other persons who can significantly aid the political, scientific, and military objectives of the U.S. and whose credibility has been established.

2 Organizations. These include any organization or group which is an actual or potential threat to the security of JTF. or other allied forces and must be neutralized. However, an organization or group may present a threat that is not immediately apparent. The enemy frequently camouflages his espionage or subversive activities by establishing front organizations or groups. If these organizations are permitted to continue their activities, they could impede the success of the military operations. Examples of hostile organizations and groups which are of major concern to the CI unit during tactical operations include:

• Hostile intelligence, sabotage, subversive, and insurgent organizations or groups.

• National and local political groups and parties known or suspected to have aims, beliefs, or ideologies contrary or in opposition to those of the United States.

- Paramilitary organizations, including student, police, military/veterans, and ex-combatant groups, known to be hostile to the United States.

- Hostile sponsored groups and organizations whose objectives are to create dissension and spread unrest among the civilian population in the area of operation.

3 Installations. The installation target is any installation, building, office, or field position that may contain information or material of CI interest or which may pose a threat to MAGTF security. Examples of installation type targets are:

- Installations formerly or currently occupied by enemy espionage, sabotage, and subversive agencies of enemy police organizations, including prisons and detention centers.

- Installations occupied by enemy intelligence, CI, security, or paramilitary organizations, including operational bases, schools, and training sites.

- Enemy communication media and signal communication centers.

- Research centers and chemicals laboratories used in the development of weapons of mass destruction.

- Enemy political administrative headquarters.

- Production facilities, supply areas, and other installations to be taken under control to deny support to hostile guerrilla and partisan elements.

- Public utilities and other installations to be taken under early control to prevent sabotage. These installations are usually necessary for the rehabilitation of civil areas under U.S. control.

- Embassies and consulates of hostile governments.

4 Incidents. The recording of details of incidents occurring within the area of operations allows for trend analysis which may reveal patterns and indications of future intentions. Incidents do not occur in a vacuum. They are planned, organized, and carried out by individuals acting alone or in groups. Detailed recording of incidents that occur within an area of operations is a critical ingredient in the analysis of trends and patterns designed to identify indications of future intentions. Matrix manipulation, link analysis, and visual investigative analysis are tools often used in the incident analysis process. The matrix allows for a considerable amount of information to be stored in a relatively small space. Link analysis then analyzes these bits of information by displaying the links that exist between them. Visual investigative analysis is used to time sequence names and events to show an even clearer picture of these relationships.

(c) Counterintelligence Target Reduction. The timely seizure and exploitation of CI targets requires a detailed and well coordinated CI reduction plan. This plan should be prepared well in advance and kept current. CI elements supporting tactical assault units normally prepare the reduction plan. All assigned or developed targets located within the unit's area of operation, are listed in the reduction plan. This plan is based on the MAGTF's scheme of maneuver, with CI targets listed in the sequence in which they are expected to appear in the area of operation. However, the target priority designations remain as assigned on the CI target list with highest priority targets covered first when more than one target is located in the same general area. Neutralized and exploited targets are deleted from the CI reduction plan and appropriate reports are submitted. A well-prepared and comprehensive CI reduction plan ensures coverage of all significant CI targets. It also allows all CI units to conduct daily operations based on established priorities. (See appendix E for a sample CI reduction plan.)

(d) Counterintelligence Measures Worksheet. The CI worksheet is prepared or revised based on the conclusions reached in the intelligence estimate of the enemy capabilities for intelligence, subversion, terrorist activities and sabotage. This worksheet is an essential aid in CI planning for the CIHO and CI/HUMINT Company Commander. It is also the basis for preparing CI orders and requests. See appendix E for an example of a CI measures worksheet. (See appendix E for a sample CI measures worksheet.)

(2) CI Production. Analysis and production is the heart of CI as it is with intelligence. No matter what quality and quantity of information is gathered, it does absolutely no good if the information is not turned into intelligence and disseminated to commanders and planners in time to use for decisionmaking. Critical to the success of MAGTF CI activities is taking collected information and producing tactically relevant intelligence (usually via all-source intelligence production), and providing it to commanders and planners in a timely manner. The transition of raw information into finished intelligence is the process of analysis. Fusing the finished intelligence into something usable by the customer is known as production.

(a) CI Production Threat Focus. CI analysis and production is focused on three well-defined threat activities: HUMINT, IMINT and SIGINT.

- **Counter Human Intelligence (C-HUMINT).** C-HUMINT requires effective and aggressive offensive and defensive measures as shown in figure 6-6. Our enemies collect against MAGTFs using both sophisticated and unsophisticated methods. We must combat all of these methods to protect our force and to ensure the success of our operations. MAGTF CI elements recommends countermeasures developed by CI analysts that the commander can take against enemy collection activities. CI C-HUMINT analysis focuses not only upon the standard enemy CI targets within the area of operations, but also upon the intelligence product most likely being developed through their collection activities. The analytical effort should attempt to identify the enemy's HUMINT cycle (collection, analysis, production, targeting) and key personalities. To produce a complete product, the CI analyst may need access to considerable data and require significant resources. The CI analyst will require collection in the areas of subversion, espionage, sabotage, terrorism, and other HUMINT supported

activities. Collection of friendly force data is also required to substantiate CI analytical findings and recommendations. Consistent with time, mission, and availability of resources, efforts must be made to provide an analytical product that identifies the enemy's intelligence, espionage, subversion, sabotage, and terrorism efforts. To accomplish C-HUMINT, MAGTF CI elements will conduct CI investigations, collection, and operations. Key C-HUMINT tasks include:

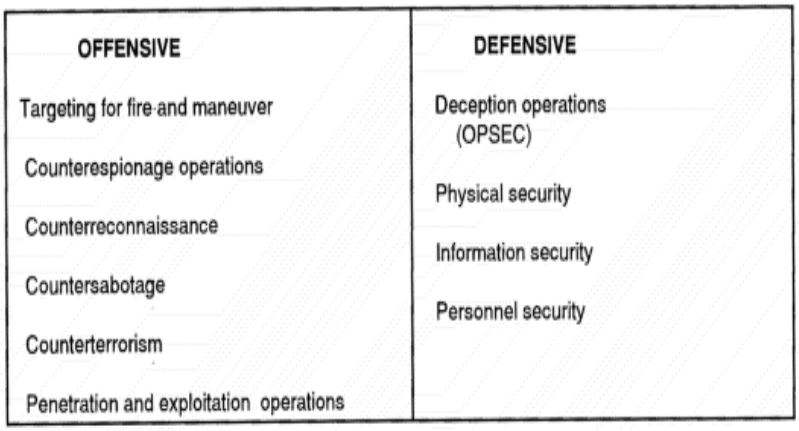


Figure 6-6. C-HUMINT Operations

➢ Identify the hostile HUMINT collectors and producers.

➢ Developing, maintaining, and disseminating multi-discipline threat data and intelligence on organizations, locations, and individuals of CI interest. This includes insurgent and terrorist infrastructure and individuals who can assist in the CI mission. Performing personnel security investigations and records checks on persons in sensitive positions and those whose loyalty is questionable. Also, all personnel must be educated and trained in all aspects of command security. A component of this is the muiti-discipline threat briefing. Briefings can and should be tailored, both in scope and classification level. Briefings could then be used to familiarize MAGTF units with the nature of the multi-discipline threat posed against the command or activity. Additionally, CI elements must search for enemy personnel who pose an intelligence collection or terrorist threat to the MAGTF. Should CI investigations result in identifying the location of terrorists, their apprehension is done in conjunction with military, civil and law enforcement authorities. Also, debriefing of selected personnel (friendly and hostile) including combat patrols, aircraft pilots, or other elements who may possess information of CI interest is necessary. (See appendix D, section I, for additional information on C-HUMINT.)

➢ Neutralize or exploit these to deny the enemy key friendly force information.

➢ Control our own information and indicators of operations so they are not readily accessible to the enemy's HUMINT operations.

➢ Support C-HUMINT commanders through effective and stringent adherence to physical, information, and personnel security procedures. They apply force or assets to ensure security daily. MAGTF CI and intelligence elements provide continuous and current threat information so the command can carry out its security responsibilities.

• **Counter Imagery Intelligence (C-IMINT).** C-IMINT requires the CI analyst to have an in-depth knowledge of the supported commander's plans, intentions, and proposed AO as far in advance as possible. The analyst must have access to all available data and intelligence on enemy IMINT methodology, systems, and processing as well as in-depth information on commercial satellite systems and the availability of their products to the enemy or to other parties supporting him. The CI analyst attempts to define the specific imagery platform deployed against the MAGTF and the cycle involved (time-based) from time of imaging through analysis to targeting. Knowledge of enemy intelligence support to targeting is critical in developing countermeasures to defeat, destroy, or deceive enemy IMINT. For ground-based HUMINT oriented IMINT (video cassette recorders, cameras, host nation curiosity, news media organizations), MAGTF CI elements will be required to collect the data for the analyst. This type of information cannot be reasonably considered to exist in any current database. Traditional enemy IMINT data is readily available and should not require any CI collection effort. However, collection to support CI (overflights of friendly forces by friendly forces) during identified, critical, and IMINT vulnerable times will validate CI C-IMINT findings and support countermeasures planning and execution. This will be of immense value to the CI analyst and the supported commander in determining what, if anything, enemy imagery has been able to exploit. (See appendix D, section II, for additional information on C-IMINT.)

The enemy may possess or acquire IMINT systems or products with a comprehensive and sophisticated capabilities. The MAGTF must have in place carefully developed countermeasures to negate any tactical and strategic threat. The enemy may acquire IMINT through a variety of ways, from handheld cameras to sophisticated satellite reconnaissance systems. Such IMINT capabilities may include:

➢ Aerial cameras.

➢ Infrared sensors.

➢ Imaging radars.

➢ Electro-optical sensors (TV).

➢ Multispectral and digital imagery products.

• **Counter Signals Intelligence (C-SIGINT).** C-SIGINT operations, including COMSEC monitoring and information systems security, are conducted during peace, war, and MOOTW to enhance MAGTF force protection, survivability, mobility and training; to provide data to identify friendly CIS vulnerabilities; to develop countermeasures recommendations and plans; and when implemented, to determine if countermeasures are effective. C-SIGINT includes full identification of the threat and an integrated set of offensive and defensive actions designed to counter the threat as shown in figure 6-7. Counter-SIGINT focuses upon the enemy's entities which can conduct SIGINT and EW against friendly forces. It also focuses on the intelligence which is most likely being collected and produced from their efforts. C-SIGINT analysis effort should be fully automated (data storage, sorting, and filing). The CI analyst requires SIGINT data collection to support vulnerability assessment and countermeasures evaluation. Validation of vulnerabilities (data and operations that are exploitable by the enemy's SIGINT operations) and the effectiveness of implemented countermeasures (a before and after comparison of MAGTF electromagnetic signatures and data) will be nearly impossible without active and timely collection as a prerequisite to analysis. The CI analyst requires a comprehensive database consisting of enemy SIGINT systems, installations, methodology, and associated SIGINT cycle information. In addition, all friendly CIS systems and user unit identification must be readily available, as well as a library of friendly countermeasures and a history of those previously implemented countermeasures and results achieved. Ideally, the CI analyst should, at any given time, be able to forecast enemy SIGINT activity. However, such estimates must rely upon other CI, interrogator, SIGINT, and IMINT collection as well as access to adjacent friendly unit CI files. Information on enemy SIGINT must be readily accessible from intelligence elements higher as well as lower in echelon than the supported command. Effective conduct of C-SIGINT requires close coordination and integrated production between MAGTF CI, SIGINT and all-source intelligence producers.

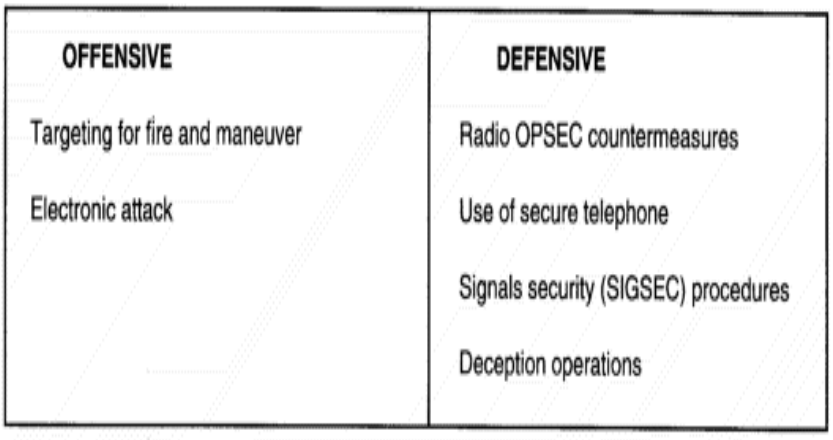


Figure 6-7. C-SIGINT Operations

C-SIGINT provides commanders and planners with the knowledge to assess the risk and probable success of alternative courses of action before a plan is implemented. C-SIGINT is a cyclic process

requiring a strong analytical approach integrating MAGTF CI, SIGINT, CIS and force protection personnel. C-SIGINT is based on a thorough knowledge of:

- ➢ Enemy SIGINT capabilities and tactics, techniques and procedures.
- ➢ MAGTF communications and information systems profiles.
- ➢ Enemy operations and plans.
- ➢ Realistic security measures, both INFOSEC and physical, that can be taken to deny information to the enemy.

(See appendix D, section III, for additional information on C-SIGINT.)

(b) CI Analytical and Production Functions. CI analysts perform the following analytical and production functions:

- Analyze the multi-discipline intelligence, espionage, subversion, sabotage and terrorism threats targeted against the MAGTF.
- Assess enemy intelligence vulnerabilities and susceptibilities to friendly deception efforts and other countermeasures.
- Support MAGTF force protection vulnerability assessment.
- Develop, evaluate, and recommend countermeasures to reduce, eliminate, or take advantage of MAGTF vulnerabilities.
- Support rear area operations by identifying intelligence, espionage, subversion, sabotage and terrorism threats to rear area units and installations (to include low-level agents responsible for sabotage and subversion).
- Nominate CI targets for exploitation, neutralization, or destruction.
- Develop and maintain a comprehensive and current CI database.
- Identify CI IRs and provide these to the collection officer.

(c) CI Products. CI products convey pertinent intelligence resulting from CI analysis to the commanders and planners in a readily useable form. CI analysts prepare a range of products, some focused upon specific needs and others of a more general nature. Among these products of most use to commanders and planners are CI estimates, CI surveys/vulnerability assessments, CI summary, and CI threat assessments.

- **Counterintelligence Estimate.** Normally a CI estimate is prepared only by the MAGTF G/S-2 and higher command echelons. The CI estimate forms the basis of the CI plan and operations. It includes the enemy's capabilities and limitations for intelligence, subversion, terrorism, and sabotage and the effects of the characteristics of the area on these capabilities and friendly CI measures. If a CI estimate is not prepared, such CI planning information can be consolidated within the basic intelligence estimate (appendix 8 to annex B, Intelligence). Key parts of the CI estimate include sections on enemy intelligence, subversion, sabotage, guerrilla warfare, terrorism, and the effects of the area on these enemy capabilities. See appendix C for a sample format of a MAGTF CI estimate.

- **CI Survey/Vulnerability Assessment.** CI surveys/vulnerability assessments are studies conducted by CI personnel to provide a supported command or agency a picture of its susceptibility to foreign intelligence collection. The CI survey/vulnerability assessment assesses a unit's security posture against threats detailed in the CI estimate. The survey should identify vulnerabilities to specific hostile intelligence, espionage, sabotage, subversion or terrorist capabilities and provide viable recommendations to eliminate or minimize these vulnerabilities. The survey should be as detailed as possible and combine the expertise of other disciplines such as engineers, Provost Marshall, and civil affairs personnel. The survey must look forward, in both space and time, to support the development of CI measures necessary to protect the unit as it carries out successive phases of the operation. The objective of a CI survey/vulnerability is to provide the MAGTF or other supported elements a realistic tool with which to evaluate internal force protection or security programs, and to provide a decisionmaking aid for the enhancement of these programs. CI surveys/vulnerability assessments include:

  - ➢ Estimating the enemy's likely PIRs and then evaluating the enemy's and any potential supporting forces' multi-discipline intelligence collection and production capabilities to answer these.

  - ➢ Identifying MAGTF activity patterns (physical and electronic), friendly physical and electronic signatures, and resulting profiles to enhance MAGTF OPSEC.

  - ➢ Monitoring or collecting MAGTF CIS transmissions to aid in vulnerability assessments, and providing a more realistic and stable basis from which to recommend countermeasures. (Note: these operations are generally conducted either by elements of the radio battalion or other supporting elements.)

  - ➢ Identifying MAGTF vulnerabilities based upon analysis of collected information and recommendations of countermeasures.

  - ➢ Analyzing the effectiveness of implemented countermeasures.

See appendix E for a CI survey checklist and the format for a CI Survey/Vulnerability Assessment.

- **Counterintelligence Summary (CISUM).** The CISUM is a graphic portrayal of the current situation from a CI point of view. The CI analyst uses the CISUM to show known adversary intelligence units as well as known/estimated threats within the friendly area. The CISUM is a periodic report usually covering a 12-hour period. It shows friendly targets identified as adversary objectives during the specified timeframe. The CI analyst includes a clear, concise legend on each CISUM showing the time period, map reference, and symbols identifying friendly and adversary information. As the CI analyst identifies a friendly critical node, element, or resource as an adversary combat or intelligence collection target, he puts a box around it and labels it with a "T" number. The legend explains whether the "T" is:

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

  The CISUM might portray the following information:

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

- **Counterintelligence Threat Assessment.** The CI threat assessment is a four-paragraph statement which is published as often as necessary or when significant changes occur, depending on the situation and the needs of the commander. The CI threat assessment provides

justification for CI target nominations and guidance for CI production. Essentially, the CI threat assessment provides the following (see figure 6-8 for the format of a CI threat assessment):

- ➢ A quick overview of significant activity during the reporting period.
- ➢ An assessment of the intelligence damage achieved by the enemy.
- ➢ A projected assessment of enemy activity for the next reporting period.
- ➢ CI target nominations.

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

A. HUMINT: Summarize in one paragraph all known HUMINT activity during the reporting period. Compile data from HUMINT situation overlay, matrices, link diagrams, & other CI products.
B. SIGINT: Summarize in one paragraph all known SIGINT activity. Compile from SIGINT situation overlay, matrices, and other CI products.
C. IMINT: Summarize in one paragraph all known IMINT activity. Compile from IMINT situation overlay, pattern & analysis chart, and other CI products.
D. OTHER: Summarize any other pertinent enemy activity not already addressed.

2. COUNTERINTELLIGENCE DAMAGE ASSESSMENT FOR THE PERIOD ____ TO ____ (LIST DTGs)
Briefly assess the CI damage to friendly units for whom the assessment is being prepared. Assessment is based upon enemy intelligence & reconnaissance activities that were identified, analyzed, and reported, measured against the friendly force operations profile and countermeasures implemented. Coordination with the G/S-3 OPSEC/Force Protection staff is essential when preparing this paragraph.

3. ESTIMATED ENEMY ACTIVITY FOR THE PERIOD ____ TO ____ (LIST DTGs)

A. HUMINT: briefly describe estimated enemy HUMINT activity for the reporting period.
B. SIGINT: briefly describe estimated enemy HUMINT activity for the reporting period.
C. IMINT: briefly describe estimated enemy HUMINT activity for the reporting period.
D. OTHER: briefly describe any other pertinent estimated enemy activity not addressed above.

4. COUNTERINTELLIGENCE TARGET NOMINATION

A. EXPLOITATION: identify any CI targets worthy of exploitation. Provide recommended timeframes, methods of exploitation, locations, justification, and any other pertinent information.
B. NEUTRALIZATION: identify any CI targets worthy of neutralization. Provide recommended timeframes, methods of neutralization, locations, justifications, and any other pertinent information.
C. DESTRUCTION: identify any CI targets worthy of destruction. Provide recommended timeframes, methods of engagement, locations, justification, and any other pertinent information.

Figure 6-8. Counterintelligence Threat Assessment

(3) CI Dissemination. Refer to chapter 5 for a detailed review of CI dissemination planning considerations.

6004. Counterintelligence Planning Requirements and Considerations. CI planning activities follow a logical sequence consistent with the MCPP and the six functions of intelligence. The following describes the CI planning requirements, considerations and activities. It is provided as a guide for MAGTF intelligence, force protection, and CI officers in planning MAGTF operations.

a. Formulation of the Commander's Estimate

(1) Provide assistance to the command operations security program. During the initial planning phase, CI assets provide assistance to the G-3/S-3 in establishing the force protection planning and operations.

(2) Complete studies of the enemy organization, weapons and equipment, techniques, and effectiveness in conducting intelligence, subversion, terrorism, and sabotage operations. Timely completion and dissemination throughout the MAGTF of the CI estimate is critical.

(3) Complete as early as possible the CI survey/vulnerability assessment to assist with MAGTF force protection planning and countermeasures development and implementation.

(4) Release CI planning information and products in accordance with PIRs and IRs and specified reporting criteria or as directed by the G/S-2. It is critical that CI personnel follow-up with recipients of these products to ensure that the information is understood and to identify early any resulting new CI IRs.

(5) Give appropriate security classification to all key information referring to the MAGTF's operation. CI personnel will provide advice and assistance to the MAGTF security manager or force protection officer with the development of operational classification guidance. MAGTF command guidance should ensure that particularly sensitive items are identified and protected, particularly within forward areas or in aircraft flying over enemy held areas. It should be determined if code symbols are necessary for marking of vehicles and operational equipment. If so, code symbols are used to cover existing tactical marking.

(6) Avoid compromising activities. Special inoculations or the issuance of special clothing and equipment should be postponed until after embarkation or other time, when possible, to avoid providing the enemy indications of future MAGTF activities. Leave and liberty are reduced gradually since any sudden curtailment will engender speculation. Submit recommendations on the selection of embarkation, assembly, and rehearsal areas, routes, and times for the movement to these areas in order to minimize the probability of later compromise.

(7) Prepare appendix 3, *Counterintelligence*, and assist with preparation of appendix 5, *HUMINT*, to the intelligence annex.

(b) Situational Development

(1) Establish liaison with other CI agencies to ensure control of civilians in the area of operations. Screen all civilians working within MAGTF command posts and installations.

(2) Initiate an aggressive CI/HUMINT collection program in response to the MAGTF PIR and IRs developed by the G/S-2 and in support of EEFIs developed by the G/S-3.

(3) Recommend active and passive CI measures to deny the enemy access to potentially lucrative MAGTF targets.

(c) Indications & Warning

(1) Emphasize protective collection activities to reveal plans and intentions of hostile elements to inflict damage and casualties upon friendly forces.

(2) Lessen the chance of surprise by acting as an alarm to hostile intent. Extensive and aggressive CI source networks provide a protective buffer to alert the MAGTF to developments that run counter to previously made assumptions[3].

(d) Support to Force Protection

(1) Contact host nation authorities and persons known to be friendly to the U.S. to collect all available CI information and to aid with screening of local inhabitants.

(2) In conjunction with the MAGTF provost marshall, advise the commander on establishing security against sabotage and terrorism for all military installations and those civilian installations to be kept in operation.

(3) Recommend procedures for all areas vacated by MAGTF units, particularly command posts, to determine if any compromising material has been inadvertently left behind.

(4) Advise the G/S-3 on counter-reconnaissance and OPSEC measures.

(5) Identify necessary restrictions on informing MAGTF personnel about mission details, D-day, H-hour, designated landing beaches, helicopter landing zones, selected objective and other critical friendly force information requirements..

(6) In coordination with the G/S-6 and subordinate commanders, provide assistance with MAGTF communications and information systems security.

(e) Support to Targeting. Supervise the accomplishment of CI operations in accordance with the CI plan. Included are the following:

(1) Exploit sources of information to provide critical intelligence to commanders and planners. Provide pre-targeting surveillance and route reconnaissance enabling the commander to determine the appropriate method and force to be applied against the target.

---

[3] This concept was effectively applied during Somalia operations to identify, with a 95% accuracy rate, the impending attack of opposition elements of U.S. and multinational forces.

(2) Assist with identifying MAGTF security and target vulnerabilities, evaluating the relative importance of each (MAGTF targets may be personalities, organizations, installations or capabilities). Additionally, identify security vulnerabilities of nongovernmental organization, private volunteer organizations, media and other such organizations that are within the MAGTF's AO.

(3) Locate and recover contraband materials, such as arms, explosives, communication equipment, food, medical supplies, or other items not surrendered in accordance with proclamations. This denies critical capabilities to adversaries.

(4) Seize, exploit, and protect CI targets.

(f) Combat Assessment. Continue an aggressive CI/HUMINT collection program in response to the MAGTF PIR and IRs and in protection of MAGTF EEFIs in order to gauge the impact of friendly actions on the enemy and civilian populace and to evaluate the effectiveness of MAGTF security countermeasures.

See appendix G for a list of MAGTF CI planning actions associated with each step of the Marine Corps planning process.

6005. CI Plans and Orders.

a. General. Guidance for the conduct of MAGTF CI operations comes from many sources. The DIA 58 series of manuals and joint publication 2-01.2, *Counterintelligence Support to Joint Operations* (draft) are the principal references for U.S. CI operations and contains policy, direction, guidance, and instruction on how to perform the CI operations, activities and functions in compliance with national directives and security requirements (see appendix G to this publication for a detailed listing of CI and related references). Additionally, since MAGTFs will normally be part of a joint task force or naval expeditionary force, reference to pertinent orders, guidance, and CI TTPs is necessary to identify unique operating concepts and methodologies and support procedures and formats. MAGTF CI plans and orders are prepared by the G/S-2. The intelligence operations officer coordinates the overall effort and with the assistance of the CIHO, other intelligence section staff officers, and the CO/OICs of organic and supporting CI units. MAGTF CI plans and orders appear as an appendix to the intelligence annex of the MAGTF operation plan or order and will focus on internal MAGTF CI requirements, operations and TTP.

b. The CI Appendix. The CI appendix to an operations plan (OPLAN) or operations order (OPORD) will be prepared consistent with format outlined in the Joint Operational Planning and Execution System (JOPES) and appear as Appendix 3 (Counterintelligence Operations) to Annex B (Intelligence) in all operations plans and orders. See appendix C of this publication for a sample CI appendix format. The CI appendix should include the following:

(1) Friendly forces to be utilized including:

(a) Personnel augmentation requirements.

(b) CI units of adjacent or other theater forces and the support expected.

(c) In amphibious operations, JFMCC and amphibious task force CI elements that may provide support to the landing force.

(d) Within JTF operations, pertinent CI capabilities and support from the combatant command's joint intelligence center/joint analysis center, JTF J-2X, JFLCC, JFACC, and other component commanders/task forces.

(2) Planned arrangement, employment, and use of external CI support (to include any special collection, production, dissemination and CIS arrangements.)

(3) Establishment of coordinating instructions for the planning and control of CI operations to include technical support expected from higher headquarters.

(4) Tasking of MAGTF CI elements.

(5) CI production priorities and plans.

(6) CI dissemination priorities and plans, to include communication and information systems support to the MAGTF CI effort.

(7) CI unique equipment and logistics requirements.

(8) An appendix providing MAGTF countersigns challenges and passwords and supporting procedures.

CHAPTER 7

TACTICAL COUNTERINTELLIGENCE ACTIVITIES

7001. MAGTF Counterintelligence Operations

The mission assigned CI/HUMINT Co and its concept of operations depends upon many factors. Major external factors affecting CI/HUMINT Co operations include the mission, commanders' intent, the size and nature of the AO and AOI, operations and intelligence concept of operation, stated PIRs and EEFIs, and C2 of the MAGTF and the JTF. Key internal CI/HUMINT Co factors include the type of team control, various potential employment options, communication and information systems capabilities, and unique CI equipment. Finally, key tasks, such as completing necessary CI surveys/vulnerability assessments, the CI estimate, and development of a CI target-reduction plan, all affect the employment of CI/HUMINT Co.

a. Planning. The successful accomplishment of the company's mission requires thorough planning by the commander. The following must be considered when planning for CI activities:

(1) The intelligence concept of operations, designated PIRs and IRs, and supporting collection, production and dissemination plans.

(2) The force protection concept of operations and designated EEFIs.

(3) Detailed study of available maps and photographs of potential areas of operations.

(4) Study of all available intelligence products about the area of operations and threat.

(5) Location and plotting of all critical CI targets, categorized by personalities, organizations and installations. These are categorized and studied and plans formulated for coverage and reduction. Target priorities must be assigned in advance to ensure efficient use of personnel. The area surrounding a target is studied to determine points where sealing off would be most effective. Streets and approaches to targets are studied thoroughly, thereby minimizing the need for extensive physical reconnaissance. Main traffic routes are studied to determine locations in which to establish screening centers and checkpoints.

(6) Acquisition or development of personalities (black, gray, and white lists), organizations, installations and incidents Databases (POI&I) for the target area.

(7) Study of all available records to identify host country, third party or other officials and leaders within the area of operations that the enemy is hostile to. Also study of other persons who could be of value in administrative assignments. These include members of the local police force, fire

department, post office, railway, telephone, telegraph, and broadcasting stations. Much of this data can be obtained from the U.S. country team, civil affairs units, and various other sources.

(8) Acquisition of available information concerning pro-American or anti-opposition elements. These elements include guerrillas and partisans in the zone of operations and other areas that would facilitate immediate utilization of such groups if necessary.

(9) Acquisition and study of all information concerning other underground forces, groups, and personnel who, by reason of training and experience, can provide assistance in the conduct of CI interrogations.

(10) Other sources of information and intelligence such as CI contingency materials (CICM)[1], MDITDS, DCIIS and the various all-source intelligence databases..

b. Command and Control . CI/HUMINT Co operations will generally be conducted in general support of the MAGTF. Tactical and technical control of CI/HUMINT Co activities is generally centralized under the CI/HUMINT Co commander. CI/HUMINT Co direct support or attachment may be necessary in the following situations:

(1) Where the nature of subordinate units missions require organic CI support.

(2) In those situations where centralized MAGTF control is unfeasible.

c. Tactical Deployment

(1) During both static and fluid tactical situations in populated areas, CI/HUMINT Co headquarters normally is centrally located and easily accessible to indigenous personnel. The headquarters is located to provide maximum assistance to other agencies and to ensure protection by them if required. During high tempo operations, however, the CI/HUMINT Company HQ will be located near the supported unit's main command post, but outside of its key vital area perimeter, in order to enhance security while remaining accessible to key indigenous personnel.

(2) In deploying CI personnel, consideration is given to retaining at least one subteam at the headquarters for special assignments and emergencies.

(3) When CI elements are held in reserve, personnel are organized and equipped so that the augmentation subteams may be immediately dispatched to forward units that require CI support or reinforcements.

---

[1] CI Contingency Materials (CICM) are focused CI analytical products such as sanitized mapping, imagery and reference material available from the MAGTF all-source fusion center's CI analytical team; the theater JIC's CI analytical cell through the combatant command's CISO; and DIA's Operational Intelligence Coordination Center, Counterintelligence Division and Transnational Threat Division.

(4) CI elements are attached to subordinate units sufficiently in advance to coordinate operational, intelligence, communications-information systems and CI plans in support of the units mission and concepts of operations.

7002. CI Screening Operations. CI screening operations are designed to identify and apprehend enemy intelligence agents, subversives, terrorists, and saboteurs attempting to infiltrate friendly lines or conceal themselves among the population. The purpose of CI screening operations is to identify persons of CI interest or verify persons referred by interrogators who are of CI interest, and gather information of immediate CI interest. During conventional combat situations, screening operations primarily consist of screening refugees and EPWs at mobile and static checkpoints in populated areas in cooperation with other MAGTF elements such as military police, interrogator/translators, civil affairs (CA), combat units, and psychological operations teams.

a. Persons of CI Interest. The following are examples of categories of persons of CI interest (this list is not all inclusive):

(1) Persons suspected of attempting to infiltrate through refugee flow.

(2) Line crossers.

(3) Deserters from enemy units.

(4) Persons without identification papers or with forged papers (inconsistent with the norm).

(5) Repatriated prisoners of war and escapees.

(6) Members of underground resistance organizations seeking to join friendly forces.

(7) Collaborators with the enemy.

(8) Target personalities, such as those on the personalities list (black, gray, or white lists).

(9) Volunteer informants.

(10) Persons who must be questioned because they are under consideration for employment with U.S. forces or for appointment as civil officials by CA units.

b. Coordination. CI personnel plan these screening operations, as far as possible, in conjunction with the following:

(1) Commander. The commander is concerned with channeling refugees and EPWs through the AO, particularly in the attack, to prevent any hindrance to unit movement, or any adverse effect on

unit mission. Accordingly, screening operations must be compatible with the supported commander's concept of operations and scheme of maneuver.

(2) Interrogator/Translators. MAGTF interrogator/translator personnel must understand what CI is looking for and have the commander's current PIR, IRs and EEFIs. Close coordination with interrogators is essential for successful CI operations.

(3) Military Police (MP). MP elements are responsible for collecting EPW and civilian internees from capturing units as far forward as possible in the AO. MP units guard the convoys transporting EPW and civilian internees to EPW camps, and command and operate the EPW camps.

(4) Civil Affairs. CA elements are responsible for the proper disposition of refugees.

(5) Psychological Operations (PSYOP). PSYOP elements, under the G3, contribute to screening operations by informing the populace of the need for their displacement.

(6) Local Civil Authorities in Hostile Areas. Civil authorities in hostile areas are included in planning only if control has been returned to them.

c. Preparation

(1) Prior to the operation, CI personnel must become thoroughly familiar with all available information concerning the enemy intelligence organization, the military and political situation within the enemy controlled area, and the geography of the area.

(a) Enemy's Intelligence, Infrastructure and Organization. To successfully identify enemy intelligence agents, CI personnel must be knowledgeable of the enemy intelligence organization, including its mission, methods of operation, officials, schools and training, known agents, equipment, and policies and regulations.

(b) Regulations. Knowledge of the political situation and of the restrictions placed on the population within the enemy controlled area aid in detecting discrepancies during the screening. Information required includes travel restrictions, curfews, draft and conscription regulations, civilian labor forces and work patterns, and the education system.

(c) Enemy Order of Battle. Researching, analyzing and producing order of battle information is primarily the responsibility of the MAGTF G-2 AFC. Collection of order of battle information from human sources is the primary responsibility of the interrogator translators. However, CI personnel must be aware of the enemy military units operating within the area. They must also be knowledgeable of their disposition, composition, activities, training, equipment, history, and commander's personalities. This information aids in identifying military intelligence personnel or other persons attempting to hide their identity.

(d) Area of Operations. CI personnel must also be familiar with the geography and the political, social, and economic conditions of the area. Travel conditions, distances, major landmarks, customs, and composition of the population is essential to the successful screening operation.

(2) Lists and Information Sheets. CI elements should distribute apprehensions lists and information (or basic data) sheets listing indicators of CI interest to the combat units, MPs, or other personnel assisting with the screening operation. Basic data sheets should be tailored to the mission. The basic data sheets are filled out by CI personnel to aid in determining the individual's knowledge and in formulating questions for further interrogation, and provided to the individuals to be screened requiring them to record personal data. This form will aid in formulating the type of questions to be asked and in determining the information needed to satisfy PIRs and IRs. Include the following data, plus anything else judged necessary, on the form[3]:

(a) Full name, aliases, date and place of birth, current and permanent residences, sex, race, religion, marital status, and current citizenship.

(b) The same information as above concerning the father, mother, and siblings, including the occupation and whereabouts of each.

(c) If married, the names of spouse (including female maiden name), date, place of birth (DPOB), nationality, occupation, and personal data on spouse's family.

(d) The individual's education and knowledge of languages.

(e) Political affiliations and membership in other groups or organizations.

(f) Details of the individual's career to include schools, military service, technical and professional qualifications, political affiliations, and foreign travels.

(g) Details of current travel to friendly lines/point of capture, to include point of departure, destination, times, and purpose.

(h) Additional questions may be included which relate to specific indicators revealing areas of CI interest.

d. Initial Screening

(1) The initial screening is designed to identify those persons who are, or are most likely to be, of CI interest and who require interrogation by CI personnel. Initial screening is conducted as soon as

[3] The Geneva Conventions do not require all of this. If the person refuses to give the information, there is nothing that can be done about it. Prepare the form in the native language of the host nation and enemy force, if different, ensuring that it is prepared in the proper dialect of the language.

possible after the EPWs or refugees come under friendly control. EPWs and refugees normally enter EPW and refugee channels rearward of the forward line of own troops for further movement to rear areas. Unit intelligence personnel, interrogators, or CI personnel usually perform the initial screening. In the case of a large number of refugees, military police, civil affairs units, psychological operations personnel, and tactical troops, if available, may provide assistance with initial screening.

(2) Persons identified or suspected to be of CI interest are separated from other EPWs or refugees. After information of immediate tactical value has been obtained from personnel of CI interest, they are referred to CI personnel for interrogation. Personnel of CI interest are exploited, if possible. Then rear area CI elements evacuate them to higher headquarters for further detailed interrogation and exploitation. Further CI screening also continues for other EPWs and refugees at the higher echelons. Procedures for the handling of captured enemy personnel and civilian detainees are contained in MCRP 4-27C, *Enemy Prisoners of War and Civilian Internees*.

e. Conduct of the Screening

(1) The success of the screening operation is influenced by the degree of preparation and the quality of the information provided to CI and other personnel conducting the initial screening. CI interrogation is the method used to confirm or to deny that the person is of CI interest and to exploit the information obtained, when appropriate. CI interrogation is used throughout the entire screening process.

(2) In many cases, numerous EPWs and refugees preclude CI interrogation of every individual. Those persons who are of CI interest are evacuated through CI channels for further interrogation and exploitation by rear area CI elements. During the conduct of the screening process, persons who are determined not to be of CI interest are returned to EPW or refugee channels as appropriate. A screening or an interrogation report is completed on each individual referred for further interrogation. This report clearly identifies those areas of CI interest. It includes as much information as possible concerning the individual's identity and documentation, background, recent activities, and route of travel to friendly lines or point of capture.

(3) CI Screening Report. Appendix E contains formats for the CI screening report and for an interrogation report. The CI screening report should include the following:

(a) Identity. Screen all identifying documents in the form of ID cards, ration cards, draft cards, driver's license, auto registration, travel documents, and passport. Record rank, service number, and unit if a person is, or has been a soldier. Check all this information against the form previously filled out by the detainee if this was done.

(b) Background. The use of the form identified earlier will aid in obtaining the information required; however, certain information areas on the forms will have to be clarified, especially if data indicate a suspect category or the person's knowledge of intelligence information. If the form has not been filled out at this point, try to gain the information through questioning.

(c) Recent Activities. Examine the activities of persons during the days before their detainment or capture. What were they doing to make a living? What connection, if any, have they had with the enemy? Why were they in the MAGTF's area? This line of questioning may bring out particular skills such as those associated with a radio operator, linguist, or photographer. Make physical checks for certain types of calluses, bruises, or stains to corroborate or disprove his story. Sometimes soil on shoes will not match that from the area he claims to come from.

(d) Journey or Escape Route. CI personnel should determine the route the individual took to get to MAGTF lines or checkpoints. Question the individual further on time, distance, and method of travel to determine whether or not the trip was possible during the time stated and with the mode of transportation used. Discrepancies in travel time and distances can be the key to the discovery of an infiltrator with a shallow cover story. By determining what an individual observed enroute, the screener can either check the person's story or pick up intelligence information concerning the enemy forces. Interrogators/translators are well trained in this process and should be called upon for assistance and training.

f. Indicators

(1) Indicators aid with identifying possible hostile infiltrators or other targets of CI interest. They are determined after a thorough study of the enemy area, the political and military situation, and the enemy intelligence organization.

(2) For maximum effectiveness, indicators must relate to designated PIRs and other IRs tasked to CI elements. However, the following general indicators may serve as a guide to identify persons as possible infiltrators:

(a) Persons of military age who are not members of the armed forces.

(b) Persons without identification or with unusual or altered documents.

(c) Persons attempting to avoid detection or questioning, or displaying peculiar activity.

(d) Persons using enemy methods of operation.

(e) Persons possessing unusually large amounts of money, precious metals, or gems.

(f) Persons traveling alone or in pairs.

(g) Persons having a pro-enemy background, family members in enemy area, or who have collaborated with the enemy.

(h) Persons with a suspicious story, who display any peculiar activity, or who have violated regulations in enemy areas.

(i) Persons having technical skill or knowledge.

g. Other Methods of Screening. In addition to interrogation, the following methods of screening EPWs and refugees can be used separately or in combination:

(1) Insertion of informants into EPW compounds and camps; into civilian internee camps; or into refugee centers.

(2) Use of concealed informants at screening collection points.

(3) Use of technical equipment (audio and visual) in holding areas.

(4) Polygraph examination.

(5) Specialized identification equipment.

g. Mobile and Static Checkpoints

(1) Checkpoints are employed in screening operations in populated areas and along routes of travel. Checkpoints are used to detect and prevent enemy infiltration of espionage, sabotage, terrorist, and subversive agents. They are also used to collect information which may not otherwise be available to intelligence units.

(2) Checkpoints are established at key locations throughout the AO where sufficient space is available for conducting searches and assembling the people to be screened. Provision is made for the security of the checkpoint, and personnel are positioned to the front and rear of the checkpoint to apprehend anyone attempting to avoid it. Figure 7-1 depicts a typical checkpoint.

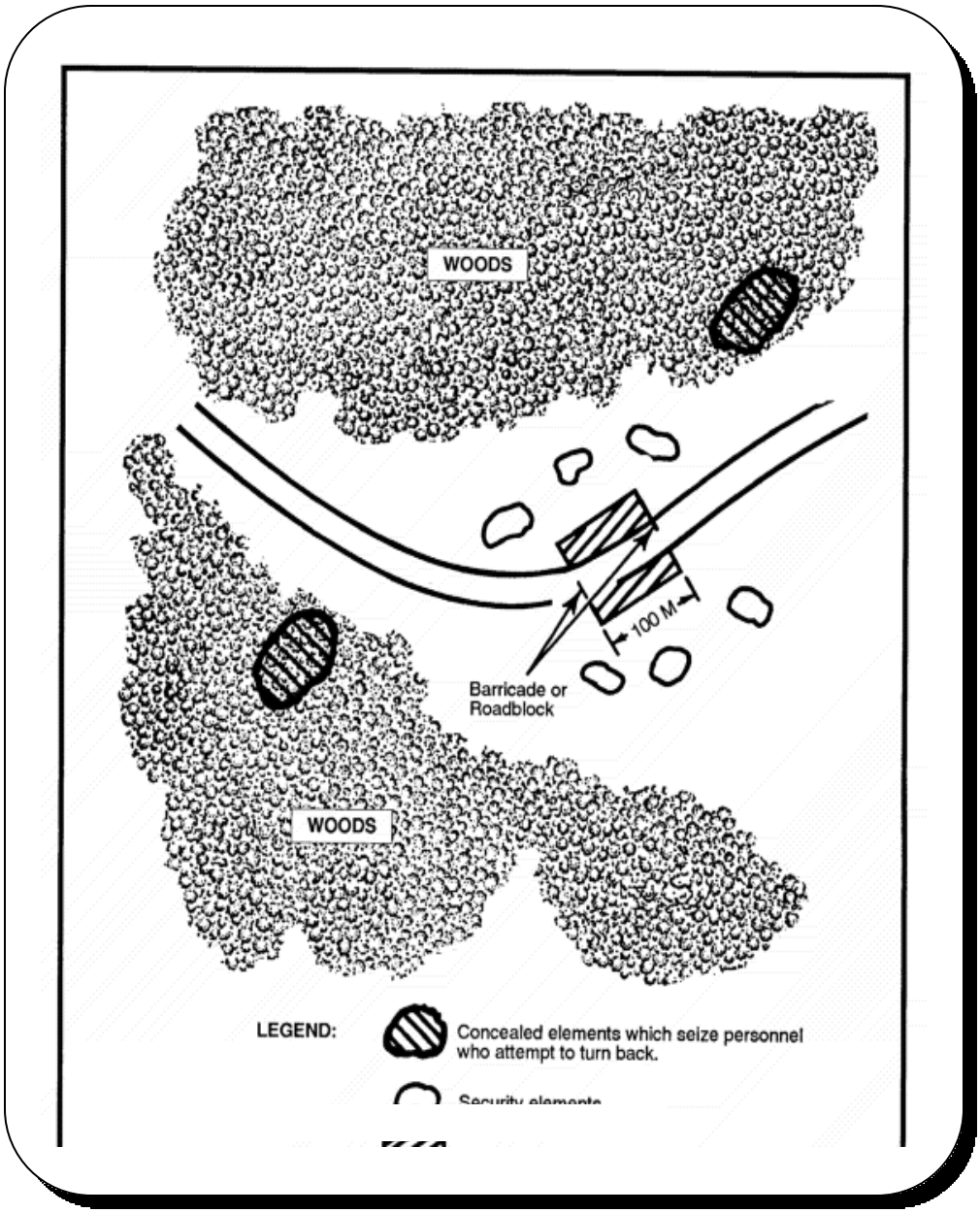


Figure 7-1. Example of a Checkpoint

(3) There are two types of checkpoints employed in a screening operation - mobile and static.

(a) A mobile checkpoint can be used as a moving system. This system consists of the screening team, either mounted in vehicles or on foot, selecting individuals to be stopped for questioning and a check of identity. The mobile checkpoint also may be established at various locations, usually for periods not to exceed one day.

(b) Static checkpoints are those manned permanently by military police or combat troops at entrances to towns, bridges, and other strategic locations.

(4) The preparation for employment of mobile and static checkpoints is the same as for other screening operations. Lists of persons known or suspected of enemy activity (black-detain and gray-of interest lists) and lists of indicators are normally utilized in the screening operation. Specialized detection equipment (e.g., metal or explosive detectors) may also be used, if available.

(5) Screening teams may be composed of combat troops, intelligence interrogators, military police, CI personnel, civil affairs personnel, or a combination of such personnel. Screening teams conduct the initial screening and refer suspects to the CI element for interrogation and further exploitation.

7003. Cordon and Search Operations

a. General

(1) The timely seizure and exploitation of CI targets require a detailed and coordinated plan that has been prepared well in advance. CI elements, in most instances, cannot neutralize, guard, or physically control targets without assistance. In some cases, this assistance must come from ground combat units for the seizure and protection of well-defended targets. In other cases, the assistance may be provided by combat support, combat service support, aviation units or even host country elements. It is essential that the required assistance be provided for during the planning phase.

(2) The senior tactical unit commander will be the individual responsible for the conduct of the cordon and search operation. That commander will plan, with advice from CI, interrogation, CA, and PSYOP personnel, the cordon which is usually deployed at night, and the search which normally begins at first light.

(3) MAGTF CI personnel normally accompany the troops used in cordon and search operations to advise, assist, and examine and/or exploit the target at the earliest possible time. In some instances, it may be advantageous for CI personnel to rendezvous with the assigned troops at the target area. Except in unusual cases, the tactical effort takes precedence over the neutralization and exploitation of CI targets. If assistance in target seizure is not available, CI elements may have to rely on their own assets to neutralize or exploit targets. In friendly controlled areas, CI elements may coordinate through the JTF TFCICA to receive assistance from other service CI elements, civil police and security agencies.

b. Types and Conduct of Cordon and Search Operations

(1) Community Operations. The basic operation is the community cordon and search operation shown in figure 7-2.

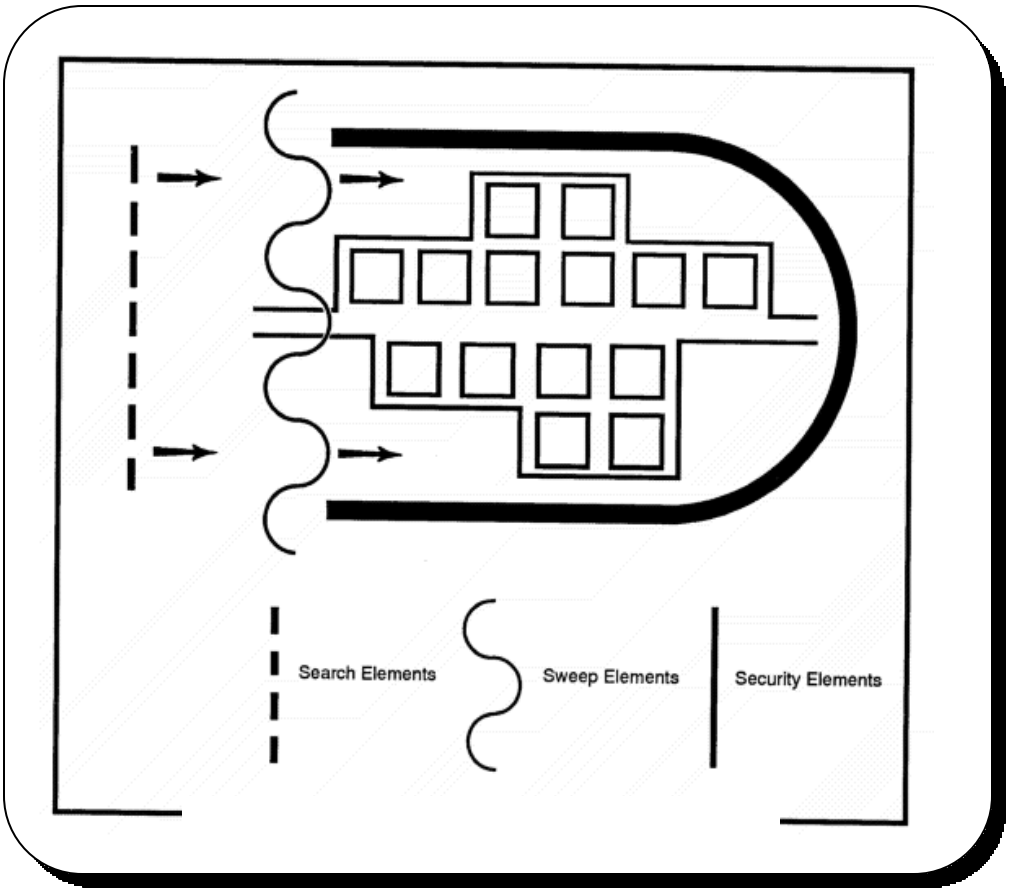


Figure 7-2. Example of a Community Cordon and Search Operation

As the screening element sets up the collection or screening station (see figure 7-3), the sweep element escorts the residents toward the station, leaving behind one resident to care for family belongings, if required by law.

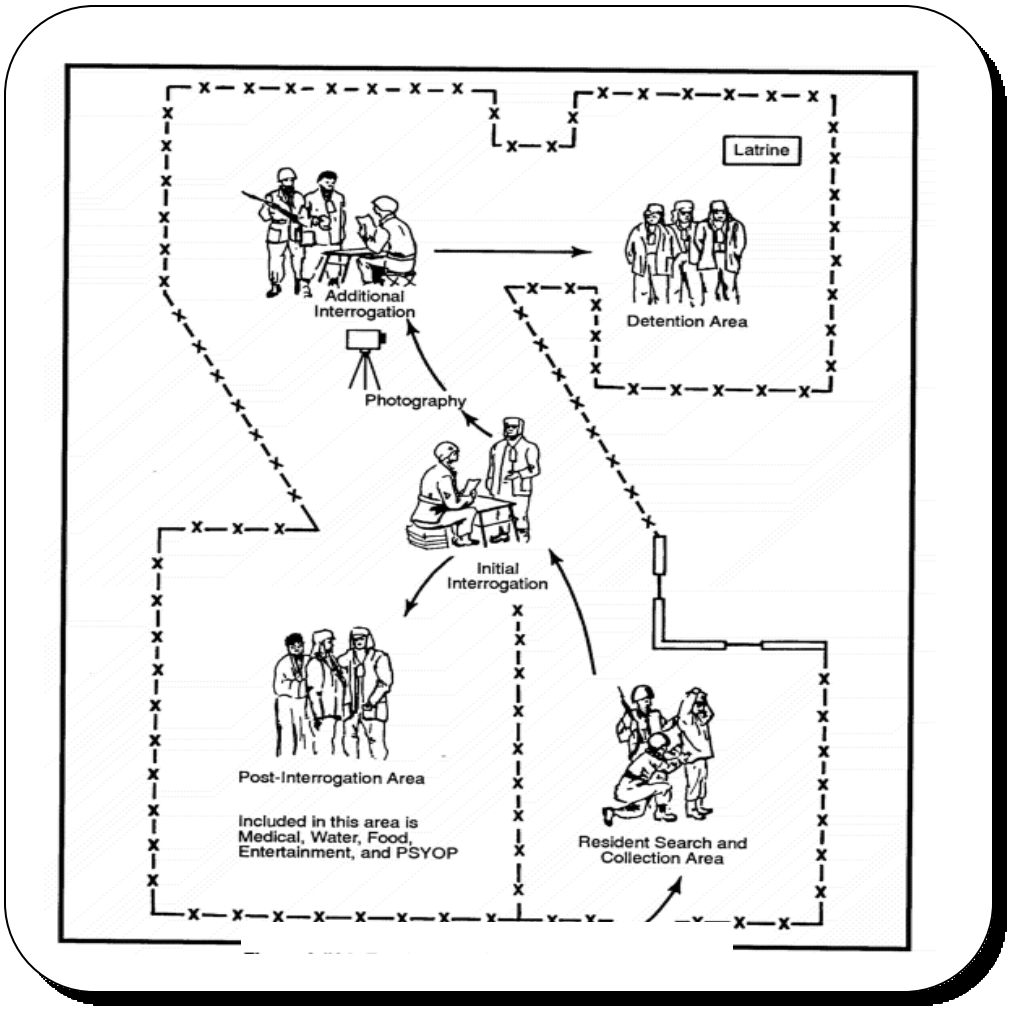


Figure 7-3. Example of a Community Collection Screening Station

(a) The search element follows behind the sweep element searching houses, storage areas, cemeteries and so forth, with dogs and metal detection equipment. CI personnel are searching for evidence of enemy intelligence collection operations to include communications codes or other such paraphernalia. Each search element should include a CI team with an interrogator/translator element as required, which will have a list of persons of CI interest.

(b) In the collection or screening station, bring the residents to the collection area (or holding area) and then systematically lead them to specific screening stations. Enroute to the screening station, search each individual for weapons. Then lead the residents past the mayor or community leaders (enemy defectors or cooperating prisoners who will be hidden from view so that they can uncompromisingly identify any recognizable enemy). These informants will be provided with the means to notify a nearby guard or a screener if they spot an enemy member. Immediately segregate this individual and interrogate by appropriate personnel.

(c) At specific screening stations, ask the residents for identification, check against personalities list (black list), and search for incriminating evidence by electronic equipment.

(d) Move suspected persons on for photographing, further interrogation, or put them in the screening area detention point to be taken back to a base area or interrogation facility for detailed interrogation upon completion of the operation.

(e) Pass innocent residents through to the post screening area where they are provided medical assistance and other civic assistance, as well as entertainment and friendly propaganda.

(f) Return any persons caught attempting to escape or break through the cordon immediately to the detention area.

(g) When the operation is terminated, allow all innocent individuals to return to their homes, and remove the enemy 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.

(2) "Soft" or area operation. The second type of cordon and search operation is very frequently referred to as the "soft" or area cordon and search. This operation includes the cordoning and searching of a rather vast area (for example, a village area incorporating a number of hamlets, boroughs, town, or villages which are subdivisions of a political area beneath country level).

(a) This type of operation requires a larger military force to cordon off the area; a pooling of all paramilitary, police, CA, CI and intelligence resources to conduct search and screening; and a formidable logistical backup. This kind of operation extends over a period of days and may take as long as a week or possibly longer.

(b) 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 each resident is screened, CI personnel will issue documents testifying to the fact that he was screened and if necessary, allow him restricted travel within the area.

(c) Other population and resource control measures are used as well. Such an opportunity may allow the chance to issue new ID cards and photograph all of the area's residents.

(d) As each community screening proceeds, send individuals who were designated for further interrogation to a centralized interrogation center in the cordoned area. Here, CI personnel will work with interrogator/translator personnel, both MAGTF and indigenous, police, and other security service interrogators.

(e) Besides field files and other expedient facilities, a quick reaction force should be located at the interrogation center to react immediately to intelligence developed during the interrogations and from informants planted among the detainees.

7004. Counterintelligence Force Protection Source Operations (CFSO). CFSO's are flexible and aggressive collection operations conducted by CI personnel to quickly respond to the needs of the supported command. CFSO are focused on the collection of force protection information designed to assess threats from foreign intelligence collectors; provide early warning of impending attack; warn of sabotage or subversive activity against U.S. forces; identify and neutralize potential enemy infiltrations; provide information on local security forces; identify population and resorce control measures; locate hostile or insurgent arms caches and safe havens; and identify local insurgent support personnel in regions where local security forces cannot or will not support U.S. operations. Additional policy guidance and procedures for the conduct of CFSOs in support of MAGTF operations is contained in classified MCO 003850.2, *Marine Corps Counterintelligence Force Protection Source Operations*, (U). (See appendix E for the format of a CFSO Concept Proposal).

7005. Tactical CI Interrogation. Within the area of operations, there may be numerous people who are viewed as threats to security based solely on their presence in the combat zone. The number of suspect personnel varies. Frequently, it precludes detailed interrogation of all but a selected few that are of primary interest. CI personnel are partly dependent on such agencies as the provost marshal, civil affairs units, and interrogator-translator platoons to identify suspect persons or persons of CI interest. In some situations, the number of persons volunteering information to CI operations permit concentration on those of the greatest potential interest or value. Most suspects are apprehended while trying to enter the area when their cover stories (which will closely parallel their true places of origin and identities) are exposed. The CI or interrogation personnel's success in such interrogations is primarily dependent on his questioning skill, linguistic ability or support, knowledge of the area of operations and adjacent areas, and familiarity with the intellectual, cultural, and psychological peculiarities of the persons encountered.

a. Types of Subjects. As the battle lines in combat change, entire segments of the population may be overrun. The local population in any area may also be increased by refugees and displaced persons (persons from other countries conscripted by enemy forces for labor). The following categories of persons are of CI interest:

(1) Refugees and displaced persons.

(2) Line crossers.

(3) Deserters from enemy units.

(4) Enemy intelligence personnel.

(5) Inmates of enemy detention camps.

(6) Members of underground resistance organizations seeking to join friendly forces.

(7) Collaborators with the enemy.

(8) Target personalities, such as black, gray, or white list personalities.

(9) Volunteer informants.

(10) Persons who must be questioned because they are under consideration for employment with MARFOR units or for appointment as civil officials.

b. Objectives of CI Interrogators. The CI interrogation in combat areas assists in the accomplishment of three major objectives:

(1) In the screening process, refugees whose very presence threatens overall security are removed from the battlefield.

(2) In detailed interrogations, enemy agents with espionage, sabotage, terrorist, or subversive missions are detected.

(3) The wide range of CI activities and types of interrogations permit the collection of information of value to other intelligence and security agencies and to the planners of military operations. CI interrogators must be especially alert to obtain and report information of immediate tactical value which may not have been previously obtained or reported.

c. Indicators Warranting Suspicion. CI personnel must be alert during interrogations for indications of intelligence activity. The following are indicators which, separately or collectively, may generate suspicion that a subject is in the employ of or acting in sympathy with enemy forces.

(1) Access to Information or Targets. A prospective terrorist, subversive, espionage, or sabotage agent must have access to the information desired by the enemy or to the target installation to be destroyed to carry out his mission. The interrogation should establish a subject's accessibility to potential targets, including his location at the time he was apprehended.

(2) Technical Skills. Proficiency in certain technical skills is frequently an attribute of an espionage or sabotage agent. The subject who has a mastery of one or several foreign languages and a knowledge of radio operation or cryptography is questioned carefully on the nature and purpose of his training in those fields. His practical experience and his work in those fields, during or shortly prior to the war, should give CI personnel cause for strong suspicion. The individual's story then must be closely examined.

(3) Documents and Funds. An overabundance of documents and new documents of questionable authenticity are reason for doubt. They provide the basis for detailed questioning. Discrepancies in the document's contents or conflicts between data and the subject's story may lead to the detection of hostile agents. Unexplainable possession of large amounts of money, valuable jewelry, or other items of great value are investigated carefully.

(4) Pro-Enemy Background. Residence or travel in enemy territory, membership in a hostile party, or known former collaboration with the enemy are facts of obvious importance. CI personnel must determine whether the subject is actually in sympathy with the enemy or has acted merely to serve his own best interests with regard to his life, the welfare of his family, or his property.

(5) Family in Enemy-Held Territory. Enemy pressure is often applied to individuals whose families reside under enemy control. Individuals who have family members threatened with death/torture/incarceration by the enemy will always be a threat to friendly forces.

(6) Inconsistent Story. Small discrepancies in the subject's story may be important. Contradictions in a subject's story do not warrant jumping to conclusions. However, CI personnel must remain alert to all possibilities. Allowances must be made for defective memory or lack of logic due to emotional stress. The following discrepancies may be warning signals to the CI interrogator:

(a) Distance compared to travel time.

(b) Accent peculiar to an area the subject refuses to acknowledge as his own.

(c) Unreasonable explanation of deferment, exemption, or discharge from military service.

(d) Exemption from labor conscription.

(e) Implausible reasons for risking the crossing of combat lines.

(7) Suspicious Actions or Activities. Indigenous persons displaying unusual interest in troop units of equipment or loitering persistently in the vicinity of troop units and installations without reasonable explanation are sufficient to warrant interrogation for the purpose of clarifying the stature of a person so involved.

(a) Violations of Civil or Military Regulations. Mere violation of military regulations in an area controlled by the military may be relatively unimportant to CI elements. These violations may be mandatory registration, curfews, travel restrictions, or declaration of weapons. However, the motives which cause such violations despite severe penalties may be compelling and possibly of great interest to CI personnel.

(b) Modus Operandi (MO). The frequent similarity in tactics of hostile agents working for the same enemy agency, their means of contact with their agent handlers, type of cover story, and

manner of collecting and reporting their information may lead to identification of suspects with a known enemy agency or group. Established patterns of activity or behavior of enemy agents are disseminated to other intelligence and security agencies to assist in the identification of agents still operating.

d. Screening or Initial Interrogation. Initial interrogation and screening are generally synonymous. However, initial interrogation indicates that there will be a follow-up detailed interrogation while screening involves the selection, by brief questioning, of a relatively small number of persons from a large group for detailed interrogation. In both cases, the technique, purpose, and scope of the questioning are generally the same. The object is to select for detailed interrogation a reasonable number of persons who appear to be knowledgeable of matters of CI interest. Initial interrogation or screening is generally concerned with identity, background, recent activities, travel or escape routes, and information of immediate value. Documents and personal belongings of a subject are examined. Then the circumstances of apprehension are studied. Finally the available files are checked.

e. Detailed Interrogation. Detailed CI interrogations may be conducted in Joint Interrogation Facilities or at MAGTF interrogation sites/collection points established by G/S-1s and manned by interrogators and CI personnel. Detailed interrogation does not differ radically from the initial interrogation except that attention is now focused on individuals who are suspect or who are known to have extensive information of interest. A study of the initial interrogation report, examination of the subject's documents and belongings, and checks of available files and information must be conducted and analyses made in preparation for the interrogation.

(1) Details of the subject's personal history must be reviewed. Should the subject admit that he is an enemy agent, he becomes an important source of information on enemy intelligence methods of operation and, perhaps, on identities of other hostile agents. This leads to exhaustive interrogations on such issues as hostile intelligence training and missions assigned. However, CI personnel must be alert to the possible insertion of confusion agents.

(2) The suspect, or any person being interrogated, may also be an important source of information of intelligence value strategic and/or tactical.

(3) The questioning usually follows a logical sequence to avoid confusing the subject and to facilitate reporting. However, an illogical sequence may be used as a technique to purposely confuse the subject so that he inadvertently contradicts himself. The interrogator must be alert for discrepancies and retain his psychological advantage.

(See the paragraph 7006 for additional information on CI interrogations.)

7006. CI Investigations. CI investigations are conducted when sabotage, espionage, spying, treason, sedition, or subversive activity is suspected or alleged. CI investigations may also be conducted regarding security matters and defections of friendly personnel to the enemy. The primary purpose of each investigation is to identify, neutralize, and exploit information of such a nature, form, and reliability, that may determine the extent and nature of action, if any, necessary to counteract the threat and

enhance security. The investigation is a duly authorized, systematic, detailed examination/inquiry to uncover and report the facts of a matter. While facts, hearsay, information, opinions, allegations, and investigators' comments may make a significant contribution, they should be clearly labeled as such in the report of investigation. The Naval Criminal Investigative Service Manual, NIS-3, *Manual for Investigations,* may be used as a guide for investigation techniques and procedures. Investigations are generally incident investigations concerning acts or activities which are committed by, or involve, known or unknown persons or groups of persons. CI agents conducting investigations must have a thorough understanding of the objectives and operations of foreign espionage, sabotage, and subversive organizations.

a. Counterintelligence Investigations. CI investigations use basic investigative techniques and procedures. The primary purpose of the investigation is to provide the commander with sufficient factual information to reach a decision or to ensure the security of his command. Investigations may be conducted overtly or discreetly depending on the type of investigation and the area of operations. Investigations will normally include the examination of records, interviews or interrogations, and the collection and handling of evidence. Surveillance and the conduct of raids and searches may also be appropriate as the investigation progresses.

(1) On assuming primary CI jurisdiction, MAGTF CI investigations are conducted in accordance with guidance and instructions published by higher authority.

(2) CI personnel are normally responsible for conducting security investigations of indigenous personnel employed by MAGTF elements. They may also be involved in the investigation of indigenous personnel retained in official civilian positions.

(a) Certain unique problems are involved in conducting investigations of indigenous personnel in a tactical environment. One problem that may hinder investigation is lack of files and records in the repositories of civilian police and investigative agencies. This documentation may have been destroyed or removed during tactical operations. Every effort must be made to check all files and records which are available.

(b) Another problem may be lack of qualified personnel to perform investigations. Special investigative techniques, such as the use of polygraph examinations by criminal investigative personnel, may be required.

(c) A problem that presents security threat to the MAGTF is the use of indigenous personnel for a wide range of support functions. Indigenous civilian employees may be sympathetic to the enemy's cause or may be coerced to serve the enemy cause. If using indigenous personnel, caution must be exercised to preclude the enemy's collection of useful information, both classified and unclassified. In addition to the initial security investigation, continual checks are made on indigenous employees. CI elements maintain close liaison with civil affairs units responsible for providing civilian labor to the MAGTF.

(d) In the conduct of a CI investigation if evidence or indicators of criminal activity is discovered, this information should be provided to the Criminal Investigation Division of the Provost Marshals Office. The information should only be provided if such disclosure does not compromise the ongoing CI investigation.

b. Investigative Plan. When required, CI personnel formulate an investigative plan at each command level down to and including the individual CI Marine. Normally the lead investigative element will develop the plan. The investigative plan must be updated as new developments arise, including an ongoing analysis of the results. Although this list is not all encompassing, an investigative plan should include as many of the following planning considerations as applicable:

(1) Purpose of the investigation.

(2) Definition of the problem.

(3) Phases or elements of the investigation which have been assigned.

(4) Whether the investigation is to be conducted overtly or discreetly.

(5) Priority and time permitted for completion.

(6) Special instructions or restrictions.

(7) Information from the unit or office files.

(8) Methods and sources used, to include surveillance and polygraph support.

(9) Coordination required.

c. Order of Investigation. All CI investigations vary, and as such, all investigative plans will be different. The following actions are typically conducted during an investigation. Tailor investigative plans to each investigation. Investigative actions selected should be sequenced to ensure a swift and successful completion of the investigation.

(1) Files and records checks for pertinent information.

(2) Individual interviews for additional information and leads.

(3) Exploitation of new leads and consolidation of all available data for analysis and planning a course of action (COA).

(4) Surveillance, both physical and technical, of the subject(s) to be investigated.

(5) Interrogation or interview of the subject(s) to prove or disprove the allegations.

(6) Polygraph examination.

d. Investigative Techniques. CI personnel use the following basic techniques in CI investigations and operations, as appropriate:

(1) Examine records to locate, gain access to, and extract pertinent data from diverse official and unofficial documents and records.

(2) Conduct interviews to obtain information. The type of interviews conducted depend upon the investigation.

(3) Use interrogation and elicitation techniques as additional methods to gather information.

(4) Conduct physical and technical surveillance to augment other investigative activities[4].

(5) Conduct cordon, search and seizure when necessary. Do not conduct searches unless directed by proper authority. CI personnel may coordinate this activity with law enforcement agencies, depending on the nature of the investigation.

e. Files and Records. Checking files and records for pertinent information on the subject of the investigation is the first action in CI investigations. Checks should begin with local unit files and expand to include other possible sources. The full exploitation of records examination as an investigative tool depends on several factors which the CI agent must consider.

(1) CI personnel must know what, where, by whom, and for what purpose records are maintained throughout the AO. Upon assignment to an operational unit, the initial orientation should stress that CI personnel be thoroughly familiar with records that may be of assistance in investigations.

(2) Most records are available to CI personnel upon official request. If all efforts to obtain the desired information through official channels are unsuccessful, the information or records cannot be subpoenaed unless legal proceedings are initiated.

(3) There are occasions when documentary information or evidence is best obtained through other investigative means. The possibility of intentional deception or false information in both official and unofficial records must always be considered. Because data is recorded in some documentary form does not in itself ensure reliability. Many recorded statistics are untrue or incorrect, particularly items of biographical data. They are often repetitious or unsubstantiated information provided by the subject being investigated and are not to be confused with fact.

---

[4] See FM 34-5, (S) *Human Intelligence and Related Counterintelligence Activities,* for a detailed explanation of surveillance operations.

(4) Reliability of records varies considerably according to the area and the status of the agency or organization keeping the records. Records found in highly industrialized areas, for example, are more extensive and generally far more reliable than those found in underdeveloped areas. Until experience with a certain type of record has been sufficient to make a thorough evaluation, treat the information with skepticism.

(5) In CI investigations, the absence of a record is often just as important as its existence. This is especially important in the investigation of biographical data furnished by the subject being investigated. The systematic and meticulous examination of records to confirm or refute the subject's story is very often the best means of breaking the cover story of an enemy intelligence agent.

(6) The types and content of records vary markedly with the AO. Regardless of the area, CI personnel must be aware of the types of records to be used in conducting investigations. Available records include police and security agencies, allied agencies, vital statistics, residence registration, education, employment, citizenship, travel, military service, foreign military records, finance records, and organization affiliation.

(a) Police and Security Agencies. Some major types of records which are often of value are local, regional, and national police agencies. Most nations maintain extensive personality files covering criminals, CI investigative subjects, victims, and other persons who have come to official police attention because of actual or alleged criminal activity. Police interest in precise descriptive details, including photographs and fingerprint cards, often make police records particularly valuable and usually more reliable than comparable records of other agencies. Police and security agency, files are usually divided into subcategories. CI personnel must be familiar with the records system to ensure all pertinent files actually have been checked.

(b) Allied Agencies. Access to records of allied intelligence agencies often depends on the personal relationship between JTF or MAGTF CI personnel and the custodian of the records of interest. Such examinations are normally the assigned responsibility of a CI liaison officer. Liaison also may be necessary with other agencies when the volume of records examinations dictate the need for a single representative of the CI element. At times it may be necessary, due to the sensitivity of a particular investigation, to conceal specific interest in a person whose name is to be checked. In this instance, the name of the individual may be submitted routinely in the midst of a lengthy list of persons (maybe five to seven) who are to be checked.

(c) Vital Statistics. The recording of births, deaths, and marriages is mandatory in nearly every nation, either by national or local law. In newly developed countries, however, this information may be maintained only in family journals, bibles, or in very old records. In any case, confirmation of such dates may be important. The records sought may be filed at the local level, as is usually the case in overseas areas; or they may be kept at the state or regional level, such as with state bureaus of vital statistics in the U.S. Rarely will original vital statistics records on individuals be maintained centrally with a national agency.

(d) Residence Registration. Some form of official residency registration is required in most nations of the world. The residence record may be for tax purposes, in which case it probably will be found on file at some local fiscal or treasury office. When the residence record is needed for police and security purposes, it is usually kept in a separate police file. Residence directories, telephone books, and utility company records also may be used.

(e) Education. Both public and private schools at all levels, from primary grades through universities, have records which can serve to verify background information. The school yearbook or comparable publication at most schools usually contains a photograph and brief resume of the activities of each graduating class member. These books are a valuable record for verification and as an aid to locating leads. Registrar records normally contain a limited amount of biographical data but a detailed account of academic activities.

(f) Employment. Personnel records usually contain information on dates of employment, positions held, salary, efficiency, reason for leaving, attendance record, special skills, and biographical and identifying data. Access to these records for CI agents is relatively simple in the U.S., but may prove difficult in some overseas areas. In such areas, it may be possible to obtain the records through liaison with local civil authorities or through private credit and business rating firms. Depending on the AO, there may be either local, regional, or national unemployment and social security program offices. Records of these offices often contain extensive background material. In most cases, these data represent unsubstantiated information provided by the applicant and cannot be regarded as confirmation of other data obtained from the same individual.

(g) Citizenship. Immigration, nationalization, passport, and similar records of all nations contain data regarding citizenship status. In most instances, an investigation has been undertaken to verify background information contained in such records; therefore, these records are generally more reliable than other types. The records of both official and private refugee welfare and assistance agencies also provide extensive details relating to the citizenship status of persons of CI interest. As a general rule, refugee records (particularly those of private welfare groups) are used as a source of leads rather than for verification of factual data, since they have been found to be unreliable in nearly all AOs.

(h) Travel. A system of access to records of international travel is especially important to overseas CI operations. Such records include customs records, passport and visa applications, passenger manifests of commercial carriers, currency exchange files, transient residence registrations, private and government travel agency records, and frontier control agency files.

(i) Military Service. Records of current and past members of the armed services of most nations are detailed and usually accurate.

(j) Foreign Military Records. Access to foreign military records in overseas areas may be difficult. In cases where it is not possible to examine official records, leads or pertinent information may be obtained from unofficial unit histories, commercially published documents, and files of various veterans organizations. Since listing or claiming military service is a convenient means of accounting for

periods of time spent in intelligence activities or periods of imprisonment, it is frequently a critical item in dealing with possible enemy agents. Special effort must be made to locate some form of record which either confirms or denies an individual's service in a particular unit or the existence of the unit at the time and place the individual claims to have served. Order of battle and personality files of various intelligence services also may be helpful.

(k) Finance Records. Finance records are an important source of information. They may provide information to indicate whether a person is living beyond one's means. They may provide numerous leads such as leave periods and places, and identification of civilian financial institutions.

(l) Organization Affiliation. Many organizations maintain records which may be of value to a particular investigation. Examples are labor unions; social, scientific, and sports groups; and cultural and subversive organizations. CI personnel should research these organizations. But when seeking sources of information, they must be thoroughly familiar with the organization before attempting to exploit it. Organizations are often established as front groups or cover vehicles for foreign intelligence operations.

f. Interrogation Techniques. Interrogation is obtaining the maximum amount of usable information through formal and systematic questioning of an individual. CI interrogations should be conducted by at least two CI personnel.

(1) CI personnel use interrogation techniques when encountering a hostile source or other subject being investigated. The self-preservation instinct is stimulated in an individual who is considered the subject. This deep-rooted reaction is frequently reflected in stubborn resistance to interrogation. The subject may consider the interrogation as a battle of wits where the subject has much to lose. The subject may look upon the CI interrogator as a prosecutor.

(2) When interrogating a subject, CI personnel must keep in mind the two-fold objective of the interrogation:

(a) Detection and prevention of activity that threatens the security of the U.S. Army.

(b) Collection of information of intelligence interest.

(3) When preparing for an interrogation, CI personnel should:

(a) Gather and digest (complete familiarization) all available material concerning the subject and the case.

(b) Be familiar with those legal principles and procedures which may apply to the case at hand. Legal requirements may differ depending on: whether the U.S. is at war or in a military occupation; status of forces agreements; whether the subject being interrogated is a U.S. citizen; or whether the subject is an EPW.

(4) Determine the best way to approach the subject. Previous investigative efforts may have determined that the subject is under great psychological pressure; therefore, a friendly approach might work best. CI personnel should carefully consider the approach and the succeeding tactics, to ensure that nothing the agent does will cause the subject to confess to a crime he or she did not commit.

(5) Before an interrogation, CI personnel must ensure the following:

(a) The interrogation room is available and free of distractions.

(b) If recording equipment is to be used, it is installed and operationally checked.

(c) All participants in the interrogation team are thoroughly briefed on the case and interrogation plan.

(d) Sources or other persons to be used to confront the subject are available.

(e) Arrangements are made to minimize unplanned interruptions.

(f) As appropriate, arrangements are made for the subject to be held in custody or provided billeting accommodations.

(6) When conducting the interrogation, the following points are important:

(a) Use background questioning to provide an opportunity to study the subject face-to-face.

(b) Avoid misinterpretation and impulsive conclusions. The fact that the person is suspected may in itself create reactions of nervousness and emotion.

(c) Do not allow note-taking to interfere with observing the subject's reaction.

(d) Seek out all details concerning the subject's implication in a prohibited activity.

(e) Examine each of the subject's statements for its plausibility, relationship to other statements or to known facts, and factual completeness. Discrepancies which require adjustment frequently weaken the subject's position.

(f) Attempt to uncover flaws in details not considered relevant to the issue; finding the story's weakness is the key to a successful interrogation.

(g) Build up to a planned final appeal as a sustained and convincing attack on the subject's wall of resistance. Eloquent and persuasive reasoning and presenting the facts of the case may succeed where piecemeal consideration of evidence failed to produce a confession. This appeal may be based

on overwhelming evidence, on contradictions, story discrepancies, or the subject's emotional weaknesses.

(h) Obtain a sworn statement if the subject wants to confess. If the subject has been given an explanation of individual rights under Article 31, Uniform Code of Military Justice (UCMJ), or the 5th Amendment to the US Constitution, any unsworn statement normally can be used in court. If the subject is neither a US citizen nor a member of the armed forces, requirements will be stipulated in the unit's SOP.

(7) CI personnel may use polygraph examinations as an aid to CI interrogations and investigations of intelligence operations, but only at the direction of higher headquarters.

g. Elicitation. Elicitation is gaining information through direct communication, where one or more of the involved parties is not aware of the specific purpose of the conversation. Elicitation is a planned, systematic process requiring careful preparation.

(1) Preparation. Always apply elicitation with a specific purpose in mind.

(a) The objective, or information desired, is the key factor in determining the subject, the elicitor, and the setting.

(b) Once the subject has been selected because of his or her access to or knowledge of the desired information, numerous areas of social and official dealings may provide the setting.

(c) Before the approach, review all available intelligence files and records, personality dossiers, and knowledge possessed by others who have previously dealt with the subject. This will help to determine the subject's background, motivation, emotions, and psychological nature.

(2) Approach. Approach the subject in normal surroundings to avoid suspicion. There are two basic elicitation approaches: flattery and provocation. The following variations to these approaches may be used:

(a) By appealing to the ego, self-esteem, or prominence of the subject, you may be able to guide him or her into a conversation on the area of operation.

(b) By soliciting the subject's opinion and by insinuating that he or she is an authority on a particular topic.

(c) By adopting an unbelieving attitude, you may be able to cause the subject to explain in detail or to answer out of irritation. CI personnel should not provoke the subject to the point where rapport is broken.

(d) By inserting bits of factual information on a particular topic, you may be able to influence the subject to confirm and further expound on the topic. Use this approach carefully since it does not lend itself to sudden impulse. Careless or over use of this technique may give away more information than gained.

(f) By offering sincere and valid assistance, you may be able to determine the subject's specific area of interest.

(3) Conversation. Once the approach has succeeded in opening the conversation, devise techniques to channel the conversation to the area of interest. Some common techniques include:

(a) An attempt to obtain more information by a vague, incomplete, or a general response.

(b) A request for additional information where the subject's response is unclear; for example, "I agree; however, what did you mean by...?"

(c) A hypothetical situation which can be associated with a thought or idea expressed by the subject. Many people who would make no comment concerning an actual situation will express an opinion on hypothetical situations.

h. Sabotage Investigations. Sabotage is defined as an act, the intent of which is to damage the national defense structure. Intent in the sabotage statute means knowing that the result is practically certain to follow, regardless of any desire, purpose, or motive to achieve the result. Because the first indication of sabotage normally will be the discovery of the injury, destruction, or defective production, most sabotage investigations involve an unknown person or persons. We expect acts of sabotage, both in overseas AOs and in CONUS, to increase significantly in wartime. Sabotage is a particularly effective weapon of guerrilla and partisan groups, operating against logistic and communications installations in occupied hostile areas, and during insurgencies. Trained saboteurs sponsored by hostile guerrilla, insurgent, or intelligence organizations may commit acts of sabotage. Individuals operating independently and motivated by revenge, hate, spite, or greed may also conduct sabotage. In internal defense or limited war situations where guerrilla forces are active, we must be careful to distinguish among those acts involving clandestine enemy agents, armed enemy units, or dissatisfied friendly personnel. Normally, we categorize sabotage or suspected sabotage according to the means employed. The traditional types of sabotage are incendiary, explosive, and mechanical. In the future, nuclear and radiological, biological, chemical, magnetic, and electromagnetic means of sabotage will pose an even greater threat to military operations. Sabotage investigations require immediate action. The possibility exists that the saboteur may still be near the scene, or that other military targets may require immediate or additional security protection to avoid or limit further damage. We must preserve and analyze the incident scene before evidence is altered or destroyed.

(1) Questions. The investigation must proceed with objective and logical thoroughness. The standard investigative interrogatives apply:

(a) Who -- Determine a list of probable suspects and establish a list of persons who witnessed or know about the act.

(b) What -- Determine what military target was sabotaged and the degree of damage to the target (both monetary and operational).

(c) When -- Establish the exact time when the act of sabotage was initiated and when it was discovered; confirm from as many sources as possible.

(d) Where -- Determine the precise location of the target and its relation to surrounding activities.

(e) Why -- Establish all possible reasons for the sabotage act through the investigation of suspects determined to have had motive, ability, and opportunity to accomplish the act.

(f) How -- Establish the type of sabotage (such as incendiary, explosive, chemical) and determine the procedures and materials employed through investigation and technical examination and analysis.

(2) Investigative Actions. An outline of possible investigative actions which may be used to investigate alleged or suspected sabotage incidents follows:

(a) Obtain and analyze the details surrounding the initial reporting of the incident to the MAGTF PM. Establish the identity of the person reporting the incident and the reasons for doing so. Determine the facts connected with the reported discovery of the sabotage and examine them for possible discrepancies.

(b) Examine the incident scene as quickly as possible. CI personnel must attempt to reach the scene before possible sources have dispersed and evidence has been disturbed. They will help MP personnel protect the scene from disruption. The MP will remove all unauthorized persons from the area, rope off the area as necessary, and post guards to deny entrance and prevent anything from being removed. Although CI personnel should help MP investigators at the sabotage scene, they should not interfere with the crime scene investigation.

(c) Preserve the incident scene by taking notes, making detailed sketches, and taking pictures. Arrange for technical experts to help search the scene and collect and preserve physical evidence and obtain all possible clues. Arson specialists, explosives experts, or other types of technicians may be required. Take steps to prevent further damage to the target and to safeguard classified information or material.

(d) Interview sources and obtain sworn statements as soon as possible to reduce the possibility of forgetting details or comparing stories.

(e) Determine the necessary files to be checked. These will be based on examination of the incident scene and by source interviews. CI conducts such action only in coordination with the MAGTF PM, which retains sabotage scene expertise and responsibility.

.

(3) Files checks should include background information on sources and the person or persons who discovered or reported the sabotage. Files of particular importance may include:

(a) Friendly unit modus operandi (MO) files.

(b) Partisan, guerrilla, or insurgent activity files.

(c) Local police files on arsonists.

(d) Local police MO files.

(e) Host country's intelligence agency MO files.

(f) Terrorist modus operandi files.

(g) Provost marshal files.

(4) Study all available information such as evidence, technical and laboratory reports, statements of sources, and information from informants in preparation for interrogation of suspects.

i. CI Walk-in Interviews. A walk-in is defined as an individual who seeks out MAGTF authorities to volunteer information which is believed to be of intelligence value. The primary concern of CI personnel is to obtain all information, both of intelligence and CI value. They must be alert to detect whether the source provides leads for further exploitation.

(1) Motivation. When interviewing such persons, CI personnel must consider the source's motives for divulging information. The motivation may not always be known, and sources may not always be truthful about their motives. If the motive can be determined early in the interview, however, it can be valuable in evaluating the information supplied and in determining the nature and extent of the source's knowledge and credibility. Motivation includes, but is not limited to: ideology, personal gain, protection of self or family ties, fear, misunderstanding of the function and mission of the MAGTF, mental instability, and revenge.

(2) Preparation. In preparing for and conducting a Walk-in Interview, CI personnel:

(a) Should adapt to the intellectual level of the source, exercise discretion, and avoid controversial discussions.

(b) Must obtain all names and whereabouts of other individuals who may directly or indirectly know the same information.

(c) Must remember security regulations and make no commitments which cannot be fulfilled.

(3) Conduct of a Walk-In Interview. Put the Source at ease. After determining that a walk-in source has information of intelligence value, display the appropriate credentials.

(a) Take the source to a private place to conduct the interview. The initial attitude frequently affects the success of the interview. The atmosphere should be pleasant and courteous, but professional. In accordance with the Privacy Act of 1974, the source must be given a four point Privacy Act Advisement to include authority, principle purpose, routine uses, and voluntary and mandatory disclosure, prior to the CI agent obtaining the source's personal information. Ask the source for some form of identification, preferably one with a picture.

(b) Record the pertinent data from the ID card and tactfully exit the room.

(c) Using the identity information just obtained from the source, check the office source or informant files to see what, if any, information on the source is on file. Determine if the source is listed as a crank, has a criminal record, or has reported information in the past, and if so, what was the validity and value of that information.

(d) If the source is listed as a crank or a nuisance continue with the interview, but include this information in the appropriate memorandum.

(e) Let the source tell the story. Suggest that the source start the story from the beginning, using the Source's own words. Once started, let the Source talk without interruption. CI personnel should, however, guide the source back if the he strays from the basic story. From time to time, interject a word of acknowledgment or encouragement. At no time, however, should CI personnel give any indication of suspicion or disbelief, regardless of how incredulous the story may seem. While the source gives an account for the first time, take minimal notes. Taking notes could distract the source or the CI interviewer. Instead, pay close attention and make mental notes of the salient points as a guide for subsequent detailed interviewing.

(f) Review the story with the source and take notes. Once the source has finished telling the basic story, he or she generally will freely answer specific questions on the details. Being assured that the information will be kept in strict confidence, the source will be less apprehensive of your note taking. Start at the beginning and proceed in a chronological order, using the salient features of the source's account. Interview the source concerning each detail in the account so that accurate, pertinent information is obtained, meticulously recorded, and that the basic interrogatives are answered for every situation. This step is crucial.

(g) Develop secondary information. The story and background frequently indicate that the source may have further information of significant intelligence interest. Also develop this information fully.

(h) Terminate the interview. When certain that the source has no further information, close the interview in a manner which leaves a favorable impression. At this point in the interview, ask the source, point blank, what motivated him or her to come in and report the information, even if the source volunteered a reason earlier in the interview. Obtain a sworn statement from the Source, regarding the information, if appropriate. It is best to have the Source write (or type) the statement. Advise the source of the Privacy Act of 1974 and, if the source is a U.S. citizen, ask for full name, rank (for military or DOD civilian personnel) or occupation for non-DOD personnel, duty position, unit of assignment (for military or DOD civilian personnel), social security number, date and place of birth (required for military or DOD civilian personnel, requested for non-DOD personnel), type of security clearance and level of access, and full current address. Determine who else knows about the incident or situation, either directly or indirectly. Determine the source's desires regarding the release of the source's identity. Determine the source's willingness to be recontacted by CI personnel or those from another agency should the need arise regarding the information provided. Obtain recontact information from the source (work or residence). Have the source execute a disclosure warning and attach the affirmation to the report as an exhibit. Finally, express appreciation for the information received.

7007. Captured Material Exploitation. If the situation permits, CI personnel should exploit enemy installations immediately following its neutralization or capture. The installation is searched thoroughly for documents, equipment, and other material of intelligence or CI interest[5], which will marked and rapidly transported to MAGTF interrogator/translators (see figure 7-4 for an example of a captive/document/equipment tag). In some instances, it may be desirable to retain the documents or material within the installation for thorough examination by technical intelligence personnel or other specialists. Due to the risks of boobytraps, mines, and explosives, extreme caution must be used when searching installations known or suspected to have been occupied by the enemy.

---

[5] Procedures for the disposition of enemy documents and material will be contained in MCWP 2-15.5, *Human Resource Intelligence*, planned for publication by the end of FY99.

DO NOT REMOVE TAG FROM CAPTIVE/DOCUMENT/EQUIPMENT

DOCUMENT TAG	INSTRUCTIONS
	(Document Tag)
TAG NUMBER_____	1. Complete lower half of tag for each document or group of documents captured from one individual or location.
DATE/TIME OF CAPTURE__ _____	
PLACE OF CAPTURE (coord.) _____	2. Wrap document to prevent loss or damage.
DOCUMENTS FOUND ON:	3. Securely affix tag to document.
__CAPTIVE	4. If captured from other than an individual, evacuate through intelligence channels.
__OTHER (Describe)_____ _____	
_____	Additional information:_____
CAPTURING UNIT_____	_____
_____	_____

DO NOT REMOVE TAG FROM CAPTIVE/DOCUMENT/EQUIPMENT

Figure 7-4. Captive/Document/Equipment Tag

7008. CI Technical Collection and Investigative Techniques. Technical collection and investigative techniques can contribute materially to the overall CI investigation and activities. They can assist in supplying the commander with factual information on which to base decisions concerning the security of the command. CI investigators selectively a variety of technical investigative techniques, of which the following are those most typically employed in support of MAGTF operations: electronic surveillance; investigative photography and videotaping; polygraph, and technical surveillance countermeasures (TSCM).

a. Electronic Surveillance. Electronic surveillance is the use of electronic devices to monitor conversations, activities, sound, or electronic impulses. It is an aid in conducting CI investigative activities. Various constitutional and directives regulate the use of wiretapping and electronic eavesdropping and must be strictly adhered to by CI personnel.

(1) Technical Surveillance Methodology. Technical surveillance methodology (including those which may be employed by enemy intelligence and security forces) consists of:

(a) Pickup Devices. A typical system involves a transducer (such as a microphone, video camera, or similar device) to pick up sound or video images and convert them to electrical impulses. Pickup devices are available in practically any size and form. They may appear to be common items, such as fountain pens, tie clasps, wristwatches, or household or office fixtures. It is important to note that the target area does not have to be physically entered to install a pickup device. The availability of a power supply is the major limitation of pickup devices. If the device can be installed so its electrical power is drawn from the available power within the target area, there will be minimal, if any, need for someone to service the device.

(b) Transmission Links. Conductors carry the impulses created by the pickup device to the listening post. In lieu of conductors, the impulses can go to a transmitter which converts the electrical impulses into a modulated radio frequency (RF) signal for transmission to the listening post. The simplest transmission system is conventional wire. Existing conductors, such as used and unused telephone and electrical wire or ungrounded electrical conduits, may also be used. The development of miniature electronic components permits the creation of very small, easily concealed RF transmitters. Such transmitters may operate from standard power sources or may be battery operated. The devices themselves may be continuously operated or remotely activated.

(c) Listening Posts. A listening post consists of an area containing the necessary equipment to receive the signals from the transmission link and process them for monitoring or recording. Listening posts use a receiver to detect the signal from an RF transmission link. The receiver converts the signal to an audio-video frequency and feeds it to the monitoring equipment. Use any radio receiver compatible with the transmitter. Receivers are small enough to be carried in pockets and may be battery operated. For wire transmission links only, a tape recorder is required. You can use many commercially available recorders in technical surveillance systems. Some of these have such features as a voice actuated start-stop and variable tape speeds (extended play). They may also have automatic volume control and can be turned on or off from a remote location.

(2) Telephone Monitoring. Monitoring telephone conversations is one of the most productive means of surreptitious collection of information. Because a telephone is used so frequently, people tend to forget that it poses a significant security threat. Almost all telephones are susceptible to "bugging" and "tapping."

(a) A bug is a small hidden microphone or other device used to permit monitoring of a conversation. It also allows listening to conversations in the vicinity of the telephone, even when the telephone is not in use.

(b) A telephone tap is usually a direct connection to the telephone line which permits both sides of a telephone conversation to be monitored. Tapping can be done at any point along the line, for example, at connector blocks, junction boxes, or the multiwire cables leading to a telephone exchange

or dial central office. Telephone lineman's test sets and miniature telephone monitoring devices are examples of taps. Indirect tapping of a line, requiring no physical connection to the line, may also be accomplished.

(c) The most thorough check is not absolute insurance against telephone monitoring. A dial central office or telephone exchange services all telephone lines. The circuits contained within the dial central office allow for the undetected monitoring of telephone communications. Most telephone circuits servicing interstate communications depend on microwave links. Communications via microwave links are vulnerable to intercept and intelligence exploitation.

(3) Miscellaneous. Current electronic technology produces technical surveillance devices that are extremely compact, highly sophisticated, and very effective. Miniaturized technical surveillance systems are available. They can be disguised, concealed, and used in a covert or clandestine manner. The variations of their use are limited only by the ingenuity of the technician. Equipment used in technical surveillance systems varies in size, physical appearance, and capacity. Many are identical to, and interchangeable with, components of commercially available telephones, calculators, and other electronic equipment.

b. Investigative Photography and Video Recording. Photography and video recording in CI investigations includes:

(1) Identification of Individuals. CI personnel perform both overt and surreptitious photography and video recording.

(2) Recording of Incident Scenes. CI personnel photograph overall views and specific shots of items at the incident scene.

(3) Recording Activities of Suspects. CI personnel use photography and video recording to provide a record of a suspect's activities observed during surveillance or cover operations.

c. Polygraph. The polygraph examination is a highly structured technique conducted by specially trained CI personnel certified by proper authority as polygraph examiners. DOD Dir 5210.48, *DOD Polygraph Program*, provides guidance for the polygraph program generally.

(1) When Used. Do not conduct a polygraph examination as a substitute for securing evidence through skillful investigation and interrogation. The polygraph examination is an investigative aid and can be used to determine questions of fact, past or present. CI personnel cannot make a determination concerning an individual's intentions or motivations, since these are states of mind, not fact. However, consider the examination results along with all other pertinent information available. Polygraph results will not be the sole basis of any final adjudication.
The conduct of the polygraph examination is appropriate, with respect to CI investigations, only:

(a) When all investigative leads and techniques have been completed as thoroughly as circumstances permit.

(b) When the subject of the investigation has been interviewed or thoroughly debriefed.

(c) When verification of the information by means of polygraph is deemed essential for completion or continuation of the investigation.

(d) To determine if a person is attempting deception concerning issues involved in an investigation.

(e) To obtain additional leads concerning the facts of an offense, the location of items, whereabouts of persons, or involvement of other, previously unknown individuals.

(f) To compare conflicting statements.

(g) To verify statements from witnesses or subjects.

(h) To provide a just and equitable resolution of a CI when the subject of such an investigation requests an exculpatory polygraph in writing.

(2) Phases. The polygraph examination consists of three basic phases: pretest, intest, and posttest.

(a) During the pretest, appropriate rights advisement are given and a written consent to undergo polygraph examination is obtained from all examinees who are suspects or accused. Advise the examinee of the Privacy Act of 1974 and the voluntary nature of examination. Conduct a detailed discussion of the issues for testing and complete the final formulation of questions to be used during testing.

(b) During the intest phase, ask previously formulated and reviewed test questions and monitor and record the examinee's responses by the polygraph instrument. Relevant questions asked during any polygraph examination must deal only with factual situations and be as simple and direct as possible. Formulate these questions so that the examinee can answer only with a yes or no. Never use or ask unreviewed questions during the test.

(c) If responses indicate deception, or unclear responses are noted during the test, conduct a posttest discussion with the examinee in an attempt to elicit information from the examinee to explain such responses.

(3) Outcomes. A polygraph examiner may render one or more of four possible opinions concerning the polygraph examination:

(a) No Opinion (NO) -- rendered when less than two charts are conducted concerning the relevant issues, or a medical reason halts the examination. Normally, three charts are conducted.

(b) Inconclusive (INCL) -- rendered when there is insufficient information upon which to make a determination.

(c) No Deception Indicated (NDI) -- rendered when responses are consistent with an examinee being truthful regarding the relevant areas.

(d) Deception Indicated (DI) -- when responses are consistent with an examinee being untruthful to the relevant test questions.

(4) Factors Affecting Polygraph Results. Certain mental or physical conditions may influence a person's suitability for polygraph examination and affect responses during testing. CI personnel should report any information they possess concerning a person's mental or physical condition to the polygraph examiner before scheduling the examination. Typical conditions of concern are:

(a) Mental disorders of any type.

(b) Any history of heart, respiratory, circulatory, or nervous disorders.

(c) Any current medical disorder, to include colds, allergies, or other conditions (such as pregnancy or recent surgery).

(d) Use of drugs or alcohol before the examination.

(e) Mental or physical fatigue.

(f) Pain or physical discomfort

.

(5) Conducting the Polygraph

(a) To avoid such conditions as mental or physical fatigue, do not conduct prolonged or intensive interrogation or questioning immediately before a polygraph examination. CI personnel tell the potential examinee to continue taking any prescribed medication and bring it to the examination. Based on information provided by CI personnel and the examiner's own observations, the polygraph examiner decides whether or not a person is fit to undergo examination by polygraph. When CI personnel ask a person to undergo a polygraph examination, the person is told that the examination is voluntary and that no adverse action can be taken based solely on the refusal to undergo examination by polygraph. Further, the person is informed that no information concerning a refusal to take a polygraph examination is recorded in any personnel file or record.

(b) CI personnel will make no attempt to explain anything concerning the polygraph instrument or the conduct of the examination. If asked, they should inform the person that the polygraph examiner will provide a full explanation of the instrument and all procedures before actual testing and that all test questions will be fully reviewed with the potential examinee before testing.

(c) Conduct polygraph examinations in a quiet, private location. The room used for the examination must contain, as a minimum, a desk or table, a chair for the examiner, and a comfortable chair with wide arms for the examinee. The room may contain minimal, simple decorations; must have at least one blank wall; and must be located in a quiet, noise-free area. Ideally, the room should be soundproof. Visual or audio monitoring devices may be used during the examination; however, the examiner must inform the examinee that such equipment is being used and whether the examination will be monitored or recorded in any manner.

(d) Normally, only the examiner and the examinee are in the room during examination. When the examinee is an accused or suspect female and the examiner is a male, a female witness must be present to monitor the examination. The monitor may be in the examination room or may observe through audio or visual equipment, if such is available.

(e) On occasion, CI personnel must arrange for an interpreter to work with the examiner. The interpreter must be fluent in English and the required language, and have a security clearance appropriate to the classification of material or information to be discussed during the examination. The interpreter should be available in sufficient time before the examination to be briefed on the polygraph procedures and to establish the proper working relationship.

(6) Miscellaneous. CI personnel will not prepare any agent reports concerning the results of a polygraph examination. This does not include information derived as a result of pretest or posttest admissions, nor does it include those situations where CI personnel must be called upon by the examiner to question the subject concerning those areas which must be addressed before the completion of the examination.

d. Technical Surveillance Countermeasures (TSCM)

(1) TSCM versus TEMPEST. TSCM is concerned with all signals leaving a sensitive or secure area, to include audio, video, and digital or computer signals. There is a definite distinction between TSCM and TEMPEST.

(a) TEMPEST is the unintentional emanation of electronic signals outside a particular piece of equipment. Information systems, computers, and electric typewriters create such signals. The words to focus on in TEMPEST are "known" and "unintentional" emanations. TEMPEST is controlled by careful engineering or shielding.

(b) TSCM is concerned with the intentional effort to gather intelligence by foreign intelligence activities by impulsing covert or clandestine devices into a U.S. facility, or modifying existing equipment

within that area. For the most part, intelligence gained through the use of technical surveillance means will be accurate, as people are unaware they are being monitored. At the same time, the implanting of such technical surveillance devices is usually a last resort.

(2) Threat. Enemy intelligence and security forces, their agents, and other persons use all available means to collect sensitive information. One way they do this is by using technical surveillance devices, commonly referred to as "bugs" and "taps." Such devices have been found in U.S. facilities worldwide. Security weaknesses in electronic equipment used in everyday work have also been found worldwide. The enemy easily exploits these weaknesses to collect sensitive or classified conversations as well as the information being processed. They are interested in those things said in (supposed) confidence, since they are likely to reveal future intentions. It should be stressed that the threat is not just audio, but video camera signals, as well as data. Devices are usually placed to make their detection almost impossible without specialized equipment and trained individuals.

(3) The TSCM Program. The purpose of the TSCM program is to locate and neutralize technical surveillance devices that have been targeted against U.S. sensitive or secure areas. The TSCM program is designed to identify and enable the correction of exploitable technical and physical security vulnerabilities. The secondary, and closely interrelated purpose, is to provide commanders with a comprehensive evaluation of their facilities' technical and physical security postures. DODINST 5240.5, *DOD Technical Surveillance Countermeasures Survey Program*", OPNAVINST C5500.46, "*Technical Surveillance Countermeasures*, and MCO 5511.11D, *Technical Surveillance Countermeasures Program*, govern the implementation of this program.

(a) The TSCM program includes four separate functions; each with a direct bearing on the program.

➢ Detection. Realizing that the threat is there, the first and foremost function of the TSCM program is to detect these devices. Many times these devices cannot be easily detected. Occasionally, TSCM personnel will discover such a device by accident. When they discover a device, they must neutralize it.

➢ Nullification. Nullification includes both passive and active measures used to neutralize or negate devices that are found. An example of passive nullification is soundproofing. But soundproofing that covers only part of a room is not very helpful. Excessive wires must be removed, as they could be used as a transmission path from the room. Nullification also refers to those steps taken to make the emplacement of technical surveillance systems as difficult as possible. An example of active nullification is the removal of a device from the area.

➢ Isolation. The third function of the TSCM program is isolation. This refers to limiting the number of sensitive or secure areas and ensuring the proper construction of these areas.

➢ Education. Individuals must be aware of the foreign intelligence threat and what part they play should a technical surveillance device be detected. Additionally, people need to be alert to

what is going on in and around their area, particularly during construction, renovations, and installation of new equipment.

(b) The TSCM program consists of CI technical investigations and services (such as surveys, inspections, pre-construction advice and assistance) and technical security threat briefings. TSCM investigations and services are highly specialized CI investigations and are not be to confused with other compliance-oriented or administrative services conducted to determine a facility's implementation of various security directives.

➢ TSCM Survey. This is an all-encompassing investigation. This investigation is a complete electronic, physical, and visual examination to detect clandestine surveillance systems. A by-product of this investigation is the identification of physical and technical security weaknesses which could be exploited by enemy intelligence forces.

➢ TSCM Inspection. Normally, once a TSCM survey has been conducted, it will not be repeated. If TSCM personnel note several technical and physical weaknesses during the survey, they may request and schedule an inspection at a later date. In addition, they will schedule an inspection if there has been an increased threat posed to the facility or if there is some indication that a technical penetration has occurred in the area. No facility, however, will qualify automatically for recurrent TSCM support.

➢ TSCM Pre-construction Assistance. As with other technical areas, it is much less expensive and more effective to build in good security from the initial stages of a new project. Thus, pre-construction assistance is designed to help security and construction personnel with the specific requirements needed to ensure that a building or room will be secure and built to standards. This saves money by precluding costly changes later on.

(c) Request for TSCM Support

➢ Requests for, or references to, a TSCM investigation will be classified SECRET, marked with the protective security marking, and receive limited dissemination (to include no dissemination to any non-U.S. recipient). The fact that support is scheduled, in progress, or completed, is classified SECRET.

➢ No request for TSCM support will be accepted via nonsecure means. Nonsecure telephonic discussion of TSCM support is prohibited.

➢ All requests will be considered on a case-by-case basis and should be forwarded through the chain of command via the unit's intelligence officer or security manager.

➢ When requesting or receiving support, the facility being inspected must be complete and operational, unless requesting pre-construction advice and assistance. If any additional equipment goes into the secure area after the investigation, the entire area is suspect and the investigation negated.

➢ Fully justified requests of an emergency nature, or for new facilities, may be submitted at any time, but should be submitted at least 30 days before the date the support is required.

(d) Compromises. The compromise of a TSCM investigation or service is a serious security violation with potentially severe impact on national security. Do not compromise the investigation or service by any action which discloses to unauthorized persons that TSCM activity will be, is being, or has been conducted within a specific area. Unnecessary discussion of a TSCM investigation or service, particularly within the subject area, is especially dangerous. If a listening device is installed in the area, such discussion can alert persons who are conducting the surveillance and permit them to remove or deactivate their devices. When deactivated, such devices are extremely difficult to locate and may require implementation of destructive search techniques. In the event a TSCM investigation or service is compromised, the TSCM team chief will terminate the investigation or service at once. Report the circumstances surrounding the compromise of the investigation or service to the supported unit's or installations intelligence officer or security manager.

(e) Completion. When a TSCM survey or inspection is completed, the requester is usually given reasonable assurance that the surveyed area is free of active technical surveillance devices or hazards.

➢ TSCM personnel inform the requester about all technical and physical security vulnerabilities with recommended regulatory corrective actions.

➢ The requester should know that it is impossible to give positive assurance that there are-no devices in the surveyed area.

➢ The security afforded by the TSCM investigation will be nullified by the admission to the secured area of unescorted persons who lack the proper security clearance. The TSCM investigation will also be negated by: (a) Failing to maintain continuous and effective surveillance and control of the serviced area; (b) allowing repairs or alterations by persons lacking the proper security clearance or not under the supervision of qualified personnel; and (c) introducing new furnishings or equipment without a thorough inspection by qualified personnel.

(f) Subsequent Security Compromises. Report immediately to the intelligence officer or security manager the discovery of an actual or suspected technical surveillance device via a secure means. All information concerning the discovery will be handled at a minimum of SECRET. Installation or unit security managers will request an immediate investigation by the supporting CI unit or supporting TSCM element.

7009. Counterintelligence Surveys/Vulnerability Assessments, Evaluations, and Inspections

a. Tactical Operations. During operations, CI surveys/vulnerability assessments, evaluations, and inspections, including TSCM inspections and surveys, are usually limited to permanent installations in

rear areas or to key MAGTF C2 facilities. Purely physical security surveys and inspections not falling under the cognizance of CI are conducted by trained physical security specialists under the purview of the MAGTF PMO. In those instances where perimeter security is the responsibility of a tactical unit, the physical security portion of the CI survey is primarily concerned with those areas within the perimeter containing classified material and areas susceptible to sabotage and terrorist attack. Special weapons sites require extra emphasis and may include CI monitoring of shipments in addition to other security services. Close and continuous liaison and coordination should be conducted with the local PMO during any CI survey, with the exception of a TSCM survey, to ensure complete coverage of the physical security aspects and any other areas with which the PMO may assist. See appendix E for a CI survery/vulnerability assessment checklist and the format for a CI survery/vulnerability assessment report.

b. Garrison Counterintelligence Inspections

(1) CI inspections are performed by commanders to determine compliance with established security policies and procedures. CI credentials are intended for use of personnel on official CI mission. CMC(CIC) is designated as the office of record for CI credentials. Credentials are not transferable and may not be reproduced nor altered. Credentials are only issued to personnel who have completed a formal course of instruction in CI which qualified them for MOS 0204/0210/0211. The presentation of CI credentials certifies the bearer as having a TOP SECRET security clearance and special compartmented information (SCI) access. Personnel are directed to render all assistance to properly identified CI personnel in the performance of their duties. CI personnel, while in the performance of their official duties are authorized access to all spaces (see MCO 3850.1H, *Counterintelligence, and* SECNAV 5510.1H for additional amplification). The commander is overall responsible for security within his command, however these responsibilities are executed by a variety of personnel to include the Command Security Manager, Intelligence Officer, Operations Officer, Classified Material Control Center (CMCC) Custodian and COMSEC Material System (CMS) Custodian. The scope of the inspection will vary depending on its type and purpose. Inspections may include the following:

(a) Determine if assigned personnel with access to classified material are properly cleared.

(b) Determine if classified material is properly safeguarded by assigned personnel.

(c) Examination of facilities and containers used for storing classified material to determine adequacy.

(d) Examination of procedures for controlling entrances and exits, guard systems, and special guard instruction relating to security of classified material and sensitive areas.

(e) Examine the security and control of unit communications and information resources.

(f) Provide back brief to command security/intelligence personnel and formal results as required.

(2) Command inspections include announced and unannounced inspections.

(a) Announced Inspections. An announced inspection is one that has been publicized. All personnel concerned are aware of the inspection schedule and make preparations as necessary. Inspections are conducted on a recurring basis to ensure security standards remain at a high level. The announced inspection is often accomplished with inspections conducted by the inspection staff of the common or a senior headquarters.

(b) Unannounced Inspections. The unannounced inspection is conducted to determine compliance with security policies and procedures at a time when special preparations have not been made. The unit or section to be inspected is not informed in advance of the inspection. The inspection may be conducted at any time during or after normal working hours.

7010. CI Support to the Crisis Action Team Intelligence Cell. When an intelligence cell is established in response to a terrorist threat or incident, CI personnel jointly man it with CID, NCIS, and if required, civilian law enforcement agents. The intelligence cell coordinates the intelligence, investigative, and criminal information needs of the installation and the on-scene operational commander. It should be separate from both the operations center and the crisis management force/on-scene commander but linked to both by a side variety of wire and wireless communications means, including a direct data link. The design of the intelligence should be flexible to allow for the rapid integration of other federal, state, and local agencies, as appropriate. An intelligence cell may be established both in a garrison and a field environment.

7011. CI Mission Profiles. The following CI mission profiles were initially developed to aid CI planning and execution in support of MEU(SOC) special operations missions. They are, however, pertinent to CI support of any MAGTF unit executing these missions.

a. Amphibious Raid. An amphibious raid is a landing from the sea on a hostile shore which involves swift incursion into or temporary occupancy of an objective and mission execution, followed by a planned withdrawal. Key CI requirements include:

(1) Assist the unit intelligence, operations and communications and information systems (CIS) officers with intelligence, CI, security and force protection planning.

(2) Provide operations security (OPSEC) guidance.

(3) Assess mission-oriented security vulnerabilities and develop requirements; provide countermeasures recommendations.

(4) Establish access to CI and HUMINT databases, automated links to JTF, other joint and services, coalitions, and host nation sources to help identify, assess, and develop countermeasures for threats.

(5) Conduct CI/HUMINT collection operations to satisfy tasked priority intelligence requirements (PIR) and intelligence requirements (IR).

(6) Explore CI database for information related to enemy or other potential hostile personalities, organizations, and installations (PO&I), and then develop the CI target reduction plan.

(7) Develop/update CI threat estimates; assist intelligence officer with development/update of all-source intelligence estimate.

(8) Conduct liaison with U.S. embassy country team for third party assistance/escape and evasion.

(9) Attach CI personnel to raid force, when required, for document and material exploitation or on-scene debriefing/interrogation of friendly and/or enemy personnel in the objective area.

(10) Provide countersigns challenges and passwords.

(11) Conduct CI debrief of raid force; update CI files and databases.

b. Limited Objective Attacks

(1) Assist the unit intelligence, operations and CIS officers with intelligence, CI, security and force protection planning.

(2) Provide OPSEC guidance.

(3) Develop/update CI threat estimates.

(4) Assess mission-oriented security vulnerabilities and develop requirements; provide countermeasures recommendations.

(5) Assist in the planning and conduct of counter-reconnaissance operations to support the attack.

(6) Establish access to CI and HUMINT databases, automated links to JTF, other joint and services, coalitions, and host nation sources to help identify, assess, and develop countermeasures for threats. Explore CI database for information related to enemy or other potential hostile personalities, organizations, and installations (PO&I), and then develop the CI target reduction plan.

(7) Conduct CI/HUMINT collection operations (e.g., photographic reconnaissance) to satisfy tasked PIRs and IRs.

(8) Identify CI targets for possible exploitation and/or neutralization.

(9) Assist ground combat element (GCE) and aviation combat element (ACE) intelligence officers with escape and evasion plans.

(10) Attach CI personnel to GCE when required.

(11) Conduct liaison with U.S. embassy country team for third party escape and evasion assistance.

(12) Provide countersigns challenges and passwords.

(13) Conduct CI debrief of assault force; update CI files and databases.

c. Noncombatant Evacuation Operation (NEO). A NEO is conducted for the purpose of evacuating civilian noncombatants from locations in a foreign faced with the threat of hostile or potentially hostile action. It will normally be conducted to evacuate U.S. citizens whose lives are in danger, but may also include the evacuation of U.S. military personnel, citizens of the host country and third country nationals friendly to the U.S. Key CI requirements include:

(1) Assist the unit intelligence, operations and CIS officers with intelligence, CI, security and force protection planning.

(2) Provide OPSEC guidance.

(3) Develop/update CI threat estimates.

(4) Assess mission-oriented security vulnerabilities and develop requirements; provide countermeasures recommendations.

(5) Assist in the planning and conduct of counter-reconnaissance operations to support key sites.

(6) Establish access to CI and HUMINT databases, automated links to JTF, other joint and services, coalitions, and host nation sources to help identify, assess, and develop countermeasures for threats. Explore CI database for information related to enemy or other potential hostile PO&I, and then develop the CI target reduction plan.

(7) Provide recommendations and planning assistance regarding antiterrorism measures.

(8) Provide countersigns challenges and passwords.

(9) Provide CI officer -- and possibly a CI subteam or HET -- to the forward command element (FCE) for on-scene liaison and support.

(10) When directed, attach CI personnel to the combat service support element (CSSE) evacuation control center (ECC) to assist in time sensitive debriefs, liaison, antiterrorism measures, and to assist in personnel screening.

(11) Provide from CI database, a sanitized copy of the black, white, and gray lists to the CSSE ECC for screening of persons of immediate interest.

(12) Conduct liaison with U.S. embassy country team for third party assistance.

(13) Conduct in-depth debriefs of non-combatant evacuees who may have information of intelligence/CI value.

d. Show of Force Operations. A show of force operation is designed to demonstrate U.S. resolve, which involves increased visibility of deployed military forces in an attempt to defuse a specific situation that, if allowed to continue, may be detrimental to U.S. interests or national objectives.

(1) Assist the unit intelligence, operations and CIS officers with intelligence, CI, security and force protection planning.

(2) Assist and coordinate with unit psychological operations, public affairs, and civil affairs planners, with emphasis on development of operational plans to target and influence attitudes and behaviors of personnel within the AO.

(3) Develop/update CI threat estimates.

(4) Provide OPSEC guidance.

(5) Conduct liaison with U.S. embassy country team for third party assistance.

e. Reinforcement Operations

(1) Assist the unit intelligence, operations and CIS officers with intelligence, CI, security and force protection planning.

(2) Provide OPSEC guidance.

(3) Assess mission-oriented security vulnerabilities and develop requirements; provide countermeasures recommendations.

(4) Assist in the planning and conduct of counter-reconnaissance operations to support key sites.

(5) Establish access to CI and HUMINT databases, automated links to JTF, other joint and services, coalitions, and host nation sources to help identify, assess, and develop countermeasures for threats. Explore CI database for information related to enemy or other potential hostile PO&I, and then develop the CI target reduction plan.

(6) Provide countersigns challenges and passwords.

(7) Attach CI personnel to GCE when directed to provide direct CI support.

f. Security Operations

(1) Assist the unit intelligence, operations and CIS officers with intelligence, CI, security and force protection planning.

(2) Provide OPSEC guidance.

(3) Provide recommendations and planning assistance regarding past hostile antiterrorism measures, capabilities, and countermeasures development.

(4) Provide estimates and recommendations on on counterespionage and countersabotage vulnerabilities and countermeasures.

(5) Conduct CI/HUMINT collection operations to satisfy tasked PIRs and IRs.

(6) Attach CI personnel to the GCE when directed for direct support to the GCE Commander and to conduct special activities ashore.

(7) Assist in the planning and conduct of counter-reconnaissance operations in the rear area..

(8) Establish access to CI and HUMINT databases, automated links to JTF, other joint and services, coalitions, and host nation sources to help identify, assess, and develop countermeasures for threats. Research CI database for information related to PO&I and development of the CI target reduction plan.

(9) Provide countersigns challenges and passwords.

g. Civic Action. Military civic action is the use of preponderantly indigenous military forces on projects useful to the local population at all levels in such fields as education, training, public works, agriculture, transportation, communications, health, sanitation, and others contributing to economic and social development, which would also serve to improve the standing of the military forces with the population.

(1) Provide OPSEC guidance.

(2) Establish access to CI and HUMINT databases, automated links to JTF, other joint and services, coalitions, and host nation sources to help identify, assess, and develop countermeasures for threats.

(3) Provide terrorist and hostile intelligence services (HOIS) threat data.

(4) Provide countersigns challenges and passwords.

(5) Conduct debriefs in support of the FORMICA[6] program.

h. Tactical Recovery of Aircraft and Personnel (TRAP). TRAP is a mission performed by an assigned and briefed aircrew for the specific purpose of the recovery of friendly personnel, equipment, and/or aircraft when the tactical situation precludes search and rescue assets from responding and when survivors and their location have been confirmed. The mission is to expeditiously recover friendly aircrews or personnel in a wide range of political environments and threat levels. Additionally, equipment will either be recovered or destroyed, dependent upon the severity of the threat and environment, and the condition of the equipment. Key CI requirements include:

(1) Assist the unit intelligence, operations and CIS officers with intelligence, CI, security and force protection planning.

(2) Provide countersigns challenges and passwords.

(3) Provide CI personnel to the recovery and security forces.

(4) Ensure isolated personnel report (ISOPREP) cards are up-to-date and readily accessible for all appropriate personnel prior to any operation. ISOPREP cards should be prepared and retained by either the unit security manager or its administrative officer. (See appendix J to Joint Publication 3-50.2, *Doctrine for Joint Combat Search and Rescue*, for the format and instructions for completing ISOPREP cards.)

(5) Conduct friendly POW/MIA investigations.

(6) Assist GCE and ACE intelligence officers and TRAP commanders in developing escape and evasion plans.

---

[6] Foreign military intelligence collection activity (FORMICA) is an overt intelligence collection program, managed by the Defense HUMINT Service, concerning the debriefing of U.S. military and DOD civilians in reference to their travels and activities. Within the MAGTF FORMICA debriefings are usually conducted by CI personnel. Additional information on the FORMICA program can be found in DIAM 58-11, *DOD HUMINT Policies and Procedures*, and MCO 003820.1, *FORMICA Program.*

(7) Conduct liaison with U.S. embassy country team for third party escape and evasion and other support.

(8) Conduct CI debrief of TRAP force.

i. In-Extremis Hostage Rescue (IHR)

(1) Assist the unit intelligence and operations officers with intelligence, CI and force protection planning.

(2) Provide countersigns challenges and passwords.

(3) Attach CI personnel to the IHR strike element when directed for target exploitation and personnel handling.

(4) Provide OPSEC guidance.

(5) Assist in rapid planning.

(6) Arrange for IHR force isolation.

(7) Conduct on-scene document and material exploitation when directed.

(8) Conduct initial hostage/terrorist debriefs.

(9) Provide assistance in training the IHR force in urban surveillance and counter-surveillance.

(10) Conduct liaison with national and theater intelligence agencies on hostage rescue and HUMINT operations.

CHAPTER 8

COUNTERINTELLIGENCE TRAINING

8001. General. The effectiveness of command and supporting CI and force protection security measures often rests on the individual Marine's ability to recognize and accurately report threats to the security of the command. It also rests on his willing acceptance of a high degree of security discipline.

a. Overall Objective. The ultimate objective of CI training is to ensure effective contribution by all MAGTF personnel to the CI effort and to instill a sense of security discipline. To ensure that the individual Marine can provide effective CI and security measures, CI training is integrated with other intelligence and command training programs.

b. CI Personnel Objective. For CI personnel, the objective of CI/HUMINT training is to ensure that MAGTF CI personnel are capable of providing CI/HUMINT support required by the commander. The desired result of CI/HUMINT training is that CI personnel can assist the commander in accomplishing the assigned missions. Additionally, it is to ensure non-MAGTF CI organizations and capabilities are understood and prepared to effectively integrate with and support MAGTF operations.

c. Basic CI Training. Basic CI and security training requirements are common to all commands. However, emphasis on certain subjects will vary according to the mission of the command and duty assignments of personnel within the unit. Generally, training can be divided into the following categories:

(1) Basic CI and security training for all personnel.

(2) Training for officers and staff noncommissioned officers.

(3) Mission-oriented training.

(4) Training for intelligence personnel.

8002. Basic Counterintelligence and Security Training for All Personnel. All personnel receive training in CI and force protection in order to safeguard friendly force information of value and operations from exploitation by the hostile intelligence threat. Although not directly related to CI or security, the following related areas should be covered to instill awareness on the part of all personnel:

a. Marine Corps personnel are subject to detention or captivity by foreign governments or organizations because of their wide range of activities. At a minimum all Marines require training -- individual, collective and unit -- in the following:

(1) Operations security, to include its purpose, how to identify unit/individual patterns and profiles that can be identified and exploited by the enemy, and countermeasures to minimize or eliminate these.

(2) Information security, to include levels of security classification, when to apply and ramifications of these on friendly operations, development of operational and functional classification guidance and criteria, downgrading and declassification,

(3) Personnel security, to include individual standards, how to identify risks and vulnerabilities, and individual and command actions to take when these are identified.

(4) Challenges and practices for each of the above when conducting MAGTF operations with non-U.S. military forces, non-governmental organizations, private volunteer organizations, and news media organizations.

(5) Purpose and procedures for the use of countersigns challenges and passwords.

(6) Survival, evasion, resistance to interrogation, escape (SERE), to include training on prospective areas of operation, the nature and attitude of the civilian populaces, and the techniques and procedures used by threat forces.[1]

(7) Communications and information security vulnerabilities and countermeasures.

(8) U.S. code of conduct.

b. Marines may be required by operational necessity to detain foreign nationals. As a result, they are required to know the laws of war and the individual rights and responsibilities under the Geneva Convention of 12 Aug 1949, for those captured or detained by MAGTF units.

8003. Training for Officers and Staff Noncommissioned Officers. All officers and enlisted personnel -- regardless of MOS -- must receive training in the following CI and security subjects. Entry level and basic military occupational specialty training programs are best suited for initial training to these areas. Follow-on training based on unit mission (mission-oriented training) and professional development/education should be conducted throughout the careers of all Marines.

---

[1] DOD Dir 1300.7, *Training and Education Measures Necessary to Support the Code of Conduct*, provides policy and guidance on SERE training. It establishes three levels:

a. Level A: the minimum level of understanding required of all Armed Forces personnel, to be provided during entry level training.

b. Level B: the minimum level of understanding required of military personnel whose military occupational specialities and assignments entail moderate risk of capture. Level B training is to be conducted as soon as possible upon assumption of the duty/MOS that makes them eligible.

c. Level C: the minimum level of understanding required of military personnel whose MOS/assignment entails significant risk of capture, or whose position, rank, or seniority make them vulnerable to greater than average targeting/exploitation by enemies or other threats. Examples include aircrews, ground reconnaissance personnel, and military attaches.

a. Operations security is a process of analyzing friendly actions attendant to military operations and other activities to:

(1) Understand, identify and properly employ the use of essential elements of friendly information (EEFI).

(2) Identify those friendly actions and operational patterns that can be observed and exploited by enemy intelligence forces.

(3) Determine indicators that hostile intelligence elements might obtain. These indicators could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

(4) Select, plan and execute friendly protective measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

b. Protecting classified material and other information that may be of value to the enemy. All personnel must be able to name and define, in general terms, the three levels of security classification, minimum security standards, and the potential damage that may be caused if this information should be exposed to unauthorized persons. Officers and SNCOs must in particular understand how to apply these to their activities and products, both generally as well as within the specific exercise/operation classification guidance.

c. Evaluating the suitability of subordinate personnel who have access to classified information. Officers and staff noncommissioned officers must be able to recognize indicators associated with potential involvement or susceptibility to espionage activities, such as unexplained affluence, erratic behavior, or mood swings, and then initiative action in accordance with OPNAVINST 5510.1.

d. Hostile intelligence services organizations, capabilities, and methods of operation and acquisition of information. Additionally, briefs on current events concerning attempts and/or acts of espionage, subversion, terrorism, or sabotage should be emphasized. Individual responsibilities for reporting foreign contact, perceived or actual attempts at espionage or subversion, and undue interest on the part of anyone to acquire terrorist countermeasures as well as intelligence collection operations should be stressed regardless of MOS. Routine threat awareness should become a part of each person's professional military education objectives. This is most easily satisfied at formal professional military education courses or correspondence courses, but can also be obtained during mission-oriented training. Special attention should be paid to indications of the level of terrorist/subversive activity through unclassified or classified articles/publications and through tailored briefs, particularly in those countries identified as high threat areas. (See DODINST 5240.6, *CI Awareness and Briefing Program*, for additional information.)

e. Use of countersigns challenges and passwords.

f. Purpose, scope, organization, capabilities and limitations of Marine Corps CI assets.

g. The identities and responsibilities of all unit personnel responsible with key leadership roles regarding unit security, to include:

(1) Unit security manager[2] -- overall coordination of unit security.

(2) G/S-1 -- principal staff cognizance for classified materials control.

(3) G/S-2 -- principal staff cognizance for sensitive compartmented information and special security, and identification of enemy intelligence capabilities and operations.

(4) G/S-3 -- principal staff cognizance for force protection, command and control protection, operations security, counter-reconnaissance, deception, and electronic protection.

(5) G/S-6 -- principal staff cognizance for communications and information systems (CIS) security, cryptographic materials system.

(6) Headquarters commandant -- principal staff cognizance for physical security.

h. Handling of personnel of CI interest during MAGTF operations, to include the identification, control, and reporting of persons, installations and materials of CI interest.

8004. Mission-Oriented Training

a. General. Mission-oriented training ensures that the unit's objectives are achieved by employing the proper CI measures. Unit SOPs and training exercises should include the following:

(1) Operations security measures and passive countermeasures to protect sensitive or classified information from the enemy or unauthorized personnel.

(2) Counter-reconnaissance activity to prevent observation from opposing forces, such as patrols, camouflage, and other measures.

(3) Other security measures designed specifically for each type of unit and the nature of the operation.

(4) CIS security procedures designed to lessen friendly signatures and susceptibility to hostile radio electronic combat operations.

(5) SERE training for those personnel whose military jobs, specialties, or assignments entail moderate risk of capture.

---

[2] The unit security manager is generally either the chief of staff or executive officer.

b. Counterintelligence Personnel. A complete listing and description of mission performance standards for CI personnel can be found in MCO 1510.58. The following identifies the principal individual and mission training standards.

(1) Supervise marine staff counterintelligence/HUMINT section garrison activities

(2) Supervise marine staff counterintelligence/HUMINT section in a tactical environment

(3) Supervise counterintelligence team/HUMINT exploitation team headquarters activities and operations

(4) Monitor counterintelligence training plan for counterintelligence personnel

(5) Prepare the counterintelligence standing operating procedures (SOP)

(6) Brief CI/HUMINT mission and authorizing directives and regulations.

(7) Conduct counterintelligence screening

(8) Conduct mobile and static checkpoints

(9) Conduct counterintelligence activities in support of cordon and search

(10) Conduct counterintelligence survey

(11) Conduct missing in action investigation

(12) Conduct an investigation of an act of espionage, sabotage, subversion, or terrorism

(13) Conduct counterintelligence surveillance

(14) Conduct counterintelligence countersurveillance

(15) Conduct HUMINT operations

(16) Conduct counterintelligence interrogation

(17) Conduct map tracking during interrogation and interviews

(18) Exploit captured documents and equipment

(19) Conduct counterintelligence elucidation

(20) Conduct counterintelligence debrief

(21) Conduct counterintelligence interview

(22) Conduct counterintelligence/humint liaison

(23) Account for operational funds

(24) Conduct technical surveillance countermeasures service

(25) Maintain counterintelligence and human resources equipment

(26) Operate current automated intelligence systems

(27) Provide counterintelligence support to MAGTF operations

(28) Conduct CI activities in support of noncombatant evacuation operations

8005. Training of Intelligence Section Personnel. The following subjects are considered appropriate for the CI training of intelligence section personnel and should incorporate MAGTF, other services, joint and national capabilities, issues and operations:

a. Counterintelligence Collection, Processing, Production and Dissemination Capabilities and Organizations

b. C2 and CIS Architecture. C2 and supporting communication-information systems operations, both for internal CI activities and for overall integrated CI/intelligence operations.

c. Counterintelligence Sources of Information and Methods of Reporting. Walk-ins, host nation liaison activity, and line crossers and CFSO are examples of sources utilized in CI/HUMINT operations to support command information objectives.

d. CI Support Activities. This includes CI surveys/vulnerability assessments, technical support and technical surveillance countermeasures.

e. Intelligence Oversight. When intelligence specialist assets are attached/assigned, the minimum reporting requirements and prohibited activities should be strictly monitored and enforced in accordance with DOD 5240.1R *Intelligence Oversight*.

f. Unique Supply, Embarkation, Maintenance, and Other Functional Support to CI

8006. Peacetime Counterintelligence Training

a. Exercises. The conduct of CI operations in exercises is closely controlled. All aspects of CI operations require the same security precautions and controls for exercises that are required for real world operations.

(1) Planning. The use of exercise CI provides commanders, staffs, and units involved experience regarding CI operations and in working with CI information, rules, communications, and personnel. Exercise CI operations may be conducted whether or not an opposition force exists.

(a) Exercise CI may be scripted or preplanned if an opposition force does not participate in the exercise, such as for a staff exercise (STAFFEX) or a command post exercise (CPX). Use of scripted CI should be planned well in advance of the exercise to allow adequate time to script the exercise CI necessary to realistically support the exercise scenario. Coordination between exercise planners and exercise CI scripters is important to ensure that the exercise CI emulates realistic CI activities, information flow and timelines (e.g., the time-sensitive limitations of CI for timely reporting and access to sources often do not integrate well with accelerated wargaming time clocks) in relation to the notional opposition force. All security requirements, such as for the use of special CI communications, must be maintained throughout the exercise.

(b) Exercise CI operations may also be conducted against a live opposition force, such as during a MAGTF field exercise. This provides for more realistic training for both the CI element and users of SIGINT participating in the exercise, as well as better CI/other intelligence elements integration and training. Dependent on the level of the exercise, use of simulators and national systems may be requested for participation in the exercise to add realism and enhance training.

b. Real World Support. During the conduct of exercises, particularly overseas, CI performs critical, real-world support to the unit's force protection mission. This support involves protecting the force during prior to and during training process from exposure to or exploitation by hostile intelligence and security services, and terrorist actions targeting the force.

8007. CI Training Programs. CI training is a dynamic, evolutionary, and never ending process. Due to continual technological advances and ever increasing sophistication of CI/HUMINT operations and activities, its importance cannot be over emphasized. All personnel are to receive training in CI and security as a basis for fulfilling their basic responsibilities to safeguard information of value to the hostile intelligence threat. CI personnel receive additional training to improve their proficiency in accomplishing the CI mission.

a. Individual CI Personnel Training. The training of CI personnel is driven by MCO 1510.58 (Individual Training Standards [ITS]). ITS' are derived from mission performance standards (MPS). MPS are further derived from the combat requirements of the operating forces and establish a common base of training for all Marines who have the same MOS. CI personnel undergo four distinct levels of training to acquire, maintain, and increase their proficiency in the prescribed ITS.

(1) Pre-resident/on-the-job training (OJT).

(2) MAGTF CI Course, Formal Resident Training (formal MOS school, NMITC).

(3) Advanced training.

b. Responsibilities. The following personnel have the responsibility for ensuring that a viable program is established for each of the four levels of training:

(1) Pre-resident OJT -- Commanding Officer, CI/HUMINT Company.

(2) CI resident course -- Navy and Marine Corps Intelligence Training Center (NMITC).

(3) Advanced training community (CI/HUMINT Companies, MEF CIHOs, parent units, HQMC).

c. Descriptions

(1) Pre-Resident On-The-Job Training. The foundation of the pre-resident OJT program is a standardized pre-resident training course (PRTC). The pre-resident OJT program also serves as a vehicle for screening and evaluating candidates for the CI MOS. The PRTC prepares the candidate for the resident CI Course. It also provides him with a baseline knowledge from which resident training commences. All candidates for the CI MOS must successfully complete the PRTC prior to advancing to the second level of training. Commanders will diligently observe candidates during this period to ensure they meet the high personal and professional standards required of CI personnel. To better prepare a candidate for resident training, commanders should expand on the PRTC once a candidate completes it. This training will include:

(a) Correspondence procedures/administration

(b) Communications and information systems

(c) Mapping and land navigation

(d) MAGTFs, JTF and theater CI and intelligence organizations and capabilities

(e) CI methodology

(f) Report writing/writing skills

(g) Interpersonal communications

(2) CI Resident Formal School Training. CI resident entry-level formal school training for both officers and enlisted Marines is via the 17-weeks MAGTF Counterintelligence Agents Course

conducted at the NMITC, Dam Neck, Virginia. Successful completion of this course provides basic MOS qualification (officers -- MOS 0204; enlisted -- MOS 0211) and certification as *Level I Anti-Terrorism/Force Protection Instructors*. Once qualified, all CI personnel are required to maintain proficiency in those ITS' achieved.

(3) Advanced Training. Advanced training of CI personnel in specialized skills is conducted to enhance their abilities to perform increasingly complex tasks. This training supplements and is conducted with the post resident training process. This training includes, but is not limited to, the following:

(a) Intelligence cross training

(b) TSCM

(c) Photographic, video and electronic surveillance systems training

(d) Military Officer Training Course/Military Officer Familiarization Course/Officer Support Specialty Course (MOTC/MOFC/OSSC)

(e) Language training

(f) SERE training

(g) Terrorism/counterterrorism

(h) Intelligence and CI communications and information systems

CHAPTER 9

COUNTERINTELLIGENCE ADMINISTRATION

9001. General. Administration for the CI elements consists of files, reports, communications, and emergency funds. CI elements are responsible for establishing and maintaining operational files essential to their combat CI mission. The accomplishment of the CI mission requires accurate, timely, and pertinent reports disseminated in a usable form. CI has organic communications equipment to help coordinate CI activities and report information to other organizations. Emergency and extraordinary expense (E&EE) funds are made available for CI because of the nature of the missions.

9002. Files. The following operational files are normally maintained in a combat environment by CI elements at all echelons. Formats, organization and content for each should be coordinated with the MEF AFC OIC or the supported unit's intelligence officer.

a. Information concerning personalities, organizations, installations, and incidents, of current and future CI interest. Often basic information of this type is recorded in a card file/folder or automated data base for ready reference. It is also cross-indexed to more detailed information.

b. Correspondence and reports about specific operations and investigations.

c. Source records containing essential data on sources of information.

d. Area files containing basic reference data and information on enemy intelligence activity and CI measures within a particular geographic area.

9003. Reports. CI reports are prepared to transmit accurate information to units to support planning, decisionmaking and execution, to aid in the processing of intelligence, and to serve as a record of CI activities. The method of dissemination of CI information depends primarily on the nature and urgency of the information, the location of the receiving units, the security requirements, and the means available. Normally, information is disseminated by record or voice messages, personal liaison, telephone, briefings, messenger, and written reports. All CI reports will be written in accordance with the formats prescribed for a standard naval letter or message. The report formats in appendix E of this publications are DOD standardized formats meant to enhance joint interoperability and should not be modified unless absolutely necessary and following coordination with all pertinent intelligence organizations. Reports are classified according to content.

9004. Personnel

a. Augmentation. When additional personnel are needed, the requirement is identified through the intelligence officer to the personnel officer for validation by the commander. The request will then be

forwarded through the chain of command to the MEF G-2 for follow-on tasking to the CI/HUMINT company.

b. Global Sourcing. When the MEF's CI/HUMINT company resources are insufficient to fulfill a validated requirement, it is then forwarded to Headquarters, Marine Corps, for global sourcing support from either the other MEFs or Marine Forces Reserve (MARFORRES).

c. Reserves. There are three reserve CI teams within MARFORRES. The 10th and 12th CI teams are located at Anacostia Naval Air Station, Washington DC, while the 14th CI team is located at Miramar Naval Air Station, San Diego, CA. The reserve CI teams are a lucrative source of experienced CI personnel.

9005. Emergency and Extraordinary Expense (E&EE) Funds. The nature of certain CI and intelligence activities are such that security considerations, opportunity, timeliness, or other circumstances may make the use of normal military funds impractical or undesirable. Accordingly, the Secretary of the Navy has authorized the use of E&EE funds for certain intelligence and CI activities.

a. Intelligence collection funds to support HUMINT operations conducted by Marine Corps CI assets are available through E&EE (subhead 123.A[2]) funds. These funds are not authorized for the conduct of CI activities.

b. CI funds to support offensive and defensive CI operations are available through E&EE (subhead 123.B[3]) funds. These funds are not authorized for the conduct of positive HUMINT or other controlled intelligence collection activities.

c. The MAGTF CIHO initiates early planning and coordination to ensure the availability of both types of funds. This function is performed by the CI detachment or HET OICs within MEU(SOC)s or SPMAGTFs.

d. See MCO 7040.10A, *Emergency and Extraordinary Expense Funds*, for additional information on the use, control and accounting of E&EE funds.

---

[2] Subhead 123.a funds are General Defense Intelligence Program (GDIP) monies intended for use by Naval Attaches in the performance of their official duties and are managed by the Office of Naval Intelligence and coordinated by CMC (CIC).

[3] Subhead 123.b funds are Foreign Counterintelligence Program (FCIP) monies intended for CI functions only and are managed through NCIS.

CHAPTER 10

GARRISON COUNTERINTELLIGENCE SUPPORT

10001. Mission. The primary garrison mission of CI activities is planning, preparing, and training to accomplish MAGTF CI functions and operations. A secondary mission is to advise and assist the commander in implementing the command's force protection and security programs and supporting command initiated security measures. CI is designed to identify and neutralize the effectiveness of both potential and active hostile collection efforts and to identify and neutralize the effectiveness of individuals, activities, or organizations capable of engaging in hostile intelligence collection, sabotage, subversion, or terrorism directed against his command. Additional doctrine pertaining to combating terrorism is contained in MCO 3302.1, *Antiterrorism Program*.

10002. Counterintelligence Survey/Vulnerability Assessment

a. Basis. The CI survey/vulnerability assessment is designed to assist commanders in establishing security systems, procedures, and safeguards to protect military personnel, organizations and installations from espionage, sabotage, terrorism, or subversion. The survey assesses a unit's overall security posture against threats identified in the CI estimate. The CI survey/vulnerability assessment will identify specific vulnerabilities to hostile intelligence, espionage, sabotage, subversion or terrorist capabilities and provide recommendations on how to eliminate or minimize these vulnerabilities. The survey/vulnerability assessment is not a recurring event. Once it is conducted, the survey/vulnerability assessment will remain valid for that specific installation until there are major changes in the physical security of the installation, the mission of the command, or potential threats. It is necessary that the survey/vulnerability assessment look forward in both space and time to support the development of CI measures necessary to protect the unit as it carries out successive phases of the operation. The CI survey/vulnerability assessment includes:

(1) Analysis of CI factors influencing security within the unit or installation.

(2) A determination of CI measures required by the sensitivity or criticality of the installation.

(3) An assessment of CI measures and deficiencies that currently exist and their effectiveness.

(4) Recommendations for improvements to these measures or the initiation of new security measures to achieve required security standards and protection.

b. Initiation. The initiation of a CI survey/vulnerability assessment begins with a request from the commander of a unit or installation concerned or with a higher commander in the same chain of command. That request will normally occur under the following circumstances:

(1) Changes in known or estimated threat risks.

(2) Activation or reactivation of an installation or a major command.

(3) Significant change in the mission, functions, or physical reorganization of an installation or major command.

(4) New hazardous conditions affecting an installation which necessitate the reevaluation of the security systems in place.

(5) Significant changes in the level/scope of classified material stored, handled, processed, and/or produced.

(6) Change in locale or environment in which the installation is located.

c. Preparation. When preparing to conduct a CI survey/vulnerability assessment, there are four areas that need to be considered: selection of personnel, collection of data, coordination, and the preparation of checklists. The scope and depth to which each of the areas will be considered will depend entirely on the unit or installation itself. The following paragraphs offer some ideas.

(1) Selection of Personnel. Selection of personnel will consider the number of persons required to complete the task and available assets and should include TSCM personnel, if possible.

(2) Collection of Data. At a minimum, data collected should include the mission, organization, functions, and security directives pertinent to the installations. Also, reports of previous CIsurveys/vulnerability assessments, inspections, or evaluations should be acquired and reviewed.

(3) Coordination. Coordination with the commander of the unit or installation should be conducted by a CI officer/specialist. This coordination will help in determining the scope of the survey/vulnerability assessment, arrange for access to any/all required records or areas, procurement of any directives if not already acquired, arrangements for any required escorts, and arrangements for any necessary briefings.

(4) Preparation of Checklist. Checklist preparation will evolve once a thorough review of the commander's objectives and the unit/installation's mission, organization and operations has been completed. The checklist includes general and specific points to be covered during the survey/vulnerability assessment. It also serves as a reminder to the surveying personnel to satisfy the predetermined scope of the survey/vulnerability assessment. In an effort to assist in formulating a checklist, areas of emphasis typically include document security, personnel security, communications and information systems security, and actual physical security requirements (less those physical security requirements falling under the purview of the provost marshal). Physical security requirements should be coordinated with the PMO because the PMO has resident knowledge and expertise as the primary agency for physical security aboard the installation. From those three general points, more specific

points will evolve. A comprehensive CI survey/vulnerability assessment checklist is contained in appendix E of this publication.

d. Conduct. The actual conduct of the CI survey/vulnerability assessment will depend solely on the findings set forth in the data collected and the needs developed in the checklist(s). The judgment of the leader will determine just how/what the team will do. There are several things that should be noted as specific methods and/or ways to conduct the CI survey/vulnerability assessment.

(1) Using one possible concept of concentric circles, the survey/vulnerability assessment team should make a physical tour of the installation from its perimeter areas to the center, including the area immediately outside its physical boundary. This tour should include every building, area, facility, or office which requires special security considerations or which are considered sensitive. It is also recommended the unit/installation staff personnel and subordinate commanders be interviewed, as required, to assist in determining the operational importance, know vulnerabilities and security practices of each area surveyed.

(2) The cost of replacement, (in terms of time and not necessarily dollars and cents), of personnel, documents, and materials in the event the installation is neutralized or destroyed. The potential sources for the procurement of comparable personnel and sources for copies of essential and critical documents to replace or reactivate the installation.

(3) The location of the unit/installation and the effects of the surrounding environment/elements on the overall security of the installation.

(4) The level of classified and sensitive information used, produced, stored, or compiled.

(5) The criticality of the installation with the overall defense posture of the U.S. based on its mission/function.

(6) Whether there are other units/installations/facilities that can assume the role of the surveyed unit/installation if it is neutralized or destroyed.

(7) The unit/installation's vulnerability to terrorist or special operations forces attacks based on local/international threat and conditions.

e. Baseline. Once the level of security required has been determined, the posture and effectiveness of existing security measures must be assessed. Areas that should be examined include:

(1) Document Security. Document security is systematic review and inspection of all security procedures and records used in the handling of classified document, information, and other classified material. The review should include the flow of classified material beginning from its creation/receipt at the installation/unit/command/ to its final storage area or destruction.

(2) Personnel Security. Personnel security is based on the relationship that exists between a unit/installation's mission, local CI threat estimates, the actual security level of assigned personnel, and the supporting security education and awareness program.

(3) Physical Security. This assesses the system of security controls, barriers, and other devices procedures to prevent destruction, damage, unauthorized access to the installation and facilities. In accordance with MCO 3302.1 *Antiterrorism Program*, this is normally the responsibility of the provost marshal. However, in conjunction with the storage of classified material where the susceptibility to espionage, sabotage, subversion, or terrorism is a consideration, the CI survey/vulnerability assessment is applicable. Whether the installation is a controlled one or an open post, the actual physical requirements established by directives will be examined based on the unit/installation's mission and nature/type materials being used. Emphasis is on the examination of the physical security factors affecting classified storage areas, security areas, critical areas that require protection from sabotage or terrorist attack and other locations that may be designated as sensitive.

f. Exit Brief. Once the survey/vulnerability assessment has been completed and all recommendations have been formulated, the survey/vulnerability assessment team will provide the unit/installation commander with a exit brief addressing preliminary findings and recommendations. Compliance will then be the commander's responsibility.

g. CI Survey/Vulnerability Assessment Report and Recommendations. Once the CI survey/vulnerability assessment has been completed and all data compiled, a formal report of findings will be written and recommendations made. The recommendations will be based on the security measures required of the command, existing measures, and procedures. The recommendations are made to provide measures to safeguard the installation/organization against sabotage, espionage, subversion, and/or terrorism. Each recommendation will be in response to a specific identifiable hazard with consideration given to cost, time, manpower, and availability of materials. If at all possible, alternate recommendations should be included. See appendix E of this publication for the format of a CI survey/vulnerability assessment report.

10003. CI Penetration Inspection. Once a survey/vulnerability assessment has been conducted on a unit/installation/facility, a CI penetration inspection may be conducted to determine the effectiveness of recommendations implemented. The inspection is designed to provide a realistic test of established security measures and practices. It is conducted in a manner that installation personnel, other than the commander and those persons he desires to inform, are unaware that such an action is taking place. The inspection may be all-inclusive or may be limited to an attempt by CI personnel to fraudulently gain access to specific sensitive areas for performing simulated acts of espionage or sabotage. These simulated acts should be as realistic as possible. These acts should correspond to activities which could be attempted by area threats or hostile agents. The penetration inspection must be thoroughly planned and coordinated and include the following considerations:

(1) A responsible person, who is knowledgeable of the inspection, and a representative of the inspected command must be present during the inspection.

(2) In addition to the CI credentials and military identification, inspectors must carry a letter of identification and authorization for use only in emergency situations.

(3) Termination of the inspection will be done immediately if at any time personnel is subject to physical danger or other safety risks.

(4) Preparation for and conduct of the inspection must not impair or disrupt the normal operation/function of the command unless the inspection is specifically designed to do so.

(5) Command or installation personnel will not be utilized in any manner which would tend to discredit them.

10004. Counterintelligence Evaluation

a. CI evaluations are similar to surveys but are limited in scope. The CI evaluation is normally conducted for a small unit or a component of a larger organization when there has been a change in the security posture, an activation or reactivation of a facility, a physical relocation, or substantive changes to the unit's facilities or communications-information systems infrastructure. CI evaluations are normally limited to areas containing or processing classified material.

b. The CI evaluation may be limited to an assessment of only one type of security, such as document, personnel, or physical security, or it may include any combination, depending on the needs of the unit. The procedures for the preparation and conduct of the evaluation are the same as those for the CI survey/vulnerability assessment. However, the procedures usually are not as extensive. The CI evaluation also may be used to update CI surveys when only minor changes have occurred within an installation or major organization.

10005. Technical Surveillance Countermeasures (TSCM) Support

a. As discussed in chapter 7, the purpose of the TSCM program is to locate and neutralize technical surveillance devices that have been targeted against U.S. sensitive or secure areas. CI TSCM teams have specialized equipment and techniques to locate and identify threat technical surveillance activity. TSCM support consists of inspections and surveys. A TSCM inspection is an evaluation to determine the physical security measures required to protect an area against visual and audio surveillance. TSCM surveys include a complete electronic and physical search for unauthorized modification of equipment, the presence of clandestine audio and visual device, and other conditions which may allow the unauthorized transmission of any conversation out of the area being surveyed. All TSCM operations are governed by DOD Directive 5200.9, SECNAVINST 5500.31, and MCO 05511.11.

b. Historically, hostile intelligence services have used technical surveillance monitoring systems in their intelligence and espionage operations against U.S. targets, both in the continental United States and

abroad. A technical surveillance monitoring system may be defined as any visual surveillance or audio monitoring system which is used clandestinely to obtain classified or sensitive unclassified information for intelligence purposes. These monitoring systems include, but are not limited to, the following:

(1) Sound pickup devices, such as microphones and other transducers which use wire and amplifying equipment.

(2) Passive modulators.

(3) Energy beams; i.e., electromagnetic, laser, and infrared.

(4) Radio transmitters.

(5) Recording equipment.

(6) Telephones; i.e., taps and bugs.

(7) Photographic and television cameras.

c. Requests for TSCM support must be classified and no conversation concerning the inspection should take place in the vicinity of the area to be inspected. Procedures for requesting inspections and surveys, TSCM responsibilities, and further information on the audio surveillance threat are contained in OPNAVINST 0500.46 and MCO 5511.11.

d. Normally, one Marine team within the CI/HUMINT company at each MEF maintains a TSCM capability to support tactical units of the MEF. This capability, designed primarily for combat support, also supplements the NCIS TSCM responsibilities during peacetime garrison conditions.

(See chapter 7, paragraph 7008, for additional information on TSCMs.)

APPENDIX A

GLOSSARY

Part I -- ACRONYMS & ABBREVIATIONS

Note: Acronyms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official military acronyms:

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

2. MCRP 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*.

ACE	aviation combat element
AFC	all-source fusion center
ASAS	all source analysis system {Army}
ATFIC	amphibious task force intelligence center
BDA	battle damage assessment
bn	battalion
CA	civil affairs
CE	command element
C-HUMINT	counter human intelligence
CI	counterintelligence
CIAT	counterintelligence analytical team
CICM	counterintelligence contingency material
CIC	combat intelligence center
CID	criminal investigation division
CIHO	CI/HUMINT officer
CIIR	counterintelligence information report
C-IMINT	counter imagery intelligence
CINC	command-in-chief
CIS	communications-information systems
CITEX	counterintelligence training exercise
CLF	commander, landing fForce
co	company
COA	course of action
CP	command post
CPX	command post exercise
C-SIGINT	counter signals intelligence

CSS	combat service support
CSSE	combat service support element
C2	command and control
C2W	command and control warfare
det	detachment
DCID	Director Central Intelligence Directive
DF	direction finding
DIAM	Defense Intelligence Agency manual
DOD	Department of Defense
DON	Department of the Navy
DS	direct support
DST	direct support team
EEFI	essential element of friendly information
EPW	enemy prisoner of war
EW	electronic warfare
FIIU	force imagery interpretation unit
FISS	foreign intelligence and security services
FSCC	fire support coordination center
FSSG	force service support group
GCE	ground combat element
GI&S	geospatial information and services
GS	general support
HET	HUMINT exploitation team
HLZ	helicopter landing zone
HPT	high payoff target
HUMINT	human intelligence
HVT	high value target
IAS	intelligence analysis system
ICR	intelligence collection requirement
IDR	intelligence dissemination requirement
IHR	in-extremis hostage rescue
IMA	individual mobilization augmentation
IMINT	imagery intelligence
IPB	intelligence preparation of the battlespace
IPR	intelligence production requirement
IR	intelligence requirement
IT	interrogator-translator
I&W	indications and warning
J-2X	joint CI/HUMINT deconfliction cell
JCISB	joint CI support branch
JDISS	joint deployable intelligence support system
JFC	joint force commander
JIC	joint intelligence center

Joint STARS	Joint Surveillance & Target Acquisition Radar System
JISE	joint intelligence support element
JTF	joint task force
JWICS	joint worldwide intelligence communications system
MAG	Marine aircraft group
MAGTF	Marine air ground task force
MARFOR	Marine Corps Forces
MARFORLANT	Marine Corps Forces, Atlantic
MARFORPAC	Marine Corps Forces, Pacific
MARFORRES	
MASINT	measurement and signature intelligence
MAW	Marine aircraft wing
MCIA	Marine Corps Intelligence Activity
MCISU	Marine Corps Imagery Support Unit
MEF	Marine expeditionary force
MO	modus operandi
MEU(SOC)	Marine expeditionary unit (special operations capable)
MOOTW	military operations other than war
MOTC	Military Operations Training Course
MSC	major subordinate command
NAI	named area of interest
NGO	non-governmental organization
NIPRNET	nonsecure internet protocol router network
NMITC	Navy Marine Corps Intelligence Training Center
NSA	National Security Agency
obj	objective
OCAC	operations control and analysis center
OFCO	offensive counterintelligence operations
OMFTS	operational maneuver from the sea
OPCON	operational control
OPSEC	operations security
OSI	Office of Special Investigations (Air Force)
OSINT	open source intelligence
plt	platoon
PIR	priority intelligence requirement
PMO	Provost Marshal office
POI	personalities, organizations, and installations
POI&I	personalities, organizations, installations, and incidents
PSYOP	psychological operations
QSTAG	quadripartite standardization agreement
RFC	raid force commander
ROE	rules of engagement
SARC	surveillance and reconnaissance center

SASO	stabilization and security operations
SCAMP	sensor control and management platoon
SIGINT	signals intelligence
SIPRNET	SECRET internet protocol router network
SOA	sustained operations ashore
SOFA	status of forces agreement
SOP	standard operating procedures
TACON	tactical control
TDN	tactical data network
topo	topographic
TFCICA	task force CI coordinating authority
TRAP	tactical recovery of aircraft and personnel
TSCM	technical surveillance countermeasures
TTP	tactics, techniques, & procedures
UAV	unmanned aerial vehicle

Part II -- Definitions

Note: Definitions of military terms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official definitions of military terms:

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

2. MCRP 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*.

A

accountability - The obligation imposed by law or lawful order or regulation on an officer or other person for keeping accurate record of property, documents, or funds. The person having this obligation may or may not have actual possession of the property, documents, or funds. Accountability is concerned primarily with records, while responsibility is concerned primarily with custody, care, and safekeeping. (Joint Pub 1-02)

administrative control - Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. Also called ADCON. (Joint Pub 1-02)

agent - (1) One who is authorized or instructed to obtain or to assist in obtaining information for intelligence or CI purposes. (Joint Pub 1-02)

agent authentication - The technical support task of providing an agent with personal documents, accouterments, and equipment which have the appearance of authenticity as to claimed origin and which support and are consistent with the agent's cover story. (Joint Pub 1-02)

agent net - (1) An organization for clandestine purposes which operates under the direction of a principal agent. (Joint Pub 1-02)

all-source intelligence - Intelligence that incorporates all available sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the development of the finished intelligence product. (Joint Pub 1-02)

antiterrorism - Defensive measures used to reduce the vulnerability of individuals and property to terrorism. (Joint Pub 1-02)

area of interest - That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (Joint Pub 1-02)

area of operation - That portion of an area of war necessary for military operations and for the administration of such operations. Also called AO. (Joint Pub 1-02)

assessment - (1) Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. (2) Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents. (Joint Pub 1-02)

asset - (1) Any resource -person, group, relationship, instrument, installation, or supply -at the disposition of an intelligence organization for use in an operational or support role. Often used with a qualifying term such as agent asset or propaganda asset. (Joint Pub 1-02)

assign--1. To place units or personnel in an organization where such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel. 2. To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. (Joint Pub 1-02)

attach -1. The placement of units or personnel in an organization where such placement is relatively temporary. 2. The detailing of individuals to specific functions where such functions are secondary or relatively temporary, e.g., attached for quarters and rations; attached for flying duty. (Joint Pub 1-02)

B

basic intelligence - (1) Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (Joint Pub 1-02)

battle damage assessment - The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (Joint Pub 1-02) In Marine Corps usage, the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical

damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCRP 5-12C)

battlespace - All aspects of air, surface, subsurface, land, space, and electromagnetic spectrum which encompass the area of influence and area of interest. (MCRP 5-12C)

battlespace dominance - The degree of control over the dimensions of the battlespace which enhances friendly freedom of action and denies enemy freedom of action. It permits force sustainment and application of power projection to accomplish the full range of potential operational and tactical mission. It includes all actions conducted against enemy capabilities to influence future operations. (MCRP 5-12C)

biographical intelligence -That component of intelligence which deals with individual foreign personalities of actual or potential importance. (Joint Pub 1-02)

black list -An official counterintelligence listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of friendly forces. Currently known as the DETAIN category of the Personalities Database within DCIIS (Joint Pub 1-02)

border crosser - An individual, living close to a frontier, who normally has to cross the frontier frequently for legitimate purposes. (Joint Pub 1-02)

bug - (1) A concealed microphone or listening device or other audio surveillance device. **(2)** To install means for audio surveillance. (Joint Pub 1-02)

bugged - Room or object which contains a concealed listening device. (Joint Pub 1-02)

C

case - (1) An intelligence operation in its entirety. **(2)** Record of the development of an intelligence operation, including personnel, modus operandi, and objectives. (Joint Pub 1-02)

cell - Small group of individuals who work together for clandestine or subversive purposes. (Joint Pub 1-02)

center of gravity - Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. (Joint Pub 1-02).

centralized control - In military operations, a mode of battlespace management in which one echelon of command exercises total authority and direction of all aspects of one or more warfighting functions. It is a method of control where detailed orders are issued and total unity of action is the overriding consideration. (MCRP 5-12C)

clandestine operation -An activity to accomplish intelligence, counterintelligence, and other similar activities sponsored or conducted by governmental departments or agencies, in such a way as to assure secrecy or concealment. (It differs from covert operations in that emphasis is placed on concealment of the operation rather than on concealment of identity o' sponsor.) (Joint Pub 1-02)

classification -The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. (Joint Pub 1-02)

classified information - Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (Joint Pub 1-02)

code word - (1) A word which has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation. **(2)** A cryptonym used to identify sensitive intelligence data. (Joint Pub 1-02)

collection - Acquisition of information and the provision of this information to processing and/or production elements. (Joint Pub 1-02) The gathering of intelligence data and information to satisfy the identified requirements. (MCRP 5-12C)

collection (acquisition) -The obtaining of information in any manner, including direct observation, liaison with official agencies, or solicitation from official, unofficial, or public sources. (Joint Pub 1-02)

collection agency - Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (Joint Pub 1-02)

collection management - The process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (Joint Pub 1-02)

collection plan - A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (Joint Pub 1-02)

collection requirement - An established intelligence need considered in the allocation of intelligence resources to fulfill the essential elements of information and other intelligence needs of a commander. (Joint Pub 1-02)

combat data - Data derived from reporting by operational units. (MCRP 5-12C)

combatant command - One of the unified or specified combatant commands established by the President. (Joint Pub 1-02)

combat information - Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (Joint Pub 1-02)

combat information center - The agency in a ship or aircraft manned and equipped to collect, display, evaluate, and disseminate tactical information for the use of the embarked flag officer, commanding officer, and certain control agencies. Certain control, assistance and coordination functions may be delegated by command to the combat information center. Also called "action information center." (Joint Pub 1-02)

combat intelligence - That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (Joint Pub 1-02)

combatant command -A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities.

combat surveillance - A continuous, all-weather, day-and-night, systematic watch over the battle area to provide timely information for tactical combat operations. (Joint Pub 1-02)

command and control - The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (Joint Pub 1-02) In Marine Corps usage, the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCRP 5-12C)

commander's critical information requirements - Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR. NOTE: CCIRs are normally divided into three primary subcategories: priority intelligence requirement; friendly force information requirements; and essential elements of friendly information. (MCRP 5-12C)

commander's intent - A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

communications intelligence -Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (Joint Pub 1-02)

communications intelligence data base -The aggregate of technical and intelligence information derived from the interception and analysis of foreign communications (excluding press, propaganda, and public broadcast) used in the direction and redirection of communications intelligence intercept, analysis, and reporting activities. (Joint Pub 1-02)

communications security - The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes:

1. cryptosecurity - The component of communications security which results from the provision of technically sound crypto-systems and their proper use.

2. transmission security -The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

3. emission security -The component of communications security which results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto equipment and telecommunications systems.

4. physical security-The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (Joint Pub 1-02)

compartmentation -Establishment and management of an intelligence organization so that information about the personnel, organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties. (Joint Pub 1-02)

complaint-type investigation - A counterintelligence investigation in which sabotage, espionage, treason, sedition, subversive activity, or disaffection is suspected. (Joint Pub 1-02)

component command - The service command, its commander, and all its individuals, units, detachments, organizations, or installations that have been assigned to the unified command. (Joint Pub 1-02)

compromise -The known or suspected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person. (Joint Pub 1-02)

compromised - A term applied to classified matter, knowledge of which has, in whole or in part, passed to an unauthorized person or persons, or which has been subject to risk of such passing. (Joint Pub 1-02)

confidential - National security information or material which requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security. (Joint Pub 1-02)

confirmation of information (intelligence) - An information item is said to be confirmed when it is reported for the second time, preferably by another independent source whose reliability is considered when confirming information. (Joint Pub 1-02)

confusion agent - An individual who is dispatched by the sponsor for the primary purpose of confounding the intelligence or counterintelligence apparatus of another country rather than for the purpose of collecting and transmitting information. (Joint Pub 1-02)

contingency - An emergency involving military forces caused by natural disasters, terrorists, subversives, or by required military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response, and special procedures to ensure the safety and readiness of personnel, installations, and equipment. (Joint Pub 1-02)

control - (1) Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. **(2)** In mapping, charting, and photogrammetry, a collective term for a system of marks or objects on the earth or on a map or a photograph, whose positions or elevations, or both, have been or will be determined.
(3) Physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. **(4)** An indicator governing the distribution and use of documents, information, or material. Such indicators are the subject of intelligence community agreement and are specifically defined in appropriate regulations. (Joint Pub 1-02)

controlled information -Information conveyed to an adversary in a deception operation to evoke desired appreciation. (Joint Pub 1-02)

coordinating authority--A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more Military Departments or two or more forces of the same Service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations. (Joint Pub 2-01.2)

coordination - The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (MCRP 5-12C)

counter-deception - Efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. Counter-deception does not include the intelligence function of identifying foreign deception operations. (Joint Pub 1-02)

counterespionage--That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities. (Joint Pub 1-02)

counter-guerrilla warfare - Operations and activities conducted by armed forces, paramilitary forces, or nonmilitary agencies against guerrillas. (Joint Pub 1-02)

counterinsurgency - Those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency. (Joint Pub 1-02)

counterintelligence – **(1)** Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. See also counterespionage; security. (Joint Pub 1-02) **(2)** Within the Marine Corps, counterintelligence (CI) constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. (MCRP 5-12C)

counterintelligence activities - The four functions of counterintelligence: operations; investigations; collection and reporting; and analysis, production, and dissemination. See also counterintelligence. (Joint Pub 2-01.2)

counterintelligence collection - The systematic acquisition of information (through investigations, operations, or liaison) concerning espionage, sabotage, terrorism, other intelligence activities or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons which are directed against or threaten Department of Defense interests. Includes Liaison and CFSO. (Joint Pub 2-01.2)

counterintelligence force protection source operations - Collection activities conducted by CI personnel to provide force protection support. These operations respond to local command requirements for force protection and do not fall within the purview of DCID 5/1. Also called CFSO. (MCRP 5-12C)

counterintelligence investigations - Counterintelligence investigations establish the elements of proof for prosecution or administrative action. Counterintelligence investigations can provide a basis for or be developed from conducting counter-intelligence operations. Counterintelligence investigations are conducted against individuals or groups suspected of committing acts of espionage, sabotage, sedition, subversion, terrorism, and other major security violations as well as failure to follow Defense agency and

military Service directives governing reporting of contacts with foreign citizens and "out-of-channel" requests for defense information. Counterintelligence investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise to improve the security posture of threatened interests. See also counterintelligence. (Joint Pub 2-01.2)

counterintelligence production--The process of analyzing all-source information concerning espionage, or other multi-discipline intelligence collection threats, sabotage, terrorism, and other related threats to US military commanders, the Department of Defense, and the US Intelligence Community and developing it into a final product which is disseminated. Counterintelligence production is used in formulating security policy, plans, and operations. See also counterintelligence. (Joint Pub 2-01.2)

countermeasures - That form of military science that by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (Joint Pub 1-02).

counter-reconnaissance - All measures taken to prevent hostile observation of a force, area, or place. (Joint Pub 1-02)

countersabotage - That aspect of counterintelligence designed to detect, destroy, neutralize, or prevent sabotage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting sabotage activities. (Joint Pub 1-02)

countersign - A secret challenge and its reply. (Joint Pub 1-02)

countersubversion - That aspect of counterintelligence designed to detect, destroy, neutralize, or prevent subversive activities through the identification, exploitation, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting subversive activities. (Joint Pub 1-02)

countersurveillance - All measures, active or passive, taken to counteract hostile surveillance. (Joint Pub 1-02)

counterterrorism - Offensive measures taken to prevent, deter, and respond to terrorism. Also called CT. (Joint Pub 1-02)

cover - (1) The action by land, air, or sea forces to protect by offense, defense, or threat of either or both. **(2)** Those measures necessary to give protection to a person, plan, operation, formation or installation from the enemy intelligence effort and leakage of information. **(3)** The act of maintaining a continuous receiver watch with transmitter calibrated and available, but not necessarily available for immediate use. **(4)** Shelter or protection, either natural or artificial. **(5)** Photographs or other recorded images which show a particular area of ground. **(6)** A code meaning, "Keep fighters between force/base and contact designated at distance stated from force/base" (e.g., "cover bogey twenty-seven to thirty miles"). (Joint Pub 1-02)

cover (military) - Actions to conceal actual friendly intentions, capabilities, operations, and other activities by providing a plausible, yet erroneous, explanation of the observable. (Joint Pub 1-02)

covert operations - Operations which are so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. They differ from clandestine operations in that emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation. (Joint Pub 1-02)

critical information - Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (Joint Pub 1-02)

critical vulnerability - An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. Also called CV. (MCRP 5-12C)

cultivation - A deliberate and calculated association with a person for the purpose of recruitment, obtaining information, or gaining control for these or other purposes. (Joint Pub 1-02)

current intelligence - Intelligence of all types and forms of immediate interest which is usually disseminated without the delays necessary to complete evaluation or interpretation. (Joint Pub 1-02)

D

damage assessment - (1) The determination of the effect of attacks on targets. **(2)** A determination of the effect of a compromise of classified information on national security. (Joint Pub 1-02)

deception - Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1-02)

decentralized control - In military operations, a mode of battlespace management in which a command echelon may delegate some or all authority and direction for warfighting functions to subordinates. It requires careful and clear articulation of mission, intent, and main effort to unify efforts of subordinate leaders. (MCRP 5-12C)

declassification - The determination that in the interests of national security, classified information no longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation. (Joint Pub 1-02)

departmental intelligence - Intelligence that any department or agency of the Federal Government requires to execute its own mission. (Joint Pub 1-02)

descriptive intelligence - Class of intelligence which describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: *basic intelligence*, which is general background knowledge about established and relatively constant conditions; and *current intelligence*, which is concerned with describing the existing situation. (MCRP 5-12C)

detachment - 1. A part of a unit separated from its main organization for duty elsewhere. 2. A temporary military or naval unit formed from other units or parts of units. (Joint Pub 1-02)

detection - (1) In tactical operations, the perception of an object of possible military interest but unconfirmed by recognition. **(2)** In surveillance, the determination and transmission by a surveillance system that an event has occurred. **(3)** In arms control, the first step in the process of ascertaining the occurrence of a violation of an arms-control agreement. (Joint Pub 1-02)

disaffected person - A person who is alienated or estranged from those in authority or lacks loyalty to the government; a state of mind. (Joint Pub 1-02)

dissemination - The timely conveyance of intelligence to users in a suitable form. (Joint Pub 1-02)

dissemination management - Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12C)

domestic intelligence - Intelligence relating to activities or conditions within the United States that threaten internal security and that might require the employment of troops; and intelligence relating to activities of individuals or agencies potentially or actually dangerous to the security of the Department of Defense. (Joint Pub 1-02)

double agent - Agent in contact with two opposing intelligence services, only one of which is aware of the double contact or quasi-intelligence services. (Joint Pub 1-02)

E

espionage - Actions directed towards the acquisition of information through clandestine operations. (Joint Pub 1-02)

espionage against the United States -Overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the

injury of the United States or to the advantage of a foreign nation. For espionage crimes see Chapter 37 of Title 18, United States Code. (Joint Pub 1-02)

essential elements of friendly information - Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. Also called EEFI. (Joint Pub 1-02) Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. (MCRP 5-12C)

estimative intelligence - Class of intelligence which attempts to anticipate future possibilities and probabilities based on an analysis of descriptive intelligence in the context of planned friendly and assessed enemy operations. (MCRP 5-12C)

evaluation - In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. Appraisal is accomplished at several stages within the intelligence cycle with progressively different contexts. Initial evaluations, made by case officers and report officers, are focused upon the reliability of the source and the accuracy of the information as judged by data available at or close to their operational levels. Later evaluations by intelligence analysts, are primarily concerned with verifying accuracy of information and may, in effect, convert information into intelligence. Appraisal or evaluation of items of information or intelligence is indicated by a standard letter-number system. The evaluation of the reliability of sources is designated by a letter from A through F, and the accuracy of the information is designated by numeral 1 through 6. These are two entirely independent appraisals, and these separate appraisals are indicated in accordance with the system below. Thus, information adjudged to be "probably true" received from an "usually reliable source" is designated "B-2" or "B2," while information of which the "truth cannot be judged" received from "usually reliable source" is designated "B-6" or "B6." (Joint Pub 1-02)

-- Reliability of Source

A - Completely reliable
B - Usually reliable
C - Fairly reliable
D - Not usually reliable
E - Unreliable
F - Reliability cannot be judged

-- Accuracy of Information

1 - Confirmed by other sources
2 - Probably true
3 - Possibly true
4 - Doubtful
5 - Improbable

6 - Truth cannot be judged

evasion and escape intelligence - Processed information prepared to assist personnel to escape if captured by the enemy or to evade capture if lost in enemy-dominated territory. (Joint Pub 1-02)

F

fabricator - Individuals or groups who, without genuine resources, invent information or inflate or embroider over news for personal gain or for political purposes. (Joint Pub 1-02)

force protection--Security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, CI, and other security programs. (Joint Pub 1-02)

foreign intelligence - Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence (with the exception of information on international terrorist activities). (Joint Pub 1-02)

friendly force information requirement - Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances information on unit location, composition, readiness, personnel status, and logistics status could become a friendly force information requirement. Also called FFIR. (MCRP 5-12C)

fusion - In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (Joint Pub 1-02)

G

global sourcing - A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

H

host country - A nation in which representatives or organizations of another state are present because of government invitation and/or international agreement. (Joint Pub 1-02)

host nation - A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, or to operate in, or to transit through its territory. (Joint Pub 1-02)

hostage - A person held as a pledge that certain terms or agreements will be kept. (The taking of hostages is forbidden under the Geneva Conventions, 1949.) (Joint Pub 1-02)

human intelligence - intelligence derived from information collected and provided by human resources. Also called HUMINT. (Jt Pub 1-02) HUMINT operations cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, the conduct of CI force protection source operations and controlled operations. (MCRP 5-12C)

human resources intelligence - The intelligence information derived from the intelligence collection discipline that uses human beings as both sources and collectors, and where the human being is the primary collection instrument. Also called HUMINT. (Joint Pub 1-02)

I

imagery - Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. (Joint Pub 1-02)

imagery exploitation -The cycle of processing and printing imagery to the positive or negative state, assembly into imagery packs, identification, interpretation, mensuration, information extraction, the preparation of reports and the dissemination of information. (Joint Pub 1-02)

imagery intelligence - Intelligence information derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices or other media. Also called IMINT. (Joint Pub 1-02)

imagery interpretation - (1) The process of location, recognition, identification, and description of objects, activities, and terrain represented on imagery. **(2)** The extraction of information from photographs or other recorded images. (Joint Pub 1-02)

imitative deception - The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. (Joint Pub 1-02)

indications and warning - Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (Joint Pub 1-02)

indications (intelligence) - Information in various degrees of evaluation, all of which bears on the intention of a potential enemy to adopt or reject a course of action. (Joint Pub 1-02)

indicator - In intelligence usage, an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action. (Joint Pub 1-02)

infiltration - (1) The movement through or into an area or territory occupied by either friendly or enemy troops or organizations. The movement is made, either by small groups or by individuals, at extended or irregular intervals. When used in connection with the enemy, it infers that contact is avoided. **(2)** In intelligence usage, placing an agent or other person in a target area in hostile territory. Usually involves crossing a frontier or other guarded line. Methods of infiltration are: black (clandestine); gray (through legal crossing point but under false documentation); white (legal). (Joint Pub 1-02)

informant - (1) A person who, wittingly or unwittingly, provides information to an agent, a clandestine service, or the police. **(2)** In reporting, a person who has provided specific information and is cited as a source. (Joint Pub 1-02)

information - (1) In intelligence usage, unevaluated material of every description that may be used in the production of intelligence. **(2)** The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1-02)

information exchange requirement - The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom as well as why the information is necessary and how that information will be used. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement. Also called IER. (MCRP 5-12C)

informer - Person who intentionally discloses to police or to a security service information about persons or activities considered suspect, usually for a financial reward. (Joint Pub 1-02)

infrared imagery - That imagery produced as a result of sensing electromagnetic radiation emitted or reflected from a given target surface in the infrared position of the electromagnetic spectrum (approximately 0.72 to 1,000 microns). (Joint Pub 1-02)

insurgency - An organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict. (Joint Pub 1-02)

integration - (1) A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. (2) In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or the process by which several photographic images are combined into a single image. (Joint Pub 1-02)

intelligence - **(1)** The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. knowledge about the enemy or the surrounding environment needed to support decision making. **(2)** Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (Joint Pub 1-02) In Marine Corps usage, intelligence is knowledge about the enemy or the surrounding environment needed to support decisionmaking. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence contingency funds - Appropriated funds to be used for intelligence activities when the use of other funds is not applicable or would either jeopardize or impede the mission of the intelligence unit. (Joint Pub 1-02)

intelligence cycle - The process by which information is converted into intelligence and made available to users. (Joint Pub 2-01)

intelligence data - Data derived from assets primarily dedicated to intelligence collection: imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline - a well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence), and open source intelligence. (Joint Pub 2-01)

intelligence estimate - The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (Joint Pub 1-02)

intelligence operations - The variety of intelligence tasks that are carried out by various intelligence organizations and activities. (Joint Pub 1-02)

intelligence preparation of the battlespace - An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (Joint Pub 1-02) In Marine Corps usage, a systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCRP 5-12C)

intelligence-related activities - (1) Those activities outside the consolidated defense intelligence program which: a. Respond to operational commander's tasking for time-sensitive information on

foreign entities; b. Respond to national intelligence community tasking of systems whose primary mission is support to operating forces; c. Train personnel for intelligence duties; d. Provide an intelligence reserve; or e. Are devoted to research and development of intelligence or related capabilities. **(2)** Specifically excluded are programs which are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data. (Joint Pub 1-02)

intelligence report - A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP. (Joint Pub 1-02)

intelligence reporting - The preparation and conveyance of information by any means. More commonly, the term is restricted to reports as they are prepared by the collector and as they are transmitted by him to his headquarters and by this component of the intelligence structure to one or more intelligence-producing components. Thus, even in this limited sense, reporting embraces both collection and dissemination. The term is applied to normal and specialist intelligence reports. (Joint Pub 1-02)

intelligence requirements - Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. Also called IR. (Joint Pub 1-02) In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. (MCRP 5-12C)

internal security - The state of law and order prevailing within a nation. (Joint Pub 1-02)

interpretation - A stage in the intelligence cycle in which the significance of information is judged in relation to the current body of knowledge. (Joint Pub 1-02)

interrogation - Systematic effort to procure information by direct questioning of a person under the control of the questioner. (Joint Pub 1-02)

interview (intelligence) - To gather information from a person who is aware that information is being given although there is ignorance of the true connection and purposes of the interviewer. Generally overt unless the collector is other than purported to be. (Joint Pub 1-02)

investigation - A duly authorized, systematized, detailed examination or inquiry to uncover facts and determine the truth of a matter. This may include collecting, processing, reporting, storing, recording, analyzing, evaluating, producing and disseminating the authorized information. (Joint Pub 1-02)

J

joint force - A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (Joint Pub 1-02)

joint force commander - A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. Also called JFC. (Joint Pub 1-02)

joint intelligence - Intelligence produced by elements of more than one Service of the same nation. (Joint Pub 1-02)

joint intelligence center - The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (Joint Pub 1-02)

joint operational intelligence agency - An intelligence agency in which the efforts of two or more Services are integrated to furnish that operational intelligence essential to the commander of a joint force and to supplement that available to subordinate forces of the command. The agency may or may not be part of such joint force commander's staff. (Joint Pub 1-02)

Joint Worldwide Intelligence Communications System - The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (Jt Pub 1-02)

L

law of war - That part of international law that regulates the conduct of armed hostilities. Also called the law of armed conflict. (Joint Pub 1-02)

liaison -That contact or intercommunication maintained between elements of military forces to ensure mutual understanding and unity of purpose and action. (Joint Pub 1-02)

M

main effort - The designated subordinate unit whose mission at a given point in time is most critical to overall mission success. It is usually weighted with the preponderance of combat power and is directed against a center of gravity through a critical vulnerability. (MCRP 5-12C)

maneuver warfare - A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. (MCRP 5-12C)

Marine Corps planning process - A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes

on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of mission analysis, course of action development, course of action analysis, comparison/decision, orders development, and transition. Also called MCPP. NOTE: Tenets of the MCPP include top down planning, single battle concept, and integrated planning. (MCRP 5-12C)

Marine expeditionary force -The Marine expeditionary force, the largest of the Marine air-ground task forces, is normally built around a division/wing team, but can include several divisions and aircraft wings, together with an appropriate combat service support organization. The Marine expeditionary force is capable of conducting a wide range of amphibious assault operations and sustained operations ashore. It can be tailored for a wide variety of combat missions in any geographic environment. Also called MEF. (Joint Pub 1-02)

Marine expeditionary force (Forward) - The designated lead echelon of a Marine expeditionary force, task-organized to meet the requirements of a specific situation. Also called MEF(Fwd). (MCRP 5-12C)

Marine expeditionary unit (special operations capable) - The Marine expeditionary unit is a task organization which is normally built around a battalion landing team, reinforced helicopter squadron, and logistic support unit. It fulfills routine forward afloat deployment requirements, provides an immediate reaction capability for crisis situations, and is capable of relatively limited combat operations. Also called MEU(SOC). (Joint Pub 1-02)

measurement and signature intelligence - Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same. Also called MASINT. (Joint Pub 1-02)

military intelligence - Intelligence on any foreign military or military-related situation or activity which is significant to military policy making or the planning and conduct of military operations and activities. (Joint Pub 1-02)

N

national intelligence - Integrated departmental intelligence that covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency. (Joint Pub 1-02)

need to know - A criterion used in security procedures which requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his official duties. (Joint Pub 1-02)

neutralize - As pertains to military operations, to render ineffective or unusable. (Joint Pub 1-02)

O

official information - Information which is owned by, produced for or by, or is subject to the control of the United States Government. (Joint Pub 1-02)

open source intelligence - information of potential intelligence value that is available to the general public. Also called OSINT. (Joint Pub 1-02)

operational control - Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. (Joint Pub 1-02)

operations security - A process of analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

order of battle - The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called OOB. (Jt Pub 1-02)

overt operation - The collection of intelligence openly, without concealment. (Joint Pub 1-02)

P

penetration - (1) In land operations, a form of offensive which seeks to break through the enemy's defense and disrupt the defensive system. (Joint Pub 1-02) **(2)** The recruitment of agents within, or the infiltration of agents or technical monitoring devices in an organization or group for the purpose of acquiring information or of influencing its activities. (Joint Pub 1-02)

personnel security investigation - An inquiry into the activities of an individual which is designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability. (Joint Pub 1-02)

physical security - That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub 1-02)

positive intelligence - A term of convenience sometimes applied to foreign intelligence to distinguish it from foreign counterintelligence.

principal agent - An agent who, under the direction of an intelligence officer, is responsible for the operational activities of other agents.

priority intelligence requirement - Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision making. Also called PIR. (Joint Pub 1-02) In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCRP 5-12C)

production management - Encompasses determining the scope, content, and format of each product, developing a plan and schedule for the development of each product, assigning priorities among the various IPRs, allocating processing, exploitation, and production resources, and integrating production efforts with collection and dissemination. (MCRP 5-12C)

R

ratline - An organized effort for moving personnel and/or material by clandestine means across a denied area or border. (Joint Pub 1-02)

reach back - The ability to exploit resources, capabilities, expertise, etc. not physically located in the theater or a joint area of operations, when established. (MCRP 5-12C)

rear area - For any particular command, the area extending forward from its rear boundary to the rear of the area of responsibility of the next lower level of command. This area is provided primarily for the performance of combat service support functions. (Joint Pub 1-02)

refugee - A civilian who by reason of real or imagined danger has left home to seek safety elsewhere. (Joint Pub 1-02)

repatriate -A person who returns to his country or citizenship, having left his native country, either against his will or as one of a group who left for reason of politics, religion, or other pertinent reasons. (Joint Pub 1-02)

restricted area - (1) An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize interference between friendly forces. **(2)** An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry. (Joint Pub 1-02)

rules of engagement - Directive issued by competent military authority which delineate the circumstances and limitations under which US forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE. (Joint Pub 1-02)

S

sabotage - An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources. (Joint Pub 1-02)

safe area - A designated area in hostile territory that offers the evader or escapee a reasonable chance of avoiding capture and of surviving until he can be evacuated. (Joint Pub 1-02)

safe haven - (1) Designated area(s) to which noncombatants of the United States Government's responsibility, and commercial vehicles and material, may be evacuated during a domestic or other valid emergency. **(2)** Temporary storage provided Department of Energy classified shipment transporters at Department of Defense facilities in order to assure safety and security of nuclear material and/or non-nuclear classified material. Also includes parking for commercial vehicles containing Class A or Class B explosives. (Joint Pub 1-02)

safe house - An innocent-appearing house or premises established by an organization for the purpose of conducting clandestine or covert activity in relative security. (Joint Pub 1-02)

sanitize - Revise a report or other document in such a fashion as to prevent identification of sources, or of the actual persons and places with which it is concerned, or of the means by which it was acquired. Usually involves deletion or substitution of names and other key details. (Joint Pub 1-02)

scientific and technical intelligence - The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: **(a)** foreign developments in basic and applied research and in applied engineering techniques; and **(b)** scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and material, the research and development related thereto, and the production methods employed for their manufacture. (Joint Pub 1-02)

security - **(1)** Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. **(2)** A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. **(3)** With respect to classified matter, it is the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (Joint Pub 1-02)

security classification - A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. There are three such categories:

a. Top secret - National security information or material which requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

b. Secret - National security information or material which requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

c. Confidential - National security information or material which requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security. (Joint Pub 1-02)

security clearance - An administrative determination by competent authority that an individual is eligible, from a security standpoint, for access to classified information. (Joint Pub 1-02)

security countermeasures - Defensive security programs and activities that seek to protect against both foreign intelligence collection efforts and unauthorized access to, or disclosure of, protected facilities, information, and material. (Joint Pub 2-01.2)

security intelligence - Intelligence on the identity, capabilities and intentions of hostile organizations or individuals who are or may be engaged in espionage, sabotage, subversion or terrorism. (Joint Pub 1-02)

sensitive - Requiring special protection from disclosure which could cause embarrassment, compromise, or threat to the security of the sponsoring power. May be applied to an agency, installation, person, position, document, material, or activity. (Joint Pub 1-02)

sensitive compartmented information - All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DOD 5200.1-R, Information Security Program Regulation.) Also called SCI. (Joint Pub 1-02)

sensor - An equipment which detects, and may indicate, and/or record objects and activities by means of energy or particles emitted, reflected, or modified by objects. (Joint Pub 1-02)

sensor data - Data derived from sensors whose primary mission is surveillance or target acquisition: air surveillance radars, counterbattery radars, remote ground sensors. (MCRP 5-12C)

signal security - A generic term that includes both communications security and electronic security. Also called SIGSEC. (Joint Pub 1-02)

signals intelligence - A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. (Joint Pub 1-02)

situational awareness - Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, enemy and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. Also called SA. (MCRP 5-12C)

source - (1) A person, thing, or activity from which intelligence information is obtained. **(2)** In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. **(3)** In interrogation activities, any person who furnishes intelligence information, either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. (Joint Pub 1-02)

special access program - Any program established under Executive Order 12356 that imposes additional controls governing access to classified information involved with such programs beyond those required by normal management and safeguarding practices. These programs may include, but are not limited to, access approval, adjudication or investigative requirements, special designation of officials

authorized to determine a need-to-know, or special lists of persons determined to have a need-to-know. Also called SAP. (Joint Pub 1-02)

special activities - As defined in Executive Order No. 12333, activities conducted in support of national foreign policy objectives that are planned and executed so that the role of the U.S. Government is not apparent or acknowledged publicly, but which are not intended to influence U.S. political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions. (Joint Pub 1-02)

special agent - A person, either United States military or civilian, who is a specialist in military security or the collection of intelligence or counterintelligence information. (Joint Pub 1-02)

special operations - Operations conducted by specially trained, equipped, and organized DOD forces against strategic or tactical targets in pursuit of national military, political, economic, or psychological objectives. These operations may be conducted during periods of peace or hostilities. They may support conventional operations, or they may be prosecuted independently when the use of conventional forces is either inappropriate or unfeasible. (Joint Pub 1-02)

split base - Two or more portions of the same force conducting or supporting operations from separate physical locations. (MCRP 5-12C)

stay behind - Agent or agent organization established in a given country to be activated in the event of hostile overrun or other circumstances under which normal access would be denied. (Joint Pub 1-02)

strategic intelligence - Intelligence that is required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application but may also vary in terms of scope and detail. (Joint Pub 1-02)

strategic warning - A warning prior to the initiation of a threatening act. (Joint Pub 1-02)

subversion - Action designed to undermine the military, economic, psychological, political strength or morale of a regime. (Joint Pub 1-02)

subversive activity - Anyone lending aid, comfort, and moral support to individuals, groups or organizations that advocate the overthrow of incumbent governments by force and violence is subversive and is engaged in subversive activity. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage will be placed in the category of subversive activity. (Joint Pub 1-02)

subversive political action - A planned series of activities designed to accomplish political objectives by influencing, dominating, or displacing individuals or groups who are so placed as to affect the decisions and actions of another government. (Joint Pub 1-02)

surveillance - The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (Joint Pub 1-02)

surveillance and reconnaissance center - Primary element responsible for the supervision of MAGTF intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called SARC. (MCRP 5-12C)

sustained operations ashore - The employment of Marine Corps forces on land for an extended duration. It can occur with or without sustainment from the sea. Also called SOA. (MCRP 5-12C)

T

tactical intelligence - Intelligence that is required for planning and conducting tactical operations. (Joint Pub 1-02) In Marine Corps usage, tactical intelligence concerns itself primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather. (MCRP 5-12C)

tactical intelligence and related activities - Those activities outside the National Foreign Intelligence Program that: a. respond to operational commanders' tasking for time-sensitive information on foreign entities; b. respond to national intelligence community tasking of systems whose primary mission is support to operating forces; c. train personnel for intelligence duties; d. provide an intelligence reserve; or e. are devoted to research and development of intelligence or related capabilities. Specifically excluded are programs which are so closely integrated with a weapon system that their primary function is to provide immediate use targeting data. Also called TIARA. (Joint Pub 1-02)

tactical warning - (1) A warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources. **(2)** In satellite and missile surveillance, a notification to operational command centers that a specific threat event is occurring. The component elements that describe threat events are: Country of origin -country or countries initiating hostilities. Event type and size -identification of the type of event and determination of the size or number of weapons. Country under attack-determined by observing trajectory of an object and predicting its impact point. Event time-time the hostile event occurred. Also called integrated tactical warning. (Joint Pub 1-02)

target - (1) A geographical area, complex, or installation planned for capture or destruction by military forces. **(2)** In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. **(3)** An area designated and numbered for future firing. **(4)** In gunfire support usage, an impact burst which hits the target. (Joint Pub 1-02)

target intelligence - Intelligence which portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (Joint Pub 1-02)

tasking - The process of translating the allocation into orders, and passing these orders to the units involved. Each order normally contains sufficient detailed instructions to enable the executing agency to accomplish the mission successfully. (Joint Pub 1-02)

task force counterintelligence coordinating authority (TFCICA) - The counterintelligence officer, or civilian equivalent, assigned responsibility for coordinating all counterintelligence activities within a joint task force. Also called TFCICA. The TFCICA has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Together, the TFCICA and the DHS's HUMINT Operations Cell (HOC) for the nucleus of the J-2X. (Joint Pub 2-01.2)

technical control - The performance of specialized or professional service, or the exercise of professional guidance or direction through the establishment of policies and procedures. (Proposed USMC definition for next revision of MCRP 5-12C.)

technical surveillance countermeasures - Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluid, and acoustic means, as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. Also called TSCM. (Joint Pub 2-01.2)

technical survey -A complete electronic and physical inspection to ascertain that offices, conference rooms, war rooms, and other similar locations where classified information is discussed are free of monitoring systems. (Joint Pub 1-02)

telecommunication - Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. (Joint Pub 1-02)

TEMPEST - An unclassified term referring to technical investigation for compromising emanations from electrically operated, information processing equipment; they are conducted in support of emanations and emissions security. (Joint Pub 2-01.2)

terrain intelligence - Processed information on the military significance of natural and man-made characteristics of an area. (Joint Pub 1-02)

terrorism - 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. (Joint Pub 1-02)

treason - Violation of the allegiance owed to one's sovereign or state; betrayal of one's country. (Joint Pub 1-02)

U

unconventional warfare --A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape. Also called UW. (Joint Pub 1-02)

unconventional warfare forces - United States forces having an existing unconventional warfare capability consisting of Army Special Forces and such Navy, Air Force, and Marine units as are assigned for these operations. (Joint Pub 1-02)

United States country team - The senior, in-country, United States coordinating and supervising body, headed by the Chief of the United States diplomatic mission, usually an ambassador, and composed of the senior member of each represented United States department or agency. (Joint Pub 1-02)

V

validation - A process normally associated with the collection of intelligence information that provides official status to an identified requirements and confirms that the requirement is appropriate for a given collector and has not previously been satisfied. (Joint Pub 1-02)

W

warfighting functions - The six mutually supporting military activities integrated in the conduct of all military operations are:

1. Command and control -- the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.

2. Maneuver -- the movement of forces for the purpose of gaining an advantage over the enemy.

3. Fires -- those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight.

4. Intelligence -- knowledge about the enemy or the surrounding environment needed to support decisionmaking.

5. Logistics -- all activities required to move and sustain military forces.

6. Force protection -- actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. (MCRP 5-12C)

warning - A communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures, to substantial increases in readiness and force preparedness, to acts of terrorism or political, economic, or military provocation. (Joint Pub 1-02)

APPENDIX B

COUNTERINTELLIGENCE PRINCIPAL & SUPPORTING EQUIPMENT

1. Marine Corps Common Equipment. The CI detachment or HUMINT exploitation team (HET) is the basic building block for CI HUMINT support to support a MAGTF or subordinate unit. The HET reports to the supported commander with their authorized organic equipment under the table of equipment (T/E) 4714 series. This generally includes at a minimum, but is not limited to, the following organic Marine Corps common equipment for each 3-man element and would require two sets to fully equip a HET:

Qty	Description
(1)	M998, High Mobility Multi-Purpose Wheeled Vehicle (HMMWV) Complete with SINGARS Radio mount
(1)	Trailer, Cargo, ¾ Ton, 2 Wheel, M101A3
(1)	Command Post (CP) Tent, with applicable support poles
(2)	Radar Scattering nets, with applicable support poles
(1)	Records Chest
(1)	Lantern Chest with (2) lanterns and Stove
(1)	SINGARS Radio (SL-3 Complete), Radio Set, AN/PRC-140B
(1)	Radio Set, AN/PRC-119A
(1)	Navigation Set, Satellite (PLGR) AN/PSN-11
(3)	Sleeping cots
(1)	6 Cube box containing, stools, extension cords, supplies etc.

2. CI/HUMINT Equipment Program (CIHEP). In addition to that equipment brought under T/E 4714, the CI/HUMINT company maintains a special allowance account of CI unique equipment maintained in the company's CI platoon's technical surveillance countermeasures (TSCM) team. This CIHEP allotment provides increased capabilities for conducting CI operations in an urban or non-tactical environment. The CIHEP allowance is continuously upgraded. The following are items currently included:

Qty	Description
(3)	Motorola SABER, Receiver - Transmitter
(3)	Antenna, Magnetic Mount
(1)	Motorola 20 Watt Base Station/Repeater
(1)	Digital Encryption Loader (DES)
(2)	Motorola SABER Recharger bank
(6)	SABER Batteries
(1)	Kodak DCS-420 Digital Camera Set

Qty	Description
(1)	CI/HUMINT Automated Tool Set (CHATS) containing a notebook computer, color printer, color scanner, DC-50 digital camera and secure communications and FAX capability.
(1)	AT&T 1100 STU-III Telephone
(1)	Tripod
(1)	Camera, Hi-8mm Video
(1)	Video capture card
(1)	Video, Hi-8mm, TV Recorder/Player, 5-Inch Screen
(1)	Video, Hi-8mm, TV Recorder/Player, 2 Inch Screen
(2)	Recorder, Microcassette
(1)	Metal Detector

3. CI/HUMINT AUTOMATED TOOL SET (CHATS) CURRENT CAPABILITIES. CHATS is a suite of hardware designed to meet the unique requirements of MAGTF CI/HUMINT elements. Operating up to the SECRET level and using the baseline and DCIIS software suite, the system provides the capability to manage assets and analyze information collected through investigations, interrogations, collection, and document exploitation. With CHATS, MAGTF CI elements may electronically store collected information in a local database, associate information with digital photography, and transmit/receive information over existing military and civilian communications. The CHATS provides these functions primarily with commercial off-the-shelf software operating in a laptop computer within a hardened transport case. Major systems components include:

Hard Drive

- Operating System: MS Windows 95/MS Plus for Windows 95
- Hardened System: Intel Pentium 166 MHz or faster
- Disk Drive: 1.3 GB Removable
- CD-ROM: 12X
- RAM: 32 MB
- Communications: STU-III (AT&T 1100) (unit provided) or Secure Terminal

Equipment (FY98)

- Secure FAX: Ilex PCMCIA
- External Modem: PCMCIA 33.6 BPS
- Digital Camera: Kodak Color DC50
- Printer: Cannon BJC-70
- Color Scanner: Logitec PowerPage
- Comms Paths: Ethernet Thin LAN, Commercial Telephone, CNR

Figure B-1. CI/HUMINT Automated Tool Set

When fully fielded[1], the system will enhance seamless integration of CI/HUMINT information from the HET to intelligence units throughout the MAGTF. Current planning envisions the capability to be global command and control system compliant and able to support the information exchange between CHATS and the Marine Corps intelligence analysis system (IAS), the army's all source analysis system (ASAS), and the joint community's joint deployable intelligence support system (JDISS).

PLANNED IMPROVEMENTS

Continuous and incremental upgrades to the CHATS through the entire product life-cycle. Current plans include:

FY 98	FY 99
INMARSAT-B Connectivity	Multi-Media Teleconference Capabilities
Tactical Radio Interface (TCIM/ViaSat Cards)	Read/Write CD-ROM Data Services
GPS Interface	Bulk Storage (Zip, LS-120, HiFD)

[1] Full operational capability is anticipated during fiscal year 1999.

APPENDIX C

Counterintelligence Operations Appendix

(Appendix 3 to Annex B, *Intelligence*)

CLASSIFICATION

Copy no. ___ of ___ copies
Issuing Unit
PLACE OF ISSUE
Date/time group
Message reference number

APPENDIX 3 TO ANNEX B TO OPORD XXX ( )
Counterintelligence Operations (U)

( ) **REFERENCES**: List unit standing operating procedures (SOP) for intelligence and counterintelligence, maps and any other relevant documents that authorize the various levels of anticipated CI operations.

1. ( ) **GENERAL**

a. ( ) Objectives. Discuss general objectives and guidance necessary to accomplish the mission.

b. ( ) Command Responsibilities and Reporting Procedures. Provide a general statement of command responsibilities and reporting procedures to ensure the flow of pertinent counterintelligence information to higher, adjacent, or subordinate commands.

c. ( ) CI Liaison Responsibilities. Discuss responsibility to coordinate and conduct liaison between command counterintelligence elements and those of other U.S. and allied commands and agencies.

d. ( ) Restrictions. Discuss the effect of U.S. Statutes, Executive Orders, DOD and Higher Headquarters Directives, and SOFA on counterintelligence activities.

2. ( ) **HOSTILE THREAT**. Summarize the foreign intelligence activity and collection threat; foreign security and CI threat; and threats from sabotage, terrorism, and assassination directed by foreign elements. Emphasize capabilities and intentions.

3. ( ) **COUNTERINTELLIGENCE ORGANIZATIONS**

a. ( ) Command's CI Structure. Provide strengths, locations, and capabilities (to include special qualifications) of command's CI assets.

b. ( ) Supporting Command/Agencies CI Structure. Provide strengths, locations, capabilities, and type of support to be provided.

c. ( ) Allied/Host Nation CI Structure. Provide strengths, locations, capabilities, and type of support anticipated.

4. ( ) **SECURITY**. Provide planning guidance concerning procedures and responsibilities for the following security activities:

a. ( ) Force or Headquarters

b. ( ) Military Security

c. ( ) Civil Authority

d. ( ) Port, Frontier, and Travel Security

e. ( ) Safeguarding Classified Information and Codes

f. ( ) Security Discipline and Security Education

g. ( ) Protection of Critical Installations

h. ( ) Special Weapons Security

i. ( ) Counterterrorist Measures

5. ( ) **COUNTERINTELLIGENCE PLANS, ACTIVITIES, AND FUNCTIONS**

a. ( ) Defensive. Identify the staff of those commands that have supporting counterintelligence assets and provide planning guidance concerning procedures, priorities and channels for:

(1) ( ) Counterintelligence Force Protection Source Operations (CFSO).

(2) ( ) Interrogatiion of enemy prisoners of war (EPW) and defectors.

(3) ( ) Screening of indigenous refugees, displaced persons, and detained suspects.

(4) ( ) Debriefing of U.S. or other friendly personnel who evade, escape, or are released from enemy control.

(5) ( ) Exploitation of captured documents and material.

b. ( ) Offensive. Establish guidance, to include control and coordination, for approval of counterespionage, countersabotage, countersubversion, counterterorist, double agent, deception and other special operations.

6. ( ) **COUNTERINTELLIGENCE TARGETS AND REQUIREMENTS**

a. ( ) Targets. Provide guidance to subordinate commands for developing counterintelligence targets based on an assessment of the overall counterintelligence threat. Designate priorities that emphasize the relative importance of the following counterintelligence target categories:

(1) ( ) Personalities

(2) ( ) Installations.

(3) ( ) Organizations and groups.

(4) ( ) Documents and material.

b. ( ) Priorities. Identify special counterintelligence collection requirements and priorities to be fulfilled by counterintelligence operations.

c. ( ) Miscellaneous. Identify any other command information required.

7. ( ) **COUNTERINTELLIGENCE PRODUCTION AND DISSEMINATION**. Provide guidance for the analysis, production, and dissemination of CI from all sources.

8. ( ) **ADMINISTRATION AND LOGISTICS**. Provide a statement of the administrative and logistic arrangements or requirements for CI not covered in the Basic Plan or in another Annex. Specific operational details on early deployments, mode of transportation, clothing, equipment, operational or contingency funds will be discussed according to the specific operation.

9. ( ) **COMMAND AND SIGNAL**

a. ( ) Command. Include details of conditions that would prompt change of command and procedures to implement that change during execution of the plan. Address what information and activities require the commander's knowledge and approval.

b. ( ) Communication. Ensure that communications requirements are addressed in Annex K. Unique communications requirement for CI should be addressed to include identifying what communication channels should be used.

10. ( ) **COORDINATION**. Identify coordination requirements peculiar to the counterintelligence activities listed in the paragraphs above.

Tabs

A - ( ) Counterintelligence Estimate
B - ( ) Counterintelligence List of Targets
C - ( ) Countersigns Challenges and Passwords

COUNTERINTELLIGENCE ESTIMATE

Purpose. Provides a baseline of historical, threat related information to support initial MAGTF for inclusion

---

CLASSIFICATION

Copy no. __ of __ copies
ISSUING HEADQUARTERS
PLACE OF ISSUE
Date/Time Group

TAB A TO APPENDIX 3 TO ANNEX B TO OPORD XXX ( )

Counterintelligence Estimate (U)

( ) REFERENCES: a. Unit standing operating procedures (SOP) for intelligence and counterintelligence.

b. JTF, NTF, other components, theater and national intelligence and counterintelligence plans, orders and tactics, techniques and procedures; and multinational agreements pertinent to intelligence operations.

c. Maps, charts and other intelligence and counterintelligence products required for an understanding of this annex.

d. Documents and online databases that provide intelligence required for planning.

e. Others as appropriate.

1. ( ) MISSION. (State the assigned task and its purpose.)

2. ( ) CHARACTERISTICS OF THE AREA OR OPERATIONS. (State conditions and other pertinent characteristics of the area which exist and may affect enemy intelligence, sabotage, subversive and terrorist capabilities and operations. Assess the estimated effects. Also, assess their effects on friendly counterintelligence capabilities, operations and measures. Reference appendix 8, *Intelligence Estimate*, to annex B, *Intelligence*, as appropriate.)

a. ( ) Military Geography

(1) ( ) (Existing situation)

(2) ( ) (Estimated effects on enemy intelligence, sabotage, subversive and terrorist operations and capabilities.)

(3) ( ) (Estimated effects on friendly counterintelligence operations, capabilities and measures.)

b. ( ) Weather

(1) ( ) (Existing situation)

(2) ( ) (Estimated effects on enemy intelligence, sabotage, subversive and terrorist operations and capabilities.)

(3) ( ) (Estimated effects on friendly counterintelligence operations, capabilities and measures.)

c. ( ) Other Characteristics. (Additional pertinent characteristics are considered in separate subparagraphs: sociological, political, economic, psychological, and other factors. Other factors may include but are not limited to telecommunications material, transportation, manpower, hydrography, science, and technology. These are analyzed under the same headings as used for military geography and weather.)

3. INTELLIGENCE, SABOTAGE, SUBVERSIVE, AND TERRORIST SITUATION

(Discusses enemy intelligence, sabotage, subversive, and terrorist activities as to the current situation and recent/significant activities. Include known factors on enemy intelligence, sabotage, subversive, and terrorist organizations. Fact sheets containing pertinent information on each organization may be attached to the estimate or annexes.)

a. ( ) Location and disposition.

b. ( ) Composition.

c. ( ) Strength, including local available strength, availability of replacements, efficiency of enemy intelligence, sabotage, subversive, and terrorist organizations.

d. ( ) Recent and present significant intelligence, sabotage, and subversive activities/movements (including enemy knowledge of our intelligence and counterintelligence efforts).

e. ( ) Operational, tactical and technical capabilities and equipment.

f. ( ) Peculiarities and weaknesses.

g. ( ) Other factors as appropriate.

4. ( ) INTELLIGENCE, SABOTAGE, SUBVERSIVE, AND TERRORIST CAPABILITIES AND ANALYSIS. (List separately each indicated enemy capability which can affect the accomplishment of the assigned mission. Each enemy capability should contain information on what the enemy can do, where they can do it, when they can start it and get it done, and what strength they can devote to the task. Analyze each capability in light of the assigned mission, considering all applicable factors from paragraph 2, and attempt to determine and give reasons for the estimated probability of adoption by the enemy. Examine the enemy's capabilities by discussing the factors that favor or militate against its adoption by the enemy. The analysis of each capability should also include a discussion of enemy strengths and vulnerabilities associated with that capability. Also, the analysis should include a discussion of any indications that point to possible adoption of the capability. Finally, state the estimated effect the enemy's adoption of each capability will have on the accomplishment of the friendly mission**.)**

a. ( ) Capabilities

(1) ( ) Intelligence. (Include all known/estimated enemy methods.)

(2) ( ) Sabotage. (Include all possible agent/guerilla capabilities for military, political, and economic sabotage.)

(3) ( ) Subversion. (Include all types, such as propaganda, sedition, treason, disaffection, and threatened terrorists activities affecting our troops, allies, and local civilians, and assistance in the escape and evasion of hostile civilians.)

(4) ( ) Terrorist. (Include capabilities of terrorist personalities and organizations in area of operation.)

b. ( ) Analysis and discussion of enemy capabilities for intelligence, sabotage, subversive, and terrorism as a basis to judge the probability of their adoption.

5. CONCLUSIONS AND VULNERABILITIES. (Conclusions resulting from discussion in paragraph 4. Relate to current all-source intelligence estimates of the enemy's centers of gravity, critical and other vulnerabilities and estimated exploitability of these by friendly forces, enemy courses of action beginning with the most probable and continuing down the list in the estimated order of probability, and the estimated effects adoption of each capability would have on the friendly mission.)

a. ( ) Probability of enemy adoption of intelligence, sabotage, subversive, and terrorist programs or procedures based on capabilities.

b. ( ) Effects of enemy capabilities on friendly course of action.

c. ( ) Effectiveness of our own counterintelligence measures and additional requirements or emphasis needed.

1 Enclosures

2 (As appropriate)
3

CLASSIFICATION

Copy no. ___ of ___ copies
Issuing Unit
PLACE OF ISSUE
Date/time group
Message reference number

TAB B TO APPENDIX 3 TO ANNEX B TO OPORD XXX ( )

Counterintelligence List of Targets (U)

1. ( ) Friendly Infrastructure. Develop a listing of offices and agencies where CI personnel can obtain CI information and assistance.

2. ( ) Foreign Intelligence and Security Service (FISS) Infrastructure. Develop a listing of specific offices and institutions within the FISS structure that can provide information of FISS targeting, operations, etc.

3. ( ) FISS Personalities. Develop and update a specific listing of FISS personalities who, if captured, would be of CI interrogation interest.

Countersigns Challenges and Passwords

1. Guidance and Procedures

a. Countersigns (challenge/password) are used during MAGTF operations as a means of positive identification of friendly personnel. Countersigns will, be changed daily at a predetermined time to be published in Annex C to the OPORDER. Compromise of the countersign will be reported immediately to the Command Element S-2 Section.

b. The countersigns list will be issued separately as Tab C to Appendix 3 to Annex B of the OPORDER. It will appear in the following manner:

Code	Challenge	Password	Alternate
11	Lamp	Wheel	9
12	Powder	Powder	7
13	Black	Table	8

c. Dissemination of the initial primary and alternate countersigns for the initial introduction of forces will be made in Annex B to the OPORDER. Subsequent countersign dissemination will be made by other secure means (i.e. covered radio nets) prior to the effective time. A sample message form is as follows:

"Code 11 countersign effective 011201(L) through 021200 (L). Alternate countersign Code 13."

Procedure: Alternate countersigns are any two numbers, that equal the alternate number, one given as the challenge, the other as the password reply.

d. If at any time, there is reason to believe that a password or countersign has been compromised, the unit which suspects the compromise will notify the MAGTF command element G/S-2 via the fastest means available. The command element will issue alternate and any changes to the remaining countersigns.

e. Below is the basic format for the countersigns challenges and passwords tab to appendix 3.

CLASSIFICATION

Copy no. ___ of ___ copies
Issuing Unit
PLACE OF ISSUE
Date/time group
Message reference number

TAB B TO APPENDIX 3 TO ANNEX B TO OPORD XXX ( )

Countersigns Challenges and Passwords (U)

1. ( ) This tab provides the initial dissemination of the primary and alternate countersigns to be used within the MAGTF. Subsequent countersign dissemination will be made by other security means prior to the effective time.

CODE/DATE	CHALLENGE	PASSWORD	ALTERNATE

APPENDIX D

COUNTERINTELLIGENCE ANALYSIS AND PRODUCTION

Section I

TACTICS, TECHNIQUES AND PROCEDURES FOR COUNTER-HUMAN INTELLIGENCE ANALYSIS AND PRODUCTION

1. General. Counter human intelligence (C-HUMINT) analysis increases in importance with each new US involvement in worldwide operations. Especially in MOOTW, C-HUMINT analysis is rapidly becoming a cornerstone upon which commanders base their concepts operations. This section presents information for analysts to develop some of those products that can enhance the probability of successful operations.

a. Counterintelligence (CI) analysts, interrogators, and CI agents maintain the C-HUMINT database. Using this database, they produce-

(1) Time event charts.

(2) Association matrices.

(3) Activities matrices.

(4) Link diagrams.

(5) HUMINT communication diagrams.

(6) HUMINT situation overlays.

(7) HUMINT-related portions of the threat assessment.

(8) CI target lists.

b. The analytical techniques used in HUMINT analysis enable the analyst to visualize large amounts of data in graphic form. We emphasize, however, that these analytical techniques are only tools used to arrive at a logical and correct solution to a complex problem; the techniques themselves are not the solution.

c. There are three basic techniques (tools) used as aids in analyzing HUMINT-related problems. These techniques-time event charting, matrix manipulation, and link diagramming-used together, are

critical to the process of transforming diverse and incomplete bits of seemingly unrelated data into an understandable overview of an exceedingly complex situation.

(1) Time Event Charting

(a) The time event chart (see figure D-1) is a chronological record of individual or group activities designed to store and display large amounts of information in as little space as possible. This tool is easy to prepare, understand, and use. Symbols used in time event charting are very simple. Analysts use triangles to show the beginning and end of the chart. They also use triangles within the chart to show shifts in method of operation or change in ideology. Rectangles or diamonds are used to indicate significant events or activities.

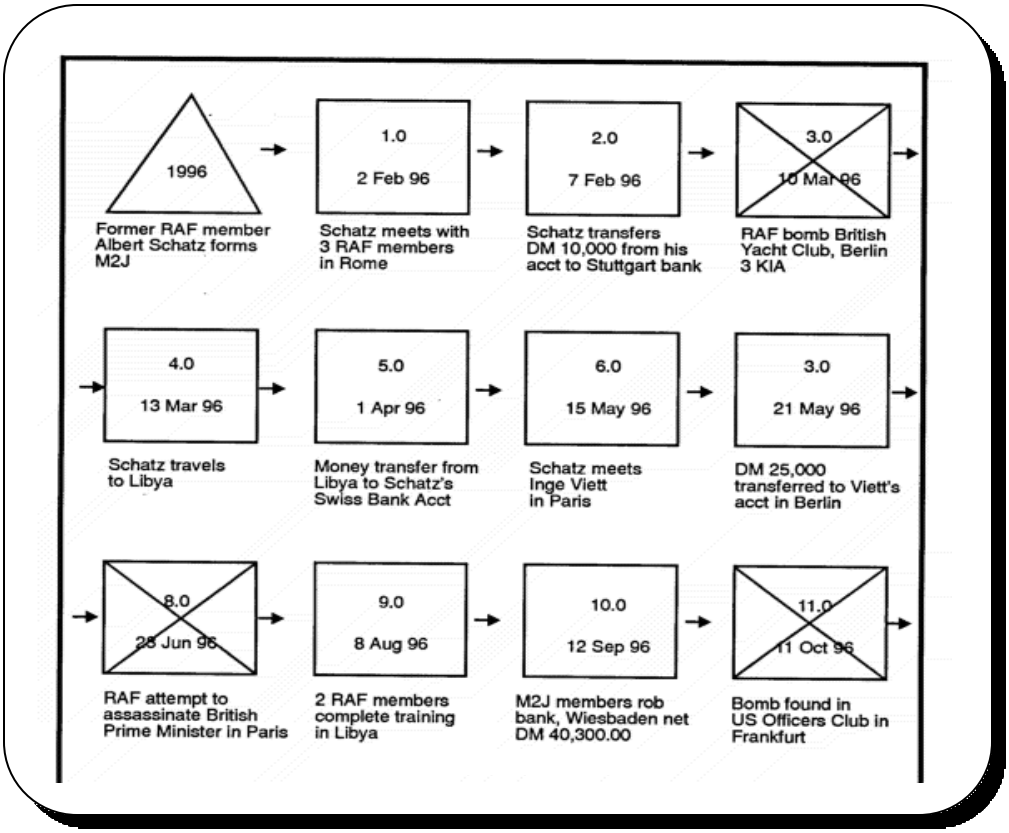


Figure D-1. Time Event Chart

(b) Analysts can highlight particularly noteworthy or important events by drawing an "X' through the event symbol (rectangle or diamond). Each of these symbols contains a chronological number (event number), date (day, month, and year of event), and may contain a file reference number. The incident description is a very brief explanation of the incident, and may include team size, type of incident or activity, place and method of operation, and duration of incident. Time flow is indicated by arrows.

(c) Analysts also use a variety of symbols such as parallelograms and pentagons, and others, to show different types of events and activities. Using these symbols and brief descriptions, the CI analyst can analyze the group's activities, transitions, trends, and operational patterns. Time event charts are excellent briefing aids as well as flexible analytical tools.

(2) Matrix Manipulation

(a) Construction of a matrix is the easiest and simplest way to show relationships between similar or dissimilar associated items. The 'items" can be anything relevant to the situation under investigation: persons, events, addressees, organizations, or telephone numbers. During this process, CI analysts use matrices to determine "who knows whom" or "who has been where or done what." This results in a clear and concise display which viewers can easily understand simply by looking at the matrix.

(b) In general terms, matrices resemble the mileage charts commonly found in a road atlas. Within the category of matrices, there are two types used in investigative analysis-association matrix and activities matrix.

1 **Association Matrix.** The association matrix is used to show that a relationship between individuals exists. Within the realm of HUMINT analysis, the part of the problem deserving the most analytical effort is the group itself. Analysts examine the group's elements (members) and their relationships with other members, other groups and associated entities, and related events. Analysts can show the connections between key players in any event or activity in an association matrix shown in (see figure D-2). It shows associations within a group or similar activity, and is based on the assumption that people involved in a collective activity know one another.

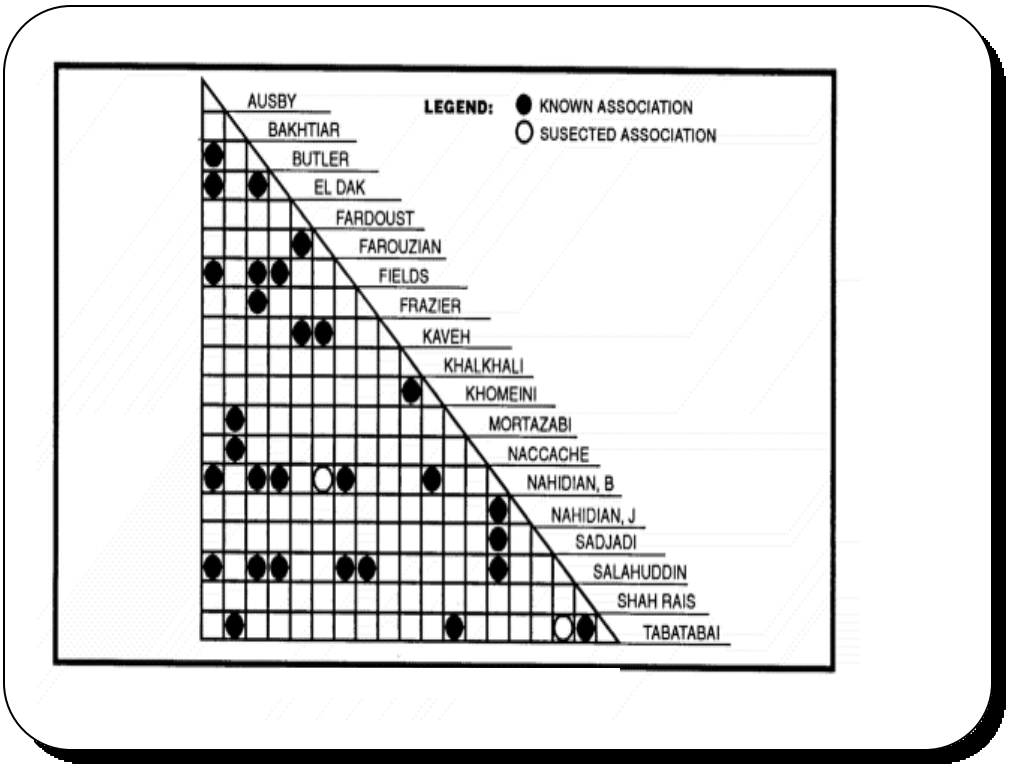


Figure D-2. Association Matrix

a This type of matrix is constructed in the form of a right triangle having the same number of rows and columns. Analysts list personalities in exactly the same order along both the rows and columns to ensure that all possible associations are shown correctly. The purpose of the personality matrix is to show who knows whom. Analysts determine a known association by "direct contact" between individuals. They determine direct contact by a number of factors, including face-to-face meetings, confirmed telephonic conversation between known parties, and all members of a particular organizational cell. (NOTE: When a person of interest dies, a diamond is drawn next to his or her name on the matrix.)

b CI analysts indicate a known association between individuals on the matrix by a dot or filled-in circle. They consider suspected or "weak" associations between persons of interest to be associations which are possible or even probable, but cannot be confirmed using the above criteria. Examples of suspected associations include-

- A known party calling a known telephone number (the analyst knows to whom the telephone number is listed), but cannot determine with certainty who answered the call.

- The analyst can identify one party to a face-to-face meeting, but may be able to only tentatively identify the other party.

(c) Weak or suspected associations on the personality matrix are indicated by an open circle. The rationale for depicting suspected associations is to get as close as possible to an objective analytic solution while staying as close as possible to known or confirmed facts. If analysts can confirm a suspected association, they can make the appropriate adjustment on the personality matrix.

(d) A secondary reason for depicting suspected associations is that it may give the analyst a focus for tasking limited intelligence collection assets to confirm the suspected association. An important point to remember about using the personality matrix: it will show only that relationships exist; not the nature, degree, or frequency of those relationships.

1 **Activities Matrix**. The activities matrix is used to determine connectivity between individuals and any organization, event, entity, address, activity, or anything other than persons. Unlike the association matrix, the activities matrix is constructed in the form of a square or a rectangle (see figure D-3). It does not necessarily have the same number of rows and can tailor rows or columns to fit the needs of the problem at hand or add them later as the problem expands in scope. The analyst determines the number of rows and columns by the needs of the problem and by the amount of information available.

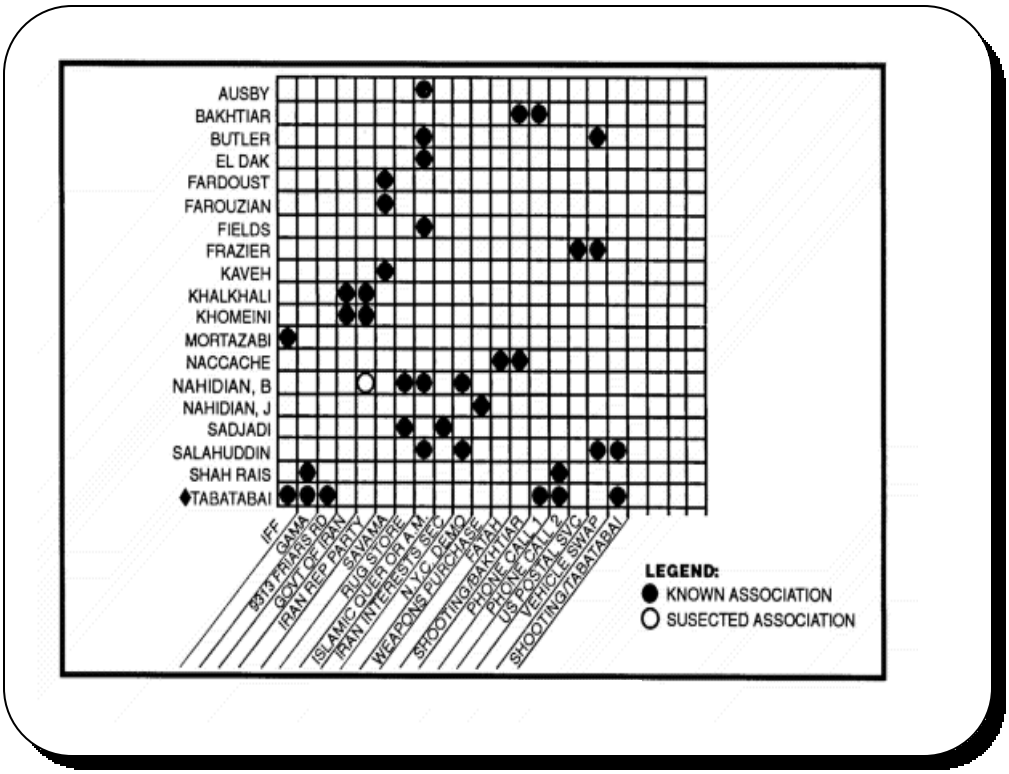


Figure D-3. Activities Matrix

a Analysts normally construct this matrix with personalities arranged in a vertical listing on the left side of the matrix; and activities, organizations, events, addresses, or any other common denominator arranged along the bottom of the matrix.

b This matrix can store an incredible amount of information about a particular organization or group, and can build on information developed in the association matrix. Starting with fragmentary information, the activities matrix can reveal an organization's-

- Membership.
- Organizational structure.
- Cell structures and size.
- Communications network.
- Support structure.
- Linkages with other organizations and entities.
- Group activities and operations.
- Organizational and national or international ties.

c As with the association matrix, known association between persons and entities is indicated by a solid circle, and suspected associations by an open circle.

d Analysts use matrices to present briefings, present evidence, or store information in a concise and understandable manner within a database. Matrices augment, but cannot replace, standard reporting procedures or standard database files. Using matrices, the analyst can:

- Pinpoint the optimal targets for further intelligence collection.
- Identify key personalities within an organization.
- Increase the analyst's understanding of an organization and its structure.

(3) **Link Diagramming.** The third analytical technique is the link diagram (see figure D-4). Analysts use this technique to depict the more complex linkages between a large number of entities, be they persons, events, organizations, or almost anything else. Analysts use link analysis in a variety of complex investigative efforts including criminal investigations, terrorism, analysis, and even medical research. Several regional law enforcement training centers are currently teaching this method as a

technique in combating organized crime. The particular method discussed here is an adaptation especially useful in CI investigative analysis in general and terrorism analysis in particular.

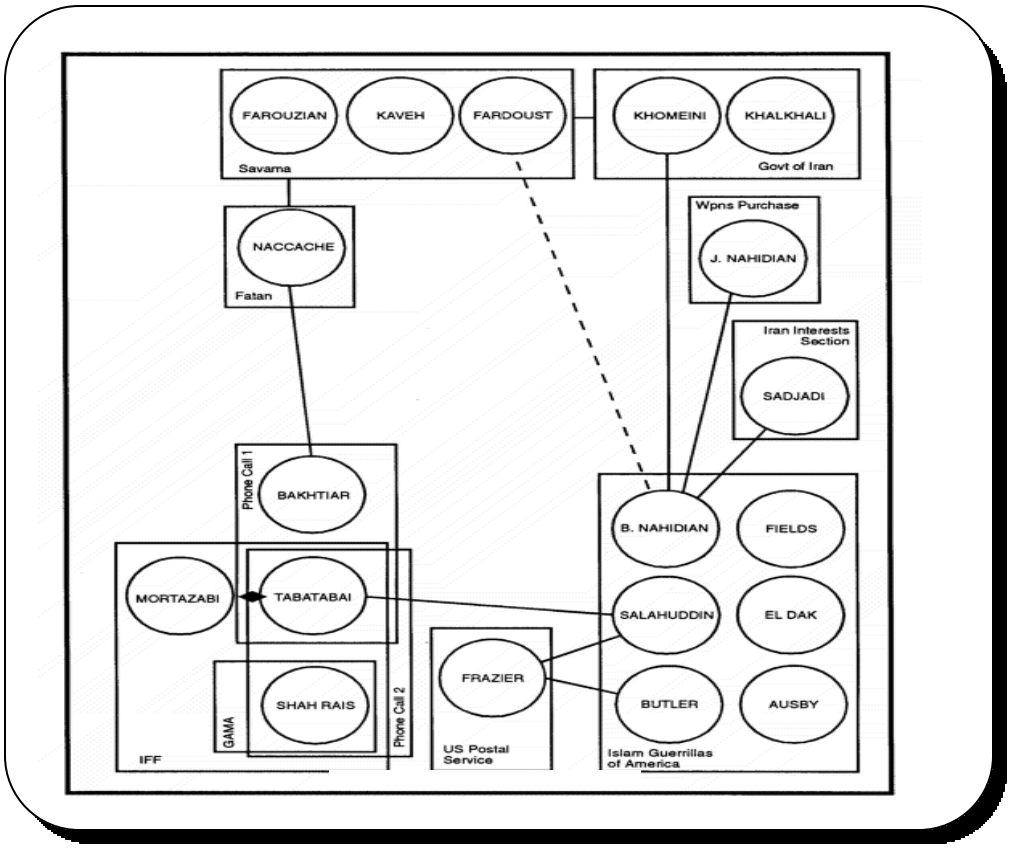


Figure D-4. Link Diagram

(a) The difference between matrices and link analysis is roughly the same as the difference between a mileage chart and a road map. The mileage chart shows the connections between cities using numbers to represent travel distances. The map uses symbols that represent cities, locations, and roads to show how two or more locations are linked to each other. Different symbols on the map have different meanings, and it is easy to display or discover the best route between two or more locations as well as identify obstacles such as unpaved roads or bodies of water.

(b) The same is true with link analysis. Different symbols are used to identify different items. Analysts can easily and clearly display obstacles, indirect routes or connections, and suspected connections. In many cases, the viewer can work with and follow the picture easier than the matrix. Link analysis can present information in a manner that ensures clarity.

(c) As with construction of association matrices, certain rules of graphics, symbology, and construction must be followed. Standardization is critical to ensure that everyone constructing, using, or reading a link diagram understands exactly what the diagram depicts. The standard rules follow:

1 1 Show persons as open circles with the name written inside the circle.

2 2 Show persons known by more than one name (alias, also known as [AKA]) as
3 overlapping circles with names in each circle.

4 3 Show deceased persons as above, with a diamond next to the circle representing that
5 person.

6 4 Show non-personal entities (organizations, governments, events, locations) by squares
7 or rectangles.

8 5 Show linkages or associations by lines: solid for confirmed and dotted for suspected.

9 6 Show each person or non-personal entity only once in a link diagram.

10 (d) Certain conventions must be followed. For the sake of clarity, analysts arrange circles
11 and squares so that whenever possible, lines of connectivity do not cross. Often, particularly when
12 dealing with a large or especially complex problem, it is difficult to construct a link diagram so that no
13 connecting lines cross. Intersecting lines, however, muddle the drawing and reduce clarity. If lines must
14 cross, show the crossing as a crossing, not as an intersection, in exactly the same manner as on an
15 electrical schematic or diagram.

16 (e) Link diagrams can show organizations, membership within the organization, action teams
17 or cells, or participants in an event. Since each individual depicted on a link diagram is shown only once,
18 and some individuals may belong to more than one organization or take part in more than one event,
19 squares or rectangles representing non-personal entities may overlap.

20 (f) Construct the appropriate association matrices showing "who knows whom," "who
21 participated in what," "who went where," and "who belongs to what group."

22 (g) Draw information from the database and intelligence reports, and relationships from the
23 matrices. Group persons into organizations or cells based on information about joint association,
24 activities, or membership. Draw lines representing connections between individuals, organizations, or
25 activities to complete the diagram. You may have to rearrange the diagram to comply with procedural
26 guidelines, such as crossed lines of connectivity. The finished product will clearly display linkages
27 between individuals, organizations, and other groupings.

28 (h) When you finish the matrices and link diagram, make recommendations about the
29 group's structure. Identify areas for further intelligence collection targeting. Task intelligence assets to
30 confirm suspected linkages and identify key personalities for exploitation or neutralization. The
31 combination of matrix manipulation and the link diagram present, in effect, a graphic depiction of an
32 extremely complex threat situation in a clear and concise picture.

(i) Overlapping organizations.

1 There is more to overlapping organizations than is immediately obvious. At first glance, the overlap indicates only that an individual may belong to more than one organization or has taken part in multiple activities. Further study and analysis would reveal connections between organizations, connections between events, or connections between organizations and events.

2 When, as is often the case, an organization or incident shown in a link diagram contains the names of more than one individual, it is not necessary to draw a solid line between those individuals to indicate connectivity. We assume that individual members of the same group or participants in the same activity know each other, and the connection between them is therefore implied.

(j) A final set of rules for link diagrams concerns connectivity between individuals who are not members of an organization or participants in an activity, but who are somehow connected to the group or activity. Two possibilities exist: The individual knows a member or members of the organization but is not directly connected with the organization itself. The person is somehow connected with the organization or activity but cannot be directly linked with any particular member of that organization or activity. In the first case, draw the connectivity line between the circle representing the individual and the circle representing the person within the organization or activity.

(k) If you keep in mind the preceding outline of principles and rules, you can construct a link diagram effectively. Because this is a rather complex form of analytical graphic display to construct, it may prove difficult at first and require a little extra time and effort. The payoff, however, is the powerful impact of the results, which are well worth the extra effort.

Section II

TACTICS, TECHNIQUES AND PROCEDURES FOR COUNTER-IMAGERY INTELLIGENCE ANALYSIS AND PRODUCTION

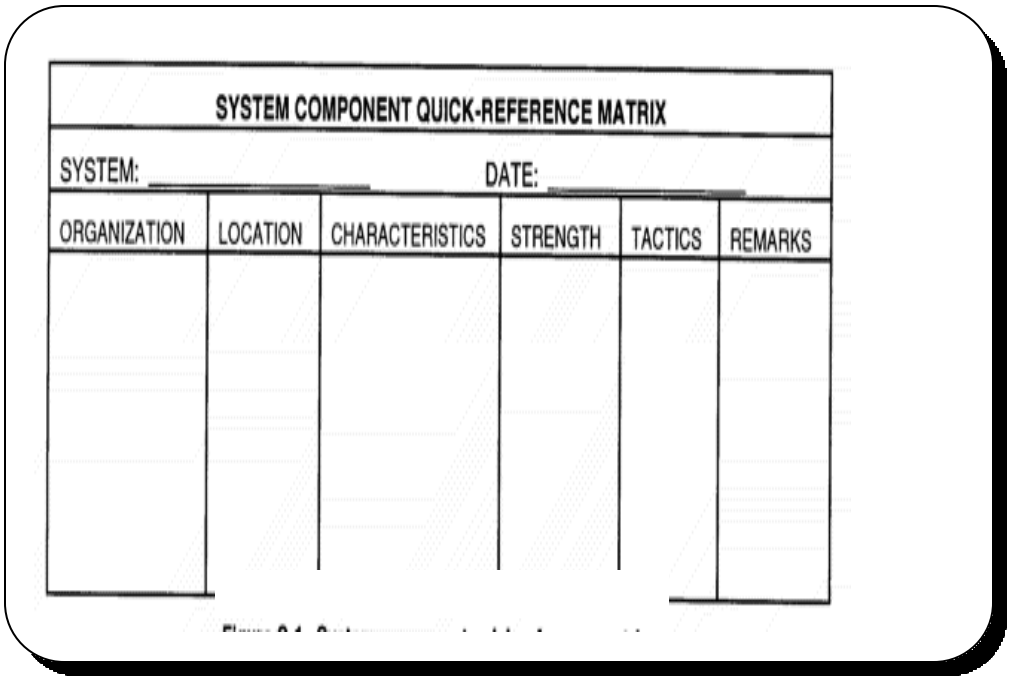
1. General. The proliferation of imagery systems worldwide, especially the platforms carrying imagery systems, makes the task of the counter imagery intelligence (C-IMINT) analyst much more complicated than ever before. Relatively inexpensive platforms that are easily transported and operated, such as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

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

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

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

(2) **System Component Quick Reference Matrix**. These matrices are concerned with adversary system's capabilities and processing times (see figure D-5). This file is part of the database which equates to an OOB file on threat IMINT systems.



SYSTEM COMPONENT QUICK-REFERENCE MATRIX

SYSTEM: _____ DATE: _____

ORGANIZATION	LOCATION	CHARACTERISTICS	STRENGTH	TACTICS	REMARKS

Figure D-5. Systems Component Quick Reference Matrix

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

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

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

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

(b) Locating command posts and other C2 facilities in the same relative position to maneuver elements and to each other.

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

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

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

(4) Analysis of a unit's movements gives significant clues to its intentions, capabilities, and objectives. By applying this technique against our own units, analysts can identify vulnerabilities. Movement analysis forms an important step in the identification and recommendation of countermeasures.

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

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

1 Conceal tracks by netting or other garnish.

2 Disperse turnouts near CPs.

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

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

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

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

3 Extending new roads beyond the CP to another termination.

4 Controlling unauthorized photographic equipment.

5 Using physical security measures to prevent optical penetration.

6 Using proper camouflage procedures.

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

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

9 Concealing equipment markings.

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

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

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

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

Section III

TACTICS, TECHNIQUES AND PROCEDURES FOR COUNTER-SIGNALS INTELLIGENCE ANALYSIS AND PRODUCTION

I. Threat SIGINT Capabilities and Assessment

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

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

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

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

d. The major information sources available to the CI analyst include:

(1) Validated finished intelligence products.

(2) Theater and national level SIGINT threat database.

(3) Previous tasking.

(4) Analyst experience.

(5) The CI database.

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

2. Procedures. There are six tasks associated with the C-SIGINT threat assessment (see figure D-6)[1].

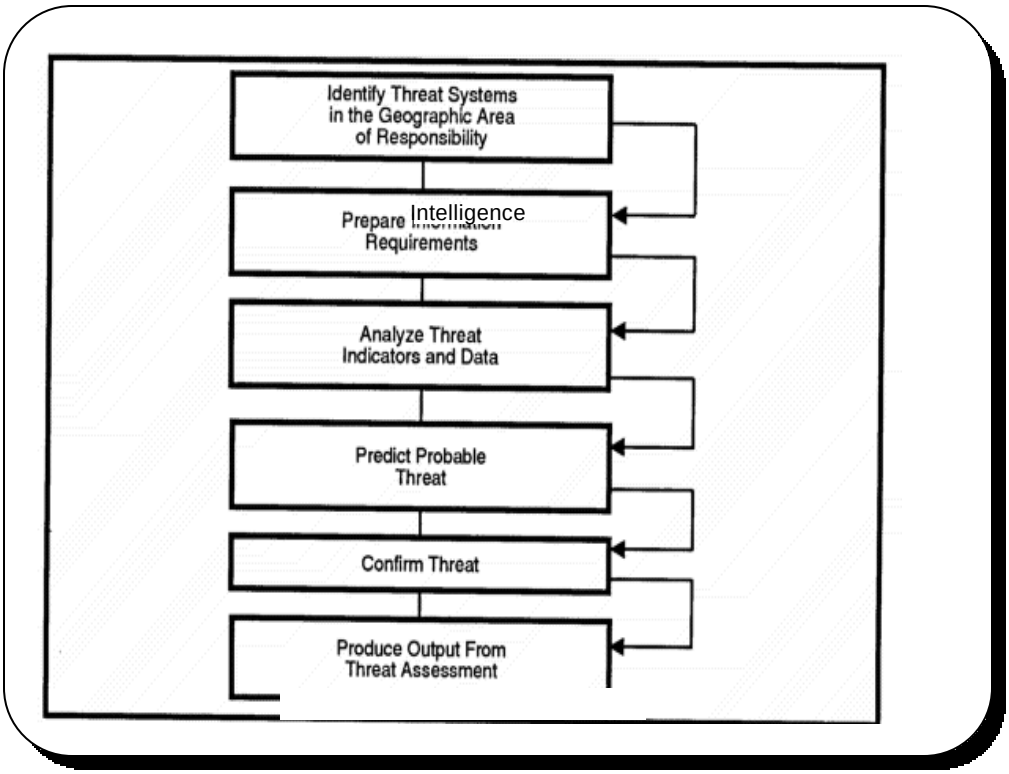


Figure D-6. C-SIGINT Threat Assessment Process

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

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

(a) ES and EA capability studies.

[1] Within a MAGTF, C-SIGINT analysis and production generally results from the integrated operations of the MAGTF all-source fusion center, the radio battalion operations control and analysis center, and the supporting CI/HUMINT company element.

(b) Hostile intelligence threat to the Army publications.

(c) SIGINT threat by country.

(d) SIGINT support to combat operations.

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

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

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

(a) Technical and operational capabilities.

(b) Typical modes of operation.

(c) Current deployment.

(d) Probable tasking.

(e) Activities of the collectors of interest.

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

(6) Summarize the data and identify the threat system. The CI analyst reviews the SIGINT situation overlay for patterns, electronic configurations, and threat C2, CIS and EW. Generally this information is available from either the MAGTF all-source fusion center (AFC) or the radio battalion's operations control and analysis center (OCAC). A common approach is to pose and answer questions, such as:

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

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

(c) How is the threat system doctrinally used?

(d) How does the threat system obtain information?

(e) How many collection systems were located?

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

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

c. Analyze threat indicators and data.

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

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

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

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

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

1 What area will the threat system target?

2 When will the targeting take place?

3 Why is the targeting taking place?

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

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

6 What does threat doctrine suggest about probable threat?

7 Does the threat system have a distinctive signature?

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

d. Estimate probable threat.

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

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

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

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

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

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

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

(2) Request additional information. If additional information is required, these intelligence requirements will be tasked to organic intelligence units or submitted to higher headquarters.

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

f. Produce output from SIGINT threat assessment. The CI analyst can present the SIGINT threat assessment in briefings or reports. Portions of the threat assessment are included and presented in other CI and all-source intelligence products.

II. MAGTF Vulnerability Assessment

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

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

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

(2) Collects and analyzes data to identify vulnerabilities.

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

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

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

(1) Technical data on C-E inventories.

(2) Doctrinal and SOP information.

(3) Output from the threat assessment step.

(4) Command friendly force information.

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

(6) PIR and IR.

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

d. MAGTF Vulnerability assessment is comprised of ten tasks. The first three tasks are ongoing determinations of general susceptibilities. The next six are specific to the commander's guidance and involve determinations of specific vulnerabilities. The final task is the output. MAGTF vulnerability assessment tasks are shown in figure D-7.

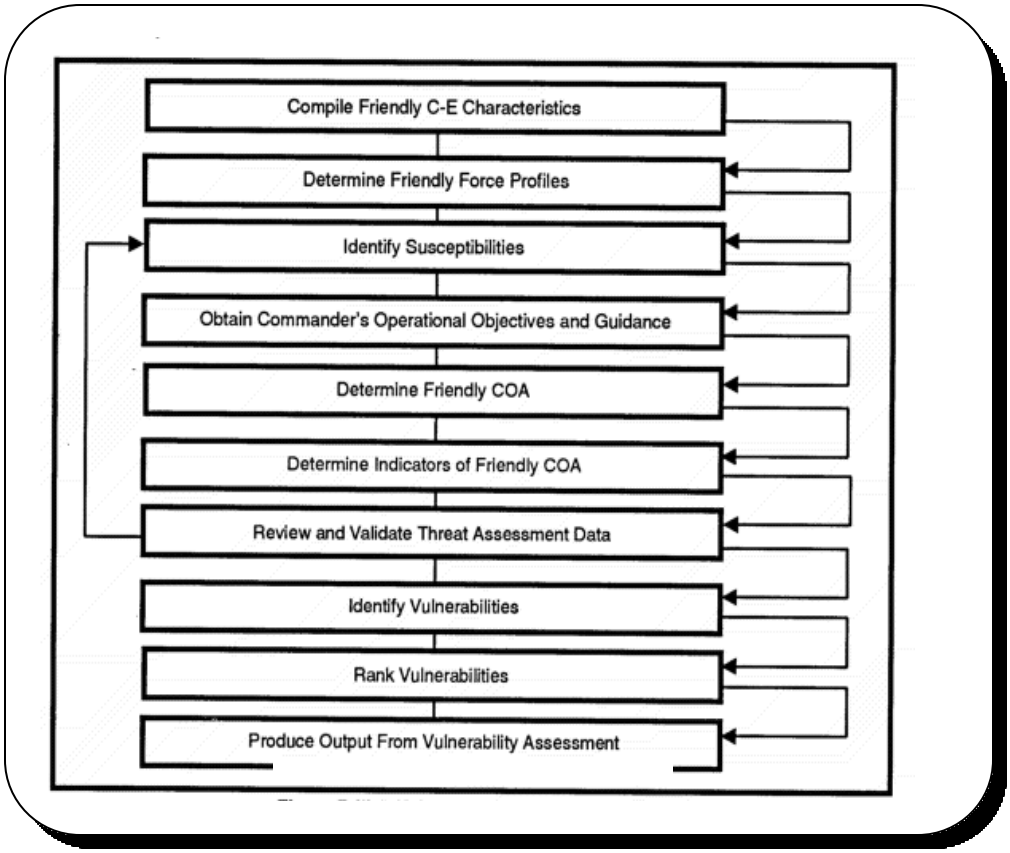


Figure D-7. MAGTF Vulnerability Assessment Process

2. Compile Friendly C-E Characteristics.

a. The CI analyst compiles friendly C-E characteristics. He collects and organizes unit C-E data and equipment characteristics for analysis. This analysis provides a baseline for analyzing friendly C-E equipment and operational susceptibilities to threat operations. The compilation of C-E characteristics is an ongoing process. Assistance from the command's communications and information systems (CIS) and electronic warfare officers should be able to provide all needed information..

b. The C-E data are a baseline for identifying friendly susceptibilities. A unit's equipment, personnel, and associated characteristics must be identified before the pattern and signature analysis can proceed. The CI analyst uses available databases to extract the table of equipment (T/E) and technical manuals (TM) on MAGTF C-E equipment.

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

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

(a) T/Es, TMs and technical data for all C-E equipment in a unit.

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

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

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

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

(f) Equipment supply requirements.

(g) Special combat support requirements.

(2) Organize C-E data. The CI analyst organizes the information into a format useful for signature analysis. The data are organized by type of unit (if the support is multi-unit), type of emitter, frequency range, number and type of vehicles or weapons which emit or carry emitters and the type of cluster.

3. Determine Friendly Force Profiles.

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

SIGNATURES + PATTERNS = PROFILE

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

(1) Analyze friendly force signatures. The CI analyst:

(a) Extracts organic equipment characteristics for the operation.

(b) Determines environmental effects.

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

(d) Determines C-E equipment employment.

(e) Compares planned use with technical parameters.

(f) Determines if further evaluation is required.

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

(h) Evaluates the information collected above.

(i) Diagrams physical and electronic signatures on an overlay or other product.

(j) Updates the CI database.

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

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

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

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

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

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

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

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

(d) Correlates signature and pattern data with past profiles to produce the current profile shown in figure D-8.

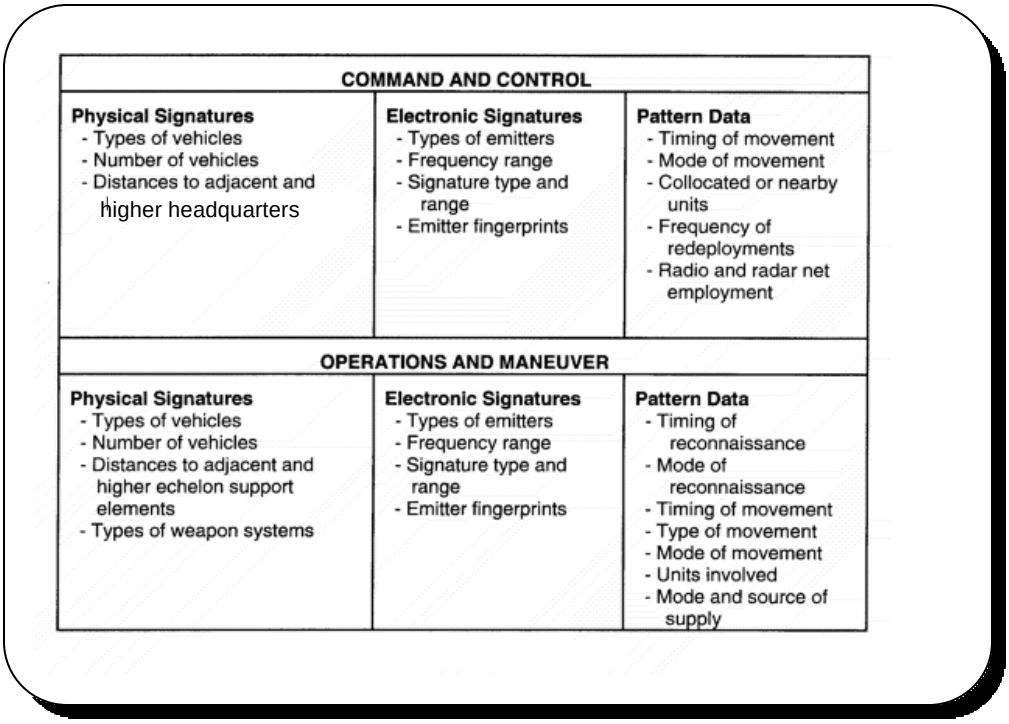


Figure D-8. Friendly Unit C-E Profile

(4) Produce unit profile. Patterns and signatures can change as commanders, staff, and operators change. Profile development must be an ongoing effort. To produce the unit profile, use the OPORD to obtain the past task organization and then select the areas of concern to that organization, that is, C2, intelligence, maneuver, fires, logistics, and force protection.

4. Identify Susceptibilities.

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

b. Information sources are of the following types:

(1) Current friendly C-E profile.

(2) Historical profiles to compare with current profile.

(3) Knowledge and experience from other analysts.

c. The procedures for identifying susceptibilities follow:

(1) Identify weaknesses:

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

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

(c) Plot friendly weaknesses to threat operations on a MAGTF electronic order of battle (EOB) overlay shown in.

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

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

(b) By activity (for example, logistic, CIS, intelligence, operations, and fire support).

(c) According to resource requirements.

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

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

5. Obtain Commander's Operational Objectives and Guidance.

a. The commander states his operational objectives for missions in OPLANs and OPORDs. The analyst uses this information to plan the most effective support for the commander and to identify the commander's preferences for types of operations. The commander's operational concept and an example of a unit EEFI statement as shown in figure D-9 are essential to the analysis of friendly COAs.

FRIENDLY SUPPORTED UNIT: 1ST MARDIV

1. **Subordinate Element: HQ, 1st MARDIV**
2. **Location: 32U NB51452035**
3. **Operational Objective: Defend to PL Gray; counterattack at 300001Z Oct 98**
4. **EEFI:**
   - **a. Significant Compromises:**
     - **(1) Time of counterattack**
     - **(2) Identification & location of regimental & & higher HQ elements**
     - **(3) Identification of attached units**
     - **(4) Loss/degradation of main C2 facilities or supporting comms & info systems**
   - **b. Insignificant Compromise: identification of 1st MARDIV**

Figure D-9. Example of a Unit EEFI Statement

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

(1) Concept of operation.

(2) OPORDs.

(3) OPLANs.

(4) Prioritized EEFIs.

6. Determine Friendly COA.

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

b. The procedures for determining friendly COA follow:

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

(a) Summary of operations.

(b) Higher headquarters support.

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

7. Determine Indicators of Friendly COA.

a. Indicators of friendly COA are those events and activities which, if known by the threat, would compromise a friendly COA.

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

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

(2) Integrate friendly profiles and COA. In the event planned location or movement data are not available, retrieve friendly operational overlays shown from the database. The overlays help identify friendly historical positions for the new COA. The integrate friendly force profiles and COAs:

(a) Noting current position and expected COA.

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

(c) Noting past C-E operational patterns.

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

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

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

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

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

(a) Inclement weather.

(b) Night activity.

(c) Terrain masking.

(d) Poor C-E equipment maintenance.

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

(6) Identify critical C-E nodes:

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

(b) List the indicators associated with a COA. Any special factors such as operational constraints, optimum weather conditions, or terrain requirements associated with an indicator should be described accordingly.

8. Review and Validate Threat Assessment Data.

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

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

(1) Summarize and reorganize threat assessment data.

(a) Compile recent threat assessment information.

(b) Identify information shortfalls.

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

(2) Extract relevant data for vulnerability assessment.

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

(b) Document threat capabilities and intentions.

(c) Store data for later application.

9. Identify Vulnerabilities.

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

b. The procedures for identifying vulnerabilities follow:

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

(a) Review indicators of friendly COA.

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

(c) Determine the probability of threat activity against MAGTF C-E operation.

(2) Determine which susceptibilities are vulnerabilities.

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

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

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

10. Rank Vulnerabilities.

a. The C-SIGINT analyst ranks the vulnerabilities by analyzing them in view of the indicators of friendly COAs and EEFIs. The ranking is based on criteria estimating the uniqueness, degree of

susceptibility, and importance of the vulnerability. The analyst designates the vulnerability as either critical, significant, or important to the success of the overall operation.

b. The procedures for ranking vulnerabilities follow:

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

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

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

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

(2) Compare vulnerabilities to criteria:

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

Vulnerability	EEFI	CRITERIA			Numerical Rating
		Uniqueness	Importance	Susceptibility	
MUX at main CP vulnerable to DF	4(a)2	5	5	4	14
MUX at main CP vulnerable to jamming	4(a)4	3	2	3	8

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 D-10. Vulnerability Matrix Format

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

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

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

(3) Develop ranking.

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

important; those between 9 and 11 are significant; and those falling between 12 and 15 would be critical.

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

11. Produce Output From Vulnerability Assessment. The CI analyst presents the vulnerability assessment findings as a briefing or a report to the commander, G/S-3, unit security manager, and other key staff members.

APPENDIX E

COUNTERINTELLIGENCE PLANS, REPORTS AND OTHER FORMATS

SECTION 1

COUNTERINTELLIGENCE ESTIMATE

Purpose. Provides a baseline of historical, threat related information for inclusion as Tab A of Appendix 3, *Counterintelligence* to Annex B, *Intelligence*.

CLASSIFICATION

Copy no. __ of __ copies
ISSUING HEADQUARTERS
PLACE OF ISSUE
Date/Time Group

COUNTERINTELLIGENCE ESTIMATE (Number)

( ) REFERENCES: a. Unit standing operating procedures (SOP) for intelligence and counterintelligence.

b. JTF, NTF, other components, theater and national intelligence and counterintelligence plans, orders and tactics, techniques and procedures; and multinational agreements pertinent to intelligence operations.

c. Maps, charts and other intelligence and counterintelligence products required for an understanding of this annex.

d. Documents and online databases that provide intelligence required for planning.

e. Others as appropriate.

1. ( ) MISSION. (State the assigned task and its purpose.)

2. ( ) CHARACTERISTICS OF THE AREA OR OPERATIONS. (State conditions and other pertinent characteristics of the area which exist and may affect enemy intelligence, sabotage, subversive and terrorist capabilities and operations. Assess the estimated effects. Also, assess their effects on friendly counterintelligence capabilities, operations and measures. Reference appendix 8, *Intelligence Estimate*, to annex B, *Intelligence*, as appropriate.)

a. ( ) Military Geography

(1) ( ) (Existing situation)

(2) ( ) (Estimated effects on enemy intelligence, sabotage, subversive and terrorist operations and capabilities.)

(3) ( ) (Estimated effects on friendly counterintelligence operations, capabilities and measures.)

b. ( ) Weather

(1) ( ) (Existing situation)

(2) ( ) (Estimated effects on enemy intelligence, sabotage, subversive and terrorist operations and capabilities.)

(3) ( ) (Estimated effects on friendly counterintelligence operations, capabilities and measures.)

c. ( ) Other Characteristics. (Additional pertinent characteristics are considered in separate subparagraphs: sociological, political, economic, psychological, and other factors. Other factors may include but are not limited to telecommunications material, transportation, manpower, hydrography, science, and technology. These are analyzed under the same headings as used for military geography and weather.)

3. INTELLIGENCE, SABOTAGE, SUBVERSIVE, AND TERRORIST SITUATION
(Discusses enemy intelligence, sabotage, subversive, and terrorist activities as to the current situation and recent/significant activities. Include known factors on enemy intelligence, sabotage, subversive, and terrorist organizations. Fact sheets containing pertinent information on each organization may be attached to the estimate or annexes.)

a. ( ) Location and disposition.

b. ( ) Composition.

c. ( ) Strength, including local available strength, availability of replacements, efficiency of enemy intelligence, sabotage, subversive, and terrorist organizations.

d. ( ) Recent and present significant intelligence, sabotage, and subversive activities/movements (including enemy knowledge of our intelligence and counterintelligence efforts).

e. ( ) Operational, tactical and technical capabilities and equipment.

f. ( ) Peculiarities and weaknesses.

g. ( ) Other factors as appropriate.

4. ( ) <u>INTELLIGENCE, SABOTAGE, SUBVERSIVE, AND TERRORIST CAPABILITIES AND ANALYSIS</u>. (List separately each indicated enemy capability which can affect the accomplishment of the assigned mission. Each enemy capability should contain information on what the enemy can do, where they can do it, when they can start it and get it done, and what strength they can devote to the task. Analyze each capability in light of the assigned mission, considering all applicable factors from paragraph 2, and attempt to determine and give reasons for the estimated probability of adoption by the enemy. Examine the enemy's capabilities by discussing the factors that favor or militate against its adoption by the enemy. The analysis of each capability should also include a discussion of enemy strengths and vulnerabilities associated with that capability. Also, the analysis should include a discussion of any indications that point to possible adoption of the capability. Finally, state the estimated effect the enemy's adoption of each capability will have on the accomplishment of the friendly mission**.)**

a. ( ) <u>Capabilities</u>

(1) ( ) <u>Intelligence</u>. (Include all known/estimated enemy methods.)

(2) ( ) <u>Sabotage</u>. (Include all possible agent/guerilla capabilities for military, political, and economic sabotage.)

(3) ( ) <u>Subversion</u>. (Include all types, such as propaganda, sedition, treason, disaffection, and threatened terrorists activities affecting our troops, allies, and local civilians, and assistance in the escape and evasion of hostile civilians.)

(4) ( ) <u>Terrorist</u>. (Include capabilities of terrorist personalities and organizations in area of operation.)

b. ( ) Analysis and discussion of enemy capabilities for intelligence, sabotage, subversive, and terrorism as a basis to judge the probability of their adoption.

5. <u>CONCLUSIONS AND VULNERABILITIES</u>. (Conclusions resulting from discussion in paragraph 4. Relate to current all-source intelligence estimates of the enemy's centers of gravity, critical and other vulnerabilities and estimated exploitability of these by friendly forces, enemy courses of action beginning with the most probable and continuing down the list in the estimated order of probability, and the estimated effects adoption of each capability would have on the friendly mission.)

a. ( ) Probability of enemy adoption of intelligence, sabotage, subversive, and terrorist programs or procedures based on capabilities.

b. ( ) Effects of enemy capabilities on friendly course of action.

c. ( ) Effectiveness of our own counterintelligence measures and additional requirements or emphasis needed.

/s/ _____
Name
Rank and Service

TABS:

(As appropriate)

DISTRIBUTION:

SECTION 2

COUNTERINTELLIGENCE REDUCTION PLAN

Purpose. A visual working tool for managing the CI targeting triad -- personalities, organizations and installations (PO&I) -- and unit assignments.

CLASSIFICATION

Counterintelligence Reduction Plan

PERSONALITY/INSTALLATION: Operation Bold Lighting MAP REF: Name, Series

TGT NO.	TARGET	LOCATION/ DESCRIPTION	PRI	CI TEAM ASSIGN	SPECIAL INSTRUCTIONS	INTERESTED UNITS/SECT.
1	Broadcasting Station	Grid coordinates 3 km NW of city on Victory Road	1	1	Locate/take into custody station state security officer and all propaganda file material	G-5/PAO
2	Government Control Center	Grid coordinates largest building in city center, gable roof	3	1	Ensure file information protected for further analysis	G-5
3	Military Intelligence Headquarters	Grid coordinates located on liberation military compound E of city	1	2	Locate/search CI and agent operations section	Task Force N2
4	Smith, John Q Intelligence Cadre	Grid coordinates military intelligence headquarters (above). Home address: 134 8th St, Apt 3B	2	2	Potential defector handle accordingly	10th Army MI
5	Infiltration Training Facility	Grid coordinates located W of city on seaward peninsula	3	2	Secure/search for file information on personalities and operations. Coordinate with Task Force N2	Task Force N2

CLASSIFICATION

CLASSIFICATION

TGT NO.	TARGET	LOCATION/ DESCRIPTION	PRI	CI TEAM ASSIGN	SPECIAL INSTRUCTIONS	INTERESTED UNITS/SECT.
6	Political Prison	Grid coordinates tri-angular shaped com-pound enclosed by 20-foot block wall bordered by Liberation Ave, 9th St, and bay	2	1	Personalities of CI interest on separate listing. Provide list of recovered personalities to HQ via most expedient means	G-5
7	National Intelligence Field Office	Grid coordinates located in concrete block building on corner of 5th St and Liberation Ave	1	2	Immediately evaluate all documents/ equipment	G-2

1 **CLASSIFICATION**

SECTION 3

COUNTERINTELLIGENCE SALUTE REPORT FORMAT

Purpose. A quick response report to get information into the All Source Correlated Database.

CLASSIFICATION

SALUTE

Reporting Unit:	(Text Field)
Record Creator:	(Text Field)
Report Number:	(Text Field)
References:	(Text Area)
Requirement Reference:	(Text Field)
Size (of Enemy Unit):	(Text Field)
Activity Type:	(Text Field w/Picklist)
Activity Status:	(Text Field w/Picklist)
Activity Location:	(Text Field)
Map Coordinates:	(Text Fields for --Latitude --Longitude --Map Grid Reference --UTM)
Activity Direction:	(Text Field)
Unit:	(Text Field)
Date Event Began/To Begin:	(Text Field)
Time Event Began/To Begin:	(Text Field)
Date Event Ended/Expected to end	(Text Field)
Time Event Ended/Expected to end	(Text Field)

CLASSIFICATION
CLASSIFICATION

Equipment:	(Text Area)
SRC #:	(Text Field)
SRC Description:	(Text Area)
SRC Reliability:	(Text Field w/Picklist)
Comments:	(Text Area)
Map Data:	(Text Field)

CLASSIFICATION

_____

Additional Requirement:

a. Army tactics, techniques and procedures requires that transmit portions of the SALUTE report to its "ASAS" (All Source Automated System). Hence, there is a requirement to parse some data elements of a completed SALUTE message into U. S. message text format.

b. The TCP for DCIIS V2.0 includes a requirement to convert the CIIR from its database record format to the USMTF message format as a step in transforming the CIIR into an IIR. The technique to accomplish the CIIR requirement may be applicable to the SALUTE requirement.

SECTION 4

COUNTERINTELLIGENCE INFORMATION REPORT

Purpose. A standard report used to report tactical CI information.

CLASSIFICATION

CI Information Report

Record ID: .....
Point of Contact: .....
Classification: .....
Abstract: .....
Discretionary Access Control: .....
Caveats: .....

Release To: .....

Record Type: .....
Record Status: .....
Date Created *(yyyymmdd)*: .....
Date Modified *(yyyymmdd)*: .....
Community of Interest: .....
Source Record: .....

Requirement Reference: .....
Requirement: .....

Title (*Text*):

Report Number: .....
Report Date *(yyyymmdd)*: .....
To: .....
Target: .....

Individual Source: .....
Reliability of the Source: .....
Source ID Number: .....
Information Reliability: .....
Information Date *(yyyymmdd)*: .....
Collection Date *(yyyymmdd)*: .....
Location: .....

Report (*Text*):

Comments (*Text*):

1

SECTION 5

COUNTERINTELLIGENCE FORCE PROTECTION SOURCE OPERATIONS CONCEPT PROPOSAL

Purpose. Serves as the planning, approval, and execution vehicles for MAGTF Counterintelligence Force Protection Source Operations.

_____

CLASSIFICATION

CFSO Umbrella Concept Proposal

From:	(Originator)	(Text Field—Picklist?)
To:	(Next Higher Echelon)	(Text Field—Picklist?)
Info:	(Addees to be informed)	(Text Area—Picklist?)

Project Number:	(Text Field)
Name:	(Text Field)
Originating Hqs:	(Text Field)
Implementing Element:	(Text Field)
Collection Requirements:	(Text Area)
References:	(Text Area)
Date Submitted:	(Text Field)
Date Approved:	(Text Field)
Approval Authority:	(Text Field)
Operation Type:	(Text Field w/Picklist)
Target Focus:	(Text Area)
Target Personnel:	(Text Area)
Target Country:	(Text Area)
Organizations:	(Text Area)
Base of Operations:	(Text Field)
Communications Methods	(Text Area)

CLASSIFICATION

CLASSIFICATION

Risks: (Text Area)

Technical Support: (Text Area)

Finances: (Text Area)

Coordination: (Text Area)

Administration and Management: (Text Area)

Additional Support Requirements: (Text Area)

Point of Contact: (Text Field)

CLASSIFICATION

SECTION 6

COUNTERINTELLIGENCE SOURCE LEAD DEVELOPMENT REPORT

Purpose. For local planning and development of counterintelligence sources.

CLASSIFICATION

Source Lead Development Report

Date:		(Text Field)	(Mandatory)
Subject:		(Text Field)	(Mandatory)
Report No:		(Text Field)	
Project No:		(Text Field)	
References:		(Text Field)	
Record Creator:		(Text Field)	(Mandatory)
Origin:			
	Source of Lead	(Text Field)	(Mandatory)
	Proposed Use of Lead	(Text Area)	
	Lead Screening Process	(Text Area)	
	Placement and Access	(Text Area)	
	Circumstances for Meeting with Source	(Text Area)	
	Security Issues	(Text Area)	
Personnel Information:			
	Lead Status	(Text Area)	
	Nationality	(Text Field)	
	Citizenship	(Text Field w/PL)	

CLASSIFICATION

CLASSIFICATION

Personality and Character Traits

Motivation	(Text Area)
Character	(Text Area)
Personality	(Text Area)
Trait Exploitation	(Text Area)

Biographical Data

(Link to the INDIVIDUAL record. When printing, whole INDIVIDUAL record needs to print out.)

Summary of Family/Personal History (Text Area)

(Consider autopopulate from INDVIDUAL *record.)*

Investigative Checks:

Type (Text Field w/PL) Status (Text Field w/PL) Date (Text Field w/PL)

Coordination Required (Text Field w/PL) (Multiple Choice)

Assessment of Operational Potential:

Type of Source	(Text Field w/PL)
Placement	(Text Area)
Access	(Text Area)
Cover (For Status & Action)	(Text Area)
Qualifications	(Text Area)
Personal	(Text Area)

Motivation (Text Area)

Strengths/Weaknesses (Text Area)

CLASSIFICATION

CLASSIFICATION

Risk

To C/O & Collection Element (Text Area)

To Source (Text Area)

Approach Plan: (Text Area)

ICF: (Text Area)***

Comments: (Text Area)

Attachments: *(Standard Repeating Group)*

CLASSIFICATION

SECTION 7

COUNTERINTELLIGENCE SCREENING REPORT

Purpose. Used to report information obtained during CI screening operations.

CLASSIFICATION

Screening Report

Reporting Unit: (Text Field)

Screener: (Text Field)

Report Date: (Text Field)

Report Time: (Text Field)

Capturing Unit: (Text Field)

Requirement Reference: (Text Field)

Status: (Text Field w/PL)

PL - Military
Paramilitary
Civilian
Other

Name: (Text Field)

Alternate Name(s): (Repeating Group)

Personal ID No: (Text Field)

EPW ID No: (Text Field)

Date of Birth: (Text Field)

Sex: (Text Field w/PL)

Marital Status: (Text Field)

CLASSIFICATION

CLASSIFICATION

Language Competence: *(Use text and field input from DCIIS Individual form)*

Language Used: (Text Field)

Education: *(Use text and field input from DCIIS Individual form)*

Employment: *(Use text and field input from DCIIS Individual form)*

Military Service: *(Use text and field input from DCIIS Individual form)*

Date Captured: (Text Field)

Time Captured: (Text Field)

Place Captured: (Text Field)

Circumstances of Capture: (Text Area)

Documents at Capture: (Text Area)

Equipment Captured: (Text Area)

Source's Physical Condition: (Text Field w/PL)

Remarks: (Text Area)

Source's Mental State: (Text Field w/PL)

Source's Intelligence Level: (Text Field w/PL)

Specific Knowledgeability: (Text Area)

Source's Cooperation: (Text Field w/PL)

EPW Category (Text Field w/PL)

1	CI Interest	(Text Field w/PL)
2	Source's Current Location:	(Text Field)
3	Approach Plan	(Text Field w/PL)
4	Comments:	(Text Area)
5	**CLASSIFICATION**	

SECTION 8

COUNTERINTELLIGENCE TACTICAL INTERROGATION REPORT

CLASSIFICATION

Tactical Interrogation Report

Reporting Unit: (Text Field)

Report No:	(Text Field)	Record Creator:	(Text Field)
Report Date:	(Text Field)	Interpreter:	(Text Field)
Report Time:	(Text Field)	Language Used:	(Text Field w/PL)

Capturing Unit: (Text Field)

Requirement Reference: (Text Field)

Map Data: (Text Area)

Source No: (Text Field)

Source Status: (Text Field w/PL)

Name: (Text Field)

Alternate Name(s): (Repeating Group)

Personal ID No: (Text Field)

EPW ID No: (Text Field)

Place of Birth: (Text Field)

Date of Birth: (Text Field)

Nationality: (Text Field)

1 Sex: (Text Field w/PL)

2 **CLASSIFICATION**
3 **CLASSIFICATION**

4 Marital Status: (Text Field)

5 Language Competence: *(Use text and field input from DCIIS Individual form)*

6 Language Used: (Text Field)

7 Education: *(Use text and field input from DCIIS Individual form)*

8 Employment: *(Use text and field input from DCIIS Individual form)*

9 Military Service: *(Use text and field input from DCIIS Individual form)*

10 Date Captured: (Text Field)

11 Time Captured: (Text Field)

12 Place Captured: (Text Field)

13 Circumstances of Capture: (Text Area)

14 Documents at Capture: (Text Area)

15 Equipment Captured: (Text Area)

16 Source's Physical Condition: (Text Field w/PL)

17 Source's Mental State: (Text Field w/PL)

18 Source's Intelligence Level: (Text Field w/PL)

19 Specific Knowledgeability: (Text Area)

20 Source's Cooperation: (Text Field w/PL)

21 EPW Category (Text Field w/PL)

1 CI/Humint Interest (Text Field w/PL)

2 Source's Current Location: (Text Field)

3 Source's Reliability: (Text Field)

4 **CLASSIFICATION**
5 **CLASSIFICATION**

6 Source's Production (Text Area)

7 Approach Plan (Text Field w/PL)

8 Comments: (Text Area)

9 **CLASSIFICATION**
10 _____

SECTION 9

INTELLIGENCE INFORMATION REPORT

Purpose. Standard report used to report unevaluated, unanalyzed intelligence information.

CLASSIFICATION

Intelligence Information Report

From: (Text Field)

To: (Text Field)

Info: (Text Field)

Serial: (Text Field)

Country: (Text Field)

//IPSP: (Text Field)

Subj: (Text Area)

WARNING: (U) THIS IS AN INFORMATION REPORT, NOT FINALLY EVALUATED INTELLIGENCE. REPORT CLASSIFIED *(Autopopulate with classification)*

DEPARTMENT OF DEFENSE

DOI: (Text Field)

REQS: (Text Area) (*Association Mechanism)*

SOURCE: (Text Area)

SUMMARY: (Text Area)

TEXT: (Text Area)

COMMENTS:

1 (FIELD COMMENT) (Text Area)

2 **CLASSIFICATION**
3 **CLASSIFICATION**

4 PROJ: (Text Field)

5 INSTR: US NO (Text Field)

6 PREP: (Text Field)

7 ENCL: (Text Field) *(Repeating Group)*

8 ACQ: (Text Field)

9 DISSEM: FIELD-- (Text Field)

10 WARNING: REPORT CLASSIFIED (Text Field) *(Autopopulate)*

11 DRV FROM-- (Text Field)

12 DECL: (Text Field)

13 **CLASSIFICATION**
14 _____

SECTION 10

INTELLIGENCE INFORMATION REPORT -- BIOGRAPHICAL

Purpose. Standard report used to report unevaluated, unanalyzed biographical intelligence information.

CLASSIFICATION

Intelligence Information Report -- Biographical

FROM: (Text Field)

TO: (Text Field)

INFO: (Text Field)

SERIAL: (Text Field)

COUNTRY: (Text Field)

//IPSP: (Text Field)

SUBJ: (Text Area)

WARNING: (U) THIS IS AN INFORMATION REPORT, NOT FINALLY EVALUATED INTELLIGENCE. REPORT CLASSIFIED *(Autopopulate with classification)*

DEPARTMENT OF DEFENSE

DOI: (Text Field)

REQS: (Text Area) (*Association Mechanism)*

SOURCE: (Text Area)

SUMMARY: (Text Area)

CLASSIFICATION

CLASSIFICATION

TEXT:

1. Name of Country (Text Field w/PL)

2. Date of Information (Text Field)

3. Date of Report (Text Field)

4A. Full Name (Text Field)

4B. Name(s) By Which Individual Prefers To Be Addressed

4B(1). In Official Correspondence (Text Field)

4B(2). Orally at Official Gatherings (Text Field)

4C. Full Name in Native Alphabet (Text Field) *(In standard telegraphic code or other transcription code)*

4D. Variants, aliases or Nicknames *(INDIVIDUAL Record repeating group autopopulate)*

Rank

5A. English Language (Text Field)

5B. Native (Text Field)

Date of Rank (Text Field)

Position/Billet

7A. Present Position (Text Field)

7B. Military Address (Text Area)

7C. Date Assumed Position (Text Field)

7D. Scheduled Date of Departure (Text Field)

CLASSIFICATION

CLASSIFICATION

7E. Name of Predecessor

7E1. Predecessor's Name (Text Field)

7E2. Predecessor's Branch of Service (Text Field)

7E3. Date Predecessor Assigned (Text Field)

7E4. Duration of Predecessor's Assignment (Text Field)

Branch of Armed Service (Text Field)

Specialty/Other Organizations

Date of Birth (Text Field)

Place of Birth (Text Field)

Sex (Text Field)

Home Address (Text Fields) *(autopopulate)*

Telephone Number

14A. Home (Text Fields)

14B. Work (Text Fields)

Marital Status (Text Field)

Citizenship (Text Field)

COMMENTS:

(FIELD COMMENT) (Text Area)

PROJ: (Text Field)

CLASSIFICATION

CLASSIFICATION

INSTR: US NO (Text Field)

PREP: (Text Field)

ENCL: (Text Field) *(Repeating Group)*

ACQ: (Text Field)

DISSEM: FIELD-- (Text Field)

WARNING: REPORT CLASSIFIED (Text Field) *(Autopopulate)*

DRV FROM-- (Text Field)

DECL: (Text Field)

CLASSIFICATION

SECTION 11

COUNTERINTELLIGENCE INSPECTION/EVALUATION REPORT

CLASSIFICATION

CI Inspection/Evaluation Report

(Normally hard copy report – not templated in DCIIS)

Reporting Unit:
Dissemination:

Report Date:
Report Time:
Reference:
Enclosure:

SYNOPSIS: (Summary of the report)

1. ( ) PREDICATION: (What initiated the inspection/evaluation).

2. ( ) PURPOSE: (What the inspection/evaluation was to determine. State any limitations that were placed on the activity.)

3. ( ) BACKGROUND: (Information on previous inspections/evaluations or surveys on the same area. Information on level and amount of classified material maintained. Identity of person(s) conducting the activity.)

4. ( ) RESULTS: (Detailed information obtained during the inspection/evaluation, describe security measures in effect, whether the measures required by appropriate references were adequate, and any identified security weaknesses/deficiencies.)

5. ( ) RECOMMENDATIONS: (List recommendations to correct security weaknesses or deficiencies as they appear in paragraph 4 above, reference the paragraph for clarity.)

(Signature on line above typed name)
REPORTED BY. (Typed name of evaluator)

(Signature on line above typed name)
APPROVED BY. (Typed name and title of approving authority)

1 **CLASSIFICATION**

SECTION 12

COUNTERINTELLIGENCE SURVEY/VULNERABILITY ASSESSMENT

CLASSIFICATION

CI Survey/Vulnerability Assessment

(Normally hard copy report – not templated in DCIIS)

Reporting Unit:
Dissemination:

Report Date:
Report Time:
Reference:
Enclosure:

SYNOPSIS: (Summary of the report)

1. PREDICATION: (How the survey was initiated.)

2. PURPOSE: (What the survey was to determine. State any limitations on the survey.)

3. BACKGROUND:

a. Person(s) conducting the survey.

b. Previous surveys.

c. Mission.

d. Inherent hazards of the area.

e. Degree of security required (Maximum, medium, or minimum based of the following factors):

(1) Mission

(2) Cost of Replacement

(3) Location

(4) Number of like installations

(5) Classified Material

CLASSIFICATION

CLASSIFICATION

(6) Importance

4. RESULTS

a. Security of information

b. Security of personnel

c. Physical security

5. RECOMMENDATIONS. (List recommendations to correct security hazards as they appear in paragraph 4 under the subparagraph heading, reference the paragraph for clarity.)

a. Security of information.

b. Security of personnel.

c. Physical security.

(Signature on line above typed name)
REPORTED BY. (Typed name of evaluator)

(Signature on line above typed name)
APPROVED BY. (Typed name and title of approving authority)

CLASSIFICATION

SECTION 13

COUNTERINTELLIGENCE SURVEY/ VULNERABILITY ASSESSMENT CHECKLIST

BACKGROUND:

Counterintelligence surveys/vulnerability assessments are conducted during peacetime as well as times of hostilities, both in and outside the continental United States.

Manning of counterintelligence survey/vulnerability assessment teams should be task-organized to meet the needs/requirements of the survey; i.e., counterintelligence officers/specialists, physical security specialists from provost marshal, communications specialists, automatic data processing security specialists, etc.

Name of Installation
Location of Installation
Type of Installation

1. Functions, Purpose, or Activities at Installation

a. What troops, units, and command elements are stationed there or use or control the installation?

b. What military activities (conventional, unconventional, or special) take place?

c. What material is produced, processed, tested, or stored?

d. What is the military importance?

2. Critical Rating of the Installation

a. How important to national security or Marine Corps forces are the activities that take place at the installation?

b. What activity on the installation should be veiled in secrecy? Why?

c. What information about the installation would be of interest to hostile intelligence? Why?

d. Is this the only location where the activities taking place can be conducted?

e. Are there substitute places available which are suitable and practical?

f. Is there a key facility/organization aboard the installation?

g. Is there any sensitive or critical material or equipment stored, tested, or developed aboard the installation?

h. Is the installation a likely target for espionage?

3. Names of Principal Officers of the Installation/Organization

4. Names of Persons Directly Responsible for the Security of the Installation

5. Physical Location and Description of the Installation

a. This is the physical description of the general area surrounding the installation, paying particular attention to road networks, rail facilities, air facilities, transportation, terrain, etc.

b. Include a general physical description of the entire installation, to be accompanied wherever possible by a map, sketch or aerial photograph, and the following information:

(1) Area and perimeter.

(2) Numbers, types, and locations of buildings, and relationships among the various buildings.

(3) Roads, paths, railroad sidings, canals, rivers, etc., on the premises of the installation.

(4) Wharves, docks, loading platforms, etc., on the premises.

(5) Any other distinctive structures or features.

c. Note any particularly vulnerable or sensitive points on the installation, and the reasons for their vulnerability or sensitivity. Pay particular attention to the following:

(1) Command element/headquarters buildings.

(2) Operations/crisis action facilities.

(3) Repair shops (armor, vehicle, aircraft, weapons, communications).

(4) Power plants.

(5) Transformer stations.

(6) Warehouses.

(7) Communications systems/facilities.

(8) Fuel storage.

(9) Water tanks, reservoirs, supply systems.

(10) Motor pools.

(11) Ammunition dumps.

(12) Aircraft

(13) Firefighting equipment.

(14) Military police/reaction force location and reliability.

(15) Special training/testing sites.

6. Perimeter Security

a. Description of the perimeter and physical barriers.

(1) Type of fence or other physical barrier around the installation that affords perimeter security?

(2) What type of material is the fence/barrier constructed?

(3) How high is the fence/barrier?

(4) Is the fence/barrier easily surmountable?

(5) Is the top protected by barbed wire outriggers?

(6) Are there any cuts, breaks, tears, holes, or gaps in the fence/barrier or any holes under it?

(7) Are there any tunnels near or under the fence/barrier?

(8) Are vehicles parked near or against the fence/barrier?

(9) Are piles of scrap, refuse, or lumber kept near the fence/barrier?

(10) Is the fence/barrier patrolled and checked daily for cuts, breaks, holes, gaps, tunnels, or evidence of tampering?

(11) Where are pedestrian and vehicle gates located?

(12) Are unguarded gates firmly and securely locked?

(13) Are the gates constructed in a manner where identity and credential checks of persons or vehicles entering or exiting are accomplished, particularly during rush hours?

(14) During what hours is each gate open?

(15) Are there any railroad rights of way, sewers, tree lines, or other weak points on the perimeter?

(16) Are these weak points guarded, patrolled, or secured in any fashion?

(17) Is high intensity lighting used to light up the perimeter during hours of darkness?

(18) Where are the lights located?

(19) Are there dead spots between lighted areas?

(20) Is there backup emergency power for the lighting?

(21) Does the lighting inhibit/hamper security force observation?

7. Perimeter Security Force

a. Description of the organization of the security force.

(1) What is the strength of perimeter security forces?

(2) What are the number and location of guard posts?

(3) What is the length of perimeter covered by each post?

(4) What is the length of watch of each post?

(5) Is there a reserve or backup or security force?

(6) What weapons do the guards carry?

(7) What is the level training for each member of the security force?

(8) What instructions are given to security forces regarding identity checks/challenges?

(9) Are there vehicle checks?

(10) Are there any watchtowers to facilitate observation of the perimeter?

(11) What are the height and location of each watchtower?

(12) Have roving patrols been utilized to patrol the perimeter? What are their number, strength, frequency, routes, and activity?

(13) What is the efficiency and manner of performance of perimeter guards and patrols?

b. Security weaknesses and recommendations.

(1) What specific weaknesses pertaining to both physical barriers and the perimeter security force were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve perimeter security?

8. Security of Buildings and Structures

a. Nature and purpose of building.

(1) Where is the location of the building?

(2) What activities take place in the building?

(3) What material/information is developed or stored?

(4) What machinery or equipment is in the building?

(5) Is the building a vulnerable point? Why?

b. Description of building -exterior, interior, and immediate surroundings.

(1) Describe the design and construction of the building.

(2) How many stories? Height?

(3) Does the building have a basement?

(4) What percentage is wood?

(5) What percentage is concrete?

(6) What other materials are used in the exterior?

(7) Describe walls.

(8) Describe floors.

(9) Describe ceilings.

(10) Describe roof.

(11) Is the building safely designed and constructed?

(12) Is the building properly maintained and constructed?

(13) Check locations of doors, windows, sewers, sidewalks, elevators, stairs, fire escapes, skylights, crawl spaces/false ceilings, and any other possible means of exit or entry.

(14) Are these entrances properly locked, or otherwise safeguarded against unauthorized entry?

(15) Are windows and skylights screened, grilled, or barred?

(16) Can unauthorized or surreptitious entry be effected in any manner?

(17) Are exit and entry facilities adequate to meet an emergency situation?

(18) Are all keys to building controlled?

(19) Where is the key control maintained?

(20) Who maintains the key control?

(21) How rigorously is it kept?

(22) Who is authorized to receipt for the keys?

(23) Are any measures taken to restrict entry into the building; i.e., pass, badges, access rosters, etc.

(24) Are controlled access methods enforced?

(25) If the building is determined to be sensitive, high threat priority, or vulnerable, has it been declared as restricted, and is the area surrounding it so designated?

(26) Are daily security checks conducted at the end of each working day in areas where classified material is stored? Are all security containers checked?

c. Guard and patrol system around the building.

(1) What are the duties of guards and patrols?

(2) Are high intensity lights used to light up the exterior and the area surrounding the buildings during hours of darkness?

(3) Is there a reactionary security force?

(4) What is the response time? Has it been tested?

(5) What is the size of the guard force? Reactionary force?

(6) What are the means of activating the reactionary force? Are there backup systems?

d. Security of electrical equipment.

(1) Is there auxiliary lighting?

(2) Are circuit breakers properly protected?

(3) Are telephone junction boards protected

e. List the frequency of periodic checks made throughout the building to detect the following:

(1) Holes, cracks, crevices which might conceal explosives, incendiary devices, or audio/visual monitoring devices. Are such repaired?

(2) Tampered wiring, or broken or electrical connections and wires.

(3) The presence of suspicious packages or bundles.

(4) Any dangerous practices, including safety, electrical, or fire hazards which may result from negligence or deliberate attempts at sabotage,

f. Security weaknesses and recommendations

(1) What specific weaknesses pertaining to the security of interiors and exteriors were noted during the survey?

(2) What specific reasonable recommendations may be made to improve the security of the buildings?

9. Security of Docks, Wharves, and Platforms

a. Description of the location, nature, and purpose of each dock, wharf, or platform.

(1) What administrative supervision of the docks, wharves, and loading platforms is exercised? By whom?

(2) What type of security force provides protection for each?

(3) What measures are taken to prevent loitering in the vicinity of each?

(4) What measures are taken to prevent unauthorized observation of loading and unloading?

(5) What protection is afforded mechanical sabotage, arson, explosion, or dangerous practices)

(6) Are same precautionary measures taken as outlined for access as outlined above for building interiors and exteriors?

b. Traffic conditions.

(1) Are inspections of deliveries made to guard against sabotage devices; i.e., explosives, caustic chemicals, etc.?

(2) What precautions are taken to conceal the loading and unloading of personnel or material if such handling requires secrecy?

(3) Are delivery trucks, railroad cars, and privately owned vehicles checked for possible sabotage devices?

(4) How much is the movement of drivers and helpers about the installation controlled?

(5) In the case of movement of personnel, equipment, and material, are identifying markings removed in an effort to assist in operations security?

c. Security weaknesses and recommendations.

(1) What specific weaknesses pertaining to the security of docks, wharves, and loading platforms were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of docks, wharves, and loading platforms?

10. Motor Pools, Dismount Points, and Parking Areas

a. Security measures at each facility.

(1) Are motor pools, dismount points, and parking areas adequately guarded?

(2) Are vehicles properly checked and accessible only to authorized personnel?

(3) What system of checking vehicles is used?

(4) What measures are taken to safeguard fuels, lubricants, tools, and equipment against sabotage, theft, fire, and explosion?

(5) Are frequent checks made of all vehicles for possible mechanical sabotage?

(6) Are drivers and mechanics instructed as to the proper checks, to be made to guard against or detect sabotage?

(7) What provisions are made to prohibit privately owned vehicle parking in motor pools, dismount points/parking areas?

(8) Are fuels and lubricants frequently tested for possible contamination?

(9) Are parking/staging areas restricted or supervised in any way?

(10) Are parking arrangements consistent with security against sabotage, terrorist, or other hazards?

(11) What provisions are made for visitors parking?

(12) Do parking arrangements/facilities impede efficient traffic flow through and near the compound?

(13) Would parking arrangements interfere with firefighting or other necessary emergency vehicles if there was an emergency?

b. Security weaknesses and recommendations.

(1) What specific weaknesses about the security of motor pools and parking lots were noted during this survey?

(2) What specific and reasonable recommendations may be made to improve the security of the motor pool and parking lots.

11. Power Facilities and Supply

a. Description of supply, facilities, and security measures.

(1) What type of power is used by the installation?

(2) What is the peak load of electric power?

(3) What percentage of the electric power is generated on the installation?

(4) What is the installation's electric generating capacity?

(5) What percentage of electric power is purchased from outside sources?

(6) Are all current sources ample to provide a reserve beyond full load demands?

(7) From whom is the electric power purchased?

(8) Is an alternate or auxiliary electric power system available for emergency use?

(9) Can the auxiliary electric power system be used immediately?

(10) How many and what kind of power substations/transformers fare on the installation?

(11) Are control panels, pressure valves, gas facilities, and control valves in good working order? How frequently are they checked? Is adequate fire protective equipment available and nearby?

(12) Are power substations/transformers adequately safeguarded against trespassers and saboteurs?

(13) Are generators properly maintained and checked with particular emphasis on oil levels and temperatures?

(14) Are combustible materials removed from their vicinity?

b. Miscellaneous features:

(1) Are replacement units for generators and motors available in safe storage?

(2) Do transformers have sufficient capacity, are they safely located and well protected by physical barriers and guards?

(3) Are oil-filled transformers located in noncombustible well-drained buildings or outside?

(4) Are frequent inspections made of the oil, contact, and control apparatus of circuit breakers and transformers?

(5) What is the system of power lines in use?

(6) What is the number of independent power feeds?

(7) Is the pole line or underground line safe, reliable, and frequently checked?

(8) Are all power lines protected by lightning arresters?

(9) Are power distribution lines properly installed and supported?

(10) Are electric circuits overloaded at any time?

(11) Are current national or civil electric codes followed?

(12) Is there a single or multiple main switch(s) for emergencies?

c. Security weaknesses and recommendations.

(1) What specific weakness about the security of power facilities and supply were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of power facilities and supply?

12. Fire Fighting Equipment and Facilities

a. Describe the amount and condition of equipment and facilities.

(1) What fire fighting and first aid equipment are available on the installation?

(2) What types of fire extinguishers are available; i.e., foam, dry chemical, halon, water, carbon dioxide, and carbon tetrachloride? Are they at locations where such types may be needed?

(3) Are all extinguishers and other equipment in working order and frequently tested and inspected?

(4) Are fire extinguishers sealed to prevent tampering?

(5) Do competent personnel make inspections of fire equipment and are the results recorded?

(6) Are both first aid and firefighting equipment painted so as to be conspicuous? Are they within reach of all personnel, unobstructed, and of reasonable size and weight to permit ease of handling by all personnel?

Is first aid equipment available? Does it include ample amounts of materials that may be needed?

(8) Are first aid supplies checked periodically and safeguarded?

(9) What type of fire alarm system(s) is/are installed?

(10) Are there sufficient numbers of alarms and sensors in the system?

(11) Is the fire alarm system frequently inspected and tested?

(12) Are vulnerable and/or important facilities equipped with sprinkler systems?

(13) What type of sprinkler system(s) is/are used? Are they fed by public mains, tanks, private reservoir, or pumps?

(14) How often and thoroughly is the sprinkler system inspected?

(15) Where are the main control valves of the system located?

(16) Are fire hydrants near vulnerable or important facilities?

(17) Are hydrants in working order? How often are they inspected and tested?

(18) Is the water pressure sufficient so that streams of water will reach and extinguish flames in all sections of the installation?

(19) Is there a secondary source of water supply available?

(20) Does the installation have its own fire department? A brigade? What equipment does it have? Are the personnel well trained?

(21) Have arrangements been made with public fire departments to furnish equipment and personnel to augment the installation department/brigade?

(22) Is the nearest public fire department paid or is it a volunteer unit?

(23) Has a program of fire drills been inaugurated? Are such drills conducted in an efficient and earnest manner?

(24) Has a fire prevention program been inaugurated?

(25) What plans have been made for the action of all personnel if there is a fire?

b. Security weaknesses and recommendations.

(1) What specific security weaknesses about the firefighting equipment and facilities were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of firefighting equipment and facilities?

13. Water Supply

a. Description of water supply and security measures taken to safeguard it.

(1) What sources of water supply are used by the installation?

(2) Are sources of water reasonably safe, adequately guarded, and protected by physical security?

(3) If a public supply is used, what is the diameter of the main line?

(4) What is the water pressure? Is it adequate for normal use as well as for emergencies?

(5) If a private reservoir or tank is used, what is its capacity, level, pressure, and condition?

(6) Is it adequate for the installation's needs?

(7) What type of pumps are used in the water system (underwater, suction, centrifugal, electric, etc.)?

(8) Are water pumping stations adequately protected, frequently inspected, and tested?

(9) Are all valves secured properly?

(10) Is a supplementary water system available? Where? Is it secure?

(11) How often is water tested for purification? By whom? Is the water treated? By whom? By what chemicals?

(12) Are taps/sources of unpotable water adequately marked?

(13) Is the sewage system adequate for the installation?

(14) Are sewer mains, control, pumps, and disposal systems adequate?

(15) Is there a possibility of water or food contamination from the sewage system?

(16) Has there been any epidemic outbreak at the installation traceable to waste disposal?

b. Security weaknesses and recommendations.

(1) What specific and reasonable recommendations may be made to improve the security of the water supply?

(2) What specific weaknesses about the water supply were noted during the survey?

14. Food Supply

a. Description of security measures.

(1) From what sources does the installation receive food and allied supplies? Can these sources be considered reliable?

(2) If food supplies are purchased from merchants and farmers in the local vicinity, have they been checked and their food tested for cleanliness?

(3) Have caterers and companies or individuals who operate food, candy, soft drink, or other concessions on or near the installation been checked? Have their products been thoroughly tested?

(4) Have local food handlers been checked for health, cleanliness, and loyalty?

(5) Is entry to kitchens and food storerooms restricted to authorized personnel? How are such restrictions enforced?

(6) Are pantries and refrigerators locked when not in use?

(7) Are kitchens and storerooms in sanitary condition?

(8) Is there any evidence of unsanitary conditions?

(9) Are frequent checks made of foods, drinks, etc., to prevent or detect toxicological or

bacteriological sabotage?

(10) Has there been any epidemic or excess absenteeism traceable to food or water supplies of the installation?

b. Security weaknesses and recommendations.

(1) What specific weaknesses about the security of food supply were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of the food supply?

15. Communications Facilities

a. General service and special communications message centers.

(1) Description.

(2) Where is the message center located?

(3) Is the message center adequately protected by physical barriers and guards?

(4) Is someone on duty at the message center at all times?

(5) Who handles the mail at the message center? Have all mail handlers been subject to background and local records checks?

(6) Are all encryption (hardware and software) devices properly safeguarded and properly destroyed when obsolete?

(7) Are logs kept of authorized couriers and message traffic distribution?

(8) Are unauthorized personnel excluded from the message center?

(9) Are classified messages handled in accordance with OPNAVINST 5510.1-'?

(10) Through what channels do classified messages pass?

(11) Have messengers, couriers, and operators been checked? Do they have appropriate security access(es)?

b. Security weaknesses and recommendations.

(1) What specific weaknesses about the security of the communications systems were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of the communications system?

16. Wire and Wireless Communications Equipment

a. Description.

(1) What means of wire and wireless communications are used throughout the installation?

(2) Where are the central points of such communications networks located?

(3) Are switchboards adequately guarded?

(4) Have operators been checked and cleared?

(5) Is auxiliary power available?

(6) Is auxiliary or replacement equipment available?

(7) Are open wires, terminal boxes, cross connecting boxes, cables, and manholes frequently inspected for indications of sabotage and/or wire tapping?

(8) Are maintenance crews alerted to search for tapping?

(9) Are civilian repairmen used? Are they checked and cleared?

(10) Have preparations been made to take care of sudden breaks in the system efficiently?

(11) Have personnel been cautioned about discussing classified or sensitive matters over unsecured telephone, teletype, or radios?

b. Security weaknesses and recommendations.

(1) What specific weaknesses about the security of the communications system were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of the communications system?

17. Security of Information

a. Where on the installation are plans, blueprints, photos, classified material/equipment, or other information of value to the enemy kept? The following list is not all-inclusive and is not a replacement for the checklist in OPNAVINST 5510.1-.

(1) Is such material centralized in a single facility or scattered through various offices or buildings?

(2) In what sections are classified material processed stored and what level of classification is authorized in each area?

(3) Is all classified or valuable information kept in authorized/approved security containers or vaults?

(4) Are fight safes and cabinets affixed to floors or chained to immovable objects?

(5) Are container doors closed and locked when not in use?

(6) Is there any protection other than the container itself.

(7) What protection is given to a combination of containers?

(8) What security measures are enforced about keys to doors, gates, or file cabinets?

(9) Is access limited to combinations and keys?

(10) Who has access to combinations and keys? Do all authorized personnel have access? Have they been cautioned about passing keys and combinations to unauthorized personnel?

(11) Is a rigid chain of custody required for classified information (Secret and above). Can custodians identify the location of classified at any time?

(12) Are only personnel with completed background checks and appropriate access assigned to positions requiring the handling of classified material?

(13) Plans, blueprints, reports, or other classified material returned as promptly as possible and properly turned in?

(14) Who has access to classified material (with and without approved access)?

(15) Is dissemination of classified material strictly limited to those with a "Need to Know?"

(16) Is rank or position considered sufficient reason for access to classified information?

(17) Is classified material left unattended on desks where persons passing by can observe or steal without detection?

(18) Have civilian janitors been checked and placed under supervision?

(19) How is classified waste disposed of? Are destruction records kept?

(20) What policy has been established regarding releases and statements to local or national news media?

(21) Have all personnel been cautioned about unauthorized statements and releases?

b. Security of personnel.

(1) What specific weaknesses about the security of information were noted during the survey?

(2) What specific and reasonable recommendations may be made to improve the security of information?

18. Security of Personnel

a. OPNAVINST 5510.1- provides guidelines on personnel security.

b. Who is responsible for the security of the installation?

c. What is the attitude towards security?

d. Is the command aware of continuous evaluation of those who have access to classified or sensitive material or equipment?

e. Are all personnel in positions of trust and confidence considered reliable?

f. What is the attitude towards security?

19. Identification System

a. What system is used to identify personnel authorized access within the confines of the installation/facility?

b. If badges are used -

(1) Are badges or identification cards of tamper-proof design and difficult to reproduce or counterfeit?

(2) Is the makeup and issue of badges and identification cards rigidly controlled to prevent:

(a) Reproduction?

(b) Theft?

(c) Unauthorized use or issue?

(d) Failure to return to issuing authority?

(3) Are photographs used on the face of the cards/badges?

(4) Is a detailed description used to positively identify holder?

(5) Are color or coded systems used to identify level of access or department personnel are granted?

(6) Are specific badges valid for specific areas?

(7) Is enforcement of such identification rigid?

(8) Do regulations prescribe that everyone wears the badge at all times and are regulations enforced?

(9) Is admittance to the installation/facility governed by the identification system?

(10) When badges are reported missing, lost, or forgotten what action is taken?

c. Is entrance permitted by wearing a military uniform?

(1) What other means of identification are used?

(2) Are access rosters passed from one facility/ command to another via secure means?

(3) Are passes or identification cards closely scrutinized?

d. What system is used to prevent persons working in one building, section, or unit from wandering about restricted areas without proper authorization.

20. Visitor Controls

a. What system is used to identify and admit authorized and legitimate visitors to the installation or facility?

(1) How and by whom is the legitimacy or necessity of a visitor's mission established?

(2) Are regulations lax in the control of visitors?

(3) On arrival at the gate, entrance of the facility or section, are visitors escorted to a reception area?

(4) Are regulations lax in the control of visitors?

(5) Is the identity of visitors verified?

(6) Is adequate information obtained visitors?

(7) Is the purpose of the visit obtained?

(8) Are visitors required to register in a logbook with the following information:

(a) Full name.

(b) Social security number.

(c) Rank.

(d) Parent Organization.

(e) Date and time of entry.

(f) Time of departure.

(g) Number of security badge issued and level of access.

(h) Reason for visit.

(i) Name of official authorizing entry or providing escort.

(9) Are visitors required to provide identity on departure?

(10) Are visitors escorted or kept under surveillance during the time they are on the installation?

b. Is a vehicle register kept which includes:

(1) Date and time of entrance.

(2) Registration numbers.

(3) Name of owner(s).

(4) Signatures of driver(s) and passengers.

(5) Brief description of contents of vehicle.

(6) Inspections conducted on vehicle.

(7) Time of departure.

c. Are news media carefully checked and verified?

(1) Are credentials examined and verified?

(2) Has their visit been checked with higher commands to verify authority?

d. Are orders and credentials of allied military personnel examined by competent personnel (linguists, etc.).

(1) Are such visits verified by higher authority?

(2) Is security unduly sacrificed to courtesy?

e. Are spot checks of persons within the installation/facility made from time to time?

f. Security weaknesses and recommendations.

(1) What specific weaknesses about identification and visitor's control were noted during the survey?

(2) What specific reasonable recommendations may be made to improve security by further identification and visitor's control?

21. Description of Guard System

a. General description of the guard force.

(1) Strength.

(2) Shifts.

(3) Reserves.

(4) Weapons.

(5) Training.

(6) Number and type of posts.

(7) Communications.

b. Check the following points.

(1) What is the organization of the guard force?

(2) What is the numerical strength of each shift or relief?

(3) How many shifts or reliefs are there?

(4) How many supervisors does each shift have?

(5) Is supervision of the guard force adequate?

(6) How many fixed posts does the force cover?

(7) Where is each post located?

(8) How many patrols are covered by the guard force?

(9) What is the route of each patrol?

(10) Are routes of the patrols varied?

(11) What is the time of each patrol?

(12) Are doors and gates closely checked by the patrols?

(13) What functions are performed by the patrols?

(14) Does the supervisor make inspection tours of the routes?

(15) How frequently and thoroughly are such tours made?

(16) Are inspections varied as to route and time?

(17) Are guard force communications and alarm systems in use? Are they adequate?

(18) What type of communication and alarm system does the guard force have? Are there backup systems?

(19) Is a record kept of all guard force activity?

(20) Does the guard force have communications with the military police?

(21) What armament does the guard force have?

(22) Are the weapons in serviceable condition?

(23) Are the weapons suitable for the mission?

(24) Are arms and ammunition adequately safeguarded when not in use?

(25) Is there a record of custody when weapons are issued during each shift?

(26) Where are the weapons and ammunition stored? Does storage prevent rapid access to the guard force?

(27) How are guards recruited?

(28) What physical, mental, age, or other qualifications must protective guards have?

(29) How thoroughly are prospective guards investigated?

(30) Are guards uniformed, and do they have credentials or badges? What other system of identification is used?

(31) Is the guard force competent and respected by personnel of the installation?

(32) How thoroughly is the guard force trained?

(33) How much time is spent on training the guard force?

(34) How is the training of the guard force conducted?

(35) Does such training cover the following points?

(a) Care and use of weapons and ammunition?

(b) Common forms of espionage and sabotage activity?

(c) Common forms of bombs explosives?

(d) Familiarization with the entire installation/facility, with particular emphasis on restricted and vulnerable areas?

(e) Location and character of hazardous material and processes?

(f) Location and operation of all important steam and gas valves and of all main electrical switches?

(g) Location and operation of fire protective equipment including use of sprinkler control valves?

(h) Conditions which may cause fires and explosions.

(i) Location and use of all first aid equipment?

(j) Duties is the event of fire, blackouts, or other emergencies that can be foreseen?

(k) Use of communication systems?

(i) Observation and description?

(m) Preservation of evidence?

(n) Patrol work?

(o) Searches of persons and places?

(p) Supervision of visitors?

(q) General and special guard orders?

(r) Location of all guard posts?

(36) Do guards have keys to gates, buildings, and offices?

(37) Do guards check the credentials of visitors and personnel working on the installation or facility?

(38) Is the strength of the guard force consistent with -

(a) The number of pedestrian, vehicle, and railroad gates and the hours they are open?

(b) The approximate number of daily visitors? Proper visitor reception?

(c) The number of loading platforms, storage facilities, working areas, etc.?

(d) The number of vehicles to cover the entire installation in a reasonable time?

(e) The number of restricted areas and vulnerable points?

(f) The number of plants or pumping stations?

(g) The number and extent of parking areas?

(h) Necessary supervision of the guard force?

(i) Sickness, leave, injury, etc., of guard personnel?

(39) What are the duties of the guard force if there are security violations? Does the guard force have security clearance and access?

c. Guard headquarters.

(1) Is the guard headquarters conveniently located?

(2) Is the guard headquarters properly secured at all times, and does it contain all necessary equipment?

(3) Does the guard headquarters contain adequate facilities for all members of the guard force?

d. Security weaknesses and recommendations.

(1) What specific security weaknesses were noted during the survey of the installation's guard force?

(2) What specific and reasonable recommendations regarding the guard force may be made to improve the security of the installation?

22. Description of Security Conditions and Security Measures of Adjacent Areas

a. What is the general nature of the population and the area surrounding the installation?

(1) Does the nationality or political nature of the surrounding populace offer a natural cover and aid to hostile agents and saboteurs?

(2) Is the installation within a commercial air zone of travel?

(3) If so, are minimum altitudes for planes published at all local airports?

(4) Is the installation isolated or screened from public view?

(5) Are restricted areas screened or isolated from public curiosity?

(6) Is the installation exposed to hazards that may be brought onto the installation by natural conditions such as floods, extreme winds, forest fires, electrical storms, etc.?

(7) Is the installation or buildings within the installation well camouflaged against both air and ground observation?

(8) Have places of amusement near the installation and persons frequenting them been investigated, scrutinized, and checked?

(9) Have night clubs, pool rooms, bowling alleys, houses of prostitution, barber shops, restaurants, taverns, stores, and other places frequented by personnel from the installation been included and thoroughly checked.

(10) Has the surrounding area been carefully scrutinized for any place likely to be used as bases for espionage or sabotage agents? Areas that could conceal antenna's, audio and visual surveillance, etc.?

b. Security weaknesses and recommendations.

(1) What specific security weaknesses were noted during the survey of the area adjacent to the installation?

(2) What specific and reasonable recommendations may be made to improve security?

23. Security of Air Installations. The security of air installations does not differ from that of any other installation. Aircraft and maintenance facilities are high priority targets of saboteurs and espionage agents. In general, checking the following major areas will assist in establishing the security afforded to the installation.

a. Is the guard system adequate?

b. Are individual aircraft guarded sufficiently?

c. Are hangers and other vital buildings in a restricted area?

d. Have precautions been taken to see that there is no smoking in the area?

e. Are aircraft stored in hangers inspected periodically against sabotage?

f. Are special precautions taken to ensure visitor control in hangars?

g. Are vital repair parts in storage areas protected from unauthorized personnel, fire, and the elements.

h. Are there fire trucks, crash and rescue vehicles available?

i. Is emergency equipment parked in a convenient location readily available to any part of the installation?

24. Practical Use of Security Checklist

a. This checklist is not all encompassing and should be used as a guide to initiate a survey. Several methods of organizing a security check may be used. The following methods, through usage, have been found to be practical and efficient.

(1) Itemize on index cards or automated data file all requirements as listed on the checklist and write the required information on each card/file as it is checked off the list.

(2) Itemize basic subdivisions of survey checklist requirements on separate pages with itemized requirements listed in required order. Write in the required information in the proper space as each item is checked off.

(3) Itemize all requirements of the survey checklist on separate pages, subdividing the pages according to main subdivision requirements. Make detailed notes about each item as it is checked off.

b. After completing notes on all requirements for each item, assemble in order and prepare report.

SECTION 14

REPORT OF INVESTIGATIVE ACTIVITY

Purpose. Standard report used to report the results of a CI investigation.

CLASSIFICATION

Report of Investigative Activity

Record ID: .....
Point of Contact: .....
Classification: .....
Abstract: .....
Discretionary Access Control: .....
Caveats: .....

Release To: .....

Record Type: .....
Record Status: .....
Date Created *(yyyymmdd)*: .....
Date Modified *(yyyymmdd)*: .....
Community of Interest: .....
Source Record: .....

Case Number Reference: .....
Case: .....
Event: .....
Date of Record (yyyymmdd): .....

Title (*Text*):

Reason for Investigation (*Text*):

Individuals Involved (*Text*):

Role: .....

Status (*Text*):

Period of Report From (yyyymmdd): .....
Period of Report To (yyyymmdd): .....

Reporting Unit: .....
Agent Name: .....

Executive Summary (*Text*):

CLASSIFICATION

SECTION 15

REPORT OF INVESTIGATIVE ACTIVITY SWORN STATEMENT

Purpose. Standard report for preparing and documenting sworn statements.

CLASSIFICATION

Record ID: .....
Point of Contact: .....
Classification: .....
Abstract: .....
Discretionary Access Control: .....
Caveats: .....

Release To: .....

Record Type: .....
Record Status: .....
Date Created *(yyyymmdd)*: .....
Date Modified *(yyyymmdd)*: .....
Community of Interest: .....
Source Record: .....

Date (yyyymmdd): .....
Case Number: .....
Lead Number: .....
ROIA Number: .....
Name: .....

Title

Sub Title

Agency: .....
Number of Investigative Materials: .....

Text

Agent Name: .....
Organization: .....

Individual Information: .....
Name: .....
Employer: .....
OR Unit: .....

Sworn Statement

Number of Witnesses: .....

CLASSIFICATION

SECTION 16

PERSONEL DATA FORM
POW/MIA/MISSING (NON-HOSTILE)

Purpose. Standard report used to record and document POW/MIA/missing personnel investigations.

CLASSIFICATION

Personnel Data Form

Persons Captured (POW),

Missing in Action or Missing (Non-hostile)

1. Personal Data

a. Name:

b. Rank:

c. SSN/MOS:

d. Former Service Number:

e. Organization:

f. Date of Birth:

g. Place of Birth:

h. Home of Record:

i. Residence (if other than home of record):

j. Marital Status (Include number, sex, citizen status, and age of children):

k. PEBD:

1. EAS/EOS:

m. Date arrived in country:

n. Duty assignment:

2. Physical Characteristics

a. Height (Metric as well as U.S. equivalent):

b. Weight (Metric as well as U.S. equivalent):

CLASSIFICATION

CLASSIFICATION

c. Build:

d. Hair:

e. Eyes:

f. Complexion:

g. Race:

h. Right/left handed:

3. Distinguishing Characteristics

a. Speech (Include accent and speech patterns used):

b. Mannerisms:

c. Scars/identifying marks (Include type, location, size, color, and detailed description):

d. Others:

4. Circumstances of Incident

a. Date:

b. Location (Coordinates and geographic name):

c. Circumstances:

d. Reported wounds:

e. Last known location:

f. Last known direction of travel:

g. Last known place of detention:

h. Status (prisoner of war/missing [non-hostile]/missing in action as reported by unit):

5. Other Pertinent Data

a. General physical condition:

b. Linguistic capabilities and fluency:

c. Religion:

d. Civilian education:

e. Military schools:

f. Clothing and equipment when last seen

CLASSIFICATION

CLASSIFICATION

g. Jewelry when last seen (Include description of glasses, rings, watches, religious medallions, etc.):

h. Other personnel listed POW/MIA during same incident:

6. Photograph

7. Handwriting Samples (Attach sample of correspondence, notes, etc. If no other sample is available, include reproduction of signature from Service Record Book/Officer's Qualification Record [SRB/OQRI.)

Enclosures: (May not be given wide dissemination based on classification or content.)

a. Clearances/Access Information. (Include information concerning security clearance, access, knowledge of recurring tactical operations, knowledge of projected or proposed operations, or any other special knowledge possessed.)

b. Medical Profile. (Include pertinent information extracted from medical records and summarized information gained concerning ability to survive in captivity, known personal problems, relationship with seniors/contemporaries or other personal, medical, or personality information which would indicate his ability to cope in a prisoner-of-war situation.)

c. References. (List any messages, letters, or other correspondence pertaining to the individual. If circumstances under which the individual is listed as captured or missing predicated a command investigation, a copy of that investigation is included as an enclosure.)

d. Unresolved Leads/investigators Comments. (Include unresolved leads or names of personnel who were unavailable for interview because of transfer, evacuation, etc. Use investigator's comments as necessary but do not recommend a casualty determination.)

CLASSIFICATION

_____

SECTION 17

COUNTERINTELLIGENCE MEASURES WORKSHEET

Purpose. The CI worksheet is prepared or revised based on the conclusions reached in the intelligence estimate of the enemy capabilities for intelligence, subversion, terrorist activities and sabotage. This worksheet is an essential aid in CI planning for the CIHO and CI/HUMINT Company Commander. It is also the basis for preparing CI orders and requests. The following is a partially completed sample of a CI measures worksheet.

			Units/Personnel Responsible for Execution of Counterintelligence Measures											
(1) Phases or Periods of the Operation	(2) Categories of Counterintelligence Activities Involved	(3) Counterintelligence Measures to be Adopted	Civil Affairs	CIS Officer	Provost Marshal	Comm Intel Unit	All Units	CI Units						(5) Instructions regarding entries in columns (3) and (4). Notes for future action, and staff coordination measures
Assault Phase	1. Military Security a. Security discipline.	(1) Cover or paint all vehicle and aircraft markings.					X							Coordinate with G-4 Provost marshal report violations
		(2) Remove identification from uniform					X							Coordinate with G-1 Provost marshal report violations
		(3) Restrict personnel to area except when on official business					X							
		(4) Emphasize security discipline in command posts/echelons, and elsewhere, with particular reference to handling of communications & information systems, documents and maps, phone conversations, loose talk, and speculation which might convey information to the enemy. All personnel will be instructed regarding same.					X							Coordinate with G-3 CI elements assist with instruction and check
		(5) Report all known or suspected security compromises to unit security manager and intelligence officer.		X	X	X	X	X						SOP
	b. Safeguarding of classified information and equipment.	(6) Collect and place under guard or evacuate as determined appropriate by unit commander civilians in position to observe critical unit C2, fires & combat service support sites.	X					X						Coordinate with G-1
	c. Communication & information security.	(7) Check SOP plans for security of cryptographic devices for destruction and for report of loss or compromise.		X	X	X	X	X						SOP CI elements check
		(8) Check plans and equipment for destruction of documents in event of imminent capture.		X			X	X						SOP CI elements check
		(9) Use only authorized call-signs, authenticators, and cryptographic codes.		X		X	X							SOP
	d. Security of unit movements.	(10) Check that unauthorized personnel are prohibited from entering CPs, message centers, and other sensitive areas.		X			X	X						SOP
		(11) Patrol all wire lines used by units.		X			X							SOP Check with CIS officer for compliance
		(12) Cut all wire lines leading into enemy-occupied territory.					X							Coordinate with other military forces
		(13) Control the movement of all vehicles and aircraft to the extend that a change in normal operations if not indicated.					X							Coordinate with G-3 and G-4 Provost marshal report violations
		(Others as required)												

APPENDIX F

COUNTERINTELLIGENCE TRAINING COURSES

1. Marine Air-Ground Task Force Counterintelligence Basic Course (U)

What This Course Offers

Provides instruction in theater, national, DOD, and organic Marine Corps intelligence assets; CI application of the combat intelligence cycle; CI hostile threat; terrorism; CI/tactical HUMINT operations; photography; interrogations; espionage, sabotage, subversion, and terrorism investigations; interview skills; intelligence report writing; and surveillance techniques.

Who Should Attend

Marine Corps, corporal through lieutenant screened by CI assets and approved for lateral move to MOS 0211/0210/0204 by HQMC in accordance with MCO 3850.1H. Other services-for example, US Army enlisted personnel have attended. Projected attendance for additional US Army and possible US Air Force personnel is anticipated

Course Activities

Lectures, videos, discussions, and practical exercises

Faculty

Navy and Marine Corps Intelligence Training Center, Dam Neck, Virginia

How Long? How Often?

Seventeen and a half weeks, 88 training days/annually

Security Clearance Needed

Top Secret based on completed SSBI and eligible for SCI access

Further Information

HQ, US Marine Corps, code CIC at (703) 614-2219/2058, DSN 224-XXXX

DESCRIPTION

Trains USMC enlisted men and officers serving as members of a CI team, or subteam, in support of a MAGTF command.

Emphasis is placed on requirements in amphibious and subsequent operations.

Trains USMC enlisted and officers in CI/HUMINT related tasks when serving as a member of a CI team, CI/HUMINT branch, or in support of MAGTF/JTF command.

Emphasizes theater and national-level CI support provided to the commander.

2. Marine Air-Ground Task Force Advanced CI Course (U)

What This Course Offers

Provides instruction to CI/Tactical HUMINT collection; intelligence architecture; systems and communications; MAGTF, theater, and national-level staff planning; MAGTF/JTF/CI/ITT employment and deployment; case method leadership practicums; CI espionage, sabotage, subversion, and terrorism theory; and legalities of investigations.

Who Should Attend

Marine Corps, Gunnery Sergeant through Lieutenant Colonel (MOSs 0211/ 0210/0204) with at least one successful tour. Other service quotas are available.

Course Activities

Lectures, videos, discussions, and practical exercises

Faculty

Navy and Marine Corps Intelligence Training Center, Dam Neck, Virginia

How Long? How Often?

Twenty-six days, 20 training days/annually

Security Clearance Needed

Top Secret/SCI

Further Information

HQ, US Marine Corps, code CIC (703) 614-2219/2058, DSN 224-XXXX

3. Advanced Foreign CI Training Course (U)

What This Course Offers

Advanced counterespionage concepts, principles, and techniques for foreign CI special agents

Who Should Attend

DOD CI special agents with three years of strategic CI experience; 12 seats per class for Army and two seats designated joint, which rotate among the military services.

Course Activities

Lectures, presentations, discussions, case studies, practical exercises, and videos

DESCRIPTION

Provides tough, demanding, realistic, mission focused counterespionage training to selected foreign CI (foreign CI) special agents who are programmed for assignment within the national foreign CI community in support of the warfighters and the DOD foreign CI strategy. Provides students with a synergistic perspective for applying advanced foreign CI skills and methodologies focusing on the foreign CI Triad of investigations, operations, and surveillance.

Faculty

Eight full-time instructors with intensive counterespionage background supplemented with guest speakers/subject-matter experts from DOD and other Intelligence Community components.

How Long? How Often?

Fifteen weeks (approximately 750 hours)/offered twice a year

Security Clearance Needed

Top Secret

Further Information

Contact the course director or senior instructor at (301) 677-5778/5779, FAX (301) 677-6362. Mailing address is Commander, US Army Foreign CI Activity (USAFCA), USAINSCOM, Attn. IAFC-TC, Fort Meade, MD 20755

Registration Data

Limited to those working in or en route to an foreign CI assignment; graduate of a basic CI course; three years of strategic CI experience; effective communicator; supervisory and command recommendations; favorable SSBI; CI-scope polygraph; and a valid civilian drivers license. Army registration procedures, a special nomination packet must be submitted to Commander, US Army Intelligence and Security Command; Attn. IAOPS-HUCI, Fort Belvoir, VA 22060-5246. An INSCOM selection board chooses students on a best qualified basis. Other military services per service directives and guidance.

4. CI Analytic Methods Course (U)

Who Should Attend

Entry-level CI analysts

Course Activities

Lectures, discussions, videos, and case studies

Faculty

Instructors from the JMITC

How Long? How Often?

One week/two times a year

Security Clearance Needed

Top Secret/SCI

Further Information

JMITC, DIAC, Bolling AFB, (202) 373-3312

DESCRIPTION

Introduction to the multi-discipline CI analytical methods, tools, matrix, link, and pattern analysis, collection threats, deception analysis, and intelligence oversight.

5. Joint CI Staff Officers Course (U)

What This Course Offers

This course introduces the student to CI support to joint operations

Who Should Attend

Personnel who will be working in a joint CI support role during contingencies in a joint environment.

Course Activities

Lectures, videos, discussions, and practical exercises

Faculty

JCISB and civilian and military members of the intelligence and CI communities

How Long? How Often?

Five day s/several times a year

Security Clearance Needed

Top Secret/SCI

DESCRIPTION

- Know how CI activities are integrated into joint-military organizations at the levels of command and into the formulation of contingency plans.
- Know how to develop and execute a CI appendix to the intelligence annex to a joint operational/exercise plan or OP order.
- Know the Joint Planning System and how it supports both deliberate and time-sensitive plans. Know the roles/responsibilities of DOD, NSA, FBI, CIA, JCS, combatant commands, and the Services CI agencies in providing CI support to contingency planning and execution.
- Know how CI HUMINT and Special Operations Forces will coordinate and

Further Information

Defense Intelligence Agency (DAC-1B), Joint CI Support Branch (JCISB), Pentagon, Room 1E821, (703) 614-9155.

6. Multi-Discipline CI Course (U)

What This Course Offers

Improves professional CI officers' understanding of the multi-discipline approach to CI. This course is not a course in analytic methods or methodology.

Who Should Attend

CI professionals from throughout DOD and the Intelligence Community (IC).

Course Activities

Lectures, discussions, videos, and case studies

Faculty

Instructors from the JMITC and subject-matter experts from the Intelligence Community

DESCRIPTION

- Learn the all-source CI national and DOD environments.
- Learn how to access HUMINT, SIGINT, IMINT, MASINT, and other information and resources in the IC.
- Learn how organizationally perceived roles effect CI policy and analysis.
- Learn the threats to US national interests from foreign intelligence and security services (FISS) and about the US resources that drive responses to FISS threats.
- Understand the complex interdependent relationships of CI organizations from operations to finished

How Long? How Often?

Two weeks/three times a year/also available as a two-three day mobile course.

Security Clearance Needed

Top Secret/SI/TK/G

Further Information

JMITC, DIAC, Bolling AFB, Washington, DC, (202) 373-3897

7. Evolution of American CI (U)

What This Course Offers

Provides the students with a broad historical perspective of the growth and development of US CI from the historical legacy of the American Revolution to the current day.

Who Should Attend

New or mid-level intelligence officers or special agents whose present or future assignments may involve CI responsibilities.

Course Activities

Lectures, videos, case studies, and class participation

Faculty

NACIC and guest speakers

How Long? How Often?

One week/twice a year

Security Clearance Needed Secret

Further Information

Community Training Branch, NACIC, (703) 874-4122

Registration Data - Three weeks before course

DESCRIPTION

- Evaluates the historical significance of key events in the development of the CI discipline in the United States.
- Applies the lessons learned to future public and legislative scrutiny and helps students make decisions based on a historical perspective.
- Projects the need for a strong CI program.
- Lists and explains the five core issues affecting CI policies and strategies in the post-Cold War era.
- Advances interagency cooperation and creates a learning environment.
- Identifies various agencies' perspectives and

8. Strategic Approaches to CI (SACI) (U)

What This Course Offers

Designed to illuminate the "big picture," emphasizes US national CI strategies and the approaches taken throughout the CI community to implement these strategies. Focuses on the five core issues that will be enduring challenges for the CI community for the next decade.

DESCRIPTION

- Analyzes foreign intelligence services CI threat data.
- Determines risks and vulnerabilities to information

Who Should Attend

New or mid-level managers in operational CI agencies or other CI community elements who demonstrate a potential for advancement to more senior CI positions, and whose present or future assignments may involve CI policy formation or interagency responsibilities.

Course Activities

Lectures, videos, case studies, and group discussions to develop a strategy with examples of successful strategies used by US companies to compete in today's world. Student presentations.

Faculty

Instructors, program managers, and subject-matter experts from throughout the intelligence and CI communities, sponsored by the NACIC

How Long? How Often? Class Size

Fifty hours/April and October/30

Security Clearance Needed

Top Secret/SCI

Further Information

Community Training Branch, NACIC, (703) 874-4122. Usually at an off-site location

Registration Data

Nomination by parent agency. Thirty days before course date

9. The Threat to Information Systems (U)

What This Course Offers

This course reviews an updated summary of various threats to information systems.

Who Should Attend

Students should have familiarity with the concept of threat from foreign intelligence services

Course Activities

Lectures, discussions, demonstrations, and practical problems

Faculty

Instructors from the National Cryptologic School (NCS)

How Long?

Twenty-four hours/three days, full-time

Security Clearance Needed

Top Secret and indoctrinated for special intelligence. Pass to NSA Office of Security electronically.

Further Information

NCS (410) 859-6336 or secure 968-8054

Registration Data

Open to CI community personnel. Registration request should be made through parent agency training coordinator to the NSA/NCS registrar.

10. INFOSEC Familiarization Course (U)

What This Course Offers

This course is a survey of communications security (COMSEC) principles and techniques with an emphasis on electronic COMSEC systems and cryptographic equipment.

Who Should Attend

Students requiring fundamental knowledge of COMSEC

Course Activities

Lectures and discussions

Faculty

Instructors from the National Cryptologic School (NCS)

How Long?

Forty hours/one week, full-time

Security Clearance Needed

Top Secret. Pass to NSA Office of Security electronically.

Further Information

NCS (410) 859-6336 or secure 968-8054

Registration Data

Open to CI community personnel. Registration request should be made through parent agency training coordinator to the NSA/NCS registrar.

DESCRIPTION

Topics include:

- A history of COMSEC and cryptology
- The national information security (INFOSEC) structure, mission, and relationships
- The vulnerability of threats to US military and civil communications systems
- Physical, cryptographic, transmissions, and emission (TEMPEST) security
- Off-line cryptosystems
- Emergency destruction
- COMSEC material production
- Computer security digital encryption theory
- Key management
- INFOSEC system and cryptographic equipment applications
- Systems and equipment under development

Appendix G

MAGTF COUNTERINTELLIGENCE PLANNING CHECKLIST

INTRODUCTION. This appendix identifies typical MAGTF counterintelligence/HUMINT during each phase of the Marine Corps Planning Process (MCPP).

MCPP STEP	MAGTF STAFF ACTIONS	COUNTERINTELLIGENCE PLANNING ACTIONS

MISSION ANALYSIS	✓ Identify the higher headquarter's (HHQ)/supported headquarters intent ✓ Identify tasks ✓ Determine the area of operations (AO) and area of interest (AOI) ✓ Review available assets and identify personnel and equipment resource shortfalls ✓ Determine constraints and restraints ✓ Determine recommended commander's critical information requirements (priority intelligence requirements, friendly force information requirements, essential elements of friendly information [EEFI]) ✓ Identify requests for information ✓ Determine assumptions ✓ Draft mission statement ✓ Present mission analysis brief ✓ Draft the warning order ✓ Convene/alert recell (if appropriate) ✓ Begin staff estimates ✓ Refine commander's intent ✓ Develop the commander's planning guidance	✓ Review HHQ and MAGTF standing intelligence plans (e.g., Annex B to an OPLAN), CI plans (Appendix 3 to Annex HUMINT plan (Appendix 5 to Annex B), etc. ✓ Assist with determination of the MAGTF AO and AOI ✓ Assess DIA's, CIA's, combatant command's and other external organizations ongoing CI operations and plans with the AO and AOI (e.g., availability and currency of CI contingency materials) ✓ Provide initial CI estimates and other CI products to support initial planning (ensure needs of subordinate units are ide and met) ✓ Determine specified, implied and essential tasks ✓ Develop proposed CI mission statement; coordinate with G/S-2 intelligence operations officer and G/S-3 force protec officer; obtain G/S-2 officer's approval ✓ Assist security manager with development of security classification guidance to support planning and subsequent ✓ Identify organic/supporting CI elements & subordinate units' points of contact; acquire an immediate operational status report from each; determine personnel and equipment deficiencies ✓ Review/prepare new CI survey/vulnerability assessment; determine and prioritize significant security vulnerabilities; provide recommendations (e.g., CI active and passive measures); identify requirements for technical surveillance count support ✓ Identify JTF/multinational CI interoperability issues; provide recommendations ✓ Establish/review/update the MAGTF CI database; special attention to current threat estimates, current CI estimates, and CI targets (personalities, organizations, and installations) ✓ Ensure subordinate units' CI POCs kept advised of pertinent actions and developments ✓ Identify external organizations CI collection and production plans, and assess against MAGTF's initial requirement ✓ Determine CI personnel & equipment deficiencies; initiate augmentation requests (coordinate with intelligence ope officer) ✓ Assign/task-organize organic CI elements (e.g., CI/HUMINT company detachments or HUMINT exploitation teams major subordinate elements; CI element to MAGTF future operations/plans sections) ✓ Validate/update JTF CI tactics, techniques and procedures and MAGTF standing operating procedures (coordinate HHQ and subordinate units) ✓ Validate and prioritize CI requirements; special attention to those needed for COA development ✓ Begin development of CI operations plan; issue orders to CI collection and production elements (coordinate with c manager and AFC OIC, respectively) ✓ Update/begin necessary CI surveys/vulnerability assessments ✓ Determine initial CI communications and information systems (CIS) requirements & dissemination plans; identify deficiencies (coordinate with dissemination manager and G/S-6) ✓ Validate CI database management procedures (coordinate with JTF and subordinate units) ✓ Ensure subordinate units' CI POCs kept advised of pertinent actions and developments	

MCPP STEP	MAGTF STAFF ACTIONS	COUNTERINTELLIGENCE PLANNING ACTIONS	

COURSE OF ACTION DEVELOP-MENT	✓ Continue intelligence preparation of the battlespace (throughout all steps of the planning process) ✓ Array friendly forces ✓ Assess relative combat power ✓ Centers of gravity and critical vulnerabilities analysis ✓ Brainstorm possibilities ✓ Develop roughcut course(s) of action (COA) ✓ Commander's input ✓ COA(s) refinement ✓ COA(s) validation ✓ COA(s) graphic and narrative development ✓ Prepare and present COA(s) briefing ✓ Commander selects/modifies COA(s)	✓ Assist with development and continued updating of the intelligence & CI estimates, with emphasis on the followi ➢ Development of CI target reduction plans ➢ Periodic CI summaries and threat estimate update ➢ Development of CI target reduction plans ➢ Recommendations and implementation of current/future CI countermeasures ✓ Assist the intelligence, operations, and other staff sections with COA development ✓ Develop the CI concept of operations for each COA; begin preparation of: ➢ Appendix 3 (CI operations) to Annex B ➢ Assistance to Appendix 5 (HUMINT operations) to Annex B ➢ Assist operations section with force protection plans to Annex C ✓ Determine CI capabilities required for each COA ✓ Coordinate CI-related collection, production, and dissemination requirements for each COA ✓ Continue development of CI estimate of supportability for each COA ✓ Ensure subordinate units' CI POCs kept advised of pertinent actions and developments
COURSE OF ACTION ANALYSIS	✓ Conduct COA analysis wargaming ✓ Refine staff estimates and estimates of supportability ✓ Develop concepts based upon warfighting functions (as required) ✓ Prepare COA analysis brief	✓ Complete CI estimate and threat assessments ✓ Complete CI estimates of supportability ✓ Assist intelligence section with completion of the intelligence estimate and the friendly intelligence estimate of supportability ✓ Assist operations section with completion of the force protection estimate ✓ Continue to monitor and update CI collection and production activities ✓ Ensure subordinate units receive necessary CI products; verify understanding; identify/update subordinates' current intelligence requirements (IR) and force protection EEFIs ✓ Validate and update CI information requirements ✓ Ensure subordinate units CI POCs kept advised of pertinent actions and developments

MCPP STEP	MAGTF STAFF ACTIONS	COUNTERINTELLIGENCE PLANNING ACTIONS
COURSE OF ACTION COMPARISON AND DECISION	✓ Evaluation of each COA ✓ Comparison of COAs ✓ Commander's decision ✓ Issuance of warning order	✓ Assist intelligence and operations sections with evaluation and comparison of each COA ✓ Continue development of Appendix 3 to Annex B consistent with the selected COA ✓ Update, validate & prioritize CI information requirements and supporting CI collection/production requirements for the selected COA; issue orders as appropriate to CI elements ✓ Coordinate CI element task-organization needs associated with the selected COA, with special attention to necessary support to the main effort ✓ Continue coordination with the G/S-6 regarding CIS requirements, to include standard and unique CIS for internal CI operations and with other joint/multinational organization ✓ Continue coordination with G/S-1 as necessary for physical couriering of CI products to subordinate units; and with the G/S-1 and PMO for EPW handling/compound related plans development ✓ Review actions associated with satisfying personnel and equipment deficiencies associated with the selected COA ✓ Ensure subordinate units receive pertinent CI products (e.g., current CI threat assessment); verify understanding; identify/task subordinates current CIRs ✓ Validate MAGTF CI IRs and tasks to support force protection EEFIs ✓ Ensure subordinate units CI POCs kept advised of pertinent actions and developments

ORDERS DEVELOP-MENT	✓ Commander's intent is refined ✓ Concept of operations turned into an operations order or a fragmentary order ✓ Staff estimates and other planning documents updated and converted into operations order (OPORD) annexes and appendices ✓ Commander approves OPORD	✓ Complete Appendix 3 to Annex B; ensure copies provided to subordinate units and they understand ✓ Update, validate & prioritize CI information requirements and associated collection operations; ✓ Monitor ongoing CI production operations; update and issue orders as appropriate to meet elements ✓ Ensure pertinent CI products are disseminated to all subordinate units ✓ Complete CI related CIS actions ✓ Maintain coordination with external CI elements

MCPP STEP	MAGTF STAFF ACTIONS	COUNTERINTELLIGENCE PLANNING ACTIONS
TRANSITION	✓ Transition brief ✓ Drills ✓ Plan refinements (as required)	✓ Assist intelligence section with transition brief ✓ Modify CI plans as necessary ✓ Monitor ongoing CI collection and production operations; update and issue orders as needed to meet elements ✓ Ensure all subordinate units' POCs and CI officers in JTF and other components fully understand plans and standing requirements; and ensure they have received necessary products ✓ Identify, validate and prioritize remaining CI IRs and force protection EEFIs ✓ Participate in drills ✓ Remain engaged in MAGTF future plans activities

APPENDIX H

REFERENCES

National

EO 12333, "United States Intelligence Activities."

NSCID 5, "U.S. Clandestine Foreign Intelligence and Counterintelligence Abroad."

DCID 1/7, "Security Control on the Dissemination of Intelligence Information."

DCID 5/1, "Espionage and Counterintelligence Abroad." (With supplemental MOAs)

Department of Defense

DOD Dir 1325.6, "Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces."

DOD Dir 0-2000.12, "DOD Combating Terrorism Program."

DOD Dir 3025.1, "Use of Military Resources During Peacetime Civil Emergencies Within the United States, Its Territories and Possessions."

DOD Dir 5105.29, "Human Resources Intelligence (HUMINT) Activities."

DOD Dir 5105.32, "Defense Attaché System."

DOD Dir 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense."

DOD Dir S-5205.1, "Acquisition and Reporting of Information Relating to National Security."

DOD Dir 5205.2, "DOD Operations Security Program."

DOD Dir 5210.48, "DOD Polygraph Program."

DOD Dir 5210.50, "Unauthorized Disclosure of Classified Information to the Public."

DODINST 5210.84, "Security of DOD personnel at U.S. Missions Abroad."

DOD Dir C-5230.23, "Intelligence Disclosure Policy."

DOD Dir 5240.1, "DOD Intelligence Activities."

DOD Dir 5240.2, "DOD Counterintelligence Activities."

DODINST 5240.4, "Reporting of Counterintelligence and Criminal Violations."

DODINST 5240.5, "DOD Technical Surveillance Countermeasures (TSCM) Survey Program."

DOD Dir 5240.6, "Counterintelligence Awareness Briefing Program."

DODINST C-5240.8, "Security Classification Guide for Information Concerning the DOD Counterintelligence Program."

DODINST S-5240.9, "Support to Department of Defense Offensive Counterintelligence Operations."

DODINST 5240.10, "DOD Counterintelligence Support to Unified and Specified Commands."

DODINST 5505.3, "Initiation of Investigations by Military Criminal Investigative Organizations."

DODINST 5505.6, "Investigation of Allegations Against Senior Officials of the DOD."

DOD Dir 5525.5, "DOD Cooperation with Civilian Law Enforcement Officials."

DIA Manual 57-1, "General Intelligence Production."

DIA Manual 57-6, "DOD Indications and Warning System."

DIA Manual 58-1, "Defense Intelligence Collection."

DIA Manual 58-7, "Time Sensitive Requirements Coordination and Management."

DIA Manual 58-11, “Department of Defense HUMINT Policies and Procedures.”

DIA Manual 58-12, "Department of Defense HUMINT Management System"

DIA Reg 60-4, "Procedures Governing DIA Intelligence Activities that Affect U.S. Persons."

Joint Publications

--------, "Concept for Future Joint Operations --- Expanding Joint Vision 2010."

Joint Pub 0-2, "Unified Action Armed Forces "

Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms."

Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations."

Joint Pub 2-01, "Joint Intelligence Support to Military Operations."

Joint Pub 2-01.2, (Draft) "Counterintelligence Support to Joint Operations" (with classified supplement)

Joint Pub 2-01.2, (Draft) "Joint Intelligence Preparation of the Battlespace."

Joint Pub 2-02, (Draft) "National Intelligence Support to Joint Operations."

Joint Pub 3-02, "Joint Doctrine for Amphibious Operations."

Joint Pub 3-07, "Joint Doctrine for Military Operations Other than War."

Joint Pub 3-07.2, "Joint Doctrine for Antiterrorism."

Joint Pub 3-10, "Joint Doctrine for Rear Area Operations."

Joint Pub 3-13, (Draft) "Information Operations" (with classified supplement)

Joint Pub 3-13.1, "Joint Doctrine for Command and Control Warfare."

Joint Pub 3-50.2, "Doctrine for Joint Combat Search and Rescue"

Joint Pub 3-50.3, "Joint Doctrine for Evasion and Recovery."

Joint Pub 3-54, "Joint Doctrine for Operations Security."

Joint Pub 3-57, "Doctrine for Joint Civil Affairs."

Joint Pub 5-00.2, "Joint Task force Planning, Guidance and Procedures."

Joint Pub 5-03.1, "Joint Operations Planning and Execution System, Volume I."

Joint Pub 6-0, "Doctrine for Command, Control, Communications and Computers Systems Support to Joint Operations."

Marine Corps Order and Publications

1 MCO 3302.1, "Antiterrorism Program".

2 MCO 3850.1H, "Policy and Guidance for Counterintelligence Activities."

3 MCO 3820.1, "Foreign Military Intelligence Collection Activities (FORMICA)."

4 MCO 003850.2 "Marine Corps Counterintelligence Force Protection Source Operations (CFSO)."

5 --------	Operational Maneuver from the Sea -- A Concept for	1996
6	the Projection of Naval Power Ashore	
7 --------	Ship to Objective Maneuver	Jul 97
8 --------	Military Operations on Urbanized Terrain	Jul 97
9 --------	Beyond Command and Control --- A Concept for	Jul 98
10	Command and Coordination of the Marine Air-Ground	
11	Task Force	
12 --------	A Concept for Information Operations	Aug 98
13 MCWP 0-1	Marine Corps Operations	(Draft)
14 MCWP 0-1.1	Componency	Jun 98
15 MCDP 1	Warfighting	Jun 97
16 MCDP 2	Intelligence	Jun 97
17 MCWP 2-1	Intelligence Operations	Feb 98
18 MCDP 3	Expeditionary Operations	Apr 98
19 MCWP 3-1	Ground Combat Operations	(Draft)
20 MCWP 3-2	Aviation Operations	(Draft)
21 MCWP 4-1	Logistics Operations	(Draft)
22 MCRP 4-27C	Enemy Prisoners of War and Civilian Internees	Apr 98
23 MCDP 5	Planning	Jun 97

MCWP 5-1	Marine Corps Planning Process	(Draft)
MCRP 5-12C	Marine Corps Supplement to the DOD Dictionary of Military and Associated Terms	Jul 98
MCDP 6	Command and Control	Oct 96
MCWP 6-1	MAGTF Command and Control Operations	(Draft)
MCWP 6-22	Communications and Information Systems	(Draft)
FMFRP 3-23-2/ FM 34-130	Intelligence Preparation of the Battlefield	Jul 94

Navy Publications

SECNAVINST 3300.2, "Combating Terrorism."

SECNAVINST 3800.8B, "Intelligence Oversight Within the Department of the Navy."

SECNAVINST S3810.5A, "Management of Foreign Intelligence, Counterintelligence and Investigative Activities within the Department of the Navy."

SECNAVINST 3820.2D, "Investigative and Counterintelligence Collection and Retention Guidelines Pertaining to the Department of the Navy."

SECNAVINST 3820.3D, "Oversight of Intelligence Activities Within the Department of the Navy."

SECNAVINST 3850.2B, "Department of the Navy Counterintelligence."

SECNAVINST S3850.3, "Support to Department of Defense Offensive Counterintelligence Operations."

SECNAVINST 3875.1, "Counterintelligence and Awareness Briefing Program."

SECNAVINST 5500.30E, "Reporting of Counterintelligence and Criminal Violations to Office of the Secretary of Defense Officials."

SECNAVINST 5500.31A, "Technical Surveillance Countermeasures (TSCM) Program."

SECNAVINST 5500.34, "Security of DOD Personnel at U.S. Missions Abroad."

SECNAVINST 5520.3B, "Criminal and Security Investigations and Related Activities Within the Department of the Navy."

OPNAVINST 1620.1A, "Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces."

OPNAVINST 3300.53, "Navy Combating Terrorism Program."

OPNAVINST S3850.5, "Support to DOD Offensive Counterintelligence Operations."

OPNAVINST C5500.46, "Technical Surveillance Countermeasures."

OPNAVINST 5510.1, "Department of the Navy Information and Personnel Security Program Regulation."

Army Publications

AR 381-10, "US Army Intelligence Activities."

AR 381-20, "The Army Counterintelligence Program."

AR 381-47, "US Army Counterespionage Activities."

AR 381-172, "Counterintelligence Force Protection Source Operations and Low Level Source Operations"

FM 34-5, "Human Intelligence and Related Counterintelligence Activities."

FM 34-60, "Counterintelligence."

FM 34-60A, "Counterintelligence Operations -- Classified Supplement."