MCWP 2-15.2

SIGNALS INTELLIGENCE

U.S. Marine Corps

Coordinating Draft of 14 June, 1999

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380-1775

22 February 1999

FOREWORD

Marine Corps Warfighting Publication (MCWP) 2-15.2, *Signals Intelligence*, serves as a basic reference for understanding concepts, operations, and procedures for the conduct of signals intelligence (SIGINT) operations in support of the Marine air-ground task force. This publication complements and expands on Marine Corps Doctrinal Publication 2, *Intelligence*, and MCWP 2-1, *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 SIGINT operations. Personnel who provide support to SIGINT or who use the results from these operations should also read this publication.

MCWP 2-15.2 describes aspects of SIGINT operations, including doctrinal fundamentals, equipment, command and control, communications and information systems support, planning, execution, security, and training. Detailed information on SIGINT operations and tactics, techniques, and procedures is classified and beyond the scope of this publication.

MCWP 2-15.2 supersedes Fleet Marine Force Manual 3-23, (C) *Signals Intelligence/Electronic Warfare Operations* (U), dated 21 September 1990.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

J. E. Rhodes

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

DISTRIBUTION: 143 000063 00

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to **smb@doctrine div@mccdc**. Recommendations should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Add, delete
  - Proposed new text, preferably double-spaced and typewritten
- Justification and/or source of change

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status.* An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: **http://www.doctrine.quantico.usmc.mil**.

Unless otherwise stated, whenever the masculine or feminine gender is used, both men and women are included.

Signals Intelligence

Table of Contents

Page

Chapter 1. Fundamentals

1001 What is Signals Intelligence? 1-1
1002 Concept of Employment 1-1
1003 SIGINT and Electronic Warfare 1-2
1004 Threats 1-3
1005 All-Source Intelligence and Operations Command Support 1-3
1006 Capabilities 1-4
1007 Limitations 1-5
1008 Organization 1-5
1009 Command and Control 1-6
1010 Operations 1-6
1011 Commanders' Responsibilities 1-8

Chapter 2. SIGINT Responsibilities in the Supporting Establishment

2001 Marine Corps SIGINT Organization 2-1
2002 SIGINT Organizations in Other Military Services 2-2
2003 National SIGINT Organizations 2-3

Chapter 3. SIGINT Responsibilities in the MAGTF

3001 Commanders, Marine Corps Forces 3-1
3002 MAGTF Staff Sections 3-1
3003 MAGTF Intelligence Section Elements 3-2
3004 Marine Divisions and Aircraft Wings 3-5
3005 Radio Battalions 3-5
3006 VMAQs 3-5

Chapter 4. Radio Battalion

4001 Tasks 4-1
4002 Organization 4-1
4003 Task Organization for MAGTF Operations SIGINT Support Unit 4-3
4004 Command and Control 4-5
4005 Notional Concepts of Employment and Task Organizations 4-5

Chapter 5. Marine Tactical Electronic Warfare Squadrons

5001 Mission and Tasks 5-1
5002 Organization and Concept of Employment 5-1
5003 EA-6B Prowler 5-2
5004 Tactical EA-6B Mission Planning System 5-4
5005 TERPES 5-4

Chapter 6. Communications and Information Systems

6001 Basic MAGTF SIGINT CIS Requirements 6-1
6002 Notional MAGTF SIGINT Operational Architectures 6-2
6003 Planning Consideration 6-7
6004 SIGINT Communications 6-7

Chapter 7. Planning and Operations

Section I SIGINT Functional Planning 7-1

7101 SIGINT Concept of Operations 7-1
7102 Enemy Characteristics 7-1
7103 Topography 7-2
7104 Planning Responsibilities 7-3
7105 Coordination of SIGINT Operations 7-3

Section II SIGINT Operational Planning 7-5

7201 Planning and Direction 7-5
7202 Collection 7-6
7203 Processing and Exploitation 7-7
7204 Production 7-8
7205 Dissemination 7-8
7206 Utilization 7-10

Section III SIGINT Plans and Orders 7-11

Section IV Execution 7-12

Chapter 8. Security of Sensitive Compartmented Information

8001 Special Security Officer 8-2
8002 Personnel Security Program 8-2
8003 Physical Security 8-3
8004 Information Systems Security 8-5

Chapter 9. Training

9001 Military Occupational Specialty Training 9-1
9002 Functional Training 9-2
9003 Exercises 9-2
9004 Operational Training Objectives 9-3

Appendices

A Radio Battalion SIGINT Support Unit Checklist A-1
B Marine Corps SIGINT Equipment B-1
C SIGINT and SCI Security Management Operations Flowchart C-1
D SIGINT Appendix Format D-1
E TSCIF Checklist E-1
F Glossary F-1
G References and Related Publications G-1

List of Figures

1-1 The Intelligence Cycle 1-7
4-1 Radio Battalion Organization 4-2
4-2 SIGINT Support Unit Elements 4-3
4-3 Notional SSU Fly-In Echelon Configuration 4-6
5-1 EA-6B Prowler 5-2
5-2 VMAQ Organization 5-2
5-3 VMAQ and TERPES Operations 5-3
6-1 Notional MEF SIGINT Operational Architecture 6-3
6-2 Notional MEF Lead Echelon SIGINT Operational Architecture 6-4
6-3 MEU(SOC) CE Afloat SIGINT Operational Architecture 6-5
6-4 MEU(SOC) CE Ashore SIGINT Operational Architecture 6-6
6-5 MEF CE CIC Communications and Information Systems Architecture 6-9
6-6 RadBn SSU Operations Control and Analysis Center Communications and Information Systems 6-10
6-7 VMAQ Operations Center and TERPES Communications and Information Systems 6-11
7-1 MAGTF and Supporting SIGINT Operations 7-13
B-1 AN/ULQ-19(V2) B-1
B-2 AN/MLQ-36 B-2
B-3 AN/MLQ-36A B-3
B-4 AN/PRD-12 B-4
B-5 AN/MSC-63A B-5
B-6 AN/MSC-63A (interior view) B-5
B-7 Technical Control and Analysis Center Concept of Employment B-6
B-8 Team Portable Collection System Upgrade B-8

B-9 Team Portable Collection System
COMINT Collection Subsystem B-8
B-10 Team Portable Collection System Analysis Subsystem B-9
B-11 Trojan Spirit II B-10
B-12 RREP SS-1 B-11
B-13 RREP SS-2 B-11
B-14 Rifle-Mounted HIDRAH B-12
B-15 EA-6B Prowler B-14
B-16 AN/TSQ-90D/E(V), TERPES Portable Unit B-14

List of Tables

2-1 Marine Support Battalion Companies 2-2
4-1 Notional MEU(SOC) SSU T/O 4-7
4-2 Notional Fly-In Echelon T/O 4-7
7-1 Emitter Technical Data 7-2

Chapter 1

Fundamentals

All military forces use the electromagnetic spectrum to command and control operating forces acquire targets, guide weapons, and direct supporting arms. These military forces also use the electromagnetic spectrum to collect, process, and report intelligence and to support other administrative and logistics operations. Most facets o military operations involve the use of some device or system that radiates or receives electromagnetic energy via air waves, metallic cable, or fiber optics. Radios, radars, sensors, smart munitions, telephone systems, and computer networks use electromagnetic radiation. Both complex and unsophisticated military organizations depend on these systems and their inherent use of the electromagnetic spectrum. Signals intelligence operations are the principal way to exploit an adversary's use of the electromagnetic spectrum.

1001. What Is Signals Intelligence?

Signals intelligence (SIGINT) is "a category o intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted" (Joint Pub 1-02). Simply, SIGINT is intelligence gained by exploiting an adversary's use of the electromagnetic spectrum with the aim of gaining undetected firsthand intelligence on the adversary's intentions, dispositions, capabilities, and limitations.

a. Communications Intelligence

Communications intelligence (COMINT) is the technical and intelligence information derived from foreign communications by anyone othe than the intended recipient.

b. Electronics Intelligence

Electronics intelligence (ELINT) is the technical and intelligence information derived from foreign noncommunication electromagnetic radiation emanating from anywhere other than nuclear detonations or radioactive sources.

c. Foreign Instrumentation Signals Intelligence

Foreign instrumentation signals intelligence (FISINT) is the technical and intelligence information derived from the intercept of foreign instrumentation signals by anyone other than the intended recipients. (FISINT is primarily strategic in nature and will not be addressed further in this manual.)

1002. Concept of Employment

SIGINT can be employed in tactical situation when the enemy uses electromagnetic spectru communications and/or systems. Optimal employment is against enemy forces that depend on tactical communications and noncommunications for command and control of their operations. SIGINT operations are more difficult against enemy forces that have established more permanent emplacements using land lines or other cabled communications systems.

SIGINT is one of several intelligence disciplines. The other key intelligence disciplines are imagery intelligence (IMINT), human resources intelligence (HUMINT), and measurement and signature intelligence (MASINT).

1003. SIGINT and Electronic Warfare

Electronic warfare (EW) is “any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy” (Joint Pub 1-02). EW denies the enemy use of the electromagnetic spectru for command and control and protects it for friendly command and control. There are three divisions of EW.

a. Electronic Warfare Support

Electronic warfare support (ES) includes actions tasked by or under the direct control of an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated enemy electromagnetic signals for the purpose of *immediate* threat recognition. ES provides information required for immediate tactical decisions and operations such as the identification of imminent hostile actions, threat avoidance, targeting, or electronic attack.

Both SIGINT and ES involve searching for, intercepting, identifying, and locating electronic emitters. The primary differences between the two are the information’s intended use, the degree of analytical effort expended, the detail of information provided, and the timeliness required.

SIGINT is used to gain information concerning the enemy, usually in response to a priority intelligence requirement (PIR), an intelligence requirement (IR), or other means. As described in chapter 6, SIGINT support is usually provided to the Marine air-ground task force (MAGTF) as a whole, but may also be provided directly to subordinate elements.

SIGINT information is normally provided to the MAGTF all-source fusion center (AFC) for inclusion into all-source intelligence products and for further dissemination throughout the MAGTF and to external organizations. See Marine Corps Warfighting Publication [MCWP] 2-1, *Intelligence Operations*. SIGINT-derived information of immediate tactical importance that does not require further processing, correlation, or analysi may be passed directly to subordinate commanders or to the operations section or supporting arms element of supported commands, in accordance with United States Signals Intelligence Directive (USSID) 316, *Non-Codeword Reporting Program*, and USSID 240, *ELINT Processing, Analysis, Reporting, and Forwarding Procedures.*

b. Electronic Attack

Electronic attack (EA) is action taken to prevent or reduce an enemy’s effective use of the electromagnetic spectrum.

The objectives of SIGINT may conflict with those of EA. For example, EA may be conducted to interfere with the adversary’s use of an emitter a the same time as SIGINT operations are designed to exploit the adversary’s use of the same emitter. Furthermore, EA operations against one target may disrupt or otherwise interfere with friendly SIGINT collection against the same or differen targets.

SIGINT operations, EA operations, and the MAGTF’s overall use of the electromagnetic spectrum for command and control (C2) operations must be carefully coordinated within the MAGTF and with pertinent external organizations. Depending on operational requirements, SIGINT and EA operations coordination and deconfliction may occur within the radio battalion operations control and analysis center (OCAC) within the electronic warfare coordination center (EWCC), or within the MAGTF command element (CE) current operations center (COC).

c. Electronic Protection

Electronic protection (EP) involves the action taken to ensure effective, friendly use of the electromagnetic spectrum despite the enemy’s use of EW. Within the MAGTF, SIGINT elements may be tasked to employ similar techniques agains friendly force electronic emitters in order to identify and help eliminate signals security vulnerabilities that could be exploited by an enemy’s SIGINT operations.

1004. Threats

a. Enemy Capabilities

The more a combat unit relies on the electromagnetic spectrum, the more vulnerable it is to the enemy's signals intelligence and electronic warfare actions. The enemy can—

- Detect a unit's devices which radiate electromagnetic energy to reveal its identity and location.
- Monitor a unit's communications to reveal its intentions, combat capabilities, logistics and personnel status, and other critical operational and tactical information.
- Inject false information into communications and information systems (CIS) to confuse and mislead a unit.
- Interrupt a unit's use of the electromagnetic spectrum, thereby degrading its ability to receive and process intelligence, plan operations, and execute C2 functions.

b. Countermeasures

To counter threats listed and to enhance effectiveness, Marines must be able to—

- Protect, to the maximum extent possible, the free use of the electromagnetic spectrum and ensure the reliable performance of ou CIS.
- Exploit the enemy's use of the electromagnetic spectrum for intelligence and targeting and intrude into the enemy's CIS and networks.
- Attack the enemy's CIS to adversely affect their decisionmaking process and operations.

1005. All-Source Intelligence and Operations Command Support

Generally, SIGINT is more useful to the commander and the decisionmaking process when has been correlated and fused with information from other intelligence sources and disseminated in easily usable, tailored, all-source intelligence products. Tactical SIGINT operations within the MAGTF, along with other services, theater, and national SIGINT support, make SIGINT a valuable source of information within the overall intelligence effort. SIGINT supports the following six functions of intelligence.

a. Commander's Estimate

SIGINT helps formulate and modify the commander's estimate of the situation by providing information needed to analyze the enemy's C2 operations, identify the current parameters of operating emitters, give insight into enemy intentions, and assess the enemy's intelligence, EW and other military capabilities.

b. Development of the Situation

SIGINT's ability to track enemy emitters and associated units and to obtain indicators of intentions can confirm or refute potential enemy courses of action. SIGINT also helps commanders to better understand the enemy and the battlespace, thereby reducing uncertainty by acquiring information regarding enemy structure, dispositions, locations, movements, and operational activities and patterns.

c. Indications and Warning

SIGINT is often the principal provider of indications and warning (I&W) because adversaries often reveal their intentions, locations, and movements in their communications and other electronic emissions.

d. Force Protection

SIGINT supports force protection by revealing critical intelligence about enemy intelligence, sabotage, subversion, and terrorism and by assessing the vulnerability of friendly C2 and CI operations.

e. Targeting

SIGINT supports targeting by providing key operational and locational intelligence on enemy C2 operations and facilities, weapons systems, force compositions, and dispositions. Information provided through SIGINT can identify high value and high payoff targets and help develop options for attacking these targets. SIGINT also supports all-source intelligence gain and loss assessments of potential enemy targets.

f. Combat Assessment

SIGINT can aid in all-source intelligence support of battle damage assessments by exploiting enemy reports of sustained battle damages and by detecting changes in enemy operations subsequen to friendly attacks.

1006. Capabilities

a. Remote Intelligence

SIGINT operations provide extended-range intelligence without the need for physical presence within or near the surveillance area. The standoff range for SIGINT operations is directly dependent on the characteristics of the terrain in which SIGINT collection is being conducted and the type, operating characteristics, and methods of employment of the enemy's electromagnetic systems. Some enemy electromagnetic systems may require that SIGINT operations be close to the transmission origin, path, or medium. Conversely, other electromagnetic systems may be exploitable from positions farther away from the transmission origin, path, or medium.

(1) Ground SIGINT Elements. Locating ground SIGINT operational elements with friendly combat forces provides the friendly commander with the capability to collect a wide range of intelligence information. Locating SIGINT element with the ground combat element (GCE) forces provides the MAGTF commander with intelligence support for decisionmaking as well as I&W and force protection intelligence reporting to the local unit.

(2) Air-Platform SIGINT Elements. Airborn SIGINT elements can provide direct support to both air and ground operations and significantly enhance collection operations by exploiting enemy targets masked or otherwise unattainable by ground-based elements. These SIGINT elements also support friendly air operations by identifying, locating, and determining the status of enemy surveillance, targeting, and weapons systems and by providing intelligence support to friendly EA operations targeting these enemy systems.

(3) Ship-Based SIGINT Elements. SIGINT elements may operate from ship-based SIGIN operations facilities in support of amphibious operations. Marine and Navy elements operating from ship-based SIGINT facilities may support amphibious operations as a part of the assault force, airborne SIGINT operations, or ship-based SIGINT operations. Within an amphibious task force (ATF), the principal SIGINT facilities are found with ship's signals exploitation spaces (SSESs) located within the intelligence centers of many ships.

b. Target Detection and Identification

SIGINT can detect enemy activity in designated areas and provide a general indication of its type and volume. Analysis of SIGINT information can provide the identity and location of specific enemy units, indications of enemy plans and future operations, and the type, function, and location of specific enemy units and systems.

c. Near-Real-Time Reporting

SIGINT operations can immediately report enemy actions or events critical to the operations of friendly units. Time-sensitive SIGINT reporting to combat units may be via standard MAGTF intelligence communications channels or any available direct communications means.

d. Continuous Operations

SIGINT operations are conducted on a 24-hou basis. The size and composition of SIGINT forces along with the supported commander(s)'s concept of operations will influence the scope, services and capabilities of SIGINT operations.

e. Stealth

SIGINT operations are a passive intelligence technique and can usually be conducted withou the enemy's knowledge or detection. EW operations include both active and passive techniques and, depending on implementation, may or may not be recognized by the enemy.

f. Flexibility

Marine SIGINT operations may be employed in a variety of means to support the MAGTF concept of operations and supporting intelligence operations. SIGINT elements may be deployed with advance forces or forward ground units; they may be aboard air platforms or ship-based. Additionally, Marine SIGINT elements routinely operate with joint and other service elements. These elements are effective at leveraging their capabilities in support of MAGTF requirements.

1007. Limitations

a. Enemy System

The primary value of SIGINT operations is against enemy systems using electromagnetic spectrum system transmissions. SIGINT operations are ineffective against systems that do no use radio frequency (RF) transmissions (e.g., fiber optics, land-line telephone systems, or other cabled systems). If the enemy conducts operations under enemy emission control (EMCON) conditions (e.g., radio silence), SIGINT operations will not be effective.

b. Terrain Masking

Heavily wooded and urban areas reduce the susceptibility of enemy transmissions to SIGINT collection. In these areas, generally, SIGINT elements must be closer to the enemy's transmission origin or medium. Mountainous or very hilly terrain also inhibits SIGINT operations (particularly ground-based operations) by effectively blocking enemy signals from detection.

c. Complex Signals

Enemy signals that are complex or encrypted reduce the intelligence information available from the transmission. Complex signals (i.e., frequency hoppers) require special equipment for intercep and signals analysis. Encrypted signals require deciphering to reveal intelligence information. Deciphering simple encryption methods may be possible, but an enemy's use of complex encryption methods is currently beyond the scope of tactical SIGINT elements.

d. SIGINT versus Electronic Attack

SIGINT operations may be affected when enemy signals are being jammed. Prior to initiating EA jamming operations, consideration must be given to the intelligence value of the enemy's signal and the effects of its loss.

1008. Organization

Within the Marine Corps, the units responsible for the conduct of tactical SIGINT are the two radio battalions and the four Marine tactical electronic warfare squadrons.

a. Radio Battalion

The radio battalion (RadBn) provides tactical SIGINT, electronic warfare, communications security monitoring and analysis, and special communications operations in support of the MAGTF. A variety of employment concepts may be used depending upon the situation. Refer to chapter 4 for a detailed description of RadBns.

b. Marine Tactical Electronic Warfare Squadron

The Marine tactical electronic warfare squadron (VMAQ) conducts tactical electronic reconnaissance and ELINT operations in support of the MAGTF.

The VMAQ provides—

- ELINT collection operations to maintain the electronic order of battle, including identification of selected emitters and location o nonfriendly emitters.
- Threat warnings for friendly aircraft, ships, and ground units.
- Intelligence support to prevent, delay, or interrupt detection and tracking by enemy early warning, acquisition, and fire or missile control radars of aviation combat elemen (ACE) operations and Marine EA-6B tacti cal jamming aircraft in support of strike aircraft.

Refer to chapter 5 for a detailed description of the VMAQ.

1009. Command and Control

a. Radio Battalion

The RadBn (or RadBn detachment) is generally a subordinate command of, or attached to, the MAGTF CE. The MAGTF commander has operational control (OPCON) of the RadBn (or RadBn detachment).

(1) Staff Cognizance. The MAGTF commander exercises C2 over the RadBn or its detachments via the MAGTF intelligence officer. Such a relationship allows for the centralized direction and effective integration of SIGINT operations within the MAGTF's broader all-source intelligence concept of operations. RadBn's EW operations fa under the staff cognizance of the MAGTF operations officer, requiring close coordination and integration among the intelligence staff officer (G-2/S-2), operations staff officer (G-3/S-3), and communications and information systems officer (G-6/S-6) to achieve optimum employment of RadBn.

(2) Support Relationships The RadBn most typically operates in general support of the MAGTF. However, RadBn or its elements may be employed in direct support of any of the MAGTF's major support elements, i.e., GCE and ACE. In such cases, the scope of the supported commander's control over assigned RadBn elements usually is specified to ensure effective support of operations while allowing the MAGTF commander to maintain effective control of broader intelligence and SIGINT operations.

b. Marine Tactical Electronic Warfare Squadron

VMAQ or its detachments are subordinate to the ACE and under the OPCON of the ACE commander.

(1) Staff Cognizance. The ACE commander will usually exercise C2 over VMAQ via the ACE operations officer or tactical air command center (TACC). The ACE intelligence officer will exercise staff cognizance over VMAQ ELINT activities beyond that required to support EA missions.

(2) Support Relationships. VMAQ elements principally operate in direct support of ACE operations or other designated commanders (e.g., the joint force air component commander). However, ELINT acquired during VMAQ operations is capable of being used in general support of MAGTF elements and supporting intelligence operations.

1010. Operations

RadBn and VMAQ conduct both COMINT and ELINT operations to varying degrees. RadBns conduct predominantly COMINT operations; they also ensure rapid dissemination of fused ELIN and COMINT from organic or external sources to the G-2/S-2 and subordinate commanders. The VMAQ's main focus is ELINT and ES.

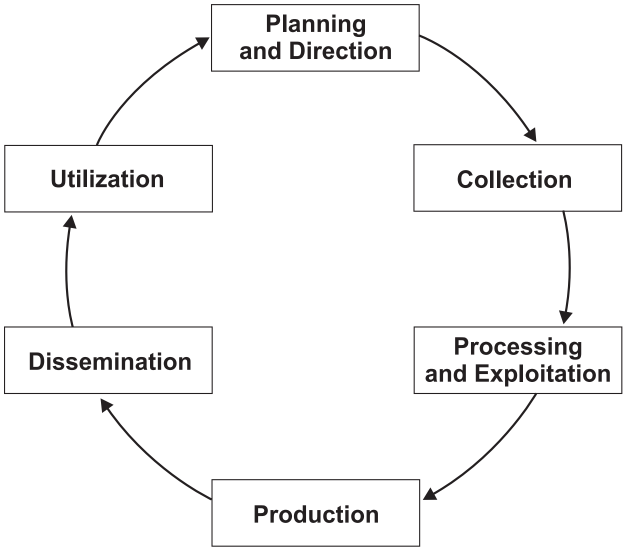

Figure 1-1. The Intelligence Cycle.

To complete intelligence tasks, RadBn an VMAQ incorporate the six intelligence cycle phases into their SIGINT methodology (see figure 1-1). Products of the SIGINT cycle are disseminated to commanders and others through the MAGTF intelligence officer. RadBn and VMAQ also provide SIGINT products to other Service and agencies as directed.

a. Planning and Direction

SIGINT direction is a continuous process that encompasses the tactical and technical employment of SIGINT assets. It begins on receipt of a warning order, initiating directive, or establishment of a planning objective and continues until termination of the mission. SIGINT unit commanders closely coordinate their operations with the MAGTF intelligence officer and pertinent external intelligence and SIGINT elements.

Planning and direction involves—

- Determining PIR and IR and SIGINT requirements to support them.
- Preparing supporting SIGINT collection, production, and dissemination plans.
- Issuing orders and requests to SIGINT units.
- Checking continuously on the productivity and effectiveness of SIGINT collectors, producers, disseminators, and other SIGINT elements and agencies.

b. Collection

During collection, organic, attached, and supporting SIGINT elements detect, collect, and record COMINT and ELINT data. The collected COMINT and ELINT data is then delivered to the appropriate SIGINT processing or production element. The OCAC is the processing and production element for RadBn, while the Tactical Electronic Reconnaissance Processing and Evaluation System (TERPES) is VMAQ’s processing and production element. In some instances, such as immediate threat information, PIRs and supporting reporting criteria may direct the SIGINT collector to disseminate SIGINT reports directly to the local commander (e.g., an infantry maneuver element) for immediate support to operations.

c. Processing and Exploitation

SIGINT processing consists of converting and formatting raw signals data to a form that is usable in follow-on SIGINT and all-source intelligence analysis. The processing and exploitation phase is usually not a discrete function, but rather one that is accomplished during collection. Once the collected information has been processed, analysis must determine its significance. Other intelligence information may also be fused together with the processed SIGINT to give a comprehensive picture and to show how the information can be used by the commander to gain an advantage.

d. Production

The production stage involves converting the SIGINT analysis into appropriately tailored SIGINT reports and all-source intelligence product that can be easily understood by the commander and other users. Specifically formatted standardized messages, graphics, and other intelligence products are required to familiarize these user with layout and content and to ensure rapid usage and automated processing of finished reports. Within the MAGTF, the RadBn OCAC and the VMAQ TERPES produce SIGINT reports and products, and the MAGTF AFC incorporates

SIGINT products and information into all-source intelligence products.

e. Dissemination

Dissemination is the process through which SIGINT products are delivered to MAGTF users: the MAGTF commander, subordinate commanders and their staffs, and others as appropriate (e.g. joint force commander, joint components, and various theater and national organizations and intelligence agencies). SIGINT products are disseminated via dedicated SIGINT or general purpose CIS channels according to available CIS resources, the classification of the product, and the intelligence dissemination plan. These products include time-sensitive voice reports, text reports, data base updates, and web-based resources (e.g., via the MAGTF sensitive compartmented information local area network).

f. Utilization

SIGINT must be exploited to have value. Commanders, G-2/S-2s, G-3/S-3s, and other principal staff officers must continuously evaluate SIGINT products for timeliness, usefulness, and overa quality and provide feedback to the intelligence officer and SIGINT elements.

1011. Commanders' Responsibilities

MAGTF commanders are responsible for the planning and direction, collection, processing production, dissemination, utilization, and security of all SIGINT information by units under their command. The Director, National Security Agency (DIRNSA), delegates SIGINT operational tasking authority (SOTA) to MAGTF commanders by name for the duration of an operation o other specified period of time. SOTA allows the designated commander to task and direct the operations of organic or attached SIGINT units. Additional information regarding SOTA may be found in USSID 4, *Concept of SIGINT Support to Military Commanders*.

Commanders are also responsible for planning integrating, and using SIGINT support, if available, from other United States or allied nationa and military SIGINT organizations. The commander's primary responsibilities fall into the following areas.

a. Tasking and Directing

The commander possessing SOTA is responsible for the effective tasking and operation of assigned SIGINT assets. Generally, once a commander determines the intelligence requirements, the G-2 S-2, with the advice and assistance of the intelligence operations officer and SIGINT officer (SIO), decides which requirements can be satisfied via organic SIGINT operations. SIGINT unit commanders or officers in charge (OICs) will also coordinate operations with other key staff officers within the intelligence section (i.e., the collections manager, the AFC OIC, the surveillance and reconnaissance center OIC, and the dissemination manager). The G-2/S-2 passes these IRs as taskings to the commanding officer (CO) or OIC o the organic or attached SIGINT unit (e.g., a RadBn unit). These requirements will be in the form of either PIRs or IRs. PIRs and IRs are further managed within the intelligence effor through the use of intelligence collection requirements (ICRs), intelligence production requirements (IPRs), and intelligence dissemination requirements (IDRs) in order to achieve effective, mutually supporting all-source intelligence operations (see MCWP 2-1, chapter 3, for detailed information on IR management). The SIGINT unit commander is then responsible for commanding and controlling resources to accomplish the assigned mission. This process is discussed further in chapter 7.

b. Reporting

The ultimate goal of tactical SIGINT operations is the timely and usable production of SIGINT information which answers the MAGTF commander's PIRs and other MAGTF IRs. SIGINT reports are discussed in detail in chapter 7.