MCRP 2-10A.2

Counterintelligence and Human Intelligence

U.S. Marine Corps

Limited Dissemination Control: None. Approved for Public Release.

PCN 144 000235 01

A no-cost copy of this document is available at:
https://www.marines.mil/News/Publications/MCPEL/

and on the Marine Corps Doctrine library website at:
https://usmc.sharepoint-mil.us/sites/MCEN_USMCDoctrine/ (requires Common Access Card [CAC] to access).

Report urgent changes, routine changes, and administrative discrepancies by letter to the Doctrine Branch at:

Commanding General
United States Marine Corps
Training and Education Command
ATTN: Policy and Standards Division, Doctrine Branch (C 466)
2007 Elliot Road
Quantico, VA 22134-5010

or by email to: USMC_Doctrine@usmc.mil

Please include the following information in your correspondence:

Location of change, publication number and title, current page number, and, if applicable, paragraph and line number.
Figure or table number (if applicable).
Nature of change.
Text addition or deletion.
Proposed new text.

Copyright Information

UNITED STATES MARINE CORPS

03 February 2025

FOREWORD

Marine Corps Reference Publication (MCRP) 2-10A.2, *Counterintelligence and Human Intelligence*, serves as a basic reference for understanding concepts, operations, and procedures for the conduct of counterintelligence (CI) and human intelligence (HUMINT) operations in support of the Marine air-ground task force across the spectrum of conflict. This publication complements and expands on Marine Corps Doctrinal Publication 2, *Intelligence*, and Marine Corps Warfighting Publication 2-10, *Intelligence Operations*, which provide doctrine and higher order tactics, techniques, and procedures for intelligence operations.

The primary target audience of this publication is intelligence personnel responsible for planning and executing CI/HUMINT operations. Personnel who provide support to CI/HUMINT or who use the results from these operations should also read this publication. MCRP 2-10A.2 describes aspects of CI/HUMINT operations, including doctrinal fundamentals, equipment, command and control, communications and information systems support, planning, execution, security, and training. Detailed information on CI/HUMINT operations and tactics, techniques, and procedures is classified and beyond the scope of this publication.

This publication supersedes MCRP 2-10A.2, *Counterintelligence and Human Intelligence*, dated 21 November 2019.

Reviewed and approved this date.

Duane A. Durant
Colonel, U.S. Marine Corps
Commanding Officer, Marine Corps Intelligence School

Publication Control Number: 144 000235 01

Dissemination Controls: None. Approved for Public Release.

Table of Contents

CHAPTER 1. FUNDAMENTALS, RESPONSIBILITIES, AND ORGANIZATIONS

CHAPTER 2. EMPLOYMENT, RESPONSIBILITIES, COMMAND AND CONTROL

CHAPTER 3. COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE PLANNING, COORDINATION, AUTHORITIES, AND PERMISSIONS

CHAPTER 4.COUNTERINTELLIGENCE ACTIVITIES

CHAPTER 5. PRODUCTION AND ANALYSIS

CHAPTER 6.HUMAN INTELLIGENCE ACTIVITIES

CHAPTER 7. REPORTING, PRODUCTION, AND DISSEMINATION

CHAPTER 8. REQUIREMENTS, ADMINISTRATION, AND COORDINATION

Appendices

Glossary

References and Related Publications

CHAPTER 1. FUNDAMENTALS, RESPONSIBILITIES, AND ORGANIZATIONS

Timely and accurate information derived from counterintelligence (CI) and human intelligence (HUMINT) activities is critical to the commander's force protection (FP) efforts, reducing uncertainty through intelligence collection, and contributing to the commanders' decision-making process (Marine Corps Doctrinal Publication [MCDP] 2, *Intelligence*).

The Marine Corps combines CI and HUMINT skill sets into a single military occupational specialty (MOS). Although CI and HUMINT activities share similarities, they are distinctly different mission sets with authorities and permissions that are derived from different laws and orders. The distinction between the authorities must be understood to effectively employ Marine Corps CI and HUMINT as a capability.

Counterintelligence and HUMINT activities assist the Marine air-ground task force (MAGTF) commander, and the MAGTF staff, to develop estimates of the situation, shape an understanding of the battlespace, plan intelligence collection, and protect the force. The senior intelligence officer, serving as the G-2, or S-2, focuses CI and HUMINT efforts by clearly identifying the commanders' priority intelligence requirements (PIRs) and creating the collection plan, leveraging both CI and HUMINT to accomplish intelligence tasks. The development of PIRs and a collection plan enables the commander to carefully assign CI and HUMINT elements missions and tasks that support the commanders' objectives (Marine Corps Warfighting Publication [MCWP] 2-10, *Intelligence Operations*).

PERSONNEL

Marine Corps CI and HUMINT activities are conducted by the same personnel trained to perform both missions. Other branches of the military, civilian counterparts, and intelligence colleagues within the United States Government (USG) clearly delineate between personnel working in CI and HUMINT capacities.

Within the Department of Defense (DoD), CI and HUMINT personnel are trained and certified in accordance with specific DoD policies and standards governing the conduct of CI and HUMINT activities. As such, only those personnel who are accredited per DoD and Service policies are authorized to conduct CI and HUMINT in accordance with Department of Defense Directive (DoDD) S-5200.37, *Management and Execution of Defense Human Intelligence (HUMINT)*, and DoDD 5240.02, *Counterintelligence (CI)*. Within the Marine Corps, personnel holding military occupational specialties as intelligence officers, CI/HUMINT officers, CI/HUMINT intelligence operations officers, and CI/HUMINT specialists are trained and certified to conduct CI and HUMINT in accordance with Marine Corps Order (MCO) 3850.1J, *Policy and Guidance for Counterintelligence (CI) and Human Source [sic] Intelligence (HUMINT) Activities*. Advanced CI or HUMINT training might be required, in addition to successful completion of the MAGTF CI/HUMINT Course, to conduct certain CI and HUMINT activities and operations. Additionally, the Director of Intelligence (DIRINT), as the Service defense human intelligence executor (DHE), can approve other trained and certified Marines to conduct HUMINT activities as required.

COUNTERINTELLIGENCE FUNDAMENTALS

Counterintelligence is the "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities" (*DoD Dictionary of Military and Associated Terms*, hereafter referred to as the *DoD Dictionary*). Counterintelligence encompasses the following five functions: collection, analysis and production, investigations, operations, and functional services (DoDD 5240.02). Counterintelligence provides critical support to command force protection efforts by helping identify potential threats, friendly vulnerabilities, adversarial threat capabilities, and hostile intentions to friendly operations.

Counterintelligence efforts seek to identify foreign adversaries and their agents, which could be witting or unwitting US persons involved with foreign intelligence entities (FIEs). Commanders have the prerogative to address command issues by applying some of the following CI activities to determine the appropriate (COA) to mitigate vulnerabilities and penetrations that could result in the loss of information or compromise the security of the force:

- A CI debrief determines the extent of a reported foreign contact.
- A technical surveillance countermeasure (TSCM) is conducted to detect, neutralize, and exploit technical surveillance and associated devices and technologies.
- A counterintelligence incident assessment (CIIA) establishes or refutes a reasonable belief that a particular person is acting for, or on behalf of, or an event is related to a foreign power engaged in spying, or committing espionage, sabotage, treason, sedition, subversion, assassination, or international terrorist activities.

Counterintelligence activities provide the commander options for determining foreign or domestic association with terrorism, espionage, sabotage, and subversion by US DoD members and foreign elements. Discretion is of great importance when conducting CI activities, particularly when dealing with US persons. All subjects and persons associated with the activity should be treated with respect and professionalism at all times to ensure that reputations and career advancements are not unduly disrupted by rumors and unwarranted accusations or assertions. Counterintelligence activities should strive to be non-attributional to the organizations they intend to assist. Unless carefully thought through, CI activities can harm the relationship between counterintelligence and the commander or the supported staff. The CI element must consider the implications and exactly how much information to provide the commander in order to accomplish the task while preserving relationships and the career progression of the supported units' staff.

The primary function of counterintelligence is to mitigate foreign intelligence and terrorism threats to personnel, information, materiel, facilities, and activities. The responsibility for CI protection measures lies with every commander. In the early stages of planning, Commanders are assisted by the CI staff elements in identifying CI requirements and protection priorities, developing CI plans, and as appropriate, directing CI activities to protect the integrity of the mission and the organization from potential threats.

Employment of Counterintelligence

Counterintelligence/HUMINT Marines could be assigned a CI mission or task within a CI element and are employed in various roles and in several different formations. Counterintelligence/HUMINT Marines are involved in all facets of planning and conducting HUMINT operations, CI activities, and sensitive activities. They are expected to have a working knowledge of the organization, operations, and techniques employed by foreign intelligence services, international terrorist organizations, insider threats, and other CI threats. Counterintelligence and HUMINT Marines conduct sensitive and non-sensitive HUMINT operations in joint operations area (JOA) and Non-JOA environments to support Marine expeditionary force (MEF) priorities, MAGTF operations, and Service requirements. They also conduct CI functional services, CI collection tasks, CI incident assessments (CIIA, and CI analysis in support of critical infrastructure, critical programs, and technology.

Representational Counterintelligence Badge and Credentials

The CI badge and credentials establish the CI agent bona fides for a representative of Marine Corps counterintelligence conducting a formally approved CI mission. The DIRINT issues these badges and credentials to Marine Corps CI personnel to signify that the bearer represents the DIRINT on CI matters and to certify that the bearer is appropriately trained; however, the badges and credentials do not bestow authorization upon any personnel to conduct CI activities. To conduct these activities, Marine CI personnel who possess applicable badges and credentials must also be trained and assigned to a billet within a unit having the authority to conduct the activity in question with an approved CI plan for that activity. Finally, the approval to conduct a CI activity must be granted by a commander at the appropriate level for the solicited authorities. Only personnel under the cognizance of the commander authorizing the CI activity are authorized to conduct that activity. Thus, the authority associated with the presentation of the badge and credentials can only be given by those personnel under that commander's authority. The expressed concurrence of the appropriate senior intelligence officer provides commander level top cover for conducting CI activities. Counterintelligence activities, which require the presentation of the badge and credentials, are authorized by the senior intelligence officer on behalf of the commander.

Detailing CI personnel to duty with an external organization does not constitute transfer of authorities associated with CI activities. The supported external organization formally requests and receives those personnel for approved CI activities. Counterintelligence personnel detailed to Naval Criminal Investigative Service (NCIS) and operating under NCIS CI authorities are issued NCIS credentials for conducting activities in support of these tasks. Marine Corps-issued badges and credentials are forfeited to command designated custodians when CI Marines are assigned to non-CI billets. Marine commanders can rescind the badge and credentials of their assigned personnel in coordination with the CI custodian at the office of the DIRINT.

HUMAN INTELLIGENCE FUNDAMENTALS

Human intelligence is "a category of intelligence derived from information collected and provided by human sources" (DoD Dictionary). Human intelligence collection activities include screening, interrogation, debriefing, liaison, source operations, support to document and media exploitation (DOMEX), and elicitation. Collection operations for HUMINT are characterized by effective planning, management, and support. Human intelligence operations can span the operational spectrum, from overt to clandestine collection operations and related intelligence activities. Only trained and certified Marine Corps HUMINT collectors (or those personnel, as directed by the DIRINT), who are assigned to organizations with a mission to conduct HUMINT, can engage in HUMINT collection and related intelligence activities to satisfy intelligence collection requirements (ICRs) (MCWP 2-10).

As an intelligence discipline, HUMINT is an intelligence collection capability utilized to collect foreign intelligence from human sources to answer information requirements. Collection through HUMINT generally takes longer than that of any other collection capability because of the time needed to develop relationships with potential sources of information. Although HUMINT takes time to fully develop, it can provide information not accessible through other intelligence collection methods. Because human interaction can collect unique human perspectives, HUMINT is often tasked to collect information that other, more technical collection capabilities, cannot obtain. Human intelligence enables the commander to understand the rationale of the adversary or enemy. This insight allows the commander to gain and maintain decision-making advantage in the operational environment. Human intelligence operations ultimately strive to fulfill HUMINT intelligence collection requirements identified in the collection plan.

Human intelligence operations should be initiated as early as possible during operational planning and are most effective when employed during steady state shaping operations (Joint Publication [JP] 3-33, Joint Land Operations). Human intelligence activities during shaping can include identifying potential sources and the conducting liaison with host country personnel, military, and other government officials. HUMINT ICRs are often not directly relevant to unit force protection efforts. Force protection, as a function of counterintelligence, can involve human source operations for force protection-related intelligence collection requirements. Both CI and HUMINT conduct human source activities, although for different purposes and under different authorities.

Human intelligence has two main limitations. First, the supported MAGTF commander must identify intelligence collection requirements before HUMINT Marines can collect the required information. A collection requirement is a valid need to close a specific gap in intelligence holdings in direct response to a request for information. The second limitation is the time it takes to develop HUMINT collection operations capable of reporting against a MAGTF commander's requirements. Human intelligence responsiveness can be limited in certain circumstances based on the time required to—

- Plan HUMINT collection.
- Coordinate HUMINT activities.

- Deploy HUMINT collectors.
- Develop and validate HUMINT sources.
- Collect required information.
- Disseminate reporting.

Employment of Human Intelligence

Counterintelligence/HUMINT-trained personnel are employed in various roles and in several different formations. The counterintelligence and human intelligence detachment (CHD) is the most commonly employed Marine Corps CI and HUMINT unit. Additionally, command counterintelligence and human intelligence staff element (2X) might create a HUMINT cell to focus on command HUMINT requirements. Human intelligence collection activities cover a range of tasks that include—

- Using persons who are deliberately trained and systematically employed to collect required information.
- Eliciting information from the civilian populace, to include transients and refugees.
- Debriefing US and allied military and civilian personnel.
- Interrogating enemy prisoners of war (EPWs) and detainees.
- Conducting triage and limited exploitation of captured adversarial documents, media, and materiel.
- Conducting liaison with other US and allied intelligence services and organizations.

CI and HUMINT Equipment Program

The CI and HUMINT Equipment Program is the Marine Corps CI/HUMINT community equipment program of record (PoR), which provides the capability to rapidly collect, process, and disseminate intelligence information in support of the MAGTF. Each suite is designed to provide integrated, standardized, and interoperable information and communication systems as well as specialized equipment to conduct the full spectrum of CI/HUMINT, and technical collection operations. The program also includes a TSCM capability designed to detect, locate, identify, neutralize, and exploit various adversarial penetration technologies that are used to obtain access to classified and sensitive information. Multiple programs of record are involved in fielding equipment in support of CI and HUMINT. The program is designed to support CI and HUMINT activities and operations and facilitate access to those designated web- based portals required to conduct reporting and dissemination of information.

MARINE CORPS Counterintelligence AND HUMINT ORGANIZATIONS

The DIRINT is designated the DHE for Marine Corps HUMINT matters. The DIRINT is charged with exercising direction, technical control and oversight of all USMC CI personnel and activities within the service. The organizations discussed in the following paragraphs comprise the CI and HUMINT infrastructure within the Marine Corps.

Information Intelligence Division, Headquarters, United States Marine Corps

Information Intelligence Division (IID), is the senior staff CI and HUMINT organization in the Marine Corps. The IID section head and deputy are assigned as the Marine Corps Service-level counterintelligence and human intelligence staff element (M-2X) and deputy M-2X and components assume all tasks and responsibilities for the purpose of oversight and management of Service-level CI and HUMINT activities, operations, and functions. Information Intelligence Division is the focal point for synchronizing and governing Service-level concepts and processes on behalf of the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE) to ensure and drive the integration, development, and enhancement of CI and HUMINT across the Marine Corps.

Marine Corps Service CI and HUMINT Staff Element

The M-2X is responsible for Service-level implementation of policy, plans, and programs developed by IID, as well as planning, coordinating, and executing CI and HUMINT activities and operations that support Service-level production requirements. The Marine Corps counterintelligence coordinating authority (MCCICA) and the Marine Corps Human Intelligence Operations Cell (MHOC) plan, manage, coordinate, synchronize, and deconflict CI and HUMINT activities and operations in support of Service-level priorities. The operations support element (OSE) provides functional skillset management used in support of Service-level priorities.

Human Intelligence Operations Cell

The MHOC serves as the senior representative for HUMINT to the M-2X and assists the DIRINT in the direction, management, and coordination of Marine Corps HUMINT interests and equities. The MHOC coordinates Service-level HUMINT operational activities and all associated functional management service issues with other Marine Corps CI and HUMINT elements, M-2X, and other DoD HUMINT executors, intelligence community organizations, and US Government agencies. The MHOC also maintains cognizance over a common operating picture of the DoD and Marine HUMINT capabilities.

Counterintelligence Coordinating Authority

The MCCICA serves as the senior representative for counterintelligence to the M-2X and assists the DIRINT in the direction, management, and coordination of Service CI activities. The MCCICA also assists commands that are responsible for protecting personnel, property, networks, and information to ensure CI planning, requirements, and tasking are integrated across the total force. The MCCICA coordinates Service-level CI activities as part of the Marine Corps overall all-source intelligence efforts while maintaining cognizance over a common operating picture of DoD and Marine Corps CI capabilities. As the senior CI representative, the MCCICA plans, coordinates, deconflicts, and executes CI activities conducted in support of Service requirements and responsibilities in coordination with the intelligence community and appropriate stakeholders.

Additionally, the MCCICA is responsible for synchronizing Marine Corps CI activities with combatant commands (CCMDs) and other defense senior intelligence officers as well as collecting and maintaining interagency, intelligence community, DoD, and Service CI best practices, lessons learned, and after-action reports, which are provided to the Fleet Marine Forces.

Operations Support Element

The OSE provides coordinated CI and HUMINT functional skillset management for Marine Corps CI and HUMINT elements conducting Service-level operations and activities. The OSE functional skillsets include source records management; reports management; coordinated CI and HUMINT collections requirements management; oversight of applicable CI and HUMINT systems, toolsets, and database usage; and CI and HUMINT lead target development. The OSE, in coordination with applicable CI and HUMINT chains of command, can also assist and provide functional skillset management support to all Marine Corps CI and HUMINT elements.

Marine Corps Component Commands

Each Marine Corps component command has a CI and HUMINT officer and staff element (G-2X) within the G-2. The Marine Corps component command G-2X is responsible for operational planning, administrative oversight, and managing CI and HUMINT policy and programs among subordinate commands. The G-2Xs in the following Marine Corps component commands exercise CI and HUMINT responsibilities within their assigned geographical, functional, and sub-unified component command area of operations:

- Marine Forces Command.
- Marine Forces Africa Command.
- Marine Forces Central Command.
- Marine Forces European Command.
- Marine Forces Northern Command.
- Marine Forces Pacific Command.
- Marine Forces Southern Command.
- Marine Corps Forces Cyberspace Command.
- Marine Forces Reserve.
- Marine Forces Special Operations Command.
- Marine Forces Strategic Command.
- Marine Forces Space Command.

Marine Expeditionary Force CI and HUMINT Elements

Similar to the Marine Corps component commands, each MEF has a G-2X within the G-2 staff section. The MEF G-2X is responsible for planning, and coordinating CI and HUMINT at the MEF level, as well as technical oversight and management of CI and HUMINT policy, programs, and activities of subordinate commands. The following CI and HUMINT elements are subordinate to each MEF:

- Intelligence battalion. Marine Corps CI/HUMINT personnel are task organized to a CI/HUMINT company within the intelligence battalion of each MEF subordinate to the

Marine expeditionary force information group (MIG). As a force provider, the intelligence battalion is responsible for organizing, training, and equipping the CI/HUMINT companies within a MEF.

- CI/HUMINT company. Within the Fleet Marine Forces, CI/HUMINT companies are directly subordinate to each of the respective intelligence battalions. The CI/HUMINT companies routinely deploy personnel and equipment in support of Marine Corps operations worldwide. These companies also have responsibility for conducting CI and HUMINT activities in support of MEF programs in garrison.
- CHD. MAGTFs could have CI and HUMINT assets attached or organic to the command element in the form of a CHD. A MAGTF CHD is task-organized based on mission analysis, typically consisting of Intelligence and CI/HUMINT personnel; however, the size and composition can be varied so that the detachment is augmented with personnel such as analysts, linguists, communicators, and security, if required.
- CI/HUMINT section. The MIG, Marine infantry divisions, Marine logistics groups, and the Marine air wings have CI/HUMINT elements within their staff G-2/S-2 sections. These CI/HUMINT elements solicit their authorities to conduct CI and HUMINT activities through the Marine Corps component commands or MEF G-2X who manages these authorities on behalf of the G-2 and commanders as delegated. Human intelligence authorities are granted through the DoD assigned HUMINT executor. The MEF G-2X is the central coordination and deconfliction section for authorities across all units subordinate to the MEF. This does not preclude the solicitation of authorities from other and higher elements such as the Marine Corps component commands and the Marine Corps as a Service.

Supporting Establishment CI and HUMINT Elements

There are numerous CI and HUMINT supporting establishment billets within units across the Marine Corps. Supporting establishment units must have the authority and permissions to conduct CI and HUMINT for the supported command. Marine Corps billets also reside within other services and CCMDs. Supporting establishment and external billets are often singular in nature, limiting the capacity of the CI/HUMINT Marine to support the assigned command. Units with limited capacity for the conduct of CI and HUMINT functions should solicit the assistance of service elements to accomplish the assigned mission.

OTHER DEPARTMENTAL AND SERVICE CI AND HUMINT ORGANIZATIONS

Department of the Navy Counterintelligence Enterprise.

The Department of the Navy (DON) CI enterprise is composed of CI elements of Naval Criminal Investigative Service (NCIS), the Marine Corps, and the Navy. The DoDD 5240.02 designates NCIS as the DON Military Department Counterintelligence Organizations (MDCO). Per Secretary of the Navy Instruction (SECNAVINST) 3850.2E, Department of the Navy Counterintelligence. The NCIS, as the MDCO, in coordination with Service-level Navy and Marine Corps CI staff elements, has established a DON CI coordination cell to coordinate CI activities throughout the DON. The NCIS MDCO maintains primary responsibility to coordinate activities between the Service CI components within the DON, while the Services (Navy and

Marine Corps) are responsible for conducting CI activities in support of service requirements and integrating counterintelligence into all service operations, programs, systems, exercises, plans, doctrine, strategies, policies, and architectures.

Naval Criminal Investigative Service

The NCIS MDCO is the only DON component authorized to conduct unilateral CI investigations as detailed in SECNAVINST 3850.2E. The NCIS is responsible for conducting CI investigations, for the Navy and the Marine Corps, on matters involving national security crimes, such as espionage, compromise of classified or sensitive material, and other acts prejudicial to national security for which Navy or Marine Corps personnel are subject to criminal prosecution

Additionally, NCIS is the primary agency for providing CI scope polygraph support to Navy and Marine Corps forces. Polygraph scheduling of Marine Corps personnel is requested through Headquarters, US Marine Corps, DCI, IID, SSO, subsequently coordinated through NCIS. The Naval Criminal Investigative Service is the DON lead agency for conducting offensive counterintelligence operations (OFCO) when it is conducted as a DON CI enterprise-coordinated activity from combined operating locations. Marine CI and HUMINT personnel can be detailed to NCIS to facilitate support to local commanders, under the authorities of NCIS.

United States Navy Intelligence

The Navy, like the Marine Corps, has CI and HUMINT responsibilities within the Navy. These responsibilities are managed and overseen by the Naval Intelligence Activity CI and HUMINT Directorate (also referred to as NIA-X) via the Navy CI and HUMINT operations cell. Navy CI and HUMINT personnel are trained alongside their Marine Corps counterparts in the MAGTF CI/HUMINT course.

Navy Counterintelligence. The Navy and the Marine Corps have a mutually supportive relationship with NCIS regarding counterintelligence as a member of the DON CI enterprise. The Navy conducts CI activities to detect, identify, assess, exploit, and deny FIEs and insiders targeting Navy information, personnel, operations, and other activities.

Navy Human Intelligence. Navy HUMINT plans, programming, and policy are centrally managed under NIA-X. Navy HUMINT crosses all operational spectrums and consists primarily of foreign military intelligence collection activities-trained debriefers aboard Navy ships assigned to naval component commands. Additionally, Navy personnel conduct HUMINT operations in response to the Navy's strategic and operational collection requirements under the direction of the Office of Naval Intelligence. Navy tactical HUMINT capabilities are primarily situated with the Navy Expeditionary Intelligence Command, whose personnel deploy as part of an intelligence exploitation team in direct support of a naval component command to conduct tactical- to operational-level HUMINT in response to the fleet commander's intelligence requirements.

United States Army Intelligence

The Army is the largest CI and HUMINT component within DoD and has both a strategic and tactical mission. The Army separates CI and HUMINT into two distinct MOSs; this separation extends to the tactical level as well. The following provides a basic overview of the Army CI and HUMINT infrastructure and missions.

United States Army Intelligence and Security Command. The United States Army Intelligence and Security Command (INSCOM) is responsible for all Army military intelligence actions above corps level to include CI analysis, collection, investigations, operations, tactical intelligence, and related activities, and HUMINT collection at the operational and strategic levels. The INSCOM staff also supports the deployed commander with information operations, polygraph support, and TSCM support. It consists of Army military intelligence brigades and groups that provide Army component commands CI and HUMINT support. This command maintains several military intelligence brigades and groups assigned regionally to provide a consistent, forward-deployed presence in a particular theater of operation.

Army Corps and Below. At the Army corps level and below (division, brigade, regiment, battalion), CI and HUMINT capabilities are embedded within the larger military intelligence battlefield structure. At the tactical level, Army CI personnel conduct CI investigations, collections, production and analysis (P&A). Army tactical HUMINT personnel conduct military support operations, interrogations, debriefings, and DOMEX. Army CI and HUMINT assets organic to corps-sized elements and below comprise most of the Army's tactical CI and HUMINT capability and are assigned within the following Army tactical intelligence organizations:

- Tactical exploitation battalions at the corps military intelligence brigade.
- Military intelligence battalions at division.
- Military intelligence companies at armored cavalry regiments and separate brigades.
- Military intelligence elements at Special Forces groups.

National Ground Intelligence Center. The National Ground Intelligence Center (NGIC) is part of INSCOM and produces and disseminates all-source integrated intelligence on foreign ground forces and related military technologies to ensure US forces have a decisive edge in current and future military operations. The NGIC mission includes—

- Serving as a producer of ground forces intelligence. The NGIC produces scientific and technical intelligence and military capabilities analysis on foreign ground forces.
- Serving as part of NGIC's Foreign Materiel Program, gathering military intelligence characteristically found on recent battlefields or other places foreign materiel might be available.

Air Force Office of Special Investigations.
The Air Force Office of Special Investigations (AFOSI) is a law enforcement investigative agency that provides CI support to the Air Force. The AFOSI maintains local and regional offices at Air Force bases throughout the United States and overseas. Additionally, AFOSI field agents deploy ahead of Air Force elements to provide CI force protection and law enforcement support to air points of embarkation, debarkation and other Air Force facilities and units. Agents of the AFOSI conduct CI collection activities, CI investigations, analysis, operations, and criminal investigations in support of the Air Force. Within the Air Force, the Air Force Director of Intelligence, Surveillance, and Reconnaissance (ISR) oversees and manages HUMINT operations and serves as the Air Force proponent for HUMINT policy, programming, and resourcing,

providing operational oversight and representation for HUMINT activities. The Director of ISR has delegated to the National Air and Space Intelligence Center specific HUMINT collection of air, space, and cyberspace information in support of Air Force and CCMD air components.

COMBATANT COMMAND AND JOINT FORCE COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE STAFF ELEMENT

Within each CCMD intelligence staff, CI and HUMINT responsibilities are assigned to the joint counterintelligence and human intelligence staff element (J-2X). The CCMD J-2X staff is responsible to direct, control, and coordinate all CI and HUMINT activity conducted by the component commands within a combatant commander's area of responsibility (AOR). The CCMD construct varies according to the combatant commander's requirements. The CCMD is a joint staff composed of elements of the Army, Navy, Marine Corps, and Air force to include other DoD, civilian and national organizations.

As a Service component command, subordinate to a CCMD, the component commander has a CI and HUMINT staff element responsibility under the G-2 intelligence staff. The Marine Corps service component G-2X is responsible for the USMC Service CI and HUMINT functions pertaining to USMC service personnel in, or deploying to, the CCMD AOR. The G-2X of a component command and the CI and HUMINT personnel assigned to the component command can conduct intelligence activities under Service authorities, or CCMD authorities, to fulfill ICRs, with appropriately solicited and coordinated permissions. When executing counterintelligence or HUMINT service authorities under a component command, it is important to coordinate and deconflict activities and operations with the CCMD J-2X.

Within a joint task force (JTF) intelligence staff, CI and HUMINT responsibilities are assigned to the JTF counterintelligence and human intelligence staff element (J-2X), which is responsible to direct, control, and coordinate all services CI and HUMINT activity within a JTF commander's AOR, and those CI and HUMINT activities associated with the JTF mission. The JTFs are created to address operations in specific locations, often a country, located in the CCMD's AOR.

Combatant Command Counterintelligence Coordinating Authority

The command counterintelligence coordinating authority (CCICA) is the title of the CCMD J-2X CI special staff function representative. The CCICA is responsible for overall CI plans, policy, programs, and operations at the CCMD level. Although a CCICA does not routinely have control over service component CI assets, there is frequent interaction and coordination between the CCICA and the senior Service component CI representative. Within the Marine Corps, the Marine Corps component command G-2X serves as the point of contact for the CCICA on CI matters. When part of a JTF, usually in support of a named operation, the role of the CICA is referred to as the task force counterintelligence coordinating authority (CICA). Within a JTF the task force CICA will direct subordinate Service CI capabilities and manage CI efforts within the mission set.

Combatant Command Human Intelligence Operations Cell

The CCMD J-2X human intelligence operations cell (HOC) is responsible for overall HUMINT plans, policy, programs, and operations within a given theater of operation. Although the HOC does not have control over service component HUMINT assets, there is frequent interaction and coordination between the HOC and the senior service component HUMINT representative. Within the Marine Corps, the HOC at the Marine Corps component command G-2X serves as the point of contact for all HUMINT matters. In a JTF, the HOC exercises direction and oversight over HUMINT efforts in the subordinate services elements.

NATIONAL-LEVEL COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE SUPPORT

National-level CI and HUMINT agencies can support CCMDs or JTF commanders. At the joint level, a national intelligence support team will work with the J-2X to coordinate national-level activities with joint and component CI and HUMINT assets. Other national level CI and HUMINT agencies that could also be represented in a joint theater of operation are the—

- Defense Intelligence Agency. The Defense Intelligence Agency (DIA) is an intelligence agency and combat support agency of the US federal government, specializing in defense and military intelligence. A component of the DoD and the intelligence community, DIA informs national civilian and defense policymakers about the military intentions and capabilities of foreign governments and non-state actors. It also provides intelligence assistance, integration, and coordination across uniformed military service intelligence components, which remain structurally separate from DIA. The agency's roles encompass the collection and analysis of military-related foreign political, economic, industrial, geographic, and medical and health intelligence. The DIA provides the following support to the DoD:
  - All-source intelligence P&A.
  - Strategic CI activities and HUMINT collection to support DoD and national requirements.
  - Disseminates finished intelligence products to answer requirements from the Joint Chief of Staff-level down to the tactical force, including—
    - Counterintelligence analytical products.
    - DOMEX.
    - HUMINT support.

- Central Intelligence Agency. The Director, Central Intelligence Agency (CIA), is the national HUMINT manager and the IC's functional manager for HUMINT. Additionally, the CIA provides the following:
  - National security intelligence to senior policymakers.
  - Furthers national security objectives by collecting intelligence; producing objective, all-source analysis; and conducting effective covert action as directed by the President.
  - Supports CCMDRs and JTF commanders through various means, all of which are coordinated primarily through the CCMD or JTF command J-2X HOC.

- Federal Bureau of Investigation. The Federal Bureau of Investigation (FBI) is responsible for countering threats to our national security and penetrating national and transnational networks that want to harm the United States. The FBI is the nation's lead agency for counterintelligence. The FBI's National Security Branch includes—
  - Counterterrorism, counterintelligence, weapons of mass destruction and intelligence elements.
  - The Terrorist Screening Center, which provides actionable intelligence to state and local law enforcement.
  - The High-Value Detainee Interrogation Group, which collects intelligence from key terror suspects to prevent attacks against the United States and its allies.
  - The joint terrorism task force is an FBI administered organization designed to share intelligence information with multiple agencies, to include the DoD, in an effort to counter terrorism, in the United States and abroad, against US interests.
- National Geospatial-Intelligence Agency. The National Geospatial-Intelligence Agency (NGA) is responsible for delivering geospatial intelligence products and services to decision makers, Service members, and the intelligence community in support of national security. The NGA mission includes—
  - Acquiring, developing, and maintaining the proper technology, people, and processes that enable overall mission success.
  - Exploiting and analyzing imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth.
- National Security Agency. The National Security Agency/Central Security Service (NSA/CSS) leads the US Government in cryptology that encompasses both signals intelligence (SIGINT) insights, cybersecurity products and services, and enables computer network operations to gain a decisive advantage for the nation and our allies. The NSA/CSS mission includes—
  - Deploying analysts, linguists, engineers, and other personnel to hostile areas to provide actionable SIGINT and cybersecurity support to warfighters on the front lines.
  - Providing intelligence support to military operations through signals intelligence activities, while cybersecurity personnel, products, and services ensure that military communications and data remain secure, and out of the hands of adversaries.
  - Creating common protocols and standards so that the US military can securely share information with allies, NATO, and coalition forces around the world.

CHAPTER 2. EMPLOYMENT, RESPONSIBILITIES, AND COMMAND AND CONTROL

Counterintelligence and human intelligence support warfighting functions across the range of military operations. The primary objective of intelligence is “to provide accurate, timely, and relevant knowledge about the enemy (or potential enemy) and the surrounding environment” (MCDP 2). As a complement to other intelligence collection disciplines, HUMINT is uniquely suited to provide insight into enemy plans, intentions, and capabilities. The secondary objective of intelligence conducts CI activities to identify threats and vulnerabilities, deny access to our most sensitive information and technologies, and deceive adversaries understanding of the intentions and capabilities of Marine Corps forces. Various CI measures are employed to deny information to the enemy, identify enemy intelligence activities, and shape the enemy’s knowledge of friendly forces. Thus, effective employment of Marine Corps CI/HUMINT personnel as a capability enhances the commander’s effectiveness, reduces battlespace uncertainty, and directly supports force protection. Appropriate CI and HUMINT employment requires a basic understanding of CI and HUMINT organizations, structure, relationships, responsibilities, and how CI/HUMINT elements interact to provide support to operations.

COMMANDER AND STAFF PRINCIPLES INVOLVED IN CI/HUMINT

Commander

Intelligence, counterintelligence, and HUMINT are inherent and essential command responsibilities that require the commander’s personal involvement. The commander is responsible for implementing sound, feasible, and acceptable strategies to mitigate foreign or adversary collection efforts. To accomplish this, commanders must have an understanding of the capabilities and limitations of CI and HUMINT. Human intelligence operations, combined with CI activities and measures, help the commander shape the battlespace.

Marine Air-Ground Task Force Intelligence Officer

The MAGTF G-2/S-2 is a primary staff member responsible for managing the overall intelligence effort and is ultimately responsible to the commander for the effective employment of CI and HUMINT in support of the assigned mission. The MAGTF G-2/S-2 is supported by the counterintelligence and human intelligence officer (CIHO). The CIHO is the lead CI/HUMINT officer for the G-2X/ S-2X, depending on the unit mission and tasking.

Counterintelligence and Human Intelligence Officer

The assigned CIHO formulates plans, measures, and countermeasures and recommends CI and HUMINT strategies to the commander. The CIHO acts as the commander's special staff officer and principal advisor on CI and HUMINT and ensures that CI and HUMINT capabilities are effectively employed during all phases of mission planning and execution. The CIHO also coordinates with the intelligence battalion and CI/HUMINT company commanders. The CIHO becomes the CI/HUMINT staff element officer in charge once assigned the capabilities to perform the functions associated with a CICA and HOC, and an OSE.

Intelligence Battalion Commander

The intelligence battalion commander directs the organizing, training, and equipping of subordinate CI/HUMINT companies and CHDs in support of operations and Fleet Marine Force requirements. The G-2/S-2 and CI/HUMINT staff element coordinate CI and HUMINT support requirements with the intelligence battalion commander to develop methods of employment and task organization of organic CI and HUMINT assets relevant to specific mission requirements. The intelligence battalion commander serves as the intelligence support coordinator for MEF or MAGTF operations.

Counterintelligence and Human Intelligence Company

The mission of the CI/HUMINT company is to provide trained CI and HUMINT capability to the MEF and other MAGTFs as directed. The CI/HUMINT company is organic to each intelligence battalion within the Fleet Marine Forces. The CI/HUMINT company commander is responsible to the intelligence battalion commander for organizing, training, and equipping CHDs in support of MAGTF operations. The CI/HUMINT company organizational responsibilities include—

- Conducting CI and HUMINT activities and operations in support of unit intelligence operations.
- Conducting screening, debriefing, and interrogation of persons of intelligence or CI interest, to include EPWs and detainees.
- Performing CI and terrorism threat analysis and assist in the preparation of CI and intelligence studies, orders, estimates, and plans.
- Planning, coordinating, and conducting HUMINT collection operations to include military source operations (MSOs), interrogations, liaisons, debriefings, and screenings.
- Conducting CI activities including military counterintelligence collection (MCC), debriefings, screenings, and CIIA on incidents involving espionage, sabotage, subversion, or terrorist activity.
- Conducting CI surveys, counterintelligence vulnerability assessment (CIVA), and CI evaluations.
- Providing CI and HUMINT support to vacated command post inspections, collected and exploitable material, document/media exploitation (DOMEX) and identity intelligence.

CONCEPT OF EMPLOYMENT AND COMMAND AND CONTROL SUPPORT RELATIONSHIPS

There are several methods to employ CI/HUMINT elements within a MAGTF. The method selected depends on the size of the MAGTF and the nature and scope of the supported operation. The G-2X is composed of a CICA, a HOC, and an OSE. Administrative support to CI and HUMINT elements remains the responsibility of the CI and HUMINT company commanders and their staffs. Those CHDs in general and direct support to other units can receive administrative support from the supported command.

A CI/HUMINT company is designed to support a MEF by deploying CHDs or individual augmentees to subordinate elements. The CI/HUMINT personnel are assigned to the G-2X of a MEF during wartime operations. The other CHDs can also be sourced to the supported unit in a direct support role. The command-and-control relationship is described in the operation order (OPORD). Some of the general concepts of employment and C2 relationships are outlined as follows:

- General and Direct Support. Counterintelligence and HUMINT teams can be placed in general support or direct support of a MAGTF, to include any of the subordinate elements (e.g., divisions, regiments, battalions, squadrons). Within a supported commander's area of operations, both general and direct support can be employed to satisfy collective CI and HUMINT operational requirements:
- General Support. When employed in general support, CI and HUMINT elements operate under the direct control of a higher HQ to satisfy CI and HUMINT collection and operational requirements. During general support these elements might support several commands and units simultaneously. Counterintelligence and HUMINT elements could be employed by geographical region in an area coverage to support all units operating in an AOR or delineated area. In general support, collection requirements are weighed against higher HQ requirements, prioritized, and fulfilled accordingly. The OPORD might describe both general support and direct support relationships simultaneously (i.e., direct support to 5th Marine Regiment, general support to 1st Bn, 2d Bn, 3d Bn).
- Direct Support. When employed in direct support, CI and HUMINT elements are assigned to a specific subordinate command and function under the direction of the supported unit. In direct support, supported unit collection requirements are the priority. The CHDs in direct support of a tactical unit are usually operational control (OPCON) to the MEF intelligence operations center (IOC), under the cognizance of the MEF G-2X and G- 2. In garrison, the intelligence battalion falls under the MIG, although while deployed the intelligence battalion becomes the IOC and is OPCON to the MEF G-2.

Counterintelligence and Human Intelligence Detachment Organization

The Marine Corps' basic organizational structure for conducting CI and HUMINT activities in support of a MAGTF is the CHD. A CHD is often augmented with additional CI/HUMINT Marines, all-source intelligence specialists, radio operators, linguists, and other capabilities as necessary. A CHD operating in a support role can be augmented with additional logistical support, such as convoy or security personnel to facilitate freedom of movement throughout the battlespace.

In support of the Major Subordinate MAGTF Elements. The following sections provides an overview of the typical command and control relationships of a CHD in support of MAGTF major subordinate elements.

Support to the Ground Combat Element. The CHDs are commonly assigned in direct support of subordinate ground combat elements (GCE) to ensure that the CI and HUMINT capability is available to commanders during forward combat operations. Considering the capability of a CHD, it is usually appropriate for the CHD to be in direct support of the battalion or above, and general support to the subordinate elements. As the GCE moves through the battlespace or conducts sustained combat operations, direct support CHDs can continuously collect and exploit time-sensitive tactical information specifically focused on the GCE's evolving requirements.

Support to the Aviation Combat Element. Aviation units typically conduct air combat operations throughout the MAGTF area of operations from one or more static air bases. A CHD assigned to an aviation combat element (ACE) can be employed in direct support of the ACE command element. In a general support role, a CHD can be in a direct support relationship with the higher headquarters and conduct activities throughout the assigned area of operations in coordination with ACE G-2/S-2 and one or more other subordinate units.

Support to the Logistics Combat Element. Operations conducted by the logistics combat element (LCE) provide combat service support from static, semi-static, and mobile positions. The CHDs assigned to the LCE can be employed in direct support of the LCE command element, and in general support of the subordinate logistics units. In a general support role, CHDs provide CI and HUMINT support at multiple locations or within a larger operational area in coordination with the LCE G-2/S-2. Counterintelligence and HUMINT operations in support of the LCE focus heavily on supporting force protection of LCE elements.

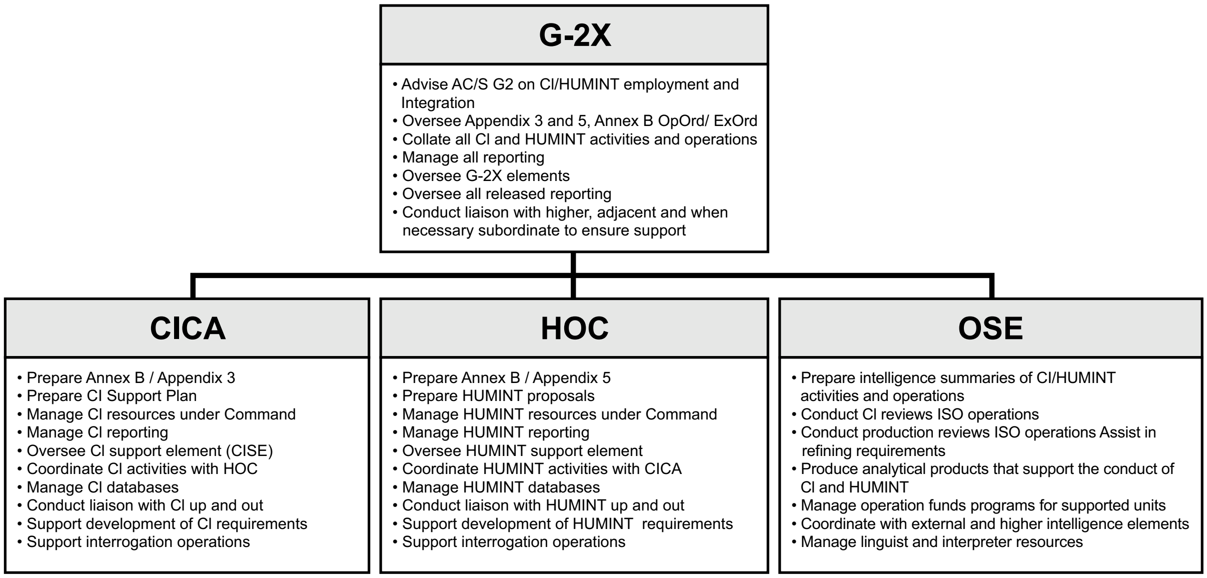
THE INTELLIGENCE STAFF

The intelligence staff (G-2X) is the doctrinal term for the MEF- or division-level CI and HUMINT staff section task organized within the command G-2 staff section. The term G-2X is often used to refer to the CI/HUMINT staff officer who is reports to the assistant chief of staff intelligence otherwise known as the AC/S G-2 or MEF senior intelligence officer. the CI/HUMINT staff element provides CI and HUMINT functions necessary to facilitate operations across the entire MAGTF or command. The 2X special staff section conducts the following functions:

- Prepares HQ-level Appendix 3 (Counterintelligence) and facilitates subordinate appendices to OPORDs.
- Prepares HQ-level Appendix 5 (Human Intelligence) and facilitate subordinate appendices to operations orders.
- Coordinates and deconflicts CI and HUMINT activities to ensure operational efficiency and focus collection.
- Receives, reviews, coordinates, and publishes operational and intelligence reporting associated with the CI and HUMINT activities and operations under its cognizance.

- Coordinates requests for and tasks CI and HUMINT support across all subordinate commands and elements.
- Manages intelligence funds associated with the conduct of CI and HUMINT activities and operations, making them available to supported unit intelligence elements.
- Focuses collection efforts of CI/HUMINT elements to ensure the ICRs are being fulfilled.
- Ensures the CI and HUMINT activities and operations are integrated into the collection plan to support the overall intelligence effort.
- Ensures CI and HUMINT activities and operations are supported with the necessary analytical support which contributes to operational effectiveness.
- Coordinates CI and HUMINT support to command security and force protection operations with the G-3/S-3 and force protection officer.
- Assists the G-2/S-2 in developing HUMINT collection requirements (HCRs), CI collection requirements, and measures in support of command operations.
- Coordinates the integration of CI and HUMINT in the development and dissemination of all-source intelligence products for the supported unit (e.g., the intelligence summary).
- Maintains liaison with higher and external CI/HUMINT agencies and services.
- Assists in the development of the CI and HUMINT reporting architecture within the MAGTF and with external organizations that require access to Marine Corps reporting.
- Serves as the principal point of contact between the command and NCIS on the investigation of actual, potential, or suspected espionage, sabotage, terrorism, or subversive activities.
- Tasks CI and HUMINT collection elements with validated intelligence collection requirements as needed to support the commander's operation plan (OPLAN). (Although the intelligence section has no authority to task elements not under OPCON, CI and HUMINT elements can be tasked appropriately through the J-3/G-3/S-3 concurrence.)
- Produces and disseminates analysis of CI and HUMINT information in support of operations and activities.

Figure 2-1 depicts the organization, relationships, and functions of the G-2X within the MAGTF IOC.



G-2X

- Advise AC/S G2 on CI/HUMINT employment and Integration
- Oversee Appendix 3 and 5, Annex B OpOrd/ ExOrd
- Collate all CI and HUMINT activities and operations
- Manage all reporting
- Oversee G-2X elements
- Oversee all released reporting
- Conduct liaison with higher, adjacent and when necessary subordinate to ensure support

CICA

- Prepare Annex B / Appendix 3
- Prepare CI Support Plan
- Manage CI resources under Command
- Manage CI reporting
- Oversee CI support element (CISE)
- Coordinate CI activities with HOC
- Manage CI databases
- Conduct liaison with CI up and out
- Support development of CI requirements
- Support interrogation operations

HOC

- Prepare Annex B / Appendix 5
- Prepare HUMINT proposals
- Manage HUMINT resources under Command
- Manage HUMINT reporting
- Oversee HUMINT support element
- Coordinate HUMINT activities with CICA
- Manage HUMINT databases
- Conduct liaison with HUMINT up and out
- Support development of HUMINT requirements
- Support interrogation operations

OSE

- Prepare intelligence summaries of CI/HUMINT activities and operations
- Conduct CI reviews ISO operations
- Conduct production reviews ISO operations Assist in refining requirements
- Produce analytical products that support the conduct of CI and HUMINT
- Manage operation funds programs for supported units
- Coordinate with external and higher intelligence elements
- Manage linguist and interpreter resources

Figure 2-1. G-2X Organization and Responsibilities.

Counterintelligence/HUMINT Staff Element Staff Headquarters Element

The doctrinal task-organized G-2X CIHO at the MEF level is typically an unrestricted officer of the rank of major with a CI and HUMINT background. The CIHO is the senior CI and HUMINT advisor to the senior intelligence officer AC/S G-2. Additionally, the HQ for the G-2X includes a chief warrant officer 4 (CI/HUMINT operations officer), a master sergeant (CI/HUMINT chief), a master sergeant (operations chief) and two gunnery sergeants. The operations officer focuses on the day-to-day operations of the G-2X and supported elements The G-2X chief is the senior enlisted CI/HUMINT Marine in the G-2X. The operations chief manages the matters of the G-2X on a day-to-day basis, overseeing operations of the elements of the G-2X. The task organization of the HQ element can include other personnel as required.

Counterintelligence Coordinating Authority

The CICA is led by the senior command representative who conducts and coordinates CI activities within an assigned AOR. The CICA develops and implements the command's CI strategy and plans, serves as the focal point for CI issues affecting the command, identifies command resource requirements, and coordinates CI support to the command. The CICA is an element of the G-2X directed and controlled by the HQ leadership in the G-2X.

Human Intelligence Operations Cell

The HOC directs, controls, deconflicts, and coordinates HUMINT activities within an assigned AOR. The HOC also assists the collection manager with prioritizing HUMINT collection requirements. The HOC prioritizes operations, positions collection assets, and tasks those organic or assigned collectors best positioned to satisfy requirements. The HOC should plan, coordinate, and conduct HUMINT activities early to identify targets and to identify leads that might help corresponding requirements. The HOC is an element of the G-2X under the direction and control of the G-2X HQ leadership.

Operations Support Element

The OSE structure and functions are determined by the scope of the CI/HUMINT operation, the staff element responsibilities, and the capabilities of the supported CHDs within the AOR. The OSE is responsible for all administrative, operational, and support functions for CHDs operating under the cognizance of the G-2X. These support functions can include source registration, validation, and management; analysis and targeting; and technical enabling operations. The OSE often serves as the nexus to coordinate and leverage other intelligence, information management, technical, and operational capabilities to strengthen CI and HUMINT activities. Without a dedicated OSE, the G-2X must request regular and recurring support from other intelligence elements. The lack of an OSE will slow operations and diminish the effectiveness of the G-2X and the supported CHDs significantly.

Counterintelligence Support Element

Dedicated CI teams, called counterintelligence support element (CISE), form for the sole purpose of conducting CI activities. The CISE conducts the range of CI functions and activities within the scope of their training and authorities for the commander. A CISE will usually operate under the operational control of the CICA. The CISE is responsible for advising and assisting the CICA in planning and conducting CI efforts activities in support of the MAGTF. The CISE can be in direct support to the MAGTF HQ and general support to the subordinate units. Counterintelligence support provided by the CISE, such as screening operations, can be requested through the G-2X.

Administrative, Logistical, and Other Support

Administrative support is provided to CI/HUMINT units via the supported MAGTF headquarters element. Counterintelligence/HUMINT companies and subordinate units can conduct field-level maintenance on organic equipment. Coordination for depot-level and above maintenance support for CI and HUMINT organic equipment is the responsibility of the G-2X. Any CHDs assigned a direct-support mission require logistical support similar to any other attachment to a supported command. During operations in a hostile environment, attached CI/HUMINT personnel might require security assistance from the supported command to conduct CI and HUMINT activities and fulfill the supported command's collection requirements.

Counterintelligence and Human Intelligence Technical Considerations

Several opportunities exist for CI and HUMINT activities to facilitate the technical collection of information.

Identity Intelligence

Identity intelligence is the study of measurable biological characteristics, such as fingerprints, retina scans, and facial features. Identity intelligence provides a useful tool for individual identification and verification, particularly in environments where public records and personal identification are not common. Identity intelligence is used in many facets of military work, including detainee identification, records keeping, security clearance verification, and law enforcement. Counterintelligence and HUMINT Marines are incidental users of the biometrics equipment. Identity equipment is used to support validation and vetting of trusted sources during asset operations.

Because Marine Corps CI/HUMINT personnel work with human sources, the ability to establish positive identification is critical. Sources could attempt to conceal their identities and hostile intentions. Therefore, CI/HUMINT Marines require an understanding of biometrics and methods of defeating or neutralizing those technologies to ensure effectiveness of source operations. Marine Corps CI/HUMINT personnel must leverage and maximize identity intelligence from both a defensive and offensive perspective. Identity intelligence databases can be used by CI/HUMINT personnel to determine cultural associates and networks that are beneficial to CI or HUMINT efforts.

Site Exploitation

Site exploitation involves the collection, triage, and subsequent dissemination of information of immediate tactical value to the commander. To triage information is to identify and prioritize items of potential intelligence value. The site exploitation generated for submission varies with what information, equipment, or evidentiary material is collected. The contents of the site exploitation package are constant, but the format of reports and reporting procedures are dictated by standard operating procedures (SOPs) and theater directives based on the operational environment.

Counterintelligence/HUMINT personnel could be requested to support site exploitation, which often involves other personnel and capabilities. For example, chemical material should be handled by chemical, biological, radiological, and nuclear Marines. Captured enemy material is provided to the expeditionary forensic exploitation for forensic exploitation. Explosives should be handled by explosive ordnance disposal personnel. Special operations forces might be needed to handle high-value individuals or sites. Follow-on site exploitation can be conducted by other intelligence disciplines. During site exploitation, it is important to recognize that CI/HUMINT might be needed to screen or process the personnel on the site as an operational priority, making them unavailable to support other site exploitation activities such as biometric enrollment or document triage. Dedicated exploitation capabilities and personnel available to the force should be leveraged when possible. Although some exploitation equipment is often made available to intelligence Marines, the exploitation mission is not uniquely an intelligence task.

Document and Media Exploitation

Document and Media exploitation enables CI/HUMINT personnel to immediately exploit and preserve information of potential intelligence value. The task of identifying and extracting information from multimedia sources requires a high level of expertise. Supporting CI/HUMINT personnel work with other intelligence disciplines, organizations, and forensic personnel as required for media exploitation. Counterintelligence/HUMINT Marines conduct focused DOMEX in support of CI and HUMINT activities. Dedicated theatre exploitation capabilities and personnel available to the force should be leveraged when possible. Although some exploitation equipment is often made available to intelligence Marines, the exploitation mission is not a uniquely intelligence task.

Technical Counterintelligence and Human Intelligence Activities

Technical support to CI and HUMINT activities includes audio and video monitoring, close-target reconnaissance, support to targeting, and asset tracking. Counterintelligence/HUMINT personnel will use organic non-networked technical collection equipment in myriad circumstances across the range of military operations in support of CI and HUMINT activities. Some PORs support technical CI and HUMINT activities. Through coordination with the program office, TSCM elements can provide technical support.

Counterintelligence and Human Intelligence in Cyberspace

Modern and emergent technologies in the cyberspace domain facilitate threats to friendly forces, requiring active and passive CI activities in response. Counterintelligence activities within the cyberspace domain can deter unauthorized persons from obtaining sensitive or classified information from USMC networks. This includes supporting defensive cyber elements in the assessment of cyber incidents and intrusions, and assisting with identifying FIE within the Marine Corps Enterprise Environment (MCEE), in accordance with Department of Defense Instruction (DoDI) 5240.23, *Counterintelligence (CI) Activities in Cyberspace*.

Counterintelligence specialists conducting operations within the cyberspace domain align with defensive cyber operation (DCO) elements (i.e., network battalions or DCO-internal defense measures Companies), ensuring mutually supportive efforts. Such relationships assist in detecting anomalous activity indicative of FIE-associated activities or insider threats, develop leads for

investigative plans, and conduct analysis of trends and behaviors to better understand threat plans. Indicators of potential threat activity of CI interest on USMC networks include—

- Known, suspected, or attempted intrusions into unclassified or classified information systems by unauthorized persons.
- Tampering of user devices while users are traveling in foreign countries.
- Traffic from high-risk countries indicative of malicious behavior.
- Unauthorized hardware connections to networks.
- Denial of service attacks and suspicious network communication failures.

Events included in categories 1, 2, 4, and 7 of the Cyber Incident or Reportable Cyber Event Categorization table in the Chairman of the Joint Chiefs of Staff Manual 6510.01B.

CHAPTER 3. COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE PLANNING, COORDINATION, AUTHORITIES, AND PERMISSIONS

Counterintelligence and HUMINT planning and execution are conducted in accordance with the intelligence cycle as it supports operations. The intelligence cycle is a procedural framework for the development of mission-focused intelligence support. The intelligence cycle is not 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 intelligence requirement individually and leverage the best collection resources against that requirement in order to obtain the required information in the most effective way to support the needs of the mission. Figure 3-1 illustrates the typical intelligence cycle.

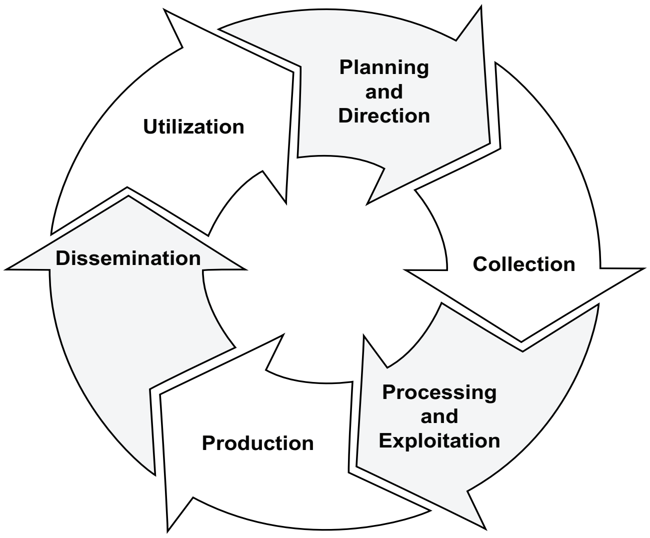


Figure 3-1. The Intelligence Cycle.

Counterintelligence/HUMINT planning is a general term that encompasses—

- Drafting CI and HUMINT appendices to the OPORD or OPLAN.
- Participating in the Marine Corps Planning Process (MCPP).
- Concepts of employment and concepts of support.
- Conducting CI and HUMINT activities in support of force protection and the collection plan.

The order of the steps depends on identification of pertinent ICRs. Counterintelligence and HUMINT planning derives from the intelligence preparation of the battlespace (IPB), which determines information gaps which then turn into collection requirements. Because establishing CI and HUMINT activities requires considerable time, early planning and execution is the key to success. Intelligence planning and direction is a continuous function within the command intelligence section. The commander directs the intelligence effort, and the intelligence officer manages this effort for the commander, based on the commander's intent, PIRs, and essential elements of friendly information (EEFI), as well as any other specific guidance unique to the operation or mission.

To conduct CI and HUMINT activities and missions, planners must solicit authorities and permissions from the appropriate level of command and clearly articulate the CI and HUMINT integration effort in the OPORDs and other coordinating documents. Annex B (Intelligence), Appendices 3 and 5, coordinate and integrate the CI and HUMINT plans and intentions to support the mission. When there is no OPLAN, such as in the case of a garrison command, additional operational documents are authored, validated, and approved by appropriate authority. Counterintelligence planners use an umbrella proposal, or a common intelligence picture to articulate the method of support and to gain concurrence by the appropriate commander or authority. For HUMINT, an operating directive is created and refreshed annually to identify the command's HUMINT collection requirements. HUMINT operations proposals are created to propose and gain military source operations approval authority (MSOAA) approval to conduct HUMINT operations.

PLANNING AND COORDINATION DOCUMENTS

Annex B of the OPORD contains Appendices 3 and 5, which serves as the basis for all CI and HUMINT activities and missions in support of a named operation. These appendices explain in detail what can be done, by whom, and the specific reporting and dissemination criteria for the mission.

Appendix 3 to Annex B.

The CI appendix is prepared by the G-2X and incorporated into Annex B of the OPLAN or OPORD. Appendix 3 addresses CI-specific issues from the perspective of overall command measures employed to support the commanders' force protection efforts and protect EEFI during all phases of the operation. This appendix addresses specific offensive and defensive measures, both active and passive, in support of the OPLAN/OPORD. see Appendix A of this publication for a sample Appendix 3 format. Key areas addressed in the CI appendix include—

- Command relationships.
- Organic CI assets to be employed.
- Employment and use of external CI assets and capabilities.
- Coordinating instructions for directing and controlling CI assets, to include any special collection emphasis and operations, production, dissemination, and support arrangements.

- Tasking MAGTF CI assets.
- Production hierarchy, priorities, and plans.
- Dissemination priorities and procedures, including communications systems support to the MAGTF CI effort.
- Unique equipment and logistics requirements.

Supporting tabs to Appendix 3 can include the following:

- Tab A – Counterintelligence Target List. A matrix or list of CI-specific targets within the MAGTF area of operations. Targets include personalities, organizations, and installations (PO&I) to be collected on, seized, searched, or otherwise exploited or neutralized by CI personnel. The CI target list is usually integrated with a CI target reduction plan, which lists specific CI measures to be implemented to address each target. The CI target list and corresponding CI target reduction plan are support tools used to develop the overall CI plan. see Appendix E for an example target reduction plan.
- Tab B – Multidiscipline Counterintelligence Threat Report. More commonly known as the CI estimate, this is a multidisciplinary assessment of the CI threat to the MAGTF. The CI estimate provides a detailed analysis of the area of operations focused on intelligence, sabotage, subversion, and terrorist capabilities, as well as the impact of these factors on friendly forces and operations.
- Tab C – Designation of Theater Counterintelligence Executive Agency. The theater counterintelligence executive agency is the organization responsible for all CI activities within the AOR. In a joint operating environment, the counterintelligence executive agency is generally the J-2X, with duties executed via a designated CICA.

Appendix 5 to Annex B.

The HUMINT Appendix is prepared by the G-2X and incorporated into the Annex B of the OPLAN or OPORD (see Appendix B for a sample format). Appendix 5 provides the concept of operations for HUMINT-specific activities, primarily those dealing with human-source operations, interrogations, debriefings of detainees, refugees, and other potential HUMINT collection activities. Additional CI and HUMINT planning tools prepared or consulted during the planning and direction phase of the intelligence cycle, to include those discussed in the following paragraphs. Key areas addressed in this appendix include—

- Employment and use of external HUMINT assets and capabilities.
- Coordinating instructions for the direction and control of CI and HUMINT assets, to include any special collection emphasis and operations, production, dissemination, and support arrangements.
- Tasking MAGTF HUMINT assets.
- Interrogation and debriefing EPWs and detainees.
- Debriefing refugees and third country nationals.
- Dissemination priorities and procedures, including communications system support to the MAGTF HUMINT effort.
- Unique equipment and logistics requirements.

- Supporting tabs as required, such as MSO proposals, intelligence source registry procedures, use of specific administrative formats germane to the management of HUMINT operations.

Counterintelligence and Human Intelligence Planning Checklist

The MAGTF CI and HUMINT planning checklist identifies typical planning tasks and activities to be considered during each phase of the planning process. Most planning tasks and activities require the coordinated action of various MAGTF G-2/S-2 sections and intelligence battalion personnel. (A sample MAGTF CI and HUMINT planning checklist is contained in Appendix C).

The Common Intelligence Picture. The common intelligence picture is a formal and living document describing the approved activities a CI element conducts in support of the designated commander, to include when they will occur, and what assistance is needed from the supported organization, program, or facility. The common intelligence picture outlines those programs to be protected, such as DoD research, development, and acquisition efforts, or those technologies that provide critical program information. The common intelligence picture is updated as threat conditions change, or annually when conditions are static. It can be written to describe support to an overall program, an individual event, or a command. The common intelligence picture is signed by the senior CI person representing the implementing CI element and the supported commander. It should be reviewed with the supported organization’s security element and appropriate military department CI organization’s field office, and it should be coordinated locally with other CI elements, law enforcement agencies, and the component appropriate G-2X office. It is then forwarded to the MCCICA for coordination within the DON CI coordination cell. For more information, see Appendix D.

Operational Proposal. The operational proposal is used to solicit the authorities necessary to conduct HUMINT missions. The HUMINT planners must have an idea of what authorities will be granted under the DHE to conduct concept of employment planning. Only DHEs and component-delegated HUMINT authorities can approve an operations proposal. Organizations seeking HUMINT authorities should coordinate with the DHE to establish the format and process for the submission. The format and process can vary in content and process between the different DHEs. As units and personnel rotate through mission sets, follow-on units and personnel might be able to fall in on already approved HUMINT proposals.

COORDINATION AND RESPONSIBILITIES

Counterintelligence and HUMINT planning involves coordination among the G-2, the G-2X, the intelligence battalion commander, and the CI/HUMINT company commander to address the many aspects of operational planning. The complexity and diversity of CI and HUMINT activities also require thorough coordination with other intelligence staff organizations, such as the supported command’s intelligence sections, JTF J-2X, or CCMD CICA and HOC. Detailed and continuous coordination ensures that CI and HUMINT activities are focused on intelligence priorities and are not duplicative, that tasks do not exceed capabilities, and that supporting resources are available prior to execution.

CHAPTER 4.
COUNTERINTELLIGENCE ACTIVITIES

All CI activities fall under one or more of the five functions of CI: collection, investigations, activities, production and analysis, and functional services. Counterintelligence functions are guided by a detailed process that identifies enemy threats and friendly vulnerabilities and develops measures to defend against threats and a plan to implement the measures and conduct CI activities as necessary.

COUNTERINTELLIGENCE PROCESS

The CI process at all levels is conducted using a standard methodology that consists of five steps: develop a CI estimate, conduct CI surveys, develop CI measures, implement the CI measures, and evaluate the CI measures. The CI process is a continuous cycle of identifying threats and vulnerabilities, implementing measures to correct vulnerabilities, and executing CI activities to deny, disrupt, and exploit the adversary's or enemy's intelligence effort. Figure 4-1 depicts the CI process.

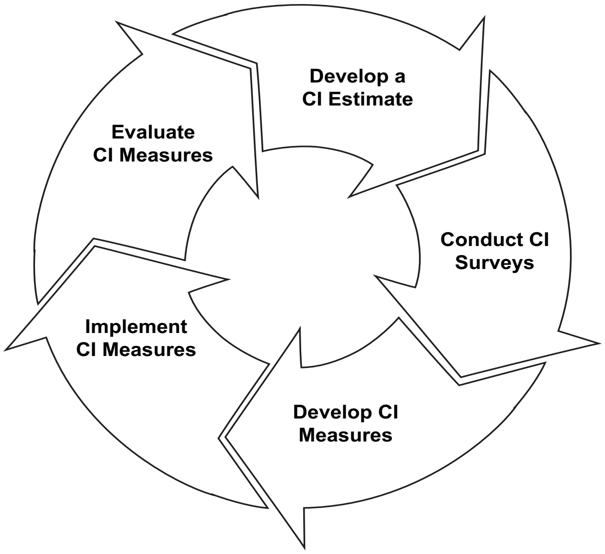


Figure 4-1. The Counterintelligence Process.

Develop a Counterintelligence Estimate

A CI estimate is an assessment of the CI threat. It includes known factors on location, disposition, composition, strength, activities, capabilities, weaknesses, and other pertinent information regarding enemy intelligence activities. A CI estimate also provides conclusions concerning probable COAs and future activities of threat organizations, effects of those activities on friendly

COAs, and effectiveness of friendly force CI measures. Within the MAGTF, intelligence and CI analysts of the MAGTF command element, the intelligence battalion, and its CI and HUMINT company or teams will typically prepare a tailored CI estimate that addresses threats to the MAGTF by using an intelligence preparation of the operational environment methodology focused on CI factors and the CI threat. The intelligence element conducting the CI estimate can use much of the CI estimate from the higher command estimate. However, each level of command must produce its own evaluation to determine which threat capabilities identified in the MAGTF CI estimate represent a threat to its particular circumstances. The CI estimate must be updated on a regular basis, and the revised estimate or appropriate CI warning reports must be disseminated to units involved in the operation.

Conduct a Counterintelligence Survey

A CI survey assesses the information security posture of a unit, facility, or installation against the threats detailed in the CI estimate. The CI survey should identify vulnerabilities to specific hostile 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 might not be possible to do a formal written survey prior to deploying. In a time-compressed situation, the survey will likely result from a brief discussion among the appropriate intelligence, CI operations, communications, and security personnel. 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. The survey helps Marines make recommendations to improve the CI posture of the command both now and in the future.

To determine the requirements for security, Marines use the CI survey, which includes—

- An analysis of the CI factors identified by the Provost Marshall Office’s Physical Security Survey that influence the security of an installation, activity or operation.
- A determination of the CI measures required by the sensitivity or criticality of the installation, activity, or operation, an assessment of the CI measures that currently exist.
- Recommendations to bring existing CI measures to the required standard.

Counterintelligence surveys must take into account all areas of military security (i.e., operational, information, physical, personnel, and embarkation). Personnel from multiple disciplines (e.g., CI military policy, physical security) should assist as necessary in conducting the CI survey.

The CI survey is not a recurring event. Its purpose is to establish requirements to fit a specific location or circumstance, rather than to test compliance with requirements already established. Once a CI survey has been conducted, it must be periodically reevaluated to ensure it remains valid in the face of changes to physical characteristics of an installation, the mission of the command, or the threat. The CI survey and its accompanying recommendation provide formal justification to the commander for adding resources for force protection.

Counterintelligence Plan

The CI plan includes the development, implementation, and evaluation of the CI measures the command uses to counter adversary intelligence, sabotage, subversion, and terrorist threats. It includes procedures for detecting and monitoring the activities of enemy intelligence and terrorist organizations and directs the implementation of active and passive measures to protect the force from these activities. The CI plan is based on threats identified in the CI estimate and the vulnerabilities detected by the CI survey. The MAGTF G-2X, assisted as necessary by the intelligence battalion commander, CI/HUMINT company commander, and the production and analysis cell officer in charge (OIC), will typically prepare a detailed, comprehensive CI plan that addresses the MEF. The CI plan is integrated with CI plans of the JTF and other pertinent forces. Included in the MAGTF CI plan are details of dedicated CI capabilities and specialized CI activities that could detect and neutralize or eliminate specific threats. Plans of subordinate MAGTF elements closely follow the MAGTF plan, typically adding only security measures that are applicable to their specific units. The CI plan must account for continuously evaluating CI measures to ensure they are still relevant and effective in countering evolving or changing CI threats.

COUNTERINTELLIGENCE IMPLEMENTATION

Counterintelligence measures—both active and passive—encompass a range of activities designed to protect against hostile intelligence, espionage, sabotage, subversion, and terrorism threats. Implementing CI measures could involve activities encompassed by any of the CI functions. Counterintelligence measures are specific, concrete actions taken to counter a CI threat or range of threats. Active and passive CI measures can be categorized into one of the three types of measures: denial measures, detection measures, or deception measures, depending on the nature of the measure.

Active (Denial, Detection, and Deception) Measures

Active CI measures are designed to neutralize the multidisciplinary intelligence effort (all disciplines used to collect intelligence, such as HUMINT, SIGINT, and imagery intelligence) and adversary efforts toward sabotage, subversion, and terrorism. Active CI measures include counter espionage, counter sabotage, counter subversion, counter terrorism, counter reconnaissance, concealment, and deception operations. These vary with the mission and capabilities of the unit.

Passive (Denial, Detection, and Deception) Measures

Passive CI measures are designed to conceal from and deny information to the enemy, protect personnel from subversion and terrorism, and protect installations and materiel against sabotage. Measures include using censorship, camouflage, concealment, light, and other security discipline to provide security for classified material, personnel, physical assets, communications, data, and electromagnetic emissions. Passive measures are codified in unit SOP, regardless of the unit’s mission.

COUNTERINTELLIGENCE MISSIONS

Marine Corps CI activities are “the active and passive measures intended to deny the enemy valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions” (Marine Corps Supplement to the DoD Dictionary of Military and Associated Terms [hereafter referred to as the USMC Dictionary]).

Counterintelligence activities support the four CI missions:

- Countering espionage, international terrorism, and the CI insider threat.
- Support to force protection.
- Support to the defense critical infrastructure protection.
- Support to research, development, and acquisition.

The five functions of counterintelligence are established in accordance with JP 2-0. Various CI functions are executed either proactively to support the implementation of CI measures and counter identified CI threats or reactively in response to emerging CI threats and incidents of a CI nature. Although CI activities are categorized within five distinct functional areas, in practice, CI activities can fall under multiple CI functions.

Counterintelligence collection is the systematic acquisition of intelligence information to answer CI collection requirements. Counterintelligence collection includes CI collections activities and MCC, and it can include any collection supporting a CI function or activity.

Counterintelligence collection includes establishing liaison with host nation (HN) intelligence, security, military services, and law enforcement agencies; interviewing walk-ins; using recruited and non-recruited sources; and debriefing EPWs, detainees, refugees, and displaced persons with knowledge of matters that are of CI interest. Marine Corps CI and HUMINT personnel collect information to support identified CI requirements, including operational efforts to detect, neutralize, and exploit FIE activities.

The MCCs are a special category of CI collection activities consisting of those deliberate and planned activities conducted by Marine CI/HUMINT personnel to collect information responsive to standing CI collection requirements and the intelligence needs of the supported commanders. The MCC can be conducted overtly or employ tradecraft to protect the asset. Recruited or non- recruited sources can be used to collect information in support of efforts to identify, deceive, exploit, or disrupt counterespionage or other clandestine activities. Military CI collections are conducted to neutralize, exploit, and mitigate threats posed by FIEs.

Some CI activities require discretion by the commander and the staff to accomplish the required task. Identifying insider threats, conducting CIIA to determine whether a CI investigation is required, activities pertaining to US personnel, offensive CI operations, the employment of technical surveillance countermeasures, and MCCs are examples of sensitive activities that require discretion by CI personnel and disclosure to only those with the need to know. Non-disclosure agreements are a standard practice during discrete CI activities.

COUNTERINTELLIGENCE INVESTIGATION

A CI investigation is a formal activity undertaken to determine whether a particular person is acting for or on behalf of, or if an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassination, or international terrorist activities and to determine actions required to neutralize such acts (*DoD Dictionary*).

The Naval Criminal Investigative Service is the Military Department Counterintelligence Organization (MDCO). Department of Defense and DON policies dictate that only NCIS as the MDCO, or Marines acting under the direction of an MDCO might conduct CI investigation s within the DON. Counterintelligence investigation s often involve investigating violations of US law, which could also involve personnel with law enforcement authorities.

Similar to a command investigation and the preceding preliminary inquiry, a commander might direct Marine CI and HUMINT personnel to conduct a CI incident assessment to examine the facts surrounding an incident of potential CI interest, and to determine whether a full CI investigation is necessary. Preliminary CI investigation s must be closely coordinated with NCIS from the onset to ensure appropriate adjudication of the incident and to preserve the potential to initiate a full CI investigation or another subsequent CI activity. A CI incident assessment and follow-on full-field CI investigation is usually conducted when the goal is to prosecute under the UCMJ or another appropriate civil legal authority. A CI investigation does not contribute to the commander’s intelligence operations because of the law enforcement focus.

Offensive Counterintelligence Operations

Offensive CI operations are CI activities conducted to support DoD and national intelligence, operational, and contingency requirements using a formally recruited asset or notional persona to develop information on a FIE. Offensive CI operations are also conducted to provide information, materials, or equipment to a FIE for the purpose of penetrating the FIE or exploiting, disrupting, or manipulating the target in order to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the DoD or the United States.

Marine CI/HUMINT personnel must undergo approved advanced training to conduct OFCO activities. Marine Corps and Navy personnel can perform OFCO activities; however, only within the DON CI enterprise. The NCIS is the DON OFCO executor and lead agency of OFCO activities and acts as a coordinator of activity from combined DON operating locations.

Counterintelligence Analysis and Production

Counterintelligence analysis is the methodical process of examining and reevaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of foreign powers, international terrorists, and other entities. Counterintelligence analysis addresses multidiscipline FIE operations and activities; illegal sale, transfer, or acquisitions of DoD-controlled technologies; terrorism, sabotage, unauthorized penetration, and related security threats; and other collection activities conducted by foreign groups targeting DoD or hostile insiders. Counterintelligence analysis can assess FIE activities throughout the operational environment and intelligence disciplines. As such, CI analysts must understand how an adversary or enemy can identify, influence, exploit, or disrupt our own intelligence activities (DoDI 5240.18, *Counterintelligence Analysis and Production*).

Counterintelligence production is the creation of finished intelligence products incorporating CI analysis in response to known or anticipated CI concerns. Counterintelligence production analyzes all-source information concerning espionage or other foreign intelligence activities, sabotage, terrorism, and other related threats and develops it into a disseminated product. Most CI production is finished intelligence and is accomplished at the Service or theater level.

Counterintelligence analysis and production supports CI activities across many functions. Although basic analysis can be conducted by CI personnel, dedicated CI analysts are required to conduct objective analysis and production in keeping with intelligence community standards. See Chapter 5 for a detailed discussion of CI analysis and production.

Counterintelligence Functional Services

Counterintelligence functional services (CIFS) are those CI activities that support other intelligence, counterintelligence, or DoD operations by providing specialized CI services to identify and counter the intelligence capabilities and activities of terrorists, foreign powers, and other entities directed against US national security (DoDI O-5240.10). Counterintelligence functional services include—

- Foreign intelligence, counterespionage, and international terrorist threat awareness briefings, debriefings, reporting, and training activities supporting the DoD component CI program (e.g., CI awareness and reporting (CIAR) annual training).
- Support to arms control and other international treaties (e.g., Open Skies Treaty inspections).
- Support to the antiterrorism and force protection program to include participation in CI surveys and CIVA (e.g., vulnerability assessment, annual training).
- Support to military services, joint, combined, and coalition (multi-national) military operations and training exercises (e.g., foreign visit, foreign disclosure, military personnel exchange programs).
- Support to war planning.
- Support to DoD foreign visitors program.
- CI incident assessments (e.g., Special Security Officer [SSO] support).
- Liaison and collection activities not associated with DoDI S-5240.17, *Counterintelligence Collection Activities (CCA)*.
- CI training.
- CI surveillance and surveillance detection.
- CI insider threat identification and mitigation.
- CI support to operational security (OPSEC) (e.g., vacated command post inspection [VCPI], after hours inspection).
- CI support to HUMINT collection, asset validation, and enabling activities (e.g., CI review, technical support).
- CI support to research, development, and acquisition to include support to supply chain risk management that is not captured by the other CI functions.
- CI support to counter proliferation and countering weapons of mass destruction.
- CI support to critical infrastructure protection that is not captured by the other CI functions.
- Intelligence information reports (IIR) generated as a result of information obtained from CIFS.
- Specialized technical CIFS.
- Polygraph and credibility assessment support.

- Technical surveillance countermeasures support.
- Track, tag, locate support.
- CI support to the Military Accessions Vital to the National Interest program.
- CI support to foreign award nominations.
- CI support in the screening of contract linguist personnel and local national personnel hired by DoD in overseas locations (e.g., polygraph, CI interview).
- CI support to cyber operations, including digital forensics and cyber vulnerability assessments.

Counterintelligence Support to Targeting

Targeting refers to the process of identifying enemy targets for possible engagement and determining the appropriate attack system to capture, degrade, destroy, or neutralize the target based on operational requirements and capabilities. The focus of targeting is on targets the adversary or enemy can least afford to lose. Counterintelligence personnel conduct CI activities that support the commanders' actions taken against the specific target. The collection of CI-related information could support the capture, degradation, destruction or neutralization of the adversaries' intelligence capabilities.

Personalities, Organizations, and Installations

The PO&I targeting triad forms the basis of CI activities. Counterintelligence targets include PO&I of intelligence or CI interest, which must be seized, exploited, neutralized, or protected. Incidents are also included within CI databases to conduct trend analysis of potential targets. The process of selecting and assigning targets is based on an assessment of the overall hostile threat, unit mission, commander's intent, EEFI, and the overarching intelligence and force protection concepts of operations. The target list must be integrated into the overall MAGTF collection plan and coordinated with MAGTF operations to determine effects on the environment. The assessment considers both the immediate and projected threats to security. The CI target list is created at the MAGTF level and includes any CI targets that have been assigned by or conducted at the MAGTF level and includes any counterintelligence targets assigned by higher headquarters (HHQ). Numerical priority designations are assigned to each target to emphasize the relative importance and value of the target. Designations also indicate the degree of security threat and urgency in neutralizing or exploiting the target. Priority designations established by HHQ are not altered; however, lower echelons can assign priorities to locally developed targets. Counterintelligence targets are usually assigned priority designations according to the following criteria:

- Priority one. Targets that represent the greatest CI threat to the MAGTF. They also possess the largest potential source of intelligence or CI information or material that must be exploited or neutralized as soon as possible.
- Priority two. Targets that are of lesser significance than priority one targets. They are to be taken under control after priority one targets have been neutralized or exploited.
- Priority three. Targets that are of lesser significance than priority one or two targets. They are to be neutralized or exploited as time and personnel permit.

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 of interest—detain, of interest, and protect—as discussed in the following sections.

Detain. A CI listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of friendly forces. The detain list includes—

- Known or suspected enemy or adversary espionage, sabotage, terrorist, political, or subversive individuals.
- Known or suspected leaders and members of adversary paramilitary, partisan, or guerrilla groups.
- Political leaders known or suspected to be hostile to the military and political objectives of the United States or an allied nation.
- Known or suspected officials of enemy governments, enemy collaborators, or sympathizers whose presence in the theater of operations pose a security threat to US or allied 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 or national departments or agencies.

Of Interest. Regardless of their leanings, personalities could be on an ‘of interest’ list when known to possess information or particular skills required by friendly forces. They could be individuals whose political motivations require further exploration before they can be used effectively. Examples of individuals who could be included in this category are—

- Potential or actual defectors from the adversary cause whose credibility has not been established.
- Individuals who have resisted, or are believed to have resisted, the enemy and who might 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 involved with enemy weapons of mass destruction and other programs against their will.

Protect. Compiled or developed at all echelons of command, protect lists contain the identities and locations of individuals in enemy-controlled areas who are of intelligence or CI interest because they might be able to provide information or assistance in the accumulation of intelligence or CI interest because they might be able to provide information or assistance in the accumulation of intelligence data or in the exploitation of existing or new intelligence AOIs. They are usually in accord with, favorably inclined, or cooperative toward US policies. Their contributions are voluntary. Decisions to place individuals on the protect list could be affected by the combat situation, critical need for specialists in scientific fields, or other intelligence needs that arise. The identities of persons on the protect list might need to be safeguarded to preserve their value and ability to be employed in CI activities (e.g., MCC). Examples of individuals included in this category are—

- Deposed political leaders of an adversary state.
- Intelligence agents employed by US or allied intelligence agencies.
- Key civilians in areas of scientific research, including faculty members of universities and staffs of industrial or national research facilities whose credibility has been established. Leaders of religious groups and other humanitarian groups.
- Other persons who can significantly aid the political, scientific, and military objectives of the United States and whose credibility has been established.

Organizations. This category includes any organization or group that is an actual or potential threat to the security of JTF or allied forces and must be neutralized. However, an organization or group could present a threat that is not immediately apparent. The enemy frequently camouflages 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 operation. Examples of adversary organizations and groups of major concern to the CI unit during tactical operations include the following:

- Adversary 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, active military and veterans, and former combatant groups known to be hostile to the United States.
- Adversarial sponsored groups and organizations whose objectives are to create dissension and spread unrest among the civilian population in the area of operations.

Installations. This category includes any installation, building, office, or field position that could contain information or material of CI interest or that could pose a threat to MAGTF security. Examples of installation-type targets are—

- Installations formerly or currently occupied by enemy espionage, sabotage, subversive, or 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 signals communication centers.
- Research centers and chemical 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 utilizes and other installations to be taken under early control to prevent sabotage. These installations are usually necessary for the rehabilitation of civil areas under US control.
- Embassies and consulates of adversary governments.

COUNTERINTELLIGENCE TOOLS

There are several common tools used to support the planning and execution of CI activities that provide both quantitative and qualitative information.

Counterintelligence Measures Worksheet

The CI measures worksheet is a quick-reference document that outlines specific CI measures to be taken to counter specific vulnerabilities outlined in the CI survey. The CI measures worksheet delineates specific units or personnel responsible for implementing each CI measure and provides amplifying information to ensure each CI measure is implemented properly. The CI measures worksheet must be updated as necessary to reflect changes in the CI estimate or CI survey and also to reflect changes in CI measures based on those that have been found to be inadequate or ineffective. The CI measures worksheet will include active and passive measures to deny, detect, and deceive adversarial intelligence efforts. Appendix F provides an example of a CI measures worksheet.

Personalities, Organizations, and Installations Database

The files in the PO&I database become the cornerstone of CI activities planning and targeting and guide their conduct. Intelligence and CI analysts at the MEF level serve a key role in establishing and maintaining CI information databases and must coordinate with lower echelons to eliminate the duplication of effort and maximize information sharing. Counterintelligence elements themselves can create and maintain local PO&I files and databases specific to their AOR, although the focus should be on cataloging information not already stored in other databases. Databases and files maintained by external entities, particularly in a joint operating environment, could also contain PO&I information relevant to the command's requirements, even if such files are not maintained specifically for CI purposes. Detain, of interest, and protect records are also maintained as a part of or in conjunction with PO&I files.

Counterintelligence Target Reduction Plan

While the CI estimate outlines threats, and the CI survey outlines friendly vulnerabilities to these threats, the CI target reduction plan outlines specific enemy targets capable of exploiting friendly vulnerabilities and outlines a plan to mitigate the threats these targets pose. The CI target reduction plan prioritizes enemy targets by the threat posed. The timely seizure and exploitation of CI targets requires a detailed and well-coordinated CI reduction plan prepared well in advance. All targets, assigned or developed, located within the unit's area of operations are listed in the reduction plan. Counterintelligence elements supporting tactical assault units typically prepare the reduction plan based on the scheme of maneuver, with the targets listed in the sequence in which they are expected to appear in the AO. The target priority designations, however, 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 target reduction plan and applicable reports are submitted. A well-prepared and comprehensive CI target reduction plan ensures coverage of all significant CI targets and allows all CI units to conduct daily operations based on established priorities.

CHAPTER 5.
PRODUCTION AND ANALYSIS

The MAGTF intelligence section provides decision makers with an understanding of the battlespace and supports the MCPP. This understanding encompasses a sophisticated knowledge of the threat and the physical, political, economic, and cultural environment in the area of operations. That knowledge is developed through intelligence production and analysis as a result of intelligence collections and force protection activities. The MAGTF CI and HUMINT production and analysis is the filtering, recording, evaluating, and analyzing of information, and developing intelligence products to enable the commanders' decision-making process, and support CI and HUMINT activities and missions.

Analysis is not proprietary to the trained all-source intelligence analyst. Collectors and operational managers can also conduct analysis in support of CI activities and HUMINT operations. There are two general areas into which CI and HUMINT production and analysis can be divided. The first is the analytical efforts, which result in finished CI and HUMINT products that might not directly support the furtherance of CI/HUMINT missions. These could be, although are not limited to, assessments, advisories, and conclusions made by analytical teams that support the commanders' decision-making process or inform the intelligence community. The second are those analytical efforts made by CI/HUMINT analysts supporting CI/HUMINT activities. This analysis might not result in finished analytical products that are directly relevant to the IPB process or the commanders' decision-making ability. These analytical efforts are necessary for the focused, methodical conduct of both CI and HUMINT in an operational element. Examples include CI reviews, production reviews, source reliability codes, prioritized PO&I matrix, and target-reduction lists.

TYPES OF COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE FINISHED ANALYTIC PRODUCTS

Assessments

Intelligence assessments require in-depth study and research. A CI assessment will explicitly express analytic judgments, identify underlying assumptions, incorporate all-source information, identify pertinent intelligence gaps that influence the analytic conclusion, and discuss a potential outlook.

Analysis Reports

Counterintelligence and HUMINT analysis reports might require in-depth study and research but generally are not as comprehensive as assessments. A CI analysis report expresses analytic judgments, incorporates all-source information, discusses a potential outlook, and identifies pertinent intelligence gaps that influence the analytic conclusion.

Threat Advisories

Counterintelligence threat advisories are short analytic reports that identify an impending foreign intelligence threat or capture the generalities of an existing or current foreign intelligence threat. A CI threat advisory often contains perishable information and involves limited study or research.

PRODUCTION AND ANALYSIS SUPPORT TO ACTIVITIES AND OPERATIONS

All-source analytical support provides CI/HUMINT Marines, and the supported commander, with information and finished products on specific sources, targets, and topics, reducing uncertainty on the battlefield and supporting CI/HUMINT activities. Analysts produce assessments for CI/HUMINT reporting and participate in evaluating the importance, accuracy, and relevancy of CI/HUMINT reporting for established information requirements. This provides CI/HUMINT operational managers and intelligence sections with information necessary to focus CI/HUMINT activities, cover gaps in intelligence collection, and contribute to more valuable CI/HUMINT reporting. Planning for CI/HUMINT activities should include analytical support requirements for the CI/HUMINT staff element if no analysts are assigned to the section. Specific analytical products are necessary for the initiation and continuation of CI/HUMINT activities. These products are critical to the fulfillment of ICRs and the mitigation of adversary or enemy intelligence collection efforts, therefore contributing to the intelligence effort.

Production and Analysis within the Marine Corps

Within the Marine Corps, CI and HUMINT analysis is conducted at all levels. Commanders can direct analysis and production to support CI and HUMINT activities can as needed to enable intelligence activities and facilitate force protection efforts.

Service level CI/HUMINT production and analysis is conducted primarily at the Marine Corps Intelligence Activity (MCIA), Marine Corps Base Quantico, Virginia. Service-level CI and HUMINT production and analysis focuses on Service CI requirements and support to Service HUMINT operations. Additionally, Service CI and HUMINT production and analysis supports Service elements around the world by offering expeditionary reach-back support resources.

The CI/HUMINT companies performing the counterintelligence or HUMINT mission in garrison might rely on the analytical personnel within the intelligence battalion to support CI/HUMINT production and analysis in support of the MEFs intelligence requirements. Additionally, the MEF CI/HUMINT staff element coordinates and facilitates CI and HUMINT activities and might have an OSE to conduct production and analysis in support of MEF elements. This is also the case with Marine Corps component commands which support the CCMDs. The MARFOR-2X might retain an OSE capability, which supports Marine Corps CI and HUMINT activities and missions in support of the assigned CCMD.

At the tactical level, CI and HUMINT production and analysis provide direct support to tactical efforts of the command and employ basic analytic techniques, methods, and resources. Regardless of the level at which production and analysis is conducted, the activity incorporates all-source intelligence into finished products to the greatest extent possible, consistent with applicable laws and authorities.

Counterintelligence and HUMINT production and analysis within the CHD is critical to the success of the commanders' intelligence collection mission and force protection efforts. Analysts in support of the CHD conduct a myriad of activities and create products which support and focus CI and HUMINT efforts.

Counterintelligence/HUMINT production and analysis can occur under the cognizance of the CI and HUMINT function, command or be outsourced to another supporting element. It is important when considering CI/HUMINT production and analysis to consider the value of a non-organic support element's input to analytical production. Bias by analytical support organic to the CI and HUMINT function can be detrimental to the overall effort if not recognized and mitigated. Objectivity in derivative conclusions reached by intelligence analysts, collectors, and operational managers is imperative to the conduct of the CI and HUMINT activities.

Analytical Support to Source Selection

Intelligence analysis also supports CI and HUMINT source selection. Source selection involves identifying individuals who are suitable CI or HUMINT sources due to their placement and access, or for their expertise on the desired information. Selection support is ongoing throughout the operational cycle for both overt and clandestine CI and HUMINT collection activities and missions. Counterintelligence and HUMINT source selection requires all-source analysis in support of CI and HUMINT collectors to develop actionable leads with access to high-value information that focuses collection efforts. Counterintelligence and HUMINT source selection uses analytical tools, databases, and intelligence reporting to corroborate and confirm source-provided information.

Counterintelligence Analytic Product Inclusion into the National Repository

Intelligence community analytical CI products, unless otherwise exempted by intelligence community directive (ICD) 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, shall be included in the Library of National Intelligence (LNI). Under the MCISRE, MCIA is the hub for all enterprise intelligence production and analysis and is responsible for submitting all finished Marine Corps intelligence products to the LNI (see *Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise Roadmap* for more information). All finished CI analytic products submitted to the LNI will adhere to the tenets of ICD 203*, Analytic Standards*; ICD 206, *Sourcing Requirements for Disseminated Analytic Products*; and DoDI 5240.18.

ANALYTIC METHODS

Counterintelligence and HUMINT analysts use visual analytic tools and structured analytic techniques, incorporating Socratic logic to produce intelligence in support of the mission.

Visual Analytic Tools

Many of the visual analytic tools used in CI and HUMINT analysis can be found in MCTP 2-10B, *MAGTF Production and Analysis*, ATP 2-22.2, *Counterintelligence Vol. I: Investigations, Analysis and Production, and Technical Services and Support Activities*, and ATP 2-22.31, *Human Intelligence Military Source Operations Techniques*, with the exception of the following: the CI PO&I database; the detainable, protectable, and of interest database; and the automatic apprehension list database. Other common, effective visual analytic tools used in CI analytical efforts include the following:

- Time Event Chart (e.g., visual investigative analysis chart [Figure 5-1]).
- Association matrices (Figure 5-2).
- Activity matrices. (Figure 5-3).
- Link diagrams (Figure 5-4).
- CI and HUMINT situation overlays.

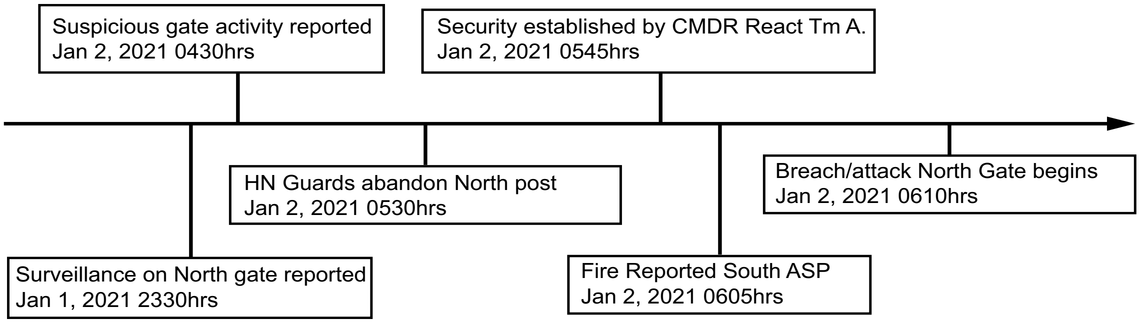
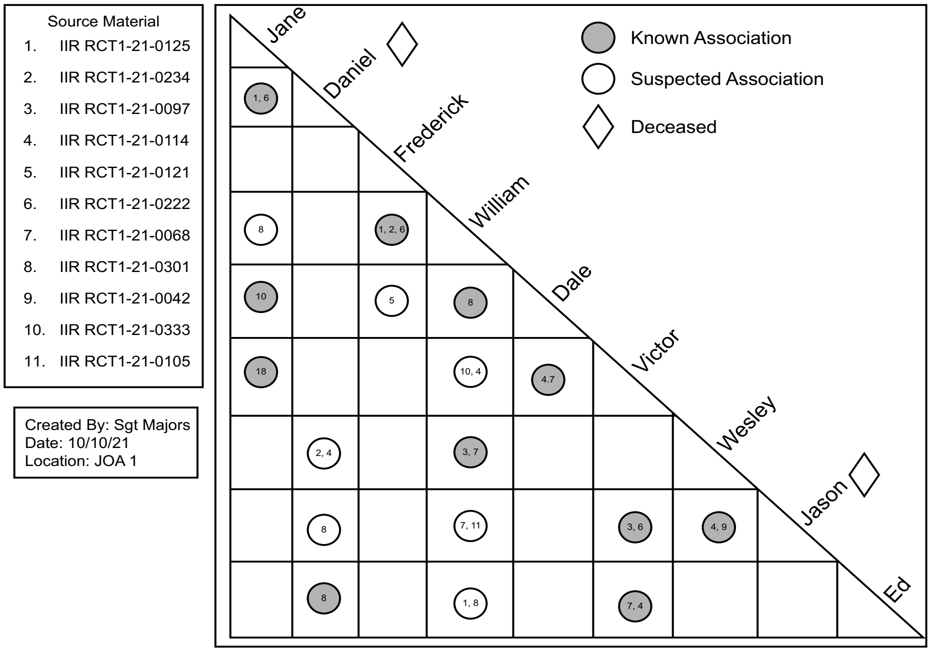

Suspicious gate activity reported
Jan 2, 2021 0430hrs
Security established by CMDR React Tm A.
Jan 2, 2021 0545hrs
HN Guards abandon North post
Jan 2, 2021 0530hrs
Breach/attack North Gate begins
Jan 2, 2021 0610hrs
Surveillance on North gate reported
Jan 1, 2021 2330hrs
Fire Reported South ASP
Jan 2, 2021 0605hrs

Figure 5-1. Time Event Chart Example.



Source Material

1.	IIR RCT1-21-0125
2.	IIR RCT1-21-0234
3.	IIR RCT1-21-0097
4.	IIR RCT1-21-0114
5.	IIR RCT1-21-0121
6.	IIR RCT1-21-0222
7.	IIR RCT1-21-0068
8.	IIR RCT1-21-0301
9.	IIR RCT1-21-0042
10.	IIR RCT1-21-0333
11.	IIR RCT1-21-0105

Created By: Sgt Majors
Date: 10/10/21
Location: JOA 1

● Known Association
○ Suspected Association
◇ Deceased

	Jane	Daniel ◇	Frederick	William	Dale	Victor	Wesley	Jason ◇
Daniel ◇	● 1, 6							
Frederick								
William	○ 8		● 1, 2, 6					
Dale	● 10		○ 5	● 8				
Victor	● 18			○ 10, 4	● 4.7			
Wesley		○ 2, 4		● 3, 7				
Jason ◇		○ 8		○ 7, 11		● 3, 6	● 4, 9	
Ed		● 8		○ 1, 8		● 7, 4		

Figure 5-2. Association Matrices.

	Attended a clandestined meeting in City Center	Works for Organization Nefarious	Suspected of participation in Bombing	Arrested by local police	Purchased materials for bombing	Seen at demonstration in front of US Consulate
William	1, 6 ○					3, 5 ○
Juan ◇			○ 2		● 9	
Ivan		3, 8 ●		● 1		
Judy ◇						
Sergei		5, 8 ○				
Antonio		3, 4 ○			● 2	
Pierre				4, 5 ○		
Bjorn	1, 3, 6 ○		2, 7 ●			
Martin						1, 5, 3 ●
Petra		● 5			○	
Achmed	○ 4		2, 6 ○		1, 3 ●	

1. IIR RCT1-21-0089
2. IIR RCT1-21-0123
3. IIR RCT1-21-0237
4. IIR RCT1-21-0108
5. IIR RCT1-21-0105
6. IIR RCT1-21-0077
7. IIR RCT1-21-0427
8. IIR RCT1-21-0427
9. IIR RCT1-21-0427

○	Suspected
●	Known
◇	Deceased

Figure 5-3. Activity Matrices.

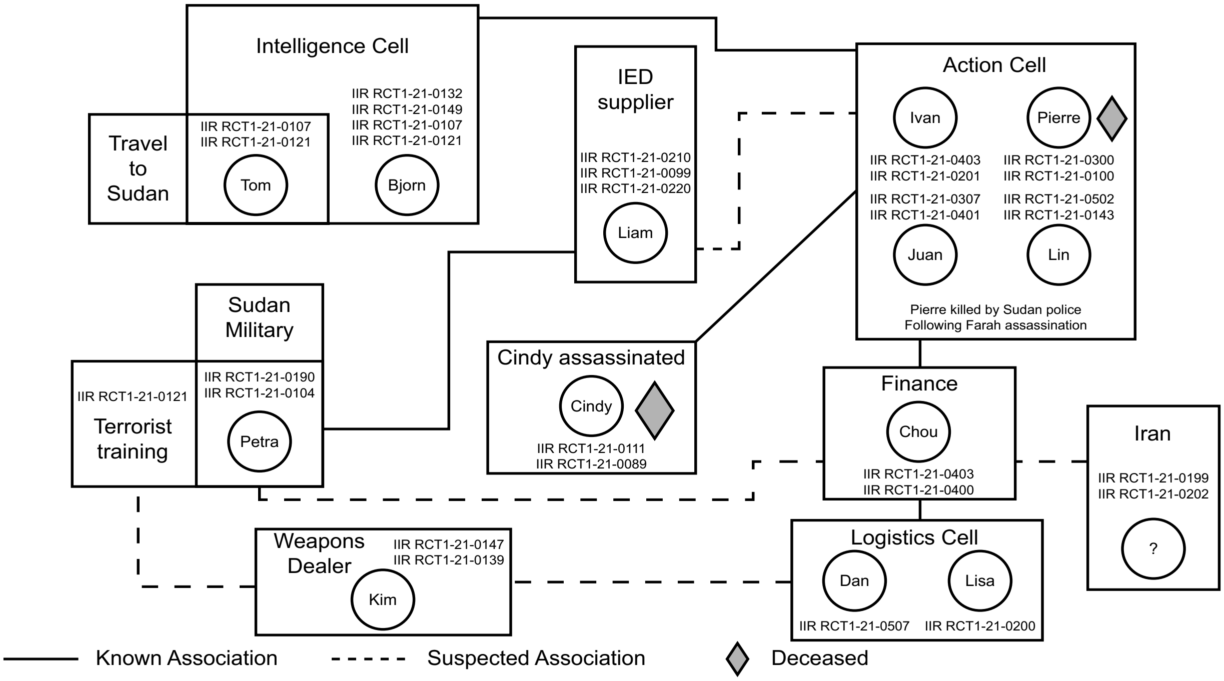


Figure 5-4. Link Diagrams.

Structured Analytic Techniques

Taken from the CIA's Kent Center for Analytic Tradecraft primer on structured analytic techniques, the following are accepted as industry standards for intelligence analysis and are required for finished community intelligence products under ICD 203:

- Key assumptions check. A list of the key working assumptions on which fundamental judgments are founded. This check is most useful at the beginning of an analytical project. It helps explain the logic of the analytic argument to more fully understand the key factors that shape an issue.
- Quality of information check. Evaluates the completeness, accuracy, and soundness of available sources of information. This technique weighs the validity of source reporting and source reliability. It can help detach deception and denial strategies and in identifying critical intelligence gaps.
- Signposts of change. A periodic review of a list of observable events or trends to track events, monitor targets, spot emerging trends, and warn of unanticipated change. This method can help establish a set of competing hypotheses and identify the most likely hypothesis, given the factors that influence change.
- Deception detection. The systematic use of checklists to determine when deception might be present and how to avoid such influences. Analysts often fail to consider deception, even when there is historical evidence of its use. This technique can add rigor to analytic logic and reinforce the effectiveness of other analytic techniques.
- Analysis of competing hypotheses. This technique identifies alternative explanations (hypotheses) and evaluates all evidence that will refute rather than confirm a hypotheses. This technique is successful when there is a large volume of information to absorb and evaluate. This technique is useful for overcoming the most common mistakes that can lead to inaccurate forecasts.
- Devil's advocacy. This technique challenges a single, strongly held view or consensus by building the best possible case for an alternative explanation. This technique is most effective when used to challenge an analytic consensus or key assumptions regarding a critically important intelligence question. This technique can be used to identify weaknesses in analytic judgments or help reaffirm confidence in a particular judgment.
- Team A and Team B. The use of separate analytic teams that contrast two or more strongly held views or competing hypotheses. This approach, different from devil's advocacy, addresses strongly held and supported analytic conclusions within an analytic section.
- High impact/low probability. This technique highlights a seemingly unlikely event that would have major policy consequences if it happened. This is a contrarian technique that sensitizes analysts to the potential effect of seemingly low probability events that could result in major repercussions. This technique can help define the high impact clearly and identify a set of indicators or observable factors to help anticipate that events were beginning to play out a particular way.
- "What if" analysis. This technique assumes that an event has occurred with potential effect, negative or positive, and explains how it might come to fruition. This is another useful contrarian technique for challenging a strong mindset, similar to high impact/low probability,

but it does not dwell on the consequences and instead focuses on how the event might come about.

- Brainstorming with divergent or convergent thinking. This is an unconstrained group process designed to generate new ideas and concepts. This technique is widely used for stimulating the thought process and can be applied to nearly all other analytic techniques. This technique maximizes creativity, often forcing analysts to think outside their own accepted norms.
- Outside-in thinking. This technique is used to identify the full range of basic forces, factors, and trends that would indirectly shape an issue. This technique is most useful at the conceptualization phase of an analytic project, when the goal is to identify all the critical external factors that could influence how a situation will develop.
- Red Team analysis. Models the behavior of an individual or group by trying to replicate how an adversary or enemy would think or act regarding an issue. History has shown that foreign actors often respond differently from US actors, based on personal, cultural, or organizational influences. This technique figuratively places the analyst into the same environment as that of the foreign actor.
- Alternative futures analysis. This technique systematically explores multiple ways a situation can develop when there is high complexity and uncertainty. This technique, also called scenarios, is most useful when a situation is viewed as too complex, or the outcomes are too uncertain to trust to a single outcome assessment. It is highly useful in extremely ambiguous situations in which not only are numerous “known unknown” factors present but also “unknown” factors exist. This technique provides an effective means of weighing multiple factors of various levels of knowledge and presents a set of plausible outcomes.

SERVICE APPLICATION OF INTELLIGENCE COMMUNITY ANALYTIC STANDARDS

The analytic standards established by the Director of National Intelligence are the core principles of the analytic craft and are employed by CI and HUMINT analysts. These standards are established to guide intelligence analysis writing, provide the basis for evaluating analytic production, and assist in training that is included in analysis teaching modules and case studies throughout the intelligence community. (See ICD 203 for more information.) The intelligence community analytic standards consist of the following:

- Objectivity. This standard requires that analysts and managers perform their analytic and informational functions from an unbiased perspective. Analysis should be free of emotional content, provide due regard to alternative perspectives and contrary reporting, and acknowledge developments that necessitate adjustments to analytic judgments.
- Independent of political considerations. Analysts and managers should provide objective assessments that are informed by available information and are not distorted or altered with the intent of supporting or advocating a particular policy, political viewpoint, or audience.
- Timeliness. Analytic products that arrive too late to support the work of consumers have a weakened utility and impact. Analysts will strive to deliver their products in time for the products to be actionable by customers. Analytic elements have a responsibility to be aware of the schedules and requirements of consumers.

- Based on all-source intelligence. Good analysis is informed by all relevant information available to the analytic element. These elements work with collectors to develop appropriate collection, dissemination, and access strategies to fill critical gaps.
- Exhibits proper analytic tradecraft standards. This encompasses multiple aspects of the craft and includes the following:
  - Describes quality and reliability of underlying source's, data, and methodologies.
  - Expresses and explains uncertainties associated with analytic judgments.
  - Differentiates between underlying intelligence and analyst's assumptions and judgments.
  - Incorporates alternative analysis where appropriate.
  - Demonstrates customer relevance, with implications addressed.
  - Uses logical argumentation.
  - Explains change to or consistency of analytic judgments.
  - Makes accurate judgments and assessments.
  - Incorporates effective visual information where appropriate.

Analytical Products Commonly Created in Support of Counterintelligence and Human Intelligence Activities and Operations

Analytic products must be created for the perpetuation of CI and HUMINT activities and operations. These products include:

- Collection Support Brief. A near-comprehensive background brief that provides detail on a collection issue to guide and enhance collection efforts.
- Counterintelligence Analysis Report. An analytical product that allows analysis Marines and CI Marines to work together to author findings from CI activities (below the threshold of an IIR).
- Counterintelligence Source Evaluation/Counterintelligence Review. An evaluation of a source to determine if the information provided is valuable and credible and to ascertain the reliability and veracity of the source. This review can also determine whether the source is under foreign influence or control.
- Collection Emphasis. A standing collection requirements message that identifies areas of emphasis and information gaps to the CI and HUMINT collector.
- Source-Directed Requirement. A requirement established and communicated to a source handler by an analyst, based on the analysts' knowledge of a source's access and placement to the necessary information and the sources' ability to fulfill the requirement.
- Investigative Support Products. Analytical products that evaluate the information collected during an investigative action. Investigative analytical products can help determine whether an investigation is necessary, identify trends, develop leads, determine methods of operation, assess damage, determine information credibility, and to identify subject or target information.

- Production Review. An evaluation of the information provided by the source to determine the value of the source and arrive at a determination for recruitment. All intelligence reporting is evaluated to determine future potential of source, access and placement.
- Intelligence Information Report Evaluation. Analysts evaluate the value of reporting and provide the collector or handler feedback on the quality of the report through the creation of an evaluation with an alpha numeric code. Evaluations must be generated when an analyst uses source reporting in an analytical product. Evaluations assist in focusing the CI and HUMINT operation.

CHAPTER 6.
HUMAN INTELLIGENCE

MAGTF commanders rely on timely, relevant, and accurate combat information and intelligence to plan, prepare, execute, and continually assess operations. Human intelligence is a critical capability commanders have, either organic to their units or through a supporting command attachment, which can provide input to the all-source intelligence picture. Human intelligence is offensively oriented. The MAGTF CI/HUMINT Marines conduct collection operations to provide the supported commander the ability to allocate, posture, and maneuver forces to conduct operations.

Human intelligence authorities are derived from HUMINT executors as defined by national policy and US law. The DIRINT for the Marine Corps is the executor for those forces retained by the service as defined by the Global Forces Management Implementation Guidance (GFMIG). Human intelligence elements attached to CCMDs can conduct HUMINT under properly solicited service HUMINT authorities in support of service requirements or execute properly solicited HUMINT authorities under CCMD HUMINT authorities. To execute HUMINT authorities, personnel must be appropriately trained and certified through one of the DoD recognized training courses, must be assigned to a HUMINT billet and be assigned to a unit with a HUMINT mission. Additionally, the conduct of HUMINT must be authorized by the DHE or delegated approval authorities. There are generally two methods to gain the authorities and permissions necessary for the conduct of HUMINT: the submission of a classified appendix 5 to the OPLAN or OPORD or the executor can require a classified operational proposal describing the proposed HUMINT operation (MCO 3850.1J, *Policy and Guidance for Counterintelligence (CI) and Human Source Intelligence [HUMINT Activities]*).

Within HUMINT there are various methods for collecting information in support of the commander's ICRs. All Marines with the MOS 0202 (NMOS 0204), 0212, and 0211, are trained in the conduct of HUMINT, although some HUMINT activities require additional training as described in Defense Human Intelligence Enterprise manual (DHE-M) 3301.001, *Defense Human Intelligence (HUMINT) Enterprise Manual, Volume I: Collection Requirements, Reporting, and Evaluation Procedures*.

Human intelligence activities are designed to obtain intelligence information using human sources and collectors as the primary collection instrument. Marine CI/HUMINT personnel have a working knowledge of the organization, operations, and techniques employed by FIE and terrorist organizations. They conduct HUMINT operations to collect information of intelligence value for the commander, and to answer intelligence community requirements. Marine CI/HUMINT personnel often undergo formal language training. Qualified Marine CI/HUMINT personnel use foreign language skills or interpreters to conduct CI and HUMINT activities involving foreign nationals and exploit foreign language documents and media.

HUMAN INTELLIGENCE ACTIVITIES

Human intelligence includes the following activities (Army Techniques Publication [ATP] 2-22.31, *Human Intelligence Military Source Operations Techniques*):

- Liaison. Liaison is conducted to obtain information and assistance, to coordinate or procure material, and develop views necessary to understand counterparts. Liaison contacts are usually members of the government, military, law enforcement, or the local or coalition infrastructure. The basic tenet of liaison is quid pro quo. An exchange of information, services, material, or other assistance is usually a part of the transaction. The nature of this exchange varies widely depending upon the culture, location, and personalities involved.
- Screening. Screening is the overt process of identifying and assessing individuals to identify those who might have information of intelligence value. Screening is not in itself an intelligence collection technique but a timesaving measure. Screening operations are conducted to identify the level of knowledge, level of cooperation, and the placement and access of a given source. Screening operations can help determine which discipline or agency can best conduct the exploitation. Screening operations include the following:
  - Tactical Screening (detainees and persons of interest during operations).
  - Checkpoint Screening (refugees and displaced persons).
  - Local population screening (cordon and search operations).
  - Detention facility screening (EPW's and detainees).
- Elicitation. In intelligence usage, elicitation is "the acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation" (*DoD Dictionary*). Elicitation is a technique used in HUMINT collection when collection is not overt.
- Debriefing. A structured activity conducted to collect intelligence information or to verify previously collected information in response to tactical, operational, or strategic collection requirements. Debriefings can be conducted using Service members, host-country nationals, third-country nationals, cooperative detainees, or EPWs as the source of information (DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*).
- Clandestine MSOs. Clandestine MSOs involve the use of a person in the employ or under the control of an intelligence activity and responding to intelligence tasking. In operational and strategic operational environments, clandestine MSOs can take months or years to fully develop and recruit, based on the political sensitively involved with this type of activity. However, during a contingency or combat operation, there is generally less political risk associated with this type of activity because the United States and multinational partners control the operational environment and there is usually a lack of a functioning government. Tactical clandestine MSOs can typically be developed in a few days to a few weeks depending upon the security conditions of the operational environment, operational pace of the collector, supported unit, and the commander's critical information requirements (CCIRs) (DoDD S-5200.37, *Management and Execution of Defense Human Intelligence (HUMINT) (U)*).

- Foreign military intelligence collection activities. Entails the overt debriefing by trained and certified HUMINT personnel of all US persons employed by the DoD who have access to information of potential national security value (S-5205.01, *DoD Foreign Military Intelligence Collection Activities [FORMICA]*).
- Tactical questioning. The field-expedient initial questioning of a captured or detained person at or near the point of capture and before the individual is placed in a detention facility, seeking information of immediate tactical value. Tactical questioning is generally conducted by members of patrols but can be done by any appropriately trained DoD personnel. Tactical questioning is limited to direct questioning (DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*).
- HUMINT collection management. The process of converting information requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and re-tasking as required. Service-level HUMINT collection management is conducted in the M-2X HOC. All other subordinate HUMINT collection management takes place in the CI/HUMINT staff element HOC (MCTP 2-10A, *MAGTF Intelligence Collection*; and DoDD S-5200.37).
- HUMINT source management and deconfliction. The process of registering and monitoring the use of sources involved in CI and HUMINT activities to protect the security of those operations and avoid conflicts among operational elements. The M-2X, serves as the Service-level source management and deconfliction agency within the Marine Corps. All sources used in conducting Marine Corps-sponsored CI/HUMINT activities are registered, via the M-2X, in the USMC Service-designated DoD source registry.

MILITARY SOURCE OPERATIONS

Military source operations are “the collection from, by, and/or via humans, of foreign and military and military-related intelligence” (*DoD Dictionary*). These activities include human-source contact operations, debriefing, and liaison. Military source operations are conducted under the authorities of a defense human intelligence executor (DHE) to answer Service and DoD requirements in compliance with Service, DoD, and national-level policy. Within the Marine Corps, MSO are conducted by trained and certified personnel assigned to a unit with a HUMINT collection mission. These personnel employ the range of HUMINT collection activities, including one-time, continuous, and recruited sources, and interrogations, debriefings, and liaison activities. A source is a “person, thing, or activity from which information is obtained; in clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes” (*DoD Dictionary*).

Military source operations have specific operational requirements, legal restrictions, and operational guidelines. Human intelligence collection activities require specific approval, coordination, and review in accordance with DoDD S-5200.37. All CI/HUMINT Marines are certified via the MAGTF CI/HUMINT Course to conduct MSO. Military source operations endeavor to fulfill HUMINT ICRs through the conduct of overt or clandestine operations. Only personnel trained in MSO can conduct these types of activities.

Human Intelligence Information Collection Requirements

Human intelligence is responsive to the commander's information requirements. Human intelligence is the least responsive of intelligence collection disciplines, due to the length of time it takes to identify and develop sources with access to the required information. Additionally, HUMINT can collect information that other intelligence disciplines might not be able to collect, such as intentions, social and personal aspects of the adversary or enemy, motives, and adversary or enemy ICRs. Information collection requirements are derived from the intelligence process and assigned through the collections management process. Well-developed and assigned ICRs drive focused HUMINT collection. CCIRs and PIRs, result in the tasking of MAGTF CI/HUMINT personnel to collect information through HUMINT activities, fulfilling the commander's requirements and reducing uncertainty, thereby supporting the commander's decision-making process (MCTP 2-10, *Intelligence Collections*, and DHE-M 3301.001).

Intelligence Interrogations

Intelligence interrogation is categorized as the HUMINT sub-discipline responsible for exploitation of enemy personnel and their documents to answer ICRs. Field Manual (FM) 2-22.3, *Human Intelligence Collection Operations*, which is cited in Title XIV of Public Law 109-163, "National Defense Authorization Act for Fiscal Year 2006" (also referred to in the Detainee Treatment Act of 2005) and Executive Order 13491, E*nsuring Lawful Interrogations*, is the doctrinal lawful basis for executing intelligence interrogations (FM 2-22.3).

Intelligence interrogation is a systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law (*DoD Dictionary*). Subjects of an intelligence interrogation are considered sources when that subject provides information, either with or without the knowledge that the information is used for intelligence purposes.

Compliance with the laws and regulations governing intelligence interrogations, including proper treatment of detainees, is a matter of both personal and command responsibility in accordance with DoDD 3115.09. Commanders have an affirmative duty to ensure their subordinates are not mistreating detainees or their property. The CHD leadership must supervise their subordinate collectors appropriately during interrogation operations. Supervisors must ensure that each HUMINT collector has properly completed an interrogation plan, has developed a sound collection strategy, and fully understands the information requirements prior to beginning an intelligence interrogation. Interrogations can fulfill CI collection requirements and HUMINT collection requirements.

In accordance with the Detainee Treatment Act of 2005, the only interrogation approaches and techniques that are authorized for use against any detainee, regardless of status or characterization, are those authorized and listed in FM 2-22.3. Some of the approaches and techniques authorized also require additional specified approval before implementation.

Interrogation activities are specific actions typically conducted at detention facilities and directed at the wide-scale collection of information from detainees. Field interrogations are conducted at all echelons and during operations in which there are detainees. Detention facilities where interrogation occurs are typically located only at theater or JTF level.

Military police are responsible for the humane treatment, evacuation, custody, and control (reception, processing, administration, internment, and safety) of detainees; force protection; and the operation of the internment facility, under the supervision of the provost marshal (DoDD 2310.1E, *The Department of Defense Detainee Program*). Military police do not conduct intelligence interrogations. Intelligence interrogation is strictly a HUMINT function conducted under the legal authorities of the HUMINT executor. Intelligence interrogations can only be conducted through the properly solicited permissions, under the authorities of the executor, by trained and certified intelligence interrogation personnel in a HUMINT billet within a unit that has an intelligence collection mission.

The principles and techniques of HUMINT collection are to be used within the constraints established by US law including the following:

- Title 10 and Title 50 United States Code (USC).
- The Uniform Code of Military Justice (UCMJ).
- Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (including Common Article III), August 12, 1949; hereinafter referred to as GWS.
- Geneva Convention Relative to the Treatment of Prisoners of War (including Common Article III), August 12, 1949; hereinafter referred to as GPW.
- Geneva Convention Relative to the Protection of Civilian Persons in Time of War (including Common Article III), August 12, 1949; hereinafter referred to as the Geneva Convention.
- Detainee Treatment Act of 2005, Public Law No. 109-163, Title XIV.

Human intelligence collectors must understand specific terms used to identify categories of personnel when referring to the principles and techniques of interrogation. Determining a detainee's status can take a significant time and might not be completed until well after the time of capture. Therefore, there is no difference in the treatment of a detainee of any status from the moment of capture until such a determination is made. The following are some detainee categories:

- Civilian Internee. A person entitled to "protected person" status under the Geneva Convention is detained or interned in the US or in occupied territory for: security reasons, protection, or because they have committed an offense against the detaining power.
- Enemy Prisoner of War. A detained person, as defined in Articles 4 and 5 of the GPW. An EPW is one who, while engaged in combat under orders of their government is captured by the armed forces of the enemy. As such, he or she is entitled to the combatant's privilege of immunity from the municipal law of the capturing state for warlike acts that do not amount to breaches of the law of armed conflict. For example, an EPW could be any person belonging to one of the following categories of personnel who have fallen into the power of the enemy; a member of the armed forces, organized militia or volunteer corps; a person who accompanies the armed forces, without actually being a member thereof; a member of a merchant marine or civilian aircraft crew not qualifying for more favorable treatment; or individuals who, on the approach of the enemy, spontaneously take up arms to resist invading forces.

- Other Detainees. Persons in the custody of the US Armed Forces who have not been classified as an EPW (Article 4, GPW), retained personnel (Article 33, GPW), or civilian internee (Articles 27, 41, 48, and 78 of the Geneva Convention) shall be treated as EPWs until a legal status is ascertained by competent authority (e.g., by Article 5 Tribunal).
- Retained Personnel. Retained personnel are discussed in Articles 24 and 26 of the GWS and include the following:
    - Official medical personnel of the armed forces exclusively engaged in the searching for, or the collecting, transporting, or treating of wounded or sick, or preventing of disease and staff exclusively engaged in the administration of medical units and facilities.
    - Chaplains attached to the armed forces.
    - Staff of National Red Cross and that of other volunteer aid societies, duly recognized and authorized by their governments to assist medical service personnel of their own armed forces, provided they are exclusively engaged in searching for, or collecting, transporting, treating wounded or sick personnel, or preventing disease, provided that the staff of such societies are subject to military laws and regulations.
    - Protected Persons. Civilians entitled to protection under the Geneva Convention, including those retained in the course of a conflict, no matter what the reason.
    - Enemy Combatant. In general, a person engaged in hostilities against the United States or its coalition partners during an armed conflict. The term “enemy combatant” includes both “lawful enemy combatants” and “unlawful enemy combatants.” All captured or detained personnel, regardless of status, shall be treated humanely and in accordance with the Detainee Treatment Act of 2005 and DoDD 2310.1E, *DoD Detainee Program*. No person in the custody or under the control of DoD, regardless of nationality or physical location, shall be subject to torture or cruel, inhuman, or degrading treatment or punishment, in accordance with and as defined in US law.
    - Lawful Enemy Combatant. Entitled to protections under the Geneva Convention, include members of the regular armed forces of a State Party to the conflict; militia, volunteer corps, and organized resistance movements belonging to a State Party to the conflict, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the laws of war; and members of regular armed forces who profess allegiance to a government or an authority not recognized by the detaining power.
    - Unlawful Enemy Combatant. Persons not entitled to combatant immunity, who engage in acts against the United States or its coalition partners in violation of the laws and customs of war during an armed conflict.

Screening (Enabling Interrogations)

Screening detainees might be the first step in an interrogation. Screening, for the purposes of enabling interrogations, is the act of communicating with detainees to determine which have information of intelligence or other value and could be the focus of follow-on interrogations. Screening, which can take place at the detention facility, can be used to determine which detainees to retain and which to release or to prioritize the order of interrogations and to establish positive identification of detained personnel and the circumstances of their capture. Indicators and discriminators used in screening can range from general appearance, possessions, and attitude to specific questions to assess areas of knowledge and degree of cooperation to establish if an individual matches a predetermined target profile. Screening is not in itself an intelligence collection technique but a timesaving measure. In the absence of trained HUMINT personnel, screening of detainees for practical purposes, such as further detention or future interrogation, can be conducted by non-HUMINT personnel. In this instance, the questions should be limited to direct questioning to determine which detainee(s) might be of intelligence interest.

Per United States law and CCMD policy, the capturing force must transfer the detainees from the tactical capturing unit to a DoD detention facility at the soonest opportunity. The capturing force will typically have 72 hours to arrange the detainee's transfer to a higher echelon of detention or facilitate their release. This process adheres to CCMD policy and is only subject to waiver under exigent circumstances. The requirement to transfer detainees to the detention facility gives the intelligence interrogator a nominal amount of time in which to conduct an interrogation of a detainee. In most cases, the CI/HUMINT Marine will likely only have a short amount of time to facilitate an intelligence interrogation once the detainee is in custody of US forces. It is important for the CI/HUMINT Marine to be well prepared to conduct interrogations when detainees are anticipated.

OPERATIONAL PROFILE

Relaxed Uniform Standards

In some operating environments, commanders can implement specific relaxed uniform standards for the safety and welfare of collectors and their sources. This could include allowing collectors to remove body armor and helmets during the task of engaging the civilian populace in order to seem more approachable and facilitate meaningful interaction for the purposes of HUMINT collection.

Sanitized Uniforms.

It might be necessary for the commander to authorize the sanitization of CI/HUMINT personnel uniforms. This can apply both within and outside a US controlled installation. When CI/HUMINT personnel frequently interact with detainees, host-nation employees, and third-country nationals, the security situation could require that uniforms are worn without name tapes or rank. Removing rank from the uniform could enable the CI/HUMINT Marine to interact with foreign personnel who are of a higher rank or status. Removing name tapes mitigates the chances foreign personnel will make judgments about ethnicity, race, or religion, which are detrimental to the desired relationship. Additionally, the absence of a name tape acts as a force protection measure for those CI/HUMINT personnel who might be targeted for retribution. This is particularly important in interrogation operations.

Civilian Clothing

The commander can authorize civilian clothing be worn in some operating environments. Wearing civilian clothing is typically considered an OPSEC practice which lowers the profile of the CI/HUMINT Marine, avoiding compromise of the intelligence collection mission, and deters adversary or enemy targeting. Wearing civilian clothes can significantly contribute to the security of the HUMINT activity.

Relaxed Grooming Standards

Relaxed grooming standards, like civilian clothing, provide OPSEC measures for collectors in the operating environment, as well as helps overcome cultural barriers by helping build rapport and establish trust and credibility with civilians. In some cultures, facial hair on men is a sign of manhood, wisdom, or a higher social status. Relaxed grooming standards also contribute to the security of the intelligence collection mission by improving the force protection profile of the collector. The less a collector looks like a US military member, the more secure the mission is, and the safer the collector will be during the conduct of their work. Relaxed grooming standards and civilian clothing are often authorized together since both are required to present a specific profile for the collector. An endorsed written statement identifying the name of the individual and the authorized duration applicable to relaxed grooming standards must be kept on file by the authorizing organizations representative.

Non-Tactical Vehicles

Non-tactical vehicles could be required to conduct HUMINT operations in some operating environments. Using non-tactical vehicles, which blend better than military vehicles within the local populace can reduce the collectors’ profiles and improve operation security. The combination of non-tactical vehicles, civilian clothing, and relaxed grooming standards, might be necessary to provide collectors access to sources who cannot be seen associating with US persons.

Freedom of Movement

Commanders can establish a minimum requirement on the number of personnel or vehicles allowed to leave an operating base. This could indirectly restrict collectors’ ability to conduct sensitive activities outside the operating base that support their commander. Freedom of movement must be allowed, within reason, for collectors to conduct CI/HUMINT activities. Depending on the threat level and the risks associated with the mission. Commanders might consider allowing collectors to operate in fewer numbers to perform the mission, dependent upon the risk versus gain.

Forward Deployment of Personnel

Ideally, CI/HUMINT personnel are deployed as part of the advanced element or ahead of the main force. As an advanced element, the CI/HUMINT personnel can begin identifying potential sources that can answer the commander’s information requirements. Additionally, CI/HUMINT personnel can collect information relevant to force protection to inform the commander prior to the force landing or arriving.

Language Support

Counterintelligence/HUMINT operations frequently require language support. This need cannot always be met from within the inventory of military linguists. Because of the sensitivity of the information they are often exposed to Marines conducting CI/HUMINT activities require interpreters who have a secret clearance. It is imperative that linguists and interpreters not only understand their roles in missions but also are fully integrated into CI and HUMINT activities when possible. Requirements for linguist support must be addressed in planning as early as possible as it can be challenging to find appropriately qualified personnel to support CI and HUMINT activities.

CHAPTER 7. REPORTING, PRODUCTION, AND DISSEMINATION

Reporting and dissemination are among the most important aspects of CI and HUMINT activities and missions; these are the mechanisms by which information is provided to the commander and others who use it. With the battlespace being a dynamic environment, timely and accurate dissemination of information of intelligence value is of utmost importance to commanders at all levels. Administration of CI and HUMINT, covered in Chapter 8, is the supporting architecture that acquires, coordinates, and manages resources used in the collection process that ultimately facilitates CI and HUMINT reporting and dissemination.

REPORTING

There are two categories of reporting produced by CI/HUMINT personnel: operational reports, and informational reports. Operational reports record operational details of CI and HUMINT activities, such as source meetings, interrogations, and interviews. Operational reports do not include information answering intelligence collection requirements, but rather information that describes the mechanics behind collecting such information. Operational reports are used solely within CI and HUMINT management channels to guide the planning and execution of further CI and HUMINT activities. Operational reports usually contain sensitive information regarding details of CI and HUMINT activities, sources, and methods, and must be distributed on a strict need-to-know basis.

Informational reports, on the other hand, record information of intelligence value that answers intelligence collection requirements; they contain unevaluated information, not finished intelligence. Informational reports are generally intended for the widest dissemination within the intelligence analytic community. Counterintelligence and HUMINT reports are intended to provide a means of disseminating raw information of intelligence value obtained directly from a source into the intelligence cycle for evaluation, analysis, and fusion with other intelligence information. Unless specifically designated, informational, or operational reports can contain information of both counterintelligence and foreign intelligence value.

The two types of intelligence informational reports include the—

- IIR. A DoD-mandated format used to report information that answers CI and HUMINT collection requirements. When populated with information, this report is classified as directed in the National Human Intelligence Management Directive 002.08, *HUMINT Derived Intelligence Report Format Standard*. The IIR is disseminated throughout the intelligence community and among all the Services. The DIA maintains a DoD HUMINT database of record for all HUMINT requirements and information reports. An IIR is raw information that has been collected and reported without prior analytical scrutiny. Intelligence is the product of multiple correlated pieces of information which support a conclusion.

- Situation, Position, Observation, Time Report (SPOTREP). Issued when time-sensitive information is collected. These reports are generated and disseminated to the applicable commanders as rapidly as possible and followed up with IIRs as appropriate.

The eight basic types of CI and HUMINT reports include the—

- Screening Report. Used to document persons of interest encountered during screening operations. The screening report provides a reference to persons of interest who might be contacted later for interview, debriefing, or interrogation. The screening report is also used at intermediate collection points, checkpoints, and detention centers to document the initial screening of EPWs and detainees prior to interrogation.
- Tactical Interrogation Report. Provides a record of interrogations conducted by CI/HUMINT personnel. It is an operational report, not an IIR. Tactical interrogation reports are used during both field interrogations and in detention facilities. They provide detailed biographical information on the source (e.g., EPW or detainee) and document interrogation methods used to gain information from the source, which is necessary to support subsequent interrogations and could assist legal personnel in determining EPW or detainee status.
- Contact Report. Records the details of meetings with cooperative HUMINT sources rather than those in the custody of US forces (e.g., EPWs or detainees). The contact report is one of the most important documents created in the conduct of MSO and MCC activities because it records the information necessary for CI/HUMINT Marines to interact with a particular source and is also used for planning and executing future activities.
- Liaison Contact Report. Records the proceedings of meetings with official liaison contacts.
- Lead Development Report. Reports the discovery of and contact with personnel who have the potential to be utilized in CI and HUMINT activities.
- POW/MIA/Missing (Non-hostile) Report. Used to initiate a prisoner of war (POW), missing in action (MIA), or missing (non-hostile) investigation. The report contains detailed information on the subject, to include (if available) photographs, handwriting samples, and other personal data which could assist in recovering and confirming an individual's identity.
- CI Incident Assessment Report. Documents and reports the findings of CIIA. The specific format used can be modified to suit the particular activity being reported. Information obtained during CIIA that answers intelligence collection requirements is reported via an IIR or SPOTREP, provided releasing such information would not compromise any investigative activity.
- CI Inspection/Evaluation Report. Documents the findings of CI surveys, inspections (e.g., vacated command post inspections) and evaluations. While these reports are generally not widely disseminated, they are documented for future reference by the unit that conducted the activity or by others with a need-to-know status.

Appendix H contains examples of unclassified informational and operational report formats. Examples of classified report formats are located in the DIA's intelligence enterprise manuals volumes I and II.

PRODUCTS

While information reports constitute a large part of CI and HUMINT production, information contained in reports, combined with other CI and HUMINT activities, is frequently used to create finished intelligence products for the MAGTF. Analytical tools that can enhance CI and HUMINT production are discussed in Chapter 5. In addition to formal production and analysis, CI/HUMINT Marines can also use these tools to aid in operational planning and analysis. There are many products that can be created by CI/HUMINT personnel. Products are often determined by the mission and the requirements. The following paragraphs describe some CI and HUMINT products.

Counterintelligence Vulnerability Assessment

The CIVA is produced at the conclusion of a counterintelligence survey conducted by CI/HUMINT personnel primarily in support of force protection requirements. It is a finished tactical intelligence product that provides an in-depth assessment of espionage, sabotage, subversive, and terrorist threats (and friendly vulnerabilities) associated with a physical installation such as ports, airfields, or base camps. Counterintelligence vulnerability assessments typically include multimedia (e.g., photographs, video, drawings) in addition to text. The CIVA is an extremely useful tool to the commander in identifying force protection issues and justifying resources necessary to improve the force protection posture of the command and protect it from internal and external threats. As formats for CIVAs vary based on the mission, templates for the CIVA should be solicited from the supported higher unit.

Document and Media Exploitation

In a tactical environment, CI/HUMINT personnel are capable of providing limited DOMEX support. This capability is limited by the availability of qualified CI/HUMINT linguists or quality interpreters assigned to CHDs. Typically, any documents, other written or printed material, and electronic media obtained during CI/HUMINT activities can be translated by linguists or interpreters. A copy of the field translation is provided with the original DOMEX item, along with the circumstances of how it was obtained (i.e., a capture tag). Given personnel and resource limitations, Marine Corps CI and HUMINT involvement in DOMEX is generally limited to the triage of items recovered during site exploitation or items found on or near captured enemy personnel. Neither CI/HUMINT companies nor CHDs have the personnel or language resources to systematically translate large quantities of high-density documents. Documents are submitted via the evacuation process to the tactical, theater, or national document exploitation facility for further exploitation. DOMEX related intelligence reporting is expected as an output of the activity.

Nonstandard Production

Nonstandard production refers to various products CI/HUMINT personnel prepare on an irregular basis when tasked, such as link analysis charts and association matrices.

DISSEMINATION

The dissemination of CI and HUMINT reports and products is accomplished in accordance with the doctrinal concept of MAGTF intelligence operations (MCWP 2-10). Counterintelligence and HUMINT elements assigned in general support roles report directly to the G-2X. The G-2X manages dissemination of the CI and HUMINT reports and products to the MAGTF IOC for processing, exploitation, and further dissemination throughout the MAGTF area of operations. Depending on the mission, the G-2X/S-2X might interact with the JTF J-2X, M-2X, or other governmental agencies within the intelligence community to determine requirement satisfaction, deconflict sources, request evaluation of reporting, and coordinate the release of reporting to DoD-level intelligence consumers.

Counterintelligence and HUMINT assets assigned in direct support roles provide information copies of reporting directly to the supported command G-2/S-2 when the reporting answers the supported CCIRs. Information reporting must still be passed to HHQ for formal processing, dissemination, and archiving within the intelligence community. Operational reporting must be maintained within.

CHAPTER 8. REQUIREMENTS, ADMINISTRATION, AND COORDINATION

Counterintelligence/HUMINT requirements management, funds administration, and diplomatic coordination activities are essential for effective employment of CI/HUMINT assets. These activities serve as enablers outside the MAGTF and provide collection management, source management, and intelligence funding resources that support CI/HUMINT reporting, production, and dissemination.

NATIONAL- AND SERVICE-LEVEL COLLECTION REQUIREMENTS

National level collection requirements are generated by those national-level agencies such as the NGA, the NSA, CIA, DIA, and other agencies directed as a lead national intelligence community role. A CI/HUMINT Marine can obtain access to the desired information through tactical CI and HUMINT activities or missions. If this occurs, a CI/HUMINT Marine can fulfill the intelligence collection requirement to the best extent possible as is incidental to the mission. The fulfillment of national-level collection requirements should not detract from the assigned CI/HUMINT mission. If a CI/HUMINT Marine working under the USMC DHE identifies a source who demonstrates placement and access to national-level intelligence collection requirements, the Marine's higher headquarters, will notify the M-2X. The M-2X, in coordination with the Marine's higher headquarters, will enact procedures to expedite the acquisition and reporting of future intelligence information.

The MCIA all-source collection requirements section, via the MCIA CI/HUMINT collection requirements manager is the Service-level intelligence organization responsible for coordinating ICRs with other MCISRE elements, defense executors, and national-level intelligence community organizations and agencies. The M-2X OSE, in coordination with the ICR manager, will ensure Marine Corps interests are included in national-level CI and HUMINT collection requirements. The following paragraphs describe collection requirements.

National Human Intelligence Collection Directives

National HUMINT collection directives reflect the needs of the intelligence community and are translated into national HUMINT requirements. The MCIA CI/HUMINT ICR manager and the M-2X OSE are solicited for input into these directives to ensure Marine Corps needs are addressed across the intelligence community. As the Service intelligence center and an intelligence community partner, MCIA is responsible for responding to intelligence community requests for support in answering requirements.

Human Intelligence Collection Requirements

Validated and published by DIA, HCRs are DoD-level collection requirements. Marine Corps CI and HUMINT assets, particularly those deployed with Marine expeditionary units, frequently respond to HCRs through the IIR reporting process. The MCIA CI/HUMINT manager is responsible for developing and maintaining HCR lists on issues specifically of interest to Marine Corps equities and provides them to deploying or deployed Marine Corps CI and HUMINT collectors as a Service-level collection management function.

Ad-Hoc Collection Requirements

Ad-hoc collection requirements are customer generated, short-term collection requirements for unforeseen situations or transitory events, emerging crises, or contingencies validated and published by DIA. Ad-hoc collection requirements can focus or complement HCRs for a limited period of time, not to exceed 120 days. The MCIA CI/HUMINT ICR manager is responsible for maintaining current ad-hoc collection requirements lists on issues of interest to Marine Corps equities and provides them to deploying or deployed Marine Corps CI/HUMINT elements.

Time-Sensitive Collection Requirements

Time-sensitive collection requirements are short-term crisis support requirements where action or inaction could result in harm or death to US or allied military personnel or citizens. A time-sensitive collection requirement is only valid for a period not to exceed 60 days and cannot be extended.

Source Directed Requirements

Source directed requirements are specific collection requirements that focus on satisfying existing HCRs or follow-on requirements associated with a recent IIR or other intelligence reports if continued contact is possible with the source. Source directed requirements are only valid for one year. The responsible counterintelligence and human intelligence staff element validates and coordinates source directed requirements with the customer.

Notice of Intelligence Potential and Knowledgeability Briefs

Notice of intelligence potential and knowledgeability briefs are prepared by the collector to notify the intelligence community of potential collection opportunities. Marine Corps CI/HUMINT assets frequently prepare and submit these briefs prior to deployments or after arrival in a target location. The responsible counterintelligence and human intelligence staff element coordinates source directed requirements that have been generated in response to notice of intelligence potential.

ADMINISTRATION

Counterintelligence/HUMINT administration is the supporting architecture that acquires, coordinates, and manages resources used in the collection process.

Operations Proposals

Certain types of CI/HUMINT activities require coordination and approval outside a MAGTF prior to execution. The CI/HUMINT organization responsible for execution will prepare and submit the proposal according to processes identified in USMC M-2X Operations Coordination

Standards No.1. Subsequent coordination is initiated by the MAGTF G-2X with the appropriate organizations and agencies as identified in USMC M-2X Operations Coordination Standards No.1. Military source operations and MCC activities must be coordinated and deconflicted prior to execution, and, depending on the specific activities involved, will also require approval at the JTF, CCMD, or Service level. Facilitation, coordination, and approval for MSO and MCC activities are the responsibility of the MAGTF G-2X.

Source Management

Source management is conducted at all levels within DoD by organizations responsible for conducting CI/HUMINT activities. Department of Defense policies, requirements, and procedures apply to specific categories of CI/HUMINT activities and sources. The M-2X Service source manager establishes procedures and provides guidance of Service-level source management practices employed by USMC Service-retained source managers. In a MEF-level deployment, the G-2X will oversee established CI and HUMINT source management procedures. For deployments involving CI and HUMINT assets in support of maneuver units smaller than a MEF, the MAGTF G-2X or senior CI/HUMINT officer is responsible for direction and oversight of source management in coordination with any applicable JTF or CCMD policies or directives. The M-2X is designated as the Service-level source manager for the Marine Corps.

Funds Management

Funds are programmed within the Marine Corps to support CI/HUMINT activities not provided for by other appropriations.

Defense Intelligence and Counterintelligence Expense. Intelligence and counterintelligence personnel employ defense intelligence and counterintelligence expense (DICE) authority for intelligence and counterintelligence purposes that are of a confidential, extraordinary, or emergency nature. DICE authority is appropriate if normal procedures would compromise the security of the operation, delay timely accomplishment of the operation or activity, or jeopardize the safety of personnel engaged in the operation. The M-2X is the designated program manager for the Marine Corps and serves as the central point of contact for all DICE matters within the service. DICE authority is requested via Marine Corps Service components and other designated commands via the M2-X and provided via the requesting commands' funds custodian.

COORDINATION WITH DIPLOMATIC MISSIONS

To facilitate coordination with US diplomatic missions overseas, Marine Corps components routinely conduct liaison and deconflict activities via the defense attaché accredited to the country in which activities are intended to take place.

Ambassador

Also referred to as the chief of mission, the ambassador is the senior US representative responsible for bilateral relations with the host nation. Ambassadors can be career diplomats or political appointees. The ambassador is the personal representative of the President of the United States in a given country with full authority for the direction, coordination, and supervision of all USG executive branch employees, except those under a CCMD. In practically every circumstance, the ambassador must approve or concur with DoD activities taking place in the host country and will be required to be kept informed of significant progress and incidents that can occur.

Country Teams

Ambassadors conduct diplomacy and coordinate US interaction with the host nation through the use of a country team. The country team comprises the senior representative of each Department of State section and other organizations and agencies located in country (e.g., US Agency for International Development, Department of Justice, DoD, FBI) These representatives execute their duties in exchanging information with the host nation at the direction of the ambassador and in coordination with each other to avoid a duplication or contradiction of effort.

Other Embassy Personnel

Other key embassy personnel and their duties include the following:

- Chargé d'affaires. A diplomatic official who temporarily takes the place of an ambassador.
- Deputy chief of mission. The ambassador's executive officer. This position is filled by a career diplomat.
- Political officer. Responsible for meeting with host nation government representatives to further US relations.
- Regional security officer. The senior law enforcement and security officer at the post. Responsible for maintaining contact and relations with host nation law enforcement personnel for protection of the US mission and personnel.
- Chief of station. In virtually all cases globally, the CIA chief of station serves as the DNI representative (ICD 402, *Director of National Intelligence Requirements*).
- Legal attaché. Conducts liaison with host nation law enforcement and security services regarding training and investigations involving the Department of Justice. The legal attaché is usually an experienced supervisory special agent with the FBI.
- Defense attaché. The senior DoD representative to the host nation who maintains relations with host nation military representatives. The defense attaché is usually the senior DoD representative on the US embassy staff and is responsible to the ambassador for overall diplomatic cognizance and coordination of DoD activities.
- General services officer. Controls all services at the embassy, to include vehicles, communications, and housing.
- Force protection detachment. Force protection detachments are joint DoD counterintelligence elements that provide antiterrorism, force protection, and counterterrorism indications and warnings to in transit DoD forces at locations overseas.
- Detachment commander. The staff noncommissioned officer commanding the Marine security guard detachment.

Many of these same representatives make up the embassy's emergency action committee, which is responsible for evaluating security and environmental threats to the embassy and US citizens in country as well as developing contingency plans to handle a vast array of manmade and natural emergencies. During any noncombatant evacuation operations or humanitarian missions, the emergency action committee will be involved.

APPENDIX A. COUNTERINTELLIGENCE APPENDIX 3

An OPORD contains 21 annexes, many of which include appendices. Annex B is used for intelligence and provides detailed information about the adversary and battlespace. This annex also provides guidance on intelligence and counterintelligence functions.

Appendix 3 of Annex B contains CI-specific information. It includes three tabs—Tab A: Counterintelligence Target List, Tab B: Multidiscipline Counterintelligence Threat Report, and Tab C: Designation of Threat Counterintelligence Executive Agency. Appendix 3 should explain how counterintelligence elements, either supporting or OPCON to the MAGTF, will be used to support the OPORD. The appendix should also provide guidance to subordinate commanders for conducting counterintelligence operations and supporting counterintelligence elements and personnel identified to fulfill counterintelligence requirements identified in the OPORD.

> ***Note:*** References to controlled unclassified information (CUI) markings are usage examples only.

CLASSIFICATION

Copy no. of copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

APPENDIX 3 TO ANNEX B TO OPERATION ORDER OR PLAN (Number) (U)
COUNTERINTELLIGENCE (CI) (U)

(U) REFERENCES: List documents essential to this tab.

(a) Identify DoD, DIA, CIA, and other directives; combatant commander, JTF, or other higher authorities' operations plans, orders, and tactics, techniques, and procedures or SOP for intelligence and counterintelligence operations.

(b) List pertinent maps and other geospatial information resources and any other relevant references that pertain to anticipated MAGTF counterintelligence operations.

CLASSIFICATION

1. (U) General

a. (U) Objectives. Discuss general objectives and guidance necessary to accomplish the mission.

b. (U) 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. (U) Counterintelligence Liaison Responsibilities. Discuss responsibility to coordinate and conduct liaison between command counterintelligence elements and those of other US and allied commands and agencies.

d. (U) Restrictions. Discuss the effect of US statutes, executive orders, DoD and HHQ directives, and status-of-forces agreements on counterintelligence activities.

2. (U) Adversary Threat. Refer to Annex B and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and order of battle pertinent to counterintelligence operations.

Summarize the foreign intelligence activity and collection threat; foreign security and counterintelligence threat; and threats from sabotage, terrorism, and assassination directed by foreign elements. Emphasize capabilities, limitations, and intentions. Ensure that, at a minimum, the most likely and worst cases are addressed.

3. (U) Mission. State concisely the counterintelligence mission as it relates to the MAGTF's planned operation.

4. (U) Execution

a. (U) Concept of Operations. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations) to Annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall concept of operations as they relate to counterintelligence operations. Outline the purpose and concept of counterintelligence operations, specified priorities, and summarize the means and agencies to be employed in planning, directing, collecting, processing and exploiting, analyzing and producing, disseminating, and using counterintelligence during execution of the OPORD. Address the integration of JTF, other components, theater, national, and allied forces' counterintelligence operations.

Page Number

CLASSIFICATION

CLASSIFICATION

b. (U) Tasks for Counterintelligence and Related Units and Organizations, Subordinate Units, and Task Force Commanders/OICs.

(1) (U) Orders to subordinate, attached, and supporting units. Use separate numbered subparagraphs to list detailed instructions for each unit conducting counterintelligence operations, including the originating headquarters, subordinate commands, and separate intelligence support units.

A(a) (U) Major subordinate commanders.

(b) (U) Commanding officer, intelligence battalion.

(c) (U) OIC, intelligence operations center support cell.

(d) (U) OIC, intelligence operations center surveillance and reconnaissance cell.

(e) (U) OIC, intelligence operations center production and analysis cell.

(f) (U) Commanding officer, CI and HUMINT Company.

(g) (U) OIC, HUMINT support team.

(2) (U) Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached or supporting and from which counterintelligence support is requested, including other components, JTF headquarters, allied or coalition forces, theater and national operational and intelligence elements. Provide strengths, locations, capabilities, and type of support to be provided from external US commands and agencies and allied, coalition, and host nation counterintelligence elements.

c. (U) Coordinating Instructions. Reference Appendix 16 (Intelligence Operations), and the intelligence and counterintelligence SOPs of the command, other pertinent forces, and organizations. Detail here or in supporting tabs key changes to SOPs. Additional topics to include or emphasize here are: requesting counterintelligence support; direct liaison among subordinate commanders, MAGTF counterintelligence units, staff officers, and pertinent external organizations and agencies; routine and time-sensitive counterintelligence reporting procedures and formats, etc.

Page Number

CLASSIFICATION

5. (U) Security. Provide planning guidance concerning procedures and responsibilities for the listed security activities.

a. (U) Command Element and Other Headquarters.

b. (U) Military Security.

c. (U) Civil Authority.

d. (U) Port, Border, and Travel Security.

e. (U) Safeguarding Classified Information and Cryptographic Material Systems Resources. Guidance.

f. (U) Security Discipline and Security Education.

g. (U) Protection of Critical Installations.

h. (U) Special Weapons Security.

i. (U) Counterterrorist Measures.

6. (U) Counterintelligence Plans, Activities, and Functions

a. (U) Defensive. Identify the staff of those commands that have supporting counterintelligence assets and provide planning guidance concerning procedures, priorities, and channels for:

(1) (U) MCC.

(2) (U) Interrogation of EPW and defectors.

(3) (U) Screening of indigenous refugees, displaced persons, and detained suspects.

(4) (U) Debriefing of US or other friendly personnel who evade, escape, or are released from enemy control.

(5) (U) Exploitation of captured documents and materiel.

(6) (U) The conduct of counterintelligence incident assessment and coordination of counterintelligence investigations.

(7) (CUI) Employment of TSCM.

b. (CUI) Offensive. Establish guidance, including control and coordination, for approval of counterespionage, countersabotage, countersubversion, counterterrorist, double agent, deception, and other special operations.

7. (U) Counterintelligence Targets and Requirements

a. (U) Targets. Reference Tab A (Intelligence Collection Plan) to Appendix 16 (Intelligence Operations). Provide guidance for executing and managing counterintelligence collection activities not otherwise covered by regulation or SOP, equipment status, reports, and other specialized forms of collection activity to support the plan. Provide guidance on both routine and time-sensitive reporting of counterintelligence collected intelligence information by all counterintelligence collection sources to be employed in support of the plan. Provide guidance to MAGTF major subordinate commands/elements 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) (U) Personalities.

(2) (U) Organizations and Groups.

(3) (U) Installations.

(4) (U) Documents and Material.

b. (U) Priorities. Identify special counterintelligence collection requirements and priorities to be fulfilled by counterintelligence operations.

c. (U) Miscellaneous. Identify any other command information and intelligence required.

8. (U) Counterintelligence Production. Reference Tab B (Intelligence Production Plan) to Appendix 16 (Intelligence Operations). Identify the counterintelligence production objectives and effort, including any intelligence and counterintelligence products required to support the OPLAN. Include details of management of counterintelligence production requirements along with guidance on counterintelligence production and data bases, forms/formats for products, production schedules, counterintelligence products and reports distribution, etc. Address integration of counterintelligence P&A with all-source intelligence P&A activities. Include as appropriate requirements and guidance for the following: indications and warning, support to targeting, support to combat assessment (to include battle damage assessments), and especially counterintelligence support to force protection.

9. (U) Counterintelligence Dissemination. Reference Tab C (Intelligence Dissemination Plan), Tab D (Intelligence Communications and Information Systems Plan), and Tab E (Intelligence Reports) to Appendix 16 (Intelligence Operations); and Annex K (Combat Information Systems). Stipulate requirements, means, and formats for disseminating counterintelligence reports and products (e.g., units responsible for each, periods covered, distribution, and timeline standards). Establish supporting counterintelligence communications and information systems plan and supporting procedures and criteria to satisfy expanded requirements for vertical and lateral dissemination of routine and time-sensitive counterintelligence products and reports. Address voice, network, courier, briefings, special counterintelligence communications, and other communications methods, including point-to-point and alarm methods. Establish alternate means to ensure that required counterintelligence will be provided to subordinate and supported units. Provide guidance regarding counterintelligence and information security, to include the dissemination of sensitive counterintelligence information within the force and the release ability of counterintelligence information and products to non-US forces.

10. (U) Administration and Logistics. Provide a statement of the administrative and logistic arrangements or requirements for counterintelligence not covered in the base plan or in another annex. Identify unique counterintelligence logistic and personnel requirements, concerns, and deficiencies. Discuss specific operational details on early deployments, mode of transportation, clothing, equipment, operational, or contingency funds.

11. (U) Command and Control

a. (U) Command and Control. Specify command and control and support relationships and supporting information for all MAGTF counterintelligence elements. Include details of conditions that would prompt change of C2 relationships and procedures to implement that change during execution of the plan. Address what information and activities require the commander’s knowledge and approval.

b. (U) Communications Systems. Reference Appendix 16 (Intelligence Operations) and Annex K (Combat Information Systems). Ensure that communications system requirements are addressed in Annex K. Unique communications system requirements for counterintelligence operations should be addressed to include identifying what communication channels should be used for maintenance and administration of counterintelligence databases, etc.

c. (U) Information Management. Provide any instructions necessary regarding information management (time-sensitive and routine reporting criteria, intelligence databases, reports, etc.) that will influence MAGTF counterintelligence operations.

CLASSIFICATION

d. (U) Intelligence and counterintelligence C2 Nodes and Facilities. Reference the unit's intelligence SOP and Appendix 16 (Intelligence Operations). Provide any guidance and instructions necessary regarding the establishment and operations of intelligence and counterintelligence C2 nodes and facilities (e.g., CI and HUMINT company command post; counterintelligence representation within the surveillance and reconnaissance cell and the P&A cell, etc.).

e. (U) Coordination. Identify coordination requirements peculiar to counterintelligence activities listed in the paragraphs above.

f. (U) Reports. Identify counterintelligence reports that will be used and any necessary supporting information.

ACKNOWLEDGE RECEIPT

C—Designation of Theater Counterintelligence Executive Agency

OFFICIAL:

s/ Name
Rank and Service
Title

Page Number

CLASSIFICATION

CLASSIFICATION

Copy no. of copies
ISSUING UNIT PLACE OF ISSUE
Date-time group
Message reference number

TAB A TO APPENDIX 3 TO ANNEX B TO OPERATION ORDER OR PLAN (Number)
COUNTERINTELLIGENCE (CI) TARGET LIST (U)

(U) REFERENCES: List documents essential to this tab.

1. (U) Friendly Infrastructure. Develop a listing of offices and agencies where counterintelligence personnel can obtain counterintelligence information and assistance.

2. (U) Foreign Intelligence Entity Infrastructure. Develop a listing of specific offices and institutions within the FIE structure that can provide information of FIE targeting, operations, etc.

3. (U) Foreign Intelligence Entity Personalities. Develop and update a specific listing of FIE personalities who, if captured, would be of counterintelligence interrogation interest.

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

OFFICIAL:

s/
Name
Rank and Service
Title

Page Number

CLASSIFICATION

CLASSIFICATION

Copy no. of copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/Time Group
Message reference number

TAB B TO APPENDIX 3 TO ANNEX B TO OPERATION ORDER OR PLAN (Number)
MULTIDISCIPLINE COUNTERINTELLIGENCE THREAT REPORT (U)

(U) REFERENCES: List documents essential to this appendix.

(a) Unit SOP for intelligence and CI.

(b) JTF, naval task force, other components, theater, and national intelligence; counterintelligence plans, orders, and tactics, techniques, and procedures (TTP); 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 providing intelligence required for planning.

(e) Others as appropriate.

1. (U) Mission. State concisely the counterintelligence mission as it relates to the MAGTF's planned operation.

2. (U) Characteristics of the Area of Operations. State conditions and other pertinent characteristics of the area that exist and could affect enemy intelligence, sabotage, subversive and terrorist capabilities, and operations. Assess the estimated effects on friendly counterintelligence capabilities, operations, and measures. Reference Appendix 11 (Intelligence Estimate), to annex B (Intelligence), as appropriate.

a. (U) Military Geography

(1) (U) Describe existing situation.

(2) (U) Discuss estimated effects on enemy intelligence, sabotage, subversive, and terrorist operations and capabilities.

(3) (U) Discuss estimated effects on friendly counterintelligence operations, capabilities, and measures.

Page Number

CLASSIFICATION

CLASSIFICATION

b. (U) Weather

(1) (U) Describe existing situation.

(2) (U) Discuss estimated effects on enemy intelligence, sabotage, subversive, and terrorist operations and capabilities.

(3) (U) Discuss estimated effects on friendly counterintelligence operations, capabilities, and measures.

c. (U) Other Characteristics. Additional pertinent characteristics are considered in separate subparagraphs: sociological, political, economic, psychological, and other factors. Other factors might include telecommunications material, transportation, manpower, hydrography, science, and technology. These are analyzed under the same headings used for military, geography and weather.

3 (U) Intelligence, Sabotage, Subversive, and Terrorist Situation. Discuss 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 can be attached to the estimate or annexes or can be consolidated in automated databases that can be accessed by MAGTF units. Ensure those used are identified, and location/access information is provided.

a. (U) Location and Disposition

b. (U) Composition

c. (U) Strength. Include local available strength, availability of replacements, efficiency of enemy intelligence, sabotage, subversive, and terrorist organizations.

d. (U) Recent and Present Significant Intelligence. Describe relevant activities/movements, including enemy knowledge of our intelligence and counterintelligence efforts.

e. (U) Operational, Tactical, Technical Capabilities and Equipment

f. (U) Peculiarities and Weaknesses

g. (U) Other Factors as Appropriate

4. (U) Intelligence, Sabotage, Subversive, and Terrorist Capabilities and Analysis. List separately each indicated enemy intelligence, sabotage, subversive, and terrorist capability that can affect the accomplishment of the assigned MAGTF mission. Each enemy capability should

Page Number

CLASSIFICATION

CLASSIFICATION

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. 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

(1) (U) Intelligence. Include all known/estimated enemy methods.

(2) (U) Sabotage. Include all possible agent/conventional/irregular forces capabilities for military, political, and economic sabotage.

(3) (U) Subversion. Include propaganda, sedition, treason, disaffection, and threatened terrorist activities affecting our troops, allies, and local civilians.

(4) (U) Terrorist. Include capabilities of terrorist personalities and organizations in the area of operations.

b. (U) Analysis and discussion of enemy capabilities for intelligence, sabotage, subversion, and terrorism as a basis to judge the probability of their adoption.

5. (U) 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. List enemy COAs 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. (U) Probability of enemy adoption of intelligence, sabotage, subversive, and terrorist programs or procedures based on enemy's capabilities.

b. (U) Effects of the enemy's capabilities on friendly COA.

c. (U) Effectiveness of our own counterintelligence measures and additional requirements or emphasis needed.

ACKNOWLEDGE RECEIPT

Page Number

CLASSIFICATION

Name
Rank and Service
Title

EXHIBITS

(As appropriate)

OFFICIAL:

s/
Name
Rank and Service
Title

Page Number

CLASSIFICATION

APPENDIX B.
HUMAN INTELLIGENCE APPENDIX 5 FORMAT

CLASSIFICATION

Copy no. of copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

APPENDIX 5 TO ANNEX B TO OPERATION ORDER OR PLAN (Number) HUMAN INTELLIGENCE (HUMINT) (U)

(U) REFERENCES: Identify DoD, DIA, CIA, and other directives; combatant commander, JTF, or other higher authorities' operations plans, orders, and TTP or SOP for intelligence and counterintelligence operations; pertinent maps and other geospatial information resources; and any other relevant references that pertain to anticipated MAGTF counterintelligence operations.

1. (U) General. Provide objectives and guidance for HUMINT collection operations.

2. (U) Mission. Refer to the basic plan.

3. (U) Execution

a. (U) Organization

(1) (U) Describe the structure to coordinate and manage theater HUMINT operations. Normally, this includes the establishment of a J-2X staff element (see JP 2- 0, *Joint Intelligence*) by the joint force J-2 to coordinate and deconflict HUMINT and counterintelligence collection activities. The J-2X can include an HOC to serve as the HUMINT coordination authority (see tab A).

(2) (U) Include augmentation, if required, from DIA or other intelligence organizations.

(3) (U) Describe relationships between joint force and component HUMINT activities.

CLASSIFICATION

4. (U) Non-DoD HUMINT. Describe non-DoD organizations that could contribute to the HUMINT mission. Include allied and coalition HUMINT elements and capabilities as appropriate.

a. (U) Concept of Operations. Describe the concept for deployment and employment of HUMINT resources. If appropriate, include requirements for early insertion of HUMINT resources into the area of operations.

(1) (U) Tasks. As appropriate, identify assigned/attached activities (attached DIA and component HUMINT-related forces) for conducting:

(a) (U) Exploitation of EPW/civilian detainees and debriefing of refugees (see tab B, this appendix).

(b) (U) Controlled HUMINT operations.

(c) (U) HUMINT liaison.

(d) (U) Other anticipated collection operations.

(e) (U) Support to, and mutual activities with, other US intelligence collection activities, such as SIGINT.

(f) (U) Debriefing of Returnees. Intelligence debriefings of recovered US and allied personnel who were captured, missing, or detained must be coordinated and conducted in accordance with survival, evasion, resistance, and escape regulations.

(g) (U) Combined HUMINT Activities. Describe any HUMINT activities performed in conjunction with foreign military HUMINT organizations.

(2) (U) Requirements and Reporting. Describe authorities, procedures, and formats for:

(a) (U) In-Theater Tasking. Describe the collection requirements tasking chain from the theater J-2 (collection management office) to the J-2X, HOC, or both as applicable. Address tasking both joint force HUMINT assets and in-theater assets not subordinated to the joint force (e.g., defense attaché offices).

(b) (U) External Tasking of Joint Force HUMINT Assets. Describe procedures established by the theater and joint force J-2s for external tasking of joint force HUMINT collection assets.

(c) (U) Establish joint force IIR/other HUMINT reporting procedures/formats.

Page Number

CLASSIFICATION

CLASSIFICATION

(3) (U) Coordination. Describe authorities and procedures for coordinating HUMINT operations, source utilization/registry, disclosure, and reporting. Include ICD 304.

(4) (U) Administration and Logistics. Provide administrative and logistic arrangements for requirements not covered in the basic plan or another annex. Include transportation, marshalling, billeting, clothing, equipment, and special operational funds as appropriate,

5. (U) Command, Control, and Communications:

a. (U) Command/Control. As appropriate, identify unique arrangements with the Department of Homeland Security, non-DoD US organizations, and allied/coalition forces.

b. (U) Communications. Cross-reference annex K as appropriate. Address unique communications systems interface requirements.

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

TABS (As appropriate)

OFFICIAL:

s/
Name
Rank and Service
Title

Page Number

CLASSIFICATION

APPENDIX C. MARINE AIR-GROUND TASK FORCE COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE PLANNING CHECKLIST

This appendix identifies typical MAGTF CI and HUMINT planning tasks and activities during each phase of the MCPP. Most planning tasks and activities require the coordinated action of various MAGTF G-2/S-2 sections and intelligence battalion personnel.

MCPP Step	Actions	CI and HUMINT Planning Actions
Problem Framing	Identify intent of HHQ/supported headquarters Analyze tasks Analyze the area of operations and AOI Review available assets Identify personnel and equipment resource shortfalls Determine constraints and restraints Determine recommended CCIRs (PIRs, friendly force information requirements, EEFI) Identify requests for information Determine assumptions Draft mission statement Present problem framing brief Draft the warning order Convene/alert Red Cell (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 plan (Appendix 3 to Annex B), HUMINT plan (Appendix 5 to Annex B), etc. Assist with determination of the MAGTF area of operations and AOI. Assess ongoing CI activities and HUMINT operations and plans within the area of operations and AOI (e.g., availability and currency of CI contingency materials), including those of DIA, CIA, CCMDs, and other external organizations. Provide initial CI estimates and other CI products to support initial planning, ensuring needs of subordinate units are identified and met. Identify specified, implied, and essential CI and HUMINT tasks. Identify intelligence objectives. Develop proposed CI and HUMINT mission statement. Coordinate with G-2/S-2 plans officer, the intelligence support coordinator, the CI and HUMINT company commander, and the G-3/S- 3 force protection officer. Obtain G-2/S-2 approval. Assist security manager with development of security classification guidance and foreign disclosure guidance to support planning and subsequent operations. Identify organic/supporting CI and HUMINT elements and subordinate units' CI and HUMINT 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.

MCPP Step	Actions	CI and HUMINT Planning Actions
Problem Framing		Provide G-3/S-3 recommendations (e.g., CI active and passive measures). Identify requirements for TSCM support. Identify JTF/multinational CI and HUMINT interoperability issues and dissemination procedures/methods. Provide recommendations. Establish/review/update the MAGTF CI and HUMINT databases. Pay special attention to current threat estimates, current CI estimates, and CI and HUMINT targets (i.e., personalities, organizations, and installations). Ensure subordinate units CI and HUMINT points of contact kept advised of pertinent actions and developments. Identify external organizations' CI and HUMINT collection, production, and dissemination plans, and assess against the MAGTF's initial operational requirements and plans. Determine CI and HUMINT personnel and equipment deficiencies and initiate augmentation requests (coordinate with intelligence battalion commander and the intelligence operations officer). Assign/task-organize organic CI and HUMINT elements (e.g., CI and HUMINT company detachments, support teams, major subordinate elements). Ensure that detailed C2 relationships, authorities, and restrictions are prepared and disseminated to all concerned. Validate/update JTF CI and HUMINT TTP and MAGTF SOP. Coordinate with HHQ and subordinate units. Validate and prioritize CI and HUMINT requirements, paying special attention to those needed for COA development. Begin development of CI and HUMINT collection operations plan. Issue orders to collection, production, and dissemination elements. Coordinate with intelligence support coordinator, G-2 plans and operations officers, the collection management and dissemination officer, P&A cell OIC, and surveillance and reconnaissance cell OIC. Determine initial information systems requirements and dissemination plans that support CI and HUMINT reporting and management. Identify deficiencies through coordination with the intelligence support coordinator, G-2 plans and operations officers, collection management and dissemination officer, and the G-6/S-6.

MCPP Step	Actions	CI and HUMINT Planning Actions
Problem Framing		Determine need and begin development of CI authorities/relationships with NCIS and the Marine Corps criminal investigation division. Validate CI and HUMINT database management procedures through coordination with P&A cell OIC, CI and HUMINT company commander, JTF, and subordinate units. Keep subordinate units' CI and HUMINT points of contact advised of pertinent actions and developments.
COA **Development**	Continue IPOE (throughout all steps of the planning process) Update staff estimates Develop COAs Conduct a COA brief Provide wargaming guidance and evaluation criteria (commander)	Assist with development and continued updating of the intelligence and CI estimates, with emphasis on the following: • CI target reduction plans development. • Periodic CI summaries and threat estimate update. • Recommendations and implementation of current/future CI countermeasures. Assist the intelligence, operations, and other staff sections with COA development.
COA **War Game**	War game each proposed COA Refine staff estimates Prepare COA war game brief Provide comparison and decision guidance (commander)	Continue liaison and coordination with NCIS and other relevant law enforcement agencies. Validate and update CI IIRs. Ensure subordinate units CI points of contact are kept advised of pertinent actions, developments, and CI products. Appendix 3 (Counterintelligence) to Annex B (Intelligence) and Appendix 5 (Human Resource Intelligence) to Annex B (Intelligence). Assist G-2/S-2 section with completion of the intelligence estimate and the friendly intelligence estimate of supportability. Assist G-3/S-3 section with completion of the force protection estimate. Continue to monitor and update CI and HUMINT collection, production, and dissemination activities. Continue development of CI estimate of supportability for each COA. Ensure subordinate units' CI and HUMINT points of contact are kept advised of pertinent actions and developments. Complete CI estimate and threat assessments. Complete CI and HUMINT estimates of supportability.

MCPP Step	Actions	CI and HUMINT Planning Actions
COA Comparison and Decision	Evaluate COAs Compare COAs Render commander's decision Refine concept of operations Update warning order	Assist G-2/S-2 and G-3/S-3 sections with evaluation and comparison of each COA. Update, validate, and prioritize CI and HUMINT intelligence requirements and supporting CI and HUMINT collection/production requirements for the selected COA. Issue orders as appropriate to CI and HUMINT elements. Coordinate CI and HUMINT element task-organization needs associated with the selected COA, with special attention paid to planning necessary support to the main effort. Update/develop in detail supporting C2 relationships, authorities, and restrictions. Coordinate with the G-6/S-6 regarding CI and HUMINT communications systems requirements, to include standard and unique communications systems for internal CI activities and HUMINT operations, as well as with other joint/multinational organizations.
Orders Development	Turn concept of operations into an OPORD or a FRAGO Update and convert staff estimates and other planning documents into OPORD annexes and appendices Approve OPORD (commander)	Complete Appendices 3 and 5 to Annex B and assist with other appendices as needed. Ensure copies provided to subordinate units and verify their understanding. Assist with completion of Appendix 16 (Intelligence Operations Plan). Update, validate, and prioritize CI and HUMINT requirements and associated collection, production, and dissemination operations. Monitor ongoing CI and HUMINT production operations. Ensure pertinent CI products are disseminated to subordinate units. Update and issue orders as appropriate to CI and HUMINT elements. Update/finalize criminal investigation plans with NCIS and the Marine Corps criminal investigation division. Complete CI and HUMINT-related communications systems actions.
Transition	Deliver transition brief Perform drills Plan refinements as required Deliver confirmation brief	Assist intelligence section with transition brief. Modify CI and HUMINT plans as necessary. Monitor ongoing CI activities and HUMINT collection and production operations. Update and issue orders as needed to CI and HUMINT elements. Ensure subordinate units' CI and HUMINT points of contact and CI officers in JTF and other components fully understand plans and standing requirements. Ensure their receipt of necessary CI products. Identify, validate, and prioritize remaining CI and HUMINT requirements and force protection EEFI. Participate in drills. Remain engaged in MAGTF future plans activities.

APPENDIX D.
COUNTERINTELLIGENCE PLAN FORMAT

This appendix provides the format for a typical Marine Corps unit counterintelligence plan that describes the approved activities to be conducted by a counterintelligence element in support of the designated commander. It could be written to describe support to an overall program, an individual event, or command and is intended to be updated annually or as threat conditions change.

The counterintelligence plan should be reviewed with the supported organization's security element and appropriate Military Department counterintelligence organization's field office, and it should be coordinated locally with other counterintelligence elements, law enforcement agencies, and the component appropriate G-2X office. It is then forwarded to the M-2X CICA for technical, legal review, and coordination within the DON counterintelligence coordination cell.

UNITED STATES MARINE CORPS
MARINE CORPS INTELLIGENCE ACTIVITY
2033 BARNETT AVENUE
QUANTICO, VIRGINIA 22134-5011

IN REPLY REFER TO:
3850
CI

From: Commander, UNIT
To: A/CS G-2, UNIT

Subj: U.S. MARINE CORPS UNIT COUNTERINTELLIGENCE PLAN (CIP)

Ref: (a) SECNAVINST 3850.2E, "Department of the Navy Counterintelligence", 3 January 2017
(b) CMC I WASHINGTON DC 151523Z Feb 17, "Marine Corps Counterintelligence Program Policy Guidance"
(c) CJCSI 3214.01E, "Defense Support for Chemical, Biological, Radiological, and Nuclear Incidents on Foreign Territory"
(d) CMC I WASHINGTON DC 301648Z Jan 15, "Establishment of the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise Counterintelligence and Human Intelligence (CI/HUMINT) Staff Element (M-2X)"
(e) DoDD 5240.02 W/CH 1, "Counterintelligence," 16 May 2018
(f) DoDI O-5240.10, Counterintelligence (CI) in the DoD Components 27 April 2020
(g) DoDD 5240.06 W/CH 3, "Counterintelligence Awareness and Reporting (CIAR)," 31 August 2020
(h) DoDI 5240.22, "Counterintelligence Support Counterterrorism and Force Protection," 12 October 2022
(i) CMC I WASHINGTON DC 211543 Oct 15, "Interim Policy Guidance for the Conduct of Counterintelligence Inquiries"
(j) DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," 8 August 2016
(k) DoDI 5240.26 W/CH 3, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," 07 December 2020
(l) DoDD 5205.02E W/CH 2, "DoD Operational Security Program (OPSEC)," 20 August 2020
(m) MCO 3070.2A, "The Marine Corps Operations Security (OPSEC) Program"
(n) DoDM 5200.02 W/CH 1, "Procedures for the DoD Personnel Security Program (PSP)," 29 October 2020
(o) DoDD 5230.20, "Visits and Assignments of Foreign Nationals," 22 June 2005
(p) DoDI 5240.19 W/CH 2, "Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)," 06 November 2020
(q) MCO 3501.36B, "Marine Corps Critical Infrastructure Program"
(r) DoDI S-5240.17 W/CH 1, "Counterintelligence Collection Activities (CCA)," 02 November 2020
(s) DCHE-M 3301.002, "Defense Counterintelligence and Human Intelligence Enterprise

(t) Manual, Volume II: Human Intelligence Collection Operations," 22 June 2015
(u) DoDI 5240.18 W/CH 3, "Counterintelligence (CI) Analysis and Production," 24 September 2020
(v) DoDI 5240.04 W/CH 2, "Counterintelligence (CI) Investigations," 18 September 2020
(w) DoDI S-5240.09 W/CH 1, "Offensive Counterintelligence Operations (OFCO)," 18 July 2016
(x) MCO 3850.1J, "Policy and Guidance for Counterintelligence (CI) and Human Sorce [sic] Intelligence (HUMINT) Activities"
(y) MCO 3800.2B, "Oversight of Intelligence Activities"
(z) Executive Order. 12333, "United States Intelligence Activities," as amended
(aa) DoDD 5240.01 W/CH 3, "DoD Intelligence Activities," 09 November 2020
(ab) DoDI C-5240.08, "Counterintelligence (CI) Security Classification Guide," 28 November 2011
(ac) DoDI O-5240.10, "Counterintelligence (CI) in the DoD Components," 27 April 2020
(ad) JP 2-0, "Joint Intelligence"
(ae) MCO 3058.1, "Marine Corps Mission Assurance"
(af) DoDI 5205.86 "(U) Defense Intelligence and Counterintelligence Expense (DICE).
(ag) DoDD 5148.13, Intelligence Oversight of 26 April 2017
(ah) MOA between Director of NCIS and Marine Corps DIRINT, Counterintelligence Activities of 1992/2002

Encl: (1) Counterintelligence Requirements
(2) Procedures for Counterintelligence Functional Services
(3) Procedures for Counterintelligence Collection Activities
(4) Procedures for Counterintelligence Analysis and Production
(5) Procedures for Counterintelligence Investigations
(6) Procedures for Support to Counterintelligence Operations
(7) Procedures for Counterintelligence Reporting

1. Orientation. This counterintelligence plan CIP provides guidance and direction from the Commander, UNIT for the planning and execution of counterintelligence activities conducted in support of UNIT using Service counterintelligence authorities under the direction of the Marine Corps DIRINT, per references (_) and (_). This counterintelligence plan CIP will serve as the basis for all UNIT G-2X counterintelligence activities.

2. (CUI) Situation. References (_) through (_) direct the conduct of counterintelligence activities in support of the Marine Corps and the monitoring and reporting of threats to Marine Corps installations, facilities, personnel, systems, networks, and DoD critical assets and infrastructure.

a. Foreign Intelligence Threat

(1) Country A.

(2) Country B.

b. Friendly Intelligence Threat

(1) Higher

(a) Director of Intelligence, Marine Corps. The DIRINT is the principal advisor to the Commandant of the Marine Corps for counterintelligence and intelligence matters. It is through the DIRINT's authorities that the Marine Corps counterintelligence elements execute counterintelligence activities when properly coordinated ad deconflicted. Per references (_) and (_), the DIRINT has delegated responsibility for Service- level support to Marine Corps elements engaged in counterintelligence activities to the M-2X.

(b) Per reference (_), the M-2X, in coordination with the DIRINT's Information and Intelligence Division (IID), plans, coordinates, deconflicts, synchronizes, and integrates CI and HUMINT and other related activities within the MCISRE in response to Service-level and Marine Corps component command-level requirements that exceed organic capabilities.

(c) The Marine Corps CICA serves as the senior representative for counterintelligence to the M-2X and assists the DIRINT in the direction, management, and coordination of Service counterintelligence activities. The Marine Corps CICA also assists commands across the total force that are responsible for protecting personnel, property, networks, and information to ensure counterintelligence planning, requirements, and tasking are integrated.

(2) Adjacent.

(3) Supporting.

3. Mission. UNIT G-2X plans, coordinates, and manages the employment of organic counterintelligence elements and coordinates with higher and supporting counterintelligence organizations to detect, identify, exploit, disrupt, deceive, and neutralize threats from FIE, violent extremist organizations, insider threats, or the nexus between these groups, directed against the DoD, Marine Corps, [UNIT], other Marine Corps forces personnel, systems, information, networks, facilities, and other critical infrastructure. Upon approval, and with appropriate coordination, [UNIT] G-2X can also plan, coordinate, and manage employment of counterintelligence elements to detect, identify, exploit, disrupt, deceive, and neutralize such threats against other DoD and USG entities or organizations.

4. Execution

a. Concept of Operations

b. Tasks

5. Coordinating Instructions

6. Administration and Logistics

7. Command and Signal

   a. Chain of Command

   b. Communication

   c. Communication Channels

8. Points of Contact

I.M. COMMANDER

APPENDIX E. COUNTERINTELLIGENCE TARGET REDUCTION PLAN

Target Number	Target	Location/Description	PRI	CHD	Special Instructions	Interested Units/Sections
1	Broadcasting station	3 km northwest of city on Victory Road (GEOCOORD 12345678)	1	1	Locate or take into custody station state security officer and all propaganda material.	G-5
2	Government center	Largest building in city center, gable roof (GEOCOORD 23456789)	3	1	Ensure file information protected for further analysis.	G-5
3	Military intelligence HQ	Located on Liberation military compound east of city (GEOCOORD 34567890)	1	2	Locate and search CI and agent operations section.	MAGTF G-2
4	Smith, John (intelligence officer)	Military intelligence HQ; home address 134 8th Street, Unit 3B	2	2	Potential defector; handle accordingly.	1st MARDIV
5	Insurgent training facility	West of city on peninsula (GEOCOORD 45678901)	3	2	Secure and search for file information on personalities and operations.	MAGTF G-2
6	Prison	Triangular shaped compound on Liberation Avenue enclosed by 20- foot brick wall	2	1	Personalities of CI interest on separate listing. Provide list of recovered personalities to HQ via most expedient means.	G-3 G-4 G-5
7	National intelligence field office	Concrete block building on corner of 5th Street and Liberation Avenue (GEOCOORD 78952305)	1	4	Immediately triage all documents and equipment.	G-2

Legend

GEOCOORD	geographical coordinates
HQ	headquarters
km	kilometers
MARDIV	Marine division
PRI	priority

APPENDIX F. EXAMPLE COUNTERINTELLIGENCE MEASURES WORKSHEET

			Units/Personnel Responsible for Execution of CI Measures						
Phase of Operation	Categories of CI Activities Involved	Counterintelligence Measures to be Adopted	Civil Affairs	G-6/ S-6	PMO	Comm/ Intel Units	All Units	CI Units	Comments
Assault Phase	a. Security discipline	(1) Conceal vehicle and aircraft markings.					X		Coordinate with G-4
		(2) Sanitize uniforms.					X		
		(3) Restrict personnel to area except for official business.					X		Coordinate with G-1
		(4) Emphasize security discipline with communications and information systems, documents and maps, and phone conversations which might convey information to the enemy.					X		
		(5) Report all potential security compromises to security manager or intelligence officer.		X	X	X	X	X	
	b. Safe-guarding classified information and equipment	(6) Address civilians in position to observe critical unit operations, fires, and combat service support sites.	X						CI elements assist with instruction and check SOP
	c. Communication and information security	(7) Check SOPs regarding security, destruction, and reporting of loss or compromise of cryptographic devices.	X	X	X	X	X	X	
		(8) Plan for destruction of documents in event of imminent compromise.		X			X		
		(9) Use only authorized call signs, authenticators, and cryptographic codes.		X			X		Coordinate with other military forces
	d. Security of unit movements	(10) Ensure only authorized personnel enter CPs and other sensitive areas.		X		X	X	X	Coordinate with G-1
		(11) Control the movement of all vehicles and aircraft to the extent that a change in normal operations is not detectable.		X			X		Coordinate with G-3 and G-4

Legend

Comm	communication
Intel	intelligence
PMO	provost marshal office

APPENDIX G. COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE REPORT FORMATS

CLASSIFICATION

Standard Human Intelligence Report (Message Traffic format)

FROM: Enter the plain language address of originating unit.

TO: Always enter DIA WASHINGTON DC. Enter additional plain language addresses as required.

INFO: Enter additional plain language addresses as required. Always enter the US Defense Attache Office of countries mentioned in the report.

CONFIDENTIAL// Not releasable to foreign nationals (NOFORN). NOTE: Classified only for illustrative purposes.

QQQQ

SERIAL: IIR 5 XXX XXXX YY The serial number is an organization's unique HUMINT report identifier as assigned by the originating organization.

DATE OF PUBLICATION: DDHHMMZ MMM YY. The originating organization's date on which the report is published.

- -

DEPARTMENT OF DEFENSE

INFORMATION REPORT, NOT FINALLY EVALUATED INTELLIGENCE.

- -

COUNTRY OR NON-STATE ENTITY. Inclusion of a country or non-state entity should be indicative of substantial details cited on that country or non-state entity in the text. The mere mention of a country or non-state entity might not necessarily warrant inclusion in the country line. Countries and non-state entities should appear in order of relevance based on their primary focus in the report. When several countries are mentioned in a report, only those that figure prominently should be included.

SUBJECT: IIR 5 XXX XXXX YY/TITLE OF THE REPORT. The subject should be a concise but descriptive noun phrase indicating the main topic of the report, in proper mixed case. The subject should be no longer than four lines. The project or operation name can be included at the beginning of the subject line.

Page Number

CLASSIFICATION

CLASSIFICATION

DATE OF INFORMATION: DD MMM YYYY. The date(s) of the events described in the text of the report.

CUTOFF: (optional) DD MMM YYYY. The last date the source obtained information on the topic discussed in the report; reflects the last known period of time the information was current. SUMMARY: To assist readers quickly ascertain the most relevant information in a report, the summary should not exceed 10 lines. The summary should be based only on the report's text; it should not draw on any information included in the comments section of the report. If no summary is included, the word "None" shall appear in the field.

SOURCE NUMBER: (CLASSIFICATION) The source identifier number on list line. If there are multiple sources, label as SOURCE NUMBER A, SOURCE NUMBER B, etc.

SOURCE: (CLASSIFICATION) Enter the source description. If there are multiple sources, label as SOURCE A, SOURCE B, etc.

CONTEXT: (CLASSIFICATION) Enter the source context statement. If multiple sources, label as CONTEXT A, CONTEXT B, etc.

WARNING: (CLASSIFICATION) Warning notices could be included to highlight source or foreign government sensitivities, specific handling instructions, notices regarding recall or revisions, or other pertinent non-substantive information. Issues concerning the source should be handled either in the source byline or context statement. Example: (CUI) THIS REPORT CONTAINS RAW HUMINT INFORMATION THAT HAS NOT BEEN FULLY EVALUATED, INTEGRATED WITH OTHER INFORMATION, INTERPRETED, OR ANALYZED.

TEXT: (CLASSIFICATION) Provide separate paragraphs for each main issue within the context of the subject of the report. Include subparagraphs as appropriate. Provide an organized, chronological narrative of the details pertinent to the subject of the report. Geographic locations should always be listed as Place Name//geographical coordinates: 12345N/67890W//CC (2 letter country code). When identifying persons, full names should be used as follows: ((LAST)), First Middle. If persons are reported to have multiple names or aliases, and that information was obtained from the source of this report, include the other names using the same format, ((ALIAS)); also known as ((LAST)), First Middle. All dates will be listed in the following numeric format: DD MMM YYYY. Field and source comments can be used in the TEXT section to amplify reported information, and if appropriate, can be provided within tearlines.

COMMENTS: (CLASSIFICATION) Comments are included in a report when there is a need to explain, clarify, or amplify the text; to make an observation; or to cite related information. It is essential that all commentary be properly labeled and separated from the text of the report to distinguish commentary from the actual intelligence information provided by the source.

Page Number

CLASSIFICATION

CLASSIFICATION

Comments should always be included when they make an essential contribution to the understanding of the report. Comments can be included within the text of the report or in the separate comments field. If comments are included only in the comments field, a notation should be made to the appropriate paragraphs of text to which the comments refer. Comments might include the following:

- HEADQUARTERS COMMENT: This comment reflects commentary provided by the reporting USG organization.
- FIELD COMMENT: This comment reflects the views or insights of the field elements of the originating organization.
- REPORTING OFFICER COMMENT: This comment provides unique insights from the perspective of the reporting officer.
- EMBASSY COMMENT: Comments made by embassy officials other than the ambassador or chief of mission should be labeled EMBASSY COMMENT.
- CHIEF OF MISSION COMMENTS: Comments made by the chief of mission are identified separately from other embassy officials.

SOURCE COMMENT: A source comment contains remarks made by the source in the role of the commentator, rather than reporter or transmitter of the information. Source comments might include the personal opinion or speculation of the source.

FOREIGN GOVERNMENT SERVICE COMMENT: This is a comment made by a foreign government service with which the reporting organization has an established relationship. If the identity of the foreign government service is included in the source byline, it should be identified in the comment as well.

ATTACHMENTS: Attachments can be in the form of documents, photographs, maps, video, or audio. When the length or form of the attachment prohibits inclusion in the report, instructions should be provided on where to locate the attachments. When an attachment is time sensitive, the highlights of the attachment should be summarized in the text of the report. If a report contains multiple attachments, each attachment should be uniquely identifiable. Methods of making the attachments identifiable include, but are not limited to, adding a suffix to the serial number listed on the attachments or marking the attachment as “Attachment 1 of 3," for example.

TOPIC: The appropriate topic will be included in this field. When entered into the report, the association of the ‘TOPIC’ Field with the National Intelligence Priorities Framework is classified SECRET//NOFORN.

FUNCTIONAL CODE: An intelligence function code [also referred to as IFC] should reflect the data in the report. The code that most closely reflects the content of the report should always be listed first, followed by additional applicable codes in descending order of importance.

Page Number

CLASSIFICATION

CLASSIFICATION

REQUIREMENT: The national HUMINT collection directives or national HUMINT requirements to which the report responds can be cited in this field using requirement identifiers that are unclassified. National HUMINT collection directives should be cited first, followed by national HUMINT requirements, then other requirement identifiers used by departments/ agencies, and lastly those of their subordinate elements. Multiple entries should be separated by semicolons, and the last entry should be followed by a period.

MANAGEMENT CODE: This field is used to track management data, such as codes used to facilitate automated retrieval of reports from a special intelligence technique, for funds management, or for other purposes of the using organization.

INSTRUCTIONS: This field is used to signal that a US person is identified in the report or to provide additional instructions for recipients regarding the reporting. When this field is used, information on the inclusion of US person data must be the first entry.

PREPARATION: The preparation identification code, field reporter number, or name of the reporting officer can be included in this field as OPSEC permits.

JOINT REPRESENTATION: This field is used to acknowledge joint representation of information resulting from joint operational cases or joint debriefings involving more than one organization. When the organizations agree, the identity of the contributing organization will be included in this field. While not required, a specific element or an organization can be listed when it is important to identify that element's involvement in a joint operation or debriefing. Should inclusion of a joint reporting code be source revealing, it can be excluded. In those exceptional circumstances when the contributing organization is not identified in the report, acknowledgement that the report is the result of a joint operation or joint debriefing can be made directly to the contributing organization. It is the responsibility of the organization issuing a joint intelligence report to consult with other organizations/agencies jointly involved in the collection of the intelligence and to provide a single, coordinated response to a request for subsequent use of the intelligence report, including, but not limited to, expanded dissemination, foreign release, downgrade of classification, or declassification.

DATE OF ACQUISITION: The date of acquisition reflects the date that the information was obtained by the originating organization. An approximate date of acquisition can be used if an exact date can be too source-revealing.

POINT OF CONTACT: At a minimum, this should include the office responsible for the report, a telephone number, and an e-mail address to allow consumers to contact someone should they have questions about the report. Additional instructions regarding how to submit clearance and disclosure requests, follow-up requirements, and feedback should be included.

Page Number

CLASSIFICATION

CLASSIFICATION

WARNING: Appropriate warning notices regarding the unauthorized disclosure can be included. THIS IS AN INFORMATION REPORT, NOT FINALLY EVALUATED INTELLIGENCE. REPORT CLASSIFIED CONFIDENTIAL//NOFORN (This example is classified only for informative purposes.)

DISSEMINATION: Each organization will facilitate electronic delivery of produced reporting.

CLASSIFIED BY: Insert the identification by name and position, or personal identifier, of the organization's original classification authority.

DERIVED FROM: Insert the classification derivatives based on the originating organization's derivative classification authority.

DECLASSIFY ON: Insert the duration of the classification decision based on the originating organization's declassification authorities using the format YYYYMMDD.

Page Number

CLASSIFICATION

CLASSIFICATION

SITUATION, POSITION, OBSERVATION, TIME REPORT

Report No: SPOTREP X XXX XXXX YY
DATE/TIME:
FROM: TO:
WHAT:
WHO:
WHERE:
WHEN:
DETAILS:
SOURCE:
RELIABILITY:
REMARKS:

PREPARED BY:
APPROVED BY:

Page Number

CLASSIFICATION

CLASSIFICATION

COUNTERINTELLIGENCE SCREENING REPORT

Reporting Unit:

Screener:

Date:

Time:

Capturing/Detaining Unit:

Category of Person Screened:

Military: (Country/branch of service.)

Paramilitary: (Organization/country.)

Civilian: (Identify organizational affiliation, if known.)

Other:

Personal Data:

Name:

Other Names:

Personal Identification Information: (Documents in the person's possession that were used for identification. Include document type, serial number, issuing authority, issue date, expiration and disposition of the documents.)

Detainee Identification Number: (If applicable/assigned by screening unit.)

Date and Place of Birth:

Sex:

Citizenship:

Nationality:

Page Number

CLASSIFICATION

CLASSIFICATION

Ethnic Origin: (If applicable, provide tribal affiliation, etc.) Marital Status:

Residence:

Occupation:

Languages Spoken:

Military or Government Service Information:

Date/Time/Place of Capture/Detention:

Reason and Circumstances of Capture/Detention:

Items in Possession at Time of Capture/Detention: (Comprehensive list of all items found in possession of the person screened/detained and disposition of those items.)

Physical Condition:

Disposition of Person Screened:

Remarks:

Enclosures:

Page Number

CLASSIFICATION

CLASSIFICATION

TACTICAL INTERROGATION REPORT

FROM: ORIGINATING UNIT

TO: RECEIVING UNIT

INFO: INFORMED COMMANDS
CLASSIFICATION

CITE: List any previous associated report numbers – omit if not used.

SERIAL: TIR 01 XXXX XX Insert the report number, as appropriate.

COUNTRY: NAME OF COUNTRY (Country code.)

SUBJ: TIR 01 XXXX XX/INTERROGATION OF ((LAST NAME)), FIRST NAME, MIDDLE NAME, TITLE (JOB, RANK, ETC.), UNIT/ORGANIZATION NAME, AND EPW OR DETAINEE NUMBER

DATE OF INTERROGATION: YYYYMMDD

TEXT: 1. **GENERAL**

1A. LANGUAGE USED.

1B. NAME OF INTERPRETER.

1C. CATEGORY OF EPW/DETAINEE. Identify if EPW/detainee is of counterintelligence interest.

2. PART I – PERSONAL DATA

2A. ALIAS. List all aliases or other names used by EPW/detainee.

2A1. LIST EACH ALIAS OR NAME IN A SEPARATE SUBPARAGRAPH.

2A2. FOLLOW STANDARD EXAMPLE OF ((LAST NAME)), FIRST NAME, MIDDLE NAME.

Page Number

CLASSIFICATION

CLASSIFICATION

2A3. IN CASES WHERE A SINGLE NAME IS USED AS AN ALIAS, SO STATE AND LIST AS ((“NAME”)).

2B. RANK, POSITION, OR OCCUPATION.

2C. DATE/PLACE OF BIRTH: YYYYMMDD/CITY, COUNTRY CODE.

2D. NATIONALITY/CITIZENSHIP/ETHNICITY/RELIGION. List as appropriate.

2E. RACE.

2F. HEIGHT.

2G. WEIGHT.

2H. EYES. Enter color and any abnormalities. Include use of eyeglasses if applicable.

2I. HAIR. Enter color, length; include balding areas, graying areas, and other distinctive features associated with hair.

2J. OUTSTANDING IDENTIFYING FEATURES. Enter any tattoos, scars, marks, or other physical features of distinction. Include use of dominant hand (right or left.)

2K. LANGUAGES. List by subparagraph each language the EPW/detainee speaks or has an ability in. Identify the ability for each language listed (fluent, good, poor, speaking ability but not able to read or write, etc.)

2L. UNIT/ORGANIZATION/ADDRESS. Provide a detailed location (address, geographical coordinates, etc.) of EPW place of residence, work, or organizational affiliation.

2M. FAMILY DATA. Enter appropriate information in subparagraphs. List one family member per subparagraph. Identify using examples as follows:

2M1. BROTHER/ ((LAST)), FIRST, MIDDLE.

2M2. SON/ ((LAST)), FIRST, MIDDLE.

2M3. SPOUSE/ ((LAST)) FIRST, MIDDLE.

2N. EDUCATION. List EPW/detainee’s previous education, separated into subparagraphs, if necessary, by academic (schools and universities) and professional (military training, professional training.)

Page Number

CLASSIFICATION

CLASSIFICATION

2O. CAREER. Provide a comprehensive list of EPW/detainee's professional career. List in subparagraphs by category (military, civilian, organizations, etc.), in chronological order beginning with current profession and working backwards. Include dates of positions held and summary of responsibilities. If military service is listed, identify rank, military specialty, unit of assignment, and locations served. If organizations are identified (terrorist groups, political organizations, etc.), identify full title of organization, position held, dates served, and duties while a member of the organization.

2P. SPECIAL KNOWLEDGE. Identify any special skills or knowledge (e.g., proficiency in use of explosives or communications equipment, trained in intelligence tradecraft).

3. PART II – CAPTURE INFORMATION

3A. DATE/TIME OF CAPTURE.

3B. CAPTURING UNIT.

3C. PLACE OF CAPTURE.

3D. CIRCUMSTANCES OF CAPTURE.

3E. WEAPONS, EQUIPMENT, AND DOCUMENTATION. List weapons, equipment, and documentation in the EPW/detainee's possession at the time of capture by subparagraph. After each item listed, indicate disposition of the item.

4. PART III – INFORMATION OBTAINED

4A. SUMMARY. Provide a summary of any information obtained during this interrogation.

4B. PRODUCTION. List all intelligence reports derived from this interrogation. List by report

number, subject line/title of report, and distribution, if applicable.

5. PART IV – INTERROGATOR'S REMARKS.

5A. ASSESSMENT OF EPW/DETAINEE.

5B. DISCUSSION OF INTERROGATION APPROACH TECHNIQUES.

5C. ADDITIONAL COMMENTS.

Page Number

CLASSIFICATION

CLASSIFICATION

6. PART V – DISPOSITION OF EPW/DETAINEE.

INSTR: US NO (or as appropriate).

PREP: FIELD REPORTER NUMBER OR NAME.

ACQ: CITY, COUNTRY YYYYMMDD.

Page Number

CLASSIFICATION

***WARNING*: *REPORT CLASSIFIED* (Classification.)**

PERSONAL DATA FORM FOR PRISONER OF WAR/MISSING IN ACTION/MISSING (NON-HOSTILE)

1. Personal Data

   a. Name:

   b. Rank:

   c. EDIPI/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. Martial Status: Include number, sex, citizen status, and age of children.

   k. PEBD:

   l. EAS/EOS:

   m. Date arrived in country:

   n. Duty assignment:

2. Physical Characteristics

   a. Height: Metric and US equivalent.

   b. Weight: Metric and US equivalent.

   c. Build:

Page Number

CLASSIFICATION

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: POW/MIA/missing (non-hostile) as reported by unit.

5. Other Pertinent Data

a. General physical condition:

CLASSIFICATION

b. Linguistic capabilities and fluency:

c. Religion:

d. Civilian education:

e. Military schools:

f. Clothing and equipment when last seen:

g. Jewelry when last seen: Include description of glasses, rings, watches, religious medallions, etc.

h. Other personnel listed POW/MIA/missing 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.

8. Additional Information

a. Clearances/Access Information: Include information concerning security clearance, access, or 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 that would indicate subject's ability to cope in a POW 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.

Page Number

CLASSIFICATION

CLASSIFICATION

Enclosures: Identify other reports (e.g., IIRs, SPOTREPs, witness statements/interviews, returned POW/MIA debriefing reports) that also contain information relevant to the subject of this case.

(1) IIR X XXX XXXX YY
(2) SPOTREP X XXX XXXX YY
(3) MFR S-2, 2d Bn, 5th Marines of XX Oct XX

Prepared by: Name, Rank, Title, Organization

Distribution:

Page Number

CLASSIFICATION

COUNTERINTELLIGENCE INCIDENT ASSESSMENT REPORT

Originator:

Subject:

Case Control Number:

Date:

Status:

References:

Enclosures:

1. Predication. A brief statement as to the purpose, scope, and origin of the investigative action. Cite applicable references, as appropriate. Identify any other investigative agencies notified or coordinated with during the course of this investigation (e.g., NCIS, AFOSI, military police).

2. Investigating Element. Identify the unit or organization that conducted the investigative activity (e.g., operations support platoon, CI/HUMINT support company, MCIA). Identify other organizations participating in the investigative activity.

3. Results. Provide a detailed account in an organized and chronological manner of the results of the investigative action. Fully identify all personalities, organizations, installations, equipment, and related material involved. Identify outstanding issues, leads, and status of this investigation or specific activity.

4. Recommendations. Provide recommendations as appropriate.

5. Disposition. Identify the status of the investigation and distribution of this report, to include all copies of both the report and enclosures. Status should include if the findings of this investigation were forwarded to another agency for action. Identify if forwarded for action, the agency that assumed responsibility or jurisdiction, and a point of contact within that agency.

Prepared by: Full name, Rank, Title, Service

Approved by: Full name, Rank, Title, Service

COUNTERINTELLIGENCE INSPECTION/EVALUATION REPORT

Reporting Unit:

Distribution:

Report Date:

Reference:

Enclosure:

Summary:

1. (U) Predication. What initiated the inspection/evaluation?

2. (U) Purpose. What the inspection/evaluation was to determine. State any limitations that were placed on the activity.

3. (U) Background. Information on previous inspections/evaluations or surveys on the same area. Information on the level and amount of classified material maintained. Identity of person(s) conducting the activity.

4. (U) 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. (U) Recommendations. List recommendations to correct security weaknesses or deficiencies as they appear in paragraph 4; 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)

COUNTERINTELLIGENCE SURVEY/VULNERABILITY ASSESSMENT

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 conducting the survey.

b. Previous surveys.

c. Mission.

d. Inherent hazards of the area.

e. Degree of security required (maximum, medium, or minimum) based on the following factors:

- Mission.
- Cost of replacement.
- Location.
- Number of like installations.
- Classified material.
- 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; reference the paragraph for clarity.

a. Security of information.

b. Security of personnel.

c. Physical security.

PREPARED BY: (Name, Rank, Title, Organization)

APPROVED BY: (Name, Rank, Title, Organization)

COUNTERINTELLIGENCE SOURCE LEAD DEVELOPMENT REPORT

Date: (Mandatory)

Subject: (Mandatory)

Report No:

Project No:

References:

Record Creator: (Mandatory)

Origin:

Source of Lead: (Mandatory)

Proposed Use of Lead:

Lead Screening Process:

Placement and Access:

Circumstances for Meeting with Source:

Security Issues:

Personnel Information:

Lead Status:

Nationality:

Citizenship:

Personality and Character Traits:

Motivation:

Character:

Personality:

Trait Exploitation:

Biographical Data: (Link to the INDIVIDUAL record. When printing, whole INDIVIDUAL record needs to be printed.)

Summary of Family/Personal History: (Consider auto-populate from INDIVIDUAL record.)

Investigative Checks:

Coordination Required: (Multiple Choice)

Assessment of Operational Potential:

Type of Source:

Placement:

Access:

Cover (For Status and Action):

Qualifications:

Personal:

Strengths and Weaknesses:

Risk:

To C/O & Collection Element:

To Source:

Approach Plan:

Intelligence Contingency Funds:

Comments:

Attachments:

Glossary

SECTION I. ABBREVIATIONS AND ACRONYMS

2X
counterintelligence and human intelligence staff element

ACE
aviation combat element

AOI
area of interest

AOR
area of responsibility

C2
command and control

CCICA
command counterintelligence coordinating authority

CCIR
commander's critical information requirement

CHD
counterintelligence and human intelligence detachment

CI
counterintelligence

CICA
Counterintelligence Coordinating Authority

CIA
Central Intelligence Agency

CIHO
counterintelligence and human intelligence officer

CISE
counterintelligence support element

COA
course of action

CUI
controlled unclassified information

DHE
defense human intelligence executor

DIA
Defense Intelligence Agency

DICE
Defense Intelligence and Counter Intelligence Expense

DIRINT
Director of Intelligence

DoD
Department of Defense

DoDD
Department of Defense directive

DoDI
Department of Defense instruction

DOMEX
document and media exploitation

DON
Department of the Navy

EEFI
essential elements of friendly information

EPW
enemy prisoner of war

FBI
Federal Bureau of Investigation (DOJ)

FIE
foreign intelligence entity

G-1
assistant chief of staff, personnel/personnel staff section

G-2
assistant chief of staff, intelligence/intelligence staff section

G-2X
counterintelligence and human intelligence staff element

G-3
assistant chief of staff, operations and training/operations and training staff section

G-4
assistant chief of staff, logistics/logistics staff section

G-5
assistant chief of staff, plans/plans staff section

G-6
assistant chief of staff, communications/communications staff section

GCE
ground combat element

HCR
human intelligence collection requirement

HHQ
higher headquarters

HOC
human intelligence operations cell

HUMINT
human intelligence

ICD
intelligence community directive

ICR
intelligence collection requirement

IIR
intelligence information report

J-2
intelligence directorate of a joint staff

J-2X
joint force counterintelligence and human intelligence staff element

JP
joint publication

JTF
joint task force

LCE
logistics combat element

M-2X
Marine Corps Service-level counterintelligence and human intelligence staff element

MAGTF
Marine air-ground task force

MCDP
Marine Corps doctrinal publication

MCIA
Marine Corps Intelligence Activity

MCISRE
Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise

MCO
Marine Corps order

MCPP
Marine Corps Planning Process

MCRP
Marine Corps reference publication

MCTP
Marine Corps tactical publication

MCWP
Marine Corps warfighting publication

MEF
Marine expeditionary force

MSO
military source operation

NCIS
Naval Criminal Investigative Service

NOFORN
not releasable to foreign nationals

OIC
officer in charge

OPCON
operational control

OPLAN
operation plan

OPORD
operation order

OPSEC
operations security

OSE
operations support element

P&A
production and analysis

PIR
priority intelligence requirement

PO&I
personalities, organizations, and installations

POW
prisoner of war

S-1
personnel officer/personnel office

S-2
intelligence officer/intelligence office

S-2X
counterintelligence/human intelligence section

S-3
operations and training officer/operations and training office

S-6
communications officer/communications staff office

SECNAVINST
Secretary of the Navy instruction

SIGINT
signals intelligence

SOP
standing operating procedure

SPOTREP
situation, position, observation, time report

US
United States

USG
United States Government

The following acronyms pertain to processes and entities specific to this publication.

AFOSI
Air Force Office of Special Investigations

CIAR
counterintelligence awareness and reporting

CIFS
counterintelligence functional services

CIVA
counterintelligence vulnerability assesment

IID
Intelligence Division

MCC
military counterintelligence collections

MCCICA
Marine Corps counterintelligence coordinating authority

MDCO
Military Department Counterintelligence Organizations

MHOC
Marine Corps Human Intelligence Operations Cell

OSE
operations support element

OFCO
offensive counterintelligence operation

TSCM
technical surveillance countermeasures

SECTION II. TERMS AND DEFINITIONS

analysis and production

In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (DoD Dictionary)

antiterrorism

Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. Also called AT. See also counterterrorism; terrorism. (DoD Dictionary)

area of interest

That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. Also called AOI. (DoD Dictionary)

area of operations

An operational area defined by a commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. Also called AO. (DoD Dictionary)

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." (DoD Dictionary)

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. See also attach. (DoD Dictionary)

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. See also assign. (DoD Dictionary)

battle damage assessment

(See the DoD Dictionary for core definition. Marine Corps amplification follows.) The timely and accurate estimate of the damage resulting from the application of military force. Battle damage assessment estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. **Also called** BDA. (USMC Dictionary)

battlespace

The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, maritime, and space domains; enemy and friendly forces and facilities; weather and terrain; the electromagnetic spectrum; and the information environment (which includes cyberspace) within the operational areas, areas of interest, and areas of influence. (USMC Dictionary)

cell

A subordinate organization formed around a specific process, capability, or activity within a designated larger organization of a headquarters. (DoD Dictionary)

center of gravity

(See DoD Dictionary for core definition. Marine Corps amplification follows.) A key source of strength without which an enemy cannot function. **Also called** COG. (USMC Dictionary)

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. (DoD Dictionary)

classified information

Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (DoD Dictionary)

collection

(See DoD Dictionary for core definition. Marine Corps amplification follows.) The gathering of intelligence data and information to satisfy the identified requirements. (USMC Dictionary)

collection asset

A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. See also collection. (DoD Dictionary)

collection management

In intelligence usage, 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. (DoD Dictionary)

collection operations management

The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. Also called COM. See also collection management; collection requirements management. (DoD Dictionary)

collection plan

A systematic scheme to optimize the employment of all available collection capabilities and associated processing, exploitation, and dissemination resources to satisfy specific information requirements. (DoD Dictionary)

collection requirement

(See DoD Dictionary for core definition. Marine Corps amplification follows.) An established intelligence need considered in the allocation of intelligence resources to fulfill the priority intelligence requirements and other intelligence needs of a commander. (USMC Dictionary)

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. Also called CCMD. (DoD Dictionary)

command and control

(See the DoD Dictionary for core definition. Marine Corps amplification follows.) The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. Command and control is one of the seven warfighting functions. Also called C2. (USMC Dictionary)

command element

The core element of a Marine air-ground task force (MAGTF) that is the headquarters. The command element is composed of the commander, general or executive and special staff sections, headquarters section, and requisite communications support, intelligence, and reconnaissance forces, necessary to accomplish the MAGTF's mission. The command element provides command and control, intelligence, and other support essential for effective planning and execution of operations by the other elements of the MAGTF. The command element varies in size and composition; and in a joint or multinational environment, it and can contain other Service or multinational forces assigned or attached to the MAGTF. **Also called** CE. (USMC Dictionary)

commander's critical information requirement

(See the DoD Dictionary for core definition. Marine Corps amplification follows.) 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 decision making. The two subcategories are priority intelligence requirements and friendly force information requirements. **Also called** CCIR. (USMC Dictionary)

commander's intent

(See the DoD Dictionary for core definition. Marine Corps amplification follows.) 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 that guides the exercise of initiative in the absence of instructions. (USMC Dictionary)

communications security

The protection resulting from all measures designed to deny unauthorized persons information of value that 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. (DoD Dictionary)

contingency

A situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect United States interests. (DoD Dictionary)

control

1. Authority that 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. In intelligence usage, an indicator governing the distribution and use of documents, information, or material. See also administrative control; operational control. (DoD Dictionary)

coordinating authority

A commander or individual who has the authority to require consultation between the specific functions or activities involving forces of two or more Services, joint force components, or forces of the same Service or agencies, but does not have the authority to compel agreement. (DoD Dictionary)

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. (USMC Dictionary)

counterintelligence

(See the DoD Dictionary for core definition. Marine Corps amplification follows.) The active and passive measures intended to deny the enemy valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. **Also called** CI. (USMC Dictionary)

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. (DoD Dictionary)

counterterrorism

Activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. **Also called** CT. See also antiterrorism; terrorism. (DoD Dictionary)

country team

The senior, in-country, United States coordinating and supervising body, headed by the chief of the United States diplomatic mission, and composed of the senior member of each represented United States department or agency, as desired by the chief of the United States diplomatic mission. (DoD Dictionary)

critical vulnerability

(See the DoD Dictionary for core definition. Marine Corps amplification follows.) An aspect of a center of gravity that, if exploited, will do the most significant damage to an enemy's and/or adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. **Also called** CV. (USMC Dictionary)

current intelligence

1. One of two categories of descriptive intelligence that is concerned with describing the existing situation. 2. Intelligence of all types and forms of immediate interest that is usually disseminated without the delays necessary to complete evaluation or interpretation. (USMC Dictionary)

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. 4. In chemical, biological, radiological, and nuclear environments, the act of locating chemical, biological, radiological, and nuclear hazards by use of chemical, biological, radiological, and nuclear detectors or monitoring and/or survey teams. (DoD Dictionary)

dissemination

Conveyance of intelligence to users in a suitable form. (USMC Dictionary)

essential elements of friendly information

Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. **Also called** EEFI. (USMC Dictionary)

essential elements of information

The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. **Also called** EEIs. (DoD Dictionary)

estimate

1. An analysis of a foreign situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and the prospective results of the various actions that might be taken. 2. An appraisal of the capabilities, vulnerabilities, and potential courses of action of a foreign nation or combination of nations in consequence of a specific national plan, policy, decision, or contemplated course of action. 3. An analysis of an actual or contemplated clandestine operation in relation to the situation in which it is or would be conducted to identify and appraise such factors as available as well as needed assets and potential obstacles, accomplishments, and consequences. See also intelligence estimate. (DoD Dictionary)

force protection

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. Force protection is one of the seven warfighting functions. (USMC Dictionary)

friendly force information requirement

(See DoD Dictionary for core definition. Marine Corps amplification follows.) 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 logistic status could become a friendly force information requirement. **Also called** FFIR. (USMC Dictionary)

ground combat element

The core element of a Marine air-ground task force (MAGTF) that is task-organized to conduct ground operations. It is usually constructed around an infantry organization but can vary in size from a small ground unit of any type to one or more Marine divisions that can be independently maneuvered under the direction of the MAGTF commander. It includes appropriate ground combat and combat support forces, and in a joint or multinational environment, it may also contain other Service or multinational forces assigned or attached to the MAGTF. The ground combat element itself is not a formal command. **Also called** GCE. (USMC Dictionary)

host nation

A nation which receives the forces and/or supplies from allied nations and/or North Atlantic Treaty Organizations to be located on, to operate in, or to transit through its territory. **Also called** HN. (DoD Dictionary)

human intelligence

A category of intelligence derived from information collected and provided by human sources. **Also called** HUMINT. (DoD Dictionary)

human intelligence operations

Operations that cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations. **Also called** HUMINT operations. (USMC Dictionary)

imagery intelligence

The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. **Also called** IMINT. See also intelligence. (DoD Dictionary)

indications

In intelligence usage, information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (DoD Dictionary)

indicator

In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (DoD Dictionary)

integration

In intelligence usage, the application of the intelligence to appropriate missions, tasks, and functions. (DoD Dictionary)

intelligence

(See DoD Dictionary for core definition. Marine Corps amplification follows.) Knowledge about the enemy or the surrounding environment needed to support decision making. Intelligence is one of the seven warfighting functions. (USMC Dictionary)

intelligence cycle

A six-step process by which information is converted into intelligence and made available to users. The six steps are planning and direction, collection, processing and exploitation, production, dissemination, and utilization. (USMC Dictionary)

intelligence discipline

A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. See also counterintelligence; human intelligence; imagery intelligence; intelligence; measurement and signature intelligence; open-source intelligence; signals intelligence; technical intelligence. (DoD Dictionary)

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 adversary and the order of probability of their adoption. (DoD Dictionary)

intelligence operations

The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. See also analysis and production. (DoD Dictionary)

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. (DoD Dictionary)

intelligence requirements

(See DoD Dictionary, intelligence requirement, for core definition. Marine Corps amplification follows.) Questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. (USMC Dictionary)

interoperability

1. The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (DoD Dictionary)

joint force

A force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (DoD Dictionary)

logistics combat element

The core element of a Marine air-ground task force (MAGTF) that is task-organized to provide the combat service support necessary to accomplish the MAGTF's mission. The logistics combat element varies in size from a small detachment to one or more Marine logistics groups. It provides supply, maintenance, transportation, general engineering, health services, and a variety of other services to the MAGTF. In a joint or multinational environment, it may also contain other Service or multinational forces assigned or attached to the MAGTF. The logistics combat element itself is not a formal command. Also called LCE. (USMC Dictionary)

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. (USMC Dictionary)

Marine air-ground task force

The Marine Corps principal organization for all missions across the range of military operations, composed of forces task organized under a single commander capable of responding rapidly to a contingency anywhere in the world. The types of forces in the Marine air-ground task force (MAGTF) are functionally grouped into four core elements: a command element, an aviation combat element, a ground combat element, and a logistics combat element. The four core elements are categories of forces, not formal commands. The basic structure of the MAGTF never varies, though the number, size, and type of Marine Corps units comprising each of its four elements will always be mission dependent. The flexibility of the organizational structure allows for one or more subordinate MAGTFs to be assigned. In a joint or multinational environment, other Service or multinational forces may be assigned or attached. Also called MAGTF. See also aviation combat element; command element; ground combat element; logistics combat element. (USMC Dictionary)

Marine Corps Planning Process

A six-step methodology that helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the mission and 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 problem framing, course of action development, course of action war game, course of action comparison and decision, orders development, and transition. Also called MCPP. (Note: Tenets of the MCPP include top- down planning, single-battle concept, and integrated planning.) (USMC Dictionary)

Marine expeditionary force

The largest Marine air-ground task force and the Marine Corps' principal warfighting organization, particularly for larger crises or contingencies. It is task organized around a permanent command element and normally contains one or more Marine divisions, Marine aircraft wings, and Marine logistics groups. The Marine expeditionary force is capable of missions across a range of military operations, including amphibious assault and sustained operations ashore in any environment. It can operate from a sea base, a land base, or both. In a joint or multinational environment, it may also contain other Service or multinational forces assigned or attached to the Marine air-ground task force. Also called MEF. See also aviation combat element; command element; ground combat element; logistics combat element. (USMC Dictionary)

Marine expeditionary unit

A Marine air-ground task force that is constructed around an infantry battalion reinforced, a composite squadron reinforced, and a task-organized logistics combat element. It normally fulfills Marine Corps' forward sea-based deployment requirements. The Marine expeditionary unit provides an immediate reaction capability for crisis response and is capable of limited combat operations. In a joint or multinational environment, it may contain other Service or multinational forces assigned or attached to the Marine air-ground task force. Also called MEU. See also aviation combat element; command element; ground combat element; logistics combat element. (USMC Dictionary)

measurement and signature intelligence

Information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event. Also called MASINT. See also intelligence. (DoD Dictionary)

mission assurance

Both an integrative framework and a process to protect or ensure the continued function and resilience of capabilities and assets including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains critical to the performance of Department of Defense mission essential functions in any operating environment or condition. (DoD Dictionary)

national intelligence

All intelligence that pertains to more than one agency and involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security. (DoD Dictionary)

open-source intelligence

Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. Also called OSINT. See also intelligence. (DoD Dictionary)

operational control

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. Also called OPCON. See also combatant command. (DoD Dictionary)

operation order

A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. Also called OPORD. (DoD Dictionary)

operation plan

A complete and detailed plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment list. Also called OPLAN. See also operation order. (DoD Dictionary)

operations security

A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. Also called OPSEC. (DoD Dictionary)

order of battle

The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called OB. (DoD Dictionary)

penetration

In intelligence usage, the recruitment of agents from within or the infiltration of agents and/or technical monitoring devices into an organization or group to acquire information or influence their activities. (USMC Dictionary)

physical security

1. 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. 2. In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. See also communications security; security. (DoD Dictionary)

priority intelligence requirement

(See DoD Dictionary for core definition. Marine Corps amplification follows.) An intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. Also called PIR. (USMC Dictionary)

reconnaissance

A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (DoD Dictionary)

security

1. Measures taken by a military unit, 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, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (DoD Dictionary)

security clearance

An administrative determination by competent authority that an individual is eligible for access to classified information. (DoD Dictionary)

sensitive

An agency, installation, person, position, document, material, or activity requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. (DoD Dictionary)

signals intelligence

1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. See also intelligence. (DoD Dictionary)

source

1. A person, thing, or activity from which information is obtained. 2. In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity either with or without the knowledge that the information is being used for intelligence purposes. (DoD Dictionary)

special operations

Activities or actions requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments. (DoD Dictionary)

special purpose Marine air-ground task force

A Marine air-ground task force organized, trained, and equipped with narrowly focused capabilities. It is designed to accomplish a specific mission, often of limited scope and duration. It may be any size, but normally it is a relatively small force the size of a Marine expeditionary unit or smaller. In a joint or multinational environment, it may contain other Service or multinational forces assigned or attached to the Marine air-ground task force. Also called special purpose MAGTF: SPMAGTF. (USMC Dictionary)

strategic intelligence

Intelligence required for the formulation of policy and military plans at national and international levels. (DoD Dictionary)

subversion

Actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority. (DoD Dictionary)

surveillance

(See DoD Dictionary for core definition. Marine Corps amplification follows.) The systematic visual or aural observation of an enemy force or named area of interest or an area and the activities in it to collect intelligence required to confirm or deny enemy/adversary courses of action or identify enemy/adversary critical vulnerabilities and limitations. (USMC Dictionary)

surveillance and reconnaissance cell

Primary element responsible for the supervision of Marine air-ground task force intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called SARC. (USMC Dictionary)

target

An entity or object that performs a function for the threat considered for possible engagement or other action. (DoD Dictionary)

task force counterintelligence coordinating authority

An individual in a joint force intelligence directorate, counterintelligence and human intelligence staff element, joint task force configuration that coordinates counterintelligence activities with other supporting counterintelligence organizations and agencies to ensure full counterintelligence coverage of the task force operational area. See also counterintelligence. (DoD Dictionary)

technical intelligence

Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary’s technological advantages. Also called TECHINT. (DoD Dictionary)

terrorism

The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce individuals, governments or societies in pursuit of terrorist goals. (DoD Dictionary)

validation

A process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. (DoD Dictionary)

warfighting functions

The seven mutually supporting military activities integrated in the conduct of all military operations. The seven warfighting functions are command and control, fires, force protection, information, intelligence, logistics, and maneuver. (USMC Dictionary).

REFERENCES AND RELATED PUBLICATIONS

United States Code

Title 10 Armed Forces
Director of National Intelligence Issuances

Intelligence Community Directives (ICDs)

203	Analytic Standards
206	Sourcing Requirements for Disseminated Analytic Products
304	Human Intelligence
310	Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Outside the United States
311	Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Inside the United States
402	Director of National Intelligence Representatives
501	Discovery and Dissemination or Retrieval of Information within the Intelligence Community

National Human Intelligence Management Directive (NHMD)

002.08	HUMINT Derived Intelligence Report Format Standard

Secretary of the Navy Instruction (SECNAVINST)

3850.2E	Department of the Navy Counterintelligence Department of the Army
FM 2-22.3	Human Intelligence Collection Operations

Department of Defense Issuances

Department of Defense Instruction (DoDI)

2310.1E	DoD Detainee Program
S-5200.42	Defense Human Intelligence (HUMINT) and Related Intelligence Activities

S-5205.01	DoD Foreign Military Intelligence Collection Activities (FORMICA)
5240.04	Counterintelligence (CI) Investigations
5240.05	Technical Surveillance Countermeasures (TSCM)
C-5240.08	Counterintelligence (CI) Security Classification Guide
S-5240.09	Offensive Counterintelligence Operations (OFCO)
O-5240.10	Counterintelligence (CI) in the DoD Components
S-5240.17	Counterintelligence Collection Activities (CCA)
5240.18	Counterintelligence Analysis and Production
5240.19	Counterintelligence Support to the Defense Critical Infrastructure (DCI) Program
5240.22	Counterintelligence Support to Counterterrorism and Force Protection
S-5240.23	Counterintelligence (CI) Activities in Cyberspace
O-5240.24	Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)
5240.26	Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat
3115.09	DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning
S-5200.37	Management and Execution of Defense Human Intelligence (HUMINT) (U)
5205.86	Defense Intelligence and Counterintelligence Expenses (DICE)
5240.02	Counterintelligence (CI)
5240.01	Intelligence Activities
5240.06	Counterintelligence Awareness and Reporting (CIAR)

Defense Intelligence Agency Manuals

3301.001	Defense Human Intelligence (HUMINT) Enterprise Manual, Volume I: Collection Requirements, Reporting, and Evaluation Procedures
3301.002	Defense Counterintelligence Human Intelligence Enterprise Manual, Volume II: Human Intelligence Collection Operations

Joint Issuances

Joint Publications (JPs)

2-0	Joint Intelligence

Miscellaneous

DoD Dictionary of Military and Associated Terms

Marine Corps Publications

Marine Corps Doctrinal Publication (MCDP)

2	Intelligence

Marine Corps Warfighting Publications (MCWPs)

2-10	Intelligence Operations
5-10	Marine Corps Planning Process

Marine Corps Tactical Publication (MCTP)

2-10B	MAGTF Intelligence Production and Analysis

Marine Corps Orders (MCOs)

3850.1J	Policy and Guidance for Counterintelligence (CI) and Human Source [sic] Intelligence (HUMINT) Activities
S3850.4	Technical Surveillance Countermeasures Program, dtd 13 Dec 22.

Miscellaneous

Marine Corps Supplement to the DoD Dictionary of Military and Associated Terms

Cultural Generic Information Requirements Handbook, Marine Corps Intelligence Activity.

Cultural Intelligence Indicators Guide, Marine Corps Intelligence Activity.

Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise Roadmap (2010).

Defense Intelligence Agency, Defense Intelligence Summary 188-00, dated 29 September 2000.

Riehle, Kevin. “Assessing Foreign Intelligence Threats,” American Intelligence Journal 31, no. 1 (2013): 96–101.

Salmoni, Barak A. and Paula Holmes-Eber. Operational Culture for the Warfighter: Principles and Applications. Marine Corps University Press, 2008.

Timm, Eric. “Countersabotage—a Counterintelligence Function,” Central Intelligence Agency, accessed 15 April 2013, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/ vol7no2/html/v07i2a06p_0001.htm