FIELD MANUAL
NO. 34-25-3

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington DC, 3 October 1995

ALL-SOURCE ANALYSIS SYSTEM AND THE ANALYSIS AND CONTROL ELEMENT

TABLE OF CONTENTS

Page

PREFACE iii

CHAPTER 1 – INTRODUCTION 1-1
Overview 1-1
Army Battle Command System 1-3
Intelligence Architecture 1-6
Capabilities 1-9
Limitations 1-11

CHAPTER 2 – ANALYSIS AND CONTROL ELEMENT 2-1
Mission 2-1
Organization 2-1
Structure 2-4
Responsibilities 2-5
Force Projection Operations 2-11

CHAPTER 3 – EQUIPMENT 3-1
ASAS Block I 3-1
ASAS Extended 3-11
ASAS Block II 3-14
ASAS Block III 3-16

CHAPTER 4 – INFORMATION SYSTEMS 4-1
Area Networks 4-1
Army Communications 4-1
Joint Communications 4-5
Special Purpose Intelligence Communications 4-9
Army Intelligence Processors 4-13
Joint and Service Intelligence Processors 4-15
Joint and Service Intelligence Databases 4-18

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

Page

CHAPTER 5 – OPERATIONS 5-1
Intelligence Readiness 5-1
Site Selection 5-1
Predeployment 5-2
Deployment 5-3
Workstation Configuration 5-3
Operations 5-9
Degraded Operations 5-14
Redeployment 5-15

CHAPTER 6 – SURVIVABILITY AND SECURITY 6-1
Survivability 6-1
Security 6-1

CHAPTER 7 – MAINTENANCE 7-1
Responsibilities 7-1
Hardware Maintenance 7-2
Software Maintenance 7-2
Field Software Services Support (FSSS) 7-3

CHAPTER 8 – TRAINING 8-1
New Equipment Training 8-1
Institutional Training 8-3
Sustainment Training 8-3

GLOSSARY Glossary-1

REFERENCE Reference-1

INDEX Index-1

PREFACE

This field manual (FM) describes the equipment, operations, maintenance, and training of the All-Source Analysis System (ASAS). It provides the doctrinal framework for employing the ASAS within the G2 (S2) and analysis and control element (ACE) at theater Army, corps, division, brigade, separate brigade, and armored cavalry regiment (ACR) across the range of military operations.

The ASAS is the intelligence and electronic warfare (IEW) component of the Army Battle Command System (ABCS). It is an automated intelligence fusion system that helps the commander rapidly gather, record, analyze, and disseminate the often overwhelming volume of data available on the battlefield. The system supports the G2 (S2) and his ACE in directing IEW operations and producing intelligence that meets the commander’s needs. The ASAS can automatically receive, store, and rapidly fuse battlefield information and intelligence into a variety of products and formats that aid the commander in decision making and operations. It provides connectivity between sensors and intelligence activities at multiple echelons. ASAS connectivity and processing power gives commanders and their staffs a common multi-dimensional view of the enemy situation and the battlefield.

This manual is designed for use by commanders and their staffs; all military intelligence (MI) personnel in units equipped with or supported by the ASAS. It applies equally to the Army Active and Reserve Components (RC). This manual supports training, planning, and operations by commanders and staffs of joint, multinational, and service commands. Where appropriate, other manuals having a direct bearing on the discussion of referenced.

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

This manual does not implement any international standardization agreements.

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

Chapter 1

INTRODUCTION

IEW and communications systems continue to improve in their sophistication, application of technology, and accessibility to the commander. Their increasing capabilities create an unprecedented volume of information available to commanders at all echelons. Without focus and management, this wealth of information becomes an encumbrance to effective battle command rather than a blessing.

The manual intelligence management, analysis, and dissemination methods used in the past are inadequate in this Information Age. Successful operations at the tactical and operational levels require an increased ability to synchronize fires, access intelligence, maintain situational awareness, and provide force protection. As the IEW component of the ABCS, the ASAS is an essential tool in meeting those requirements and automating the Intelligence Battlefield Operating System (BOS).

OVERVIEW

The ASAS is a tactically deployable, ruggedized, and automated information system. It consists of evolutionary hardware and software modules that support the execution of IEW tasks at regiment, brigade, division, corps, and theater Army.

The ASAS remote workstation (ASAS-RWS) provides the G2 (S2) with the means to integrate IEW into the ABCS. The ASAS all-source workstation (ASAS-ASW) and single-source workstation (ASAS-SSW) provide automation processing that aids IEW control, database development, and intelligence production within the ACE.

These workstations provide the G2 (S2) and the ACE the ability to efficiently and effectively process high volumes of perishable combat information and multidiscipline intelligence. This ability in turn supports timely, relevant, accurate, and predictive reporting and dissemination of a common threat picture to other battlefield functional areas. Figure 1-1 shows the evolutionary nature of ASAS.

ASAS DEVELOPMENT:

The ASAS is an evolutionary system. Its development and fielding support the near-term needs of units, exploit emerging technology, and comply with the standards of the ABCS. The ASAS Block I, the initial system, provides ASAS capability to corps and divisions. As ABCS Common Hardware and Software (CHS) II become available, ASAS Block II will replace Block I. Block II will have greatly improved software that meets baseline system requirements.

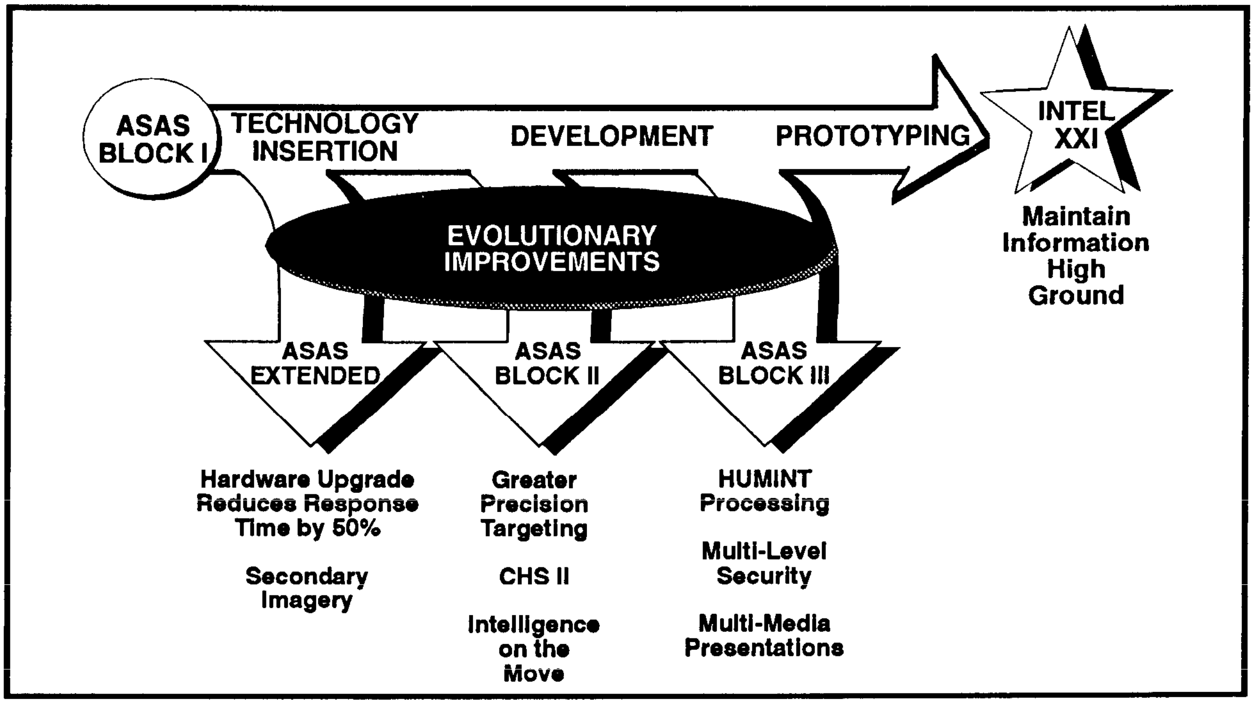


Figure 1-1. Keeping ASAS current.

The objective system, ASAS Block III, will expand upon Block II capabilities for operational, environmental, and performance requirements. In addition to these programmed materiel acquisition versions of ASAS, technology insertion and prototyping efforts will incrementally enhance ASAS and support the rapid distribution of ASAS capabilities to units in the field.

TECHNOLOGY INSERTION:

The ASAS is upgraded as new technology becomes available. An example of technology insertion is the use of the commercial Alpha Reduced Instruction Set Computing (RISC) processor. The Alpha RISC operates 30 times faster than the initially fielded processor in the Block I ASAS-ASW. It eliminates the need for the two AN/TYQ-36(V)3 Data Processing Sets (DPSs) in the ASAS Block I. Some units equipped with ASAS Block I will be upgraded with the Alpha RISC processor. The Alpha RISC processor is also used in the ASAS-Extended provided to selected units not receiving the ASAS Block I hardware.

PROTOTYPING:

Prototyping gets new technology and applications to the field quickly. Organizations like the Joint Prototyping Office use prototyping to develop software and hardware modules that are given to units for experimentation and evaluation. The Joint Prototyping Office is located at MYSTEC Associates, Inc. ATTN: Joint Prototyping Office, Suite 1200 5320S, Leesburg Pike Skyline Plaza, Falls Church, VA 22041. Based on unit recommendations, useful modules are further refined and incorporated into new software and hardware. Prototyping for ASAS focuses on high value capabilities not already defined for ASAS software applications that support emerging intelligence techniques, and high risk efforts that push technology to the edge. The WARRIOR workstation developed initially for US Army, Europe (USAREUR) is an example of ASAS prototyping efforts that have supported forces in the field and contributed to improvements to the ASAS-RWS.

ARMY BATTLE COMMAND SYSTEM

The ABCS exploits state-of-the-art sensors, processors, and communications systems to provide commanders with the technical advantages needed to meet the challenges of battle command. Leaders and operators use ABCS to maintain proficiency for and accomplish a broad range of potential missions. The ABCS provides—

- A CHS program that supports horizontal integration between battlefield functional areas and vertical integration between echelons.
- Access to a common picture of the battlefield derived from multiple sources.
- Connectivity from tactical level to national command authority (NCA) using Army, joint, and multinational standard communications.

The ABCS provides both commander and staff with the capability to identify and satisfy the commander’s critical information requirements (CCIR). The commander can view his requirements as a set of tailorable, recurring information products. These products include situation maps, graphical resource status reports, intelligence products, and textual reports. His staff can tailor these products according to the commander’s specific mission, enemy, troops, terrain and weather, and time available (METT-T). The ABCS consists of the following systems:

ARMY GLOBAL COMMAND AND CONTROL SYSTEM (AGCCS):

The AGCCS is the echelons above corps (EAC) portion of ABCS; it is also the Army component of the larger joint level Global Command and Control System (GCCS). AGCCS provides a suite of software applications that specialize in supporting functions peculiar to the national and theater levels of command. It is the primary link to joint and combined automation systems. The AGCCS integrates the following systems:

- Army World Wide Military Command and Control (WWMCC) Information System (AWIS).

- Standard Theater Army Command and Control System (STACCS).

- Combat Service Support Control System-Echelon Above Corps (CSSCS-EAC).

ARMY TACTICAL COMMAND AND CONTROL SYSTEM (ATCCS):
ATCCS consists of battlefield functional area control systems (BFACS) for maneuver, fire support, air defense artillery (ADA), IEW, and combat service support (CSS). In addition to ASAS, the BFACS of the ATCCS shown in Figure 1-2 provides situational information and decision support to commanders and staffs at brigade through corps levels. ATCCS connectivity is supported primarily by the Area Common User System (ACUS), the combat net radio (CNR) systems, and the Army Data Distribution System (ADDS). The ASAS and the following systems make up the BFACS of the ATCCS:

Maneuver Control System (MCS). The MCS is the primary automated decision support system for the tactical commander and his staff. When completely fielded, MCS will provide the principal operational interface with the force level database and enable access to "common force level information." The system will provide the applications software necessary to access and manipulate the force level information database and provide timely control of current operations. MCS will facilitate the development and distribution of plans and estimates in support of future operations. It will be interoperable with the other BFACSs, Army Brigade and Below (AB^2), and ADDSs like the Enhanced Position Location Reporting System (EPLRS).

Forward Area Air Defense Command, Control, Communications, and Intelligence ($FAADC^3I$). The $FAADC^3I$ system provides automated interface between Forward Area Air Defense nodes and weapon systems. It integrates information provided from other BFACSs, STACCS, and joint and combined theater air defense operations. System applications software supports hostile aircraft cueing to fire units; rapid dissemination and acknowledgement of air battle management control measures and information; exchange, processing, and display of air defense support. $FAADC^3I$ will support control nodes like the Air Battle Management Operations Center, the Army Airspace Command and Control (A^2C^2) cell, the battery tactical operations center (TOC), and the battery command post (CP). $FAADC^3I$ will be interoperable with systems like the Airborne Warning and Control System and Patriot air defense weapon system.

Combat Service Support Control System (CSSCS). The CSSCS provides logistical information to include all classes of supply, field services, maintenance, medical, personnel, and movements to CSS, maneuver, and theater commanders and staff. When fielded, CSSCS will

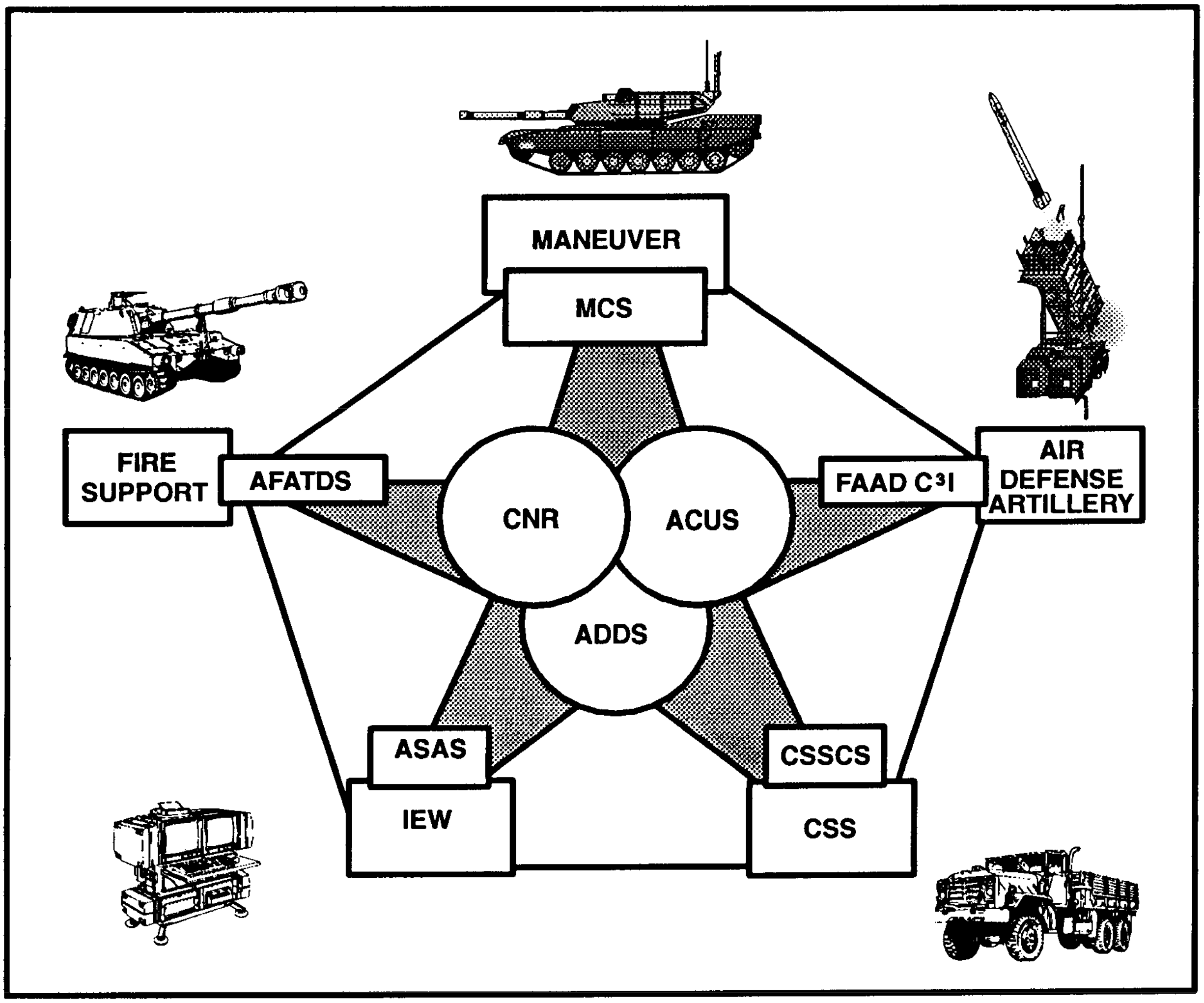


Figure 1-2. Army Tactical Command and Control System (ATCCS).

process, analyze, and integrate resource information to support evaluation of current and projected force sustainment capabilities. The system will interface with Standard Army Management Information Systems and STACCS for multi-echelon sustainment support.

Advanced Field Artillery Tactical Data System (AFATDS). The AFATDS provides automated decision support for fire support operations to include joint and combined fires. AFATDS provides a fully integrated fire support command and control (C^2) system, giving the fire support coordinator (FSCOORD) automated support for the planning, coordination, control, and execution of fires. AFATDS will perform all of the fire support operational functions, to include automated allocation and distribution of fires based upon target value analysis. AFATDS will interface with systems like Tactical Fire Direction System, Firefinder Radar System, and Multiple Launch Rocket System.

ARMY BRIGADE AND BELOW (AB^2) COMMAND AND CONTROL SYSTEM:

The AB^2 architecture is a suite of digitally interoperable, BOS-specific functional applications designed to provide near-real time (NRT) situation information to tactical commanders on the move, down to platoon and squad levels. AB^2 systems will provide the friendly automated positional location information, to include—

- Display of adjacent units to platoon or squad level resolution.
- Current tactical battlefield geometry for both friendly and known or suspected enemy forces.
- Automated situational reporting.
- Calls for fire and close air support.
- Dissemination of graphic and textual tactical orders. AB^2 applications modules will populate the force level information database within MCS at the first CP in the chain of command where full MCS capability is available.

See FM 24-7 for more information on the ABCS.

INTELLIGENCE ARCHITECTURE

The ASAS is a “linchpin” system in forming a seamless intelligence architecture between and across echelons. The architecture can be broken down into three major groups: **sensors, processors,** and **communications** systems. The systems within each group support simultaneous demands for intelligence and targeting information at multiple echelons. They form a seamless intelligence system that supports commanders from tactical through strategic levels anywhere across the range of military operations. Figure 1-3 provides a snapshot of some of the pieces that make up the intelligence architecture.

SENSORS:

Sensors come from a variety of organizations, echelons, services, and intelligence disciplines. METT-T determines the specific mix of sensors or, in a broader sense, collection assets. Types of sensors include but are not limited to—

- **Tactical —** Aeroscouts, Counterintelligence (CI) teams, ground-based IEW systems, military police patrols, scouts, target acquisition radars, and unmanned aerial vehicles (UAVs).

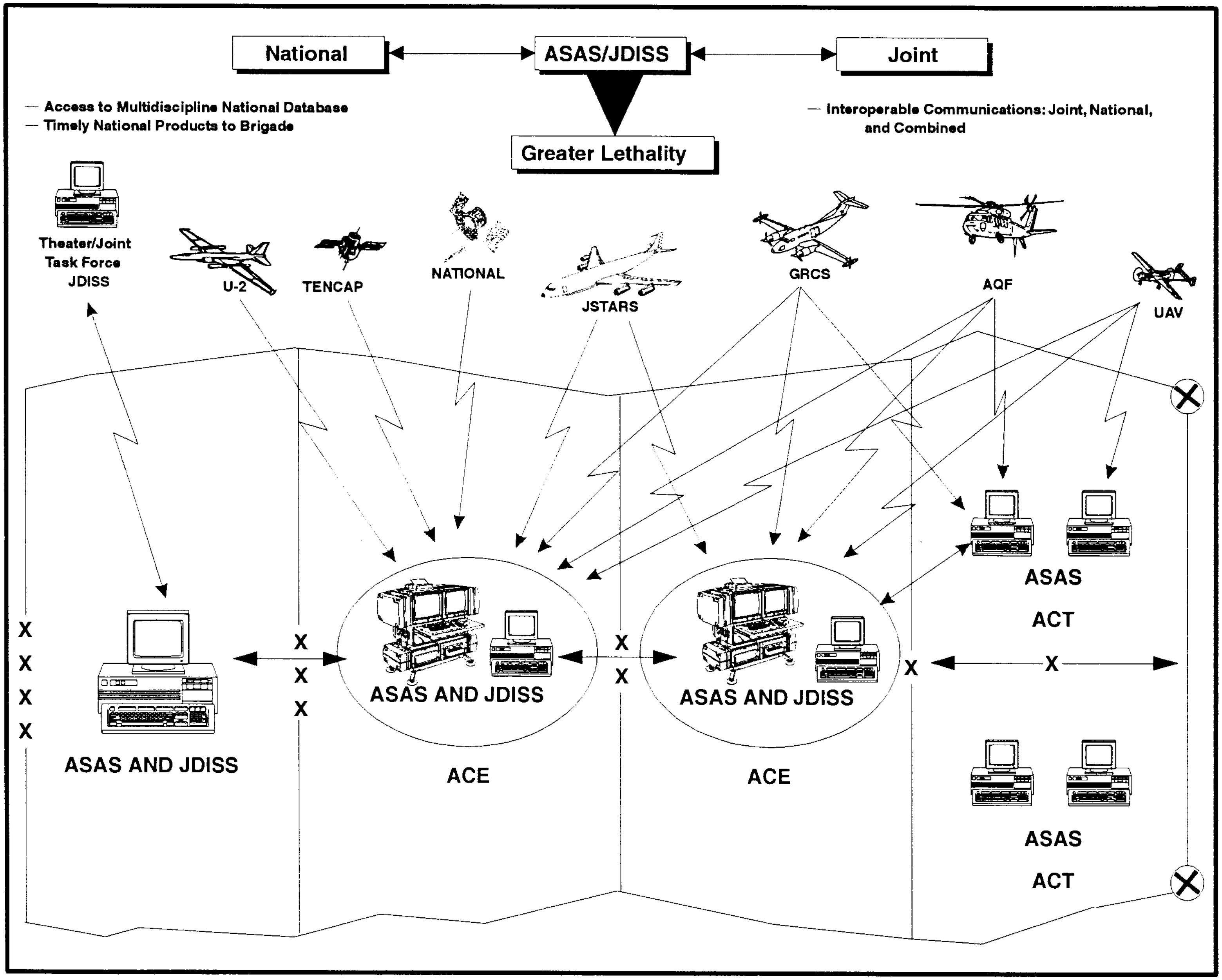

National
ASAS/JDISS
Joint
Greater Lethality
— Access to Multidiscipline National Database
— Timely National Products to Brigade
— Interoperable Communications: Joint, National, and Combined
Theater/Joint Task Force JDISS
U-2
TENCAP
NATIONAL
JSTARS
GRCS
AQF
UAV
X
X
X
X
ASAS AND JDISS
X
X
X
ASAS AND JDISS
ACE
X
X
ASAS AND JDISS
ACE
X
X
ASAS
ACT
ASAS
ACT

Figure 1-3. Intelligence architecture.

- **Operational** — Airborne signals intelligence (SIGINT) systems, Air Force SIGINT/EW aircraft, long-range surveillance (LRS) teams, Navy ship-based SIGINT systems, and joint airborne imagery intelligence (IMINT) systems.

- **Strategic** — Departmental assets of organizations such as the Central Intelligence Agency (CIA), United States Coast Guard, Defense Intelligence Agency (DIA), Drug Enforcement Agency (DEA), and National Security Agency (NSA).

PROCESSORS:

Intelligence processors are information systems that receive, convert, and correlate information into a form usable as combat information or intelligence. These processors are found at all echelons of the intelligence architecture. The majority of intelligence processors support the collection and reporting of perishable combat information. Examples of these processors are the UAV ground control station (GCS) and the GUARDRAIL Integrated Processing Facility (IPF) where raw sensor data is received, converted into video or audio data, and disseminated in an automated reporting format as combat information. Other systems like the Electronic Processing and Dissemination System (EPDS) and Mobile Integrated Tactical Terminal (MITT) provide intermediate or preprocessing of single-discipline intelligence. Intermediate processing of broadcast data and imagery products helps tailor this information to the specific needs of the echelon and mission.

The ASAS, a fusion system, is part of a new generation of processors. At echelons corps and below (ECB), it is the Army's principal intelligence fusion system for acquiring and combining combat information and single discipline intelligence reporting into an all-source picture of the enemy or threat situation. Understanding the distinction between intermediate processing and fusion systems is important in determining processing requirements, means, and responsibilities.

COMMUNICATIONS:

Communications systems provide the link between sensors, processors, and commanders. The G2 (S2) and ACE personnel must be familiar with the full range of communications options available to support their IEW mission and the commander's operation. A variety of communications systems support IEW operations. The ACUS Mobile Subscriber Equipment (MSE) and the CNR Single-Channel Ground Airborne Radio System (SINCGARS) are the primary Army communications systems supporting tactical IEW operations. Systems like the TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) II, the Joint Tactical Terminal (JTT), and the Tactical Intelligence Gathering and Exploitation Relay (TIGER) provide dedicated IEW communications support. The ASAS itself is equipped with a communications control system that provides connectivity into the multiple communications systems described above. The technology experiment that follows describes the potential of the ASAS.

Technology Experiment

24th ID)(M) ACE in Operation DESERT CAPTURE II
National Training Center Rotation 94-07
27 March to 24 April 1994

Enemy vehicles are turning north and filing through a narrow pass called the Bowling Alley. An intercept report from GUARDRAIL the previous night indicated the enemy might use this route–-a route considered to be the least likely enemy course of action (COA). The imagery analyst inside the ACE observes this activity in real-time video on his WARRIOR workstation screen. The video, received from a UAV, is being sent through the UAV GCS through the Joint STARS GSM to the ASAS.

With the GCS collocated with anti landlined into the ACE(-), the ACE imagery analyst directs the UAV pilot at the GCS to follow the vehicle Column. While continuing to observe the video, the ACG analyst types a SPOT report on his workstation and sends it to the analysis and control team (ACT) at the supported brigade over the MSE packet switch network. His assistant uses his WARRIOR terminal to freeze a video frame of the enemy battalion in the pass. He enhances the image, annotates it, and forwards it to the brigade over MSE. The field artillery intelligence officer (FAIO) sends a target report to the brigade fire support element (FSE): “One enemy battalion in engagement area (EA) Bowl.”

As the situation develops, Joint STARS moving target indicators (MTIs) are displayed on the remote display screen (RDS) in the ACE. They show the enemy column turning east out of the Bowling Alley into fhe Valley of Death, then breaking into two columns. The ACE analyst directs the UAV pilot, cued by the MTI, to observe the two columns and conduct a vehicle count. Each column has 40 or more vehicles. Two battalions have moved through the Bowling Alley and are now in the Valley of Death The UAV pilot tracks these lead battalions back to the second echelon battalion which the ACE analyst notes as turning north into the Bowling Alley. The FAIO sends a second report: “Two battalions in EA Valley and one battalion in EA Bowl.“

The entire enemy regiment is now committed to the Valley of Death. The ACE all-source analyst creates a graphic of the situation showing the current location of the three battalions with MTI data and a map background. He sends this picture of the battlefield to the brigade over MSE. SPOT reports, target reports, and graphic reports continue as the ACE follows the enemy out of the Valley of Death, north of the Whale Gap, and into the Red Pass. At each point, the brigade commander has the intelligence he needed to request close air support (CAS) and attack helicopters and to reposition his reserve company to meet the enemy concentration in the Red Pass.

CAPABILITIES

The ASAS is a quantum improvement to automated IEW operations at the operational and tactical levels. Its processing speed substantially increases the analyst's ability to correlate large volumes of information. Once correlated, the analyst can use a variety of software tools to transform the raw information into finished intelligence products. The system's communications software and hardware in turn support the rapid distribution of these products to users throughout the intelligence system. In the hands of a trained intelligence crew, supported by proper planning and adequate communications, the ASAS can provide commanders with the edge needed to win the information war.

PROCESSING SPEED:

ASAS automated information management capability eases many of the information choke points caused by time-consuming manual processing of information. ASAS can process the majority of inbound intelligence messages and update its all-source correlated database (ASCDB) on enemy units, weapon systems, and locations automatically. Trained analysts use ASAS to—

- Quickly correlate information from multiple sources.
- Provide timely enemy situation updates to the common picture of the battlefield.
- Compare new information to reports already in the database.
- Rapidly identify and nominate potential targets.
- Develop and release time-sensitive intelligence reports.

FLEXIBILITY:

The ASAS provides robust operational flexibility through its modular hardware and software design. This capability allows the G2 (S2) and ACE to—

- Perform IEW operations in peace, war, and operations other than war (OOTW).
- Tactical tailor ACE assets accompanying entry and follow-on forces.
- Support split-based intelligence operations.

ANALYSIS TOOL:

The ASAS is a powerful toolbox for the Ml soldier. The system **cannot** perform analysis but in can help make a good analyst better and more productive. Specifically, the ASAS provides the analyst—

- Automated tools that assist in both all-source and single-discipline analysis.
- A dynamic, rapidly correlated, multisource, multidiscipline, relational database linked to an organic communications center.

- A capability to develop message alarms that automatically notify the analyst when critical time-sensitive information arrives.

- A database query capability that uses criteria such as time, location, activity, equipment, call signs, or frequencies to retrieve and correlate data.

- An automated reference file, read file, message journal, order of battle (OB) workbook, and reference material.

- A graphic display of reports, results of database queries, and intelligence preparation of the battlefield (IPB) products.

AUTOMATED COMMUNICATIONS:

Historically the dissemination of combat information and intelligence products was hampered by communications bottlenecks and manual recording procedures. The ASAS communications software supports automated message processing and the conversion of a number of communications protocols. These capabilities facilitate—

- Downward flow of taskings, intelligence, and technical data to subordinate IEW assets.

- Upward flow of combat information, intelligence, and requests for information to higher echelons.

- Lateral flow of intelligence and coordinating instructions.

- Recording, sorting, filing, and monitoring inbound and outbound message traffic.

- Interoperability with joint and national IEW systems, databases, and communications.

LIMITATIONS

The ASAS is not a collection system and does not produce intelligence. it changes and automates the mechanisms by which trained soldiers perform analysis and direct IEW operations. The ASAS—

- Cannot evaluate information, develop intelligence requirements, task IEW assets, or produce intelligence. These remain the responsibilities of the commander and his intelligence personnel.

- Cannot perform automated tasks for which the technology is not available or compatible.

- Requires assured communications to support automated all-source intelligence fusion and dissemination.

- Like any equipment, depends on electrical power and is subject to the affects of adverse environmental conditions.

Chapter 2

ANALYSIS AND CONTROL ELEMENT

On the modern battlefield, the commander has access to an ever-growing volume of information from which to assess the situation and lead his command. He must quickly assimilate this information in order to influence the outcome of the operation; prioritize and allocate resources; assess and take risks; and understand the needs of higher and subordinate commanders. The commander depends upon a skilled G2 (S2) working within his intent to effectively direct and control his IEW effort. The ACE equipped with the ASAS is the G2's (S2's) primary organization for controlling IEW operations and producing intelligence.

MISSION

The mission of the ACE is to perform collection management; produce all-source intelligence; provide IEW technical control; and disseminate intelligence and targeting data. The ACE supports the commander in executing battle command and planning future missions across the range of military operations.

ORGANIZATION

The ACE integrates the missions, functions, and resources of the former technical control and analysis element (TCAE) and TOC support element (TOCSE) at corps, division, separate brigade, and ACR. At theater Army, the ACE replaces the Echelons Above Corps Intelligence Center (EACIC) and the TCAE. As the ACT, it replaces the IEW support element (IEWSE) and improves support at the divisional maneuver brigade. The ACE centralizes analysis and collection management in one organization under the operational control (OPCON) of the G2 (S2). The formation of the ACE goes beyond consolidation or collocation. The ACE provides balance to all-source analysis products and synergy to the execution of CI, human intelligence (HUMINT), IMINT, and SIGINT operations.

THEATER ARMY:

At theater Army, the ACE is organic to the operations battalion of the theater Army MI brigade. Under the direction of the theater Army G2, it works closely with the theater Joint Intelligence Center (JIC) to support the ground forces intelligence requirements of the theater Army commander and subordinates. The theater Army ACE is an integral element in IEW support to joint operations and the subordinate ground component. It supports the G2, and subordinate Army Force (ARFOR) by maintaining and deconflicting the theater's databases on contingency area threat ground forces. The ACE, like the JIC, is an all-source intelligence center that gathers and disseminates intelligence in response to the commander's requirements. In war or OOTW, the ACE complements the JIC and, with service component augmentation, can become the joint intelligence element of a joint task force (JTF). The common features of the ACE and JIC contribute to effective joint intelligence support of ARFOR units in war and OOTW.

See FM 34-37 and FM 100-7 for more information on theater Army IEW operations.

CORPS:

The corps ACE develops all-source intelligence needed to support corps contingency planning and operations. The ACE is organic to the operations battalion of the corps MI brigade although under the OPCON of the corps G2. The scope of corps ACE operations differs from those at lower echelons, although the basic process remains the same. The ACE links into a network of specialized single discipline intelligence collection assets and processors. The mix of these systems and access to joint intelligence activities are tailored to the specific demands of the operation and availability of resources.

Corps Military Intelligence Support Element (CMISE). The CMISE from the theater MI brigade provides the corps G2 and ACE with an expanded and flexible intelligence capability. Its soldiers form a team of experts familiar with corps, theater, and national intelligence systems and structures. Fully integrated into ACE operations, the CMISE provides the corps greater access to the EAC intelligence and can serve as its intelligence support base during exercises and split-base operations. Some CMISE functions are—

- Serves as a bridge between the corps and EAC intelligence organizations.
- Expands the number of regions or countries the corps ACE can monitor and provides an operational intelligence capability focused on the commander's requirements.
- Provides continuity of operations by monitoring the corps area of interest (AI) while the ACE focuses on priority contingency areas or exercises.

See FM 34-25 and FM 100-15 for more information on corps IEW operations.

DIVISION:

The ACE is organic to the Headquarters, Headquarters and Operations Company (HHOC) of the divisional Ml battalion. OPCON to the division

G2, the ACE supports the commander's all-source intelligence and targeting requirements. The ACE is the focal point for the division's IEW collection management and synchronization effort. The division ACE works closely with the MI battalion TOC to accomplish this effort. In coordination with the G2 plans and operations sections, the ACE performs requirements management, mission management, and technical control of IEW assets. The MI battalion commander performs asset management in accordance with the division commander's orders, the G2's direction, and the technical control of the ACE.

See FM 34-10 and FM 71-100 for more information on division IEW operations.

MANEUVER BRIGADE:

The ACT expands the mission, functions, and resources formerly found in the IEWSE and MI company team. The ACT is organic to the direct support (DS) MI company and normally collocates with the company CP at the brigade TOC. Unlike the ACE at higher echelons, the ACT is not normally under OPCON of the brigade S2. Under the direction of the DS MI company commander, the ACT provides the brigade S2 automated intelligence processing, analysis, and dissemination capabilities. In addition, the MI company commander uses the ACT to support asset management and reporting of subordinate CI, HUMINT, and IMINT teams. The ACT uses its ASAS workstation to access databases, reports, graphics, and other products at higher echelon organizations, primarily the division's ACE. When augmented with the TROJAN SPIRIT, the ACT can conduct split-based operations, "pulling" support from an intelligence support base outside the AO.

See FM 7-30, FM 34-10, FM 34-80, and FM 71-3 for more information on brigade IEW operations.

SEPARATE BRIGADE AND ARMORED CAVALRY REGIMENT:

The ACE integrates the missions, functions, and resources formerly found in the TCAE of the MI company and TOCSE of the separate brigade and ACR. The ACE is organic to the Ml company of the ACR or separate brigade. Although smaller in size, the mission of the ACE at the ACR and separate brigade remains the same as those at higher echelons. Under the OPCON of the S2, it performs collection management; produces all-source intelligence; provides IEW technical control; and disseminates intelligence and targeting information.

See FM 7-30, FM 17-95, FM 34-35, and FM 71-3 for additional information on separate brigade and ACE IEW operations.

STRUCTURE

The ACE is organized on the tables of organization and equipment (TO&E) of the theater MI brigade, corps MI brigade, divisional MI battalion, separate brigade MI company, and ACR MI company. It consists of a headquarters element, technical control and processing section, and an all-source intelligence section. Variations to this base ACE organization may occur based on echelon and mission. The remainder of this chapter describes the division ACE and provides a common reference for ACE operations at all echelons. Figure 2-1 outlines the A-series TO&E for the division ACE.

HEADQUARTERS ELEMENT:

The ACE headquarters element exercises overall supervision of current and future ACE operations. The ACE chief is a key player in ensuring the ACE focuses on and synchronizes IEW with the commander's concept of operation and his intelligence requirements. The headquarters is also responsible for ASAS communications control set (CCS) and TROJAN SPIRIT communications.

ALL-SOURCE INTELLIGENCE SECTION:

The all-source intelligence section consists of four major teams: all-source production, collection management, target nomination, and dissemination. In this section, analysts perform situation development, IPB, ASCDB maintenance, target development, force protection, battle damage assessment (BDA), and collection management. This section is also responsible for coordinating processing and communications support from subordinate Joint Surveillance Target Attack Radar System (Joint STARS) ground station module (GSM) and MITT teams.

TECHNICAL CONTROL AND PROCESSING SECTION:

The technical control and processing section consists of three subordinate analysis teams: SIGINT, HUMINT and CI, and IMINT. In this section, analysts perform processing, analysis, reporting, and database management by intelligence discipline or function. The section—

- Interacts with higher and lower intelligence organizations to focus analysis and access databases.
- Uses automation to develop databases for technical control and support to all-source analysis.
- Provides technical support and control of subordinate collection assets.

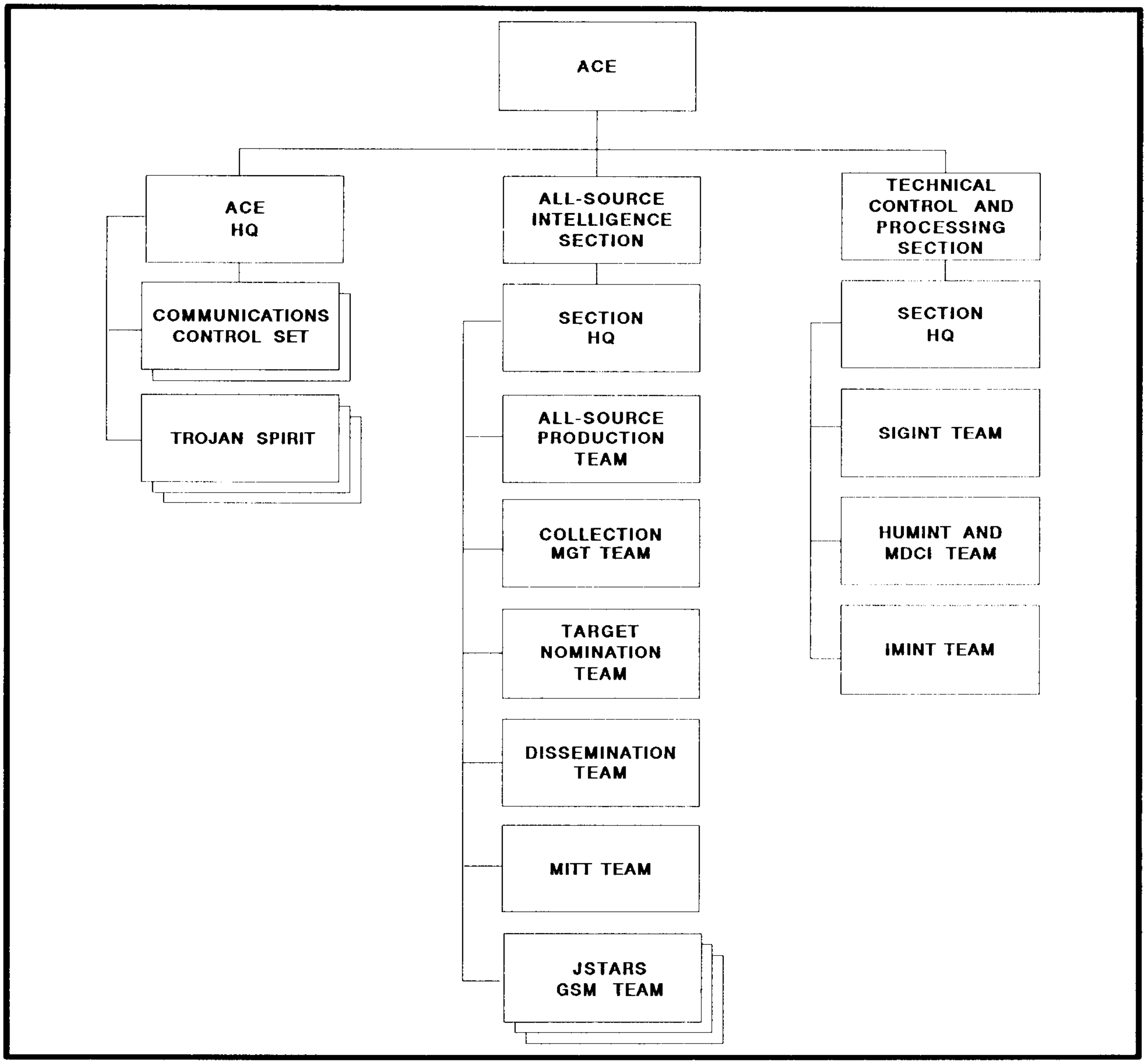


Figure 2-1. Analysis and Control Element (division, A-series base TO&E).

- Provides technical support to the collection management team, electronic warfare officer (EWO), and subordinate EW systems.

RESPONSIBILITIES

ACE operations are a team effort that depend on each soldier performing his tasks to the best of his ability and supporting the work of others. From analyst to leader, each has a responsibility for ensuring the commander is effectively supported by the Intelligence BOS. Some areas of emphasis include control and synchronization, intelligence production, and targeting. These areas and their associated key personnel are described below:

CONTROL AND SYNCHRONIZATION:

The ACE supports the integration, control, and synchronization of the commander's intelligence effort. The G2 (S2), MI commander, ACE chief, and ACE collection manager are key players in planning and executing IEW operations. They ensure IEW operations support the commander's requirements, provide situational awareness, and support targeting.

G2 (S2). As the senior intelligence officer, the G2 (S2) directs the commander's intelligence effort and exercises operational control of the ACE. As the ARFOR G2 (S2), he is responsible for establishing, reconciling, and maintaining the ARFOR'S primary "ground truth" database on threat ground forces. The G2 (S2)—

- Provides the ACE with a "window" into command and staff operations.

- Assists the MI commander and ACE chief in understanding the commander's planning, operational, and targeting requirements.

- Brings key players together to produce a coordinated, focused IEW effort.

- Has the responsibility for establishing intelligence database quality control procedures and access privileges.

MI Commander. The MI commander plans and directs the employment of his subordinate IEW assets. He must understand the supported commander's intent and priority intelligence requirements (PIR), operational or tactical objectives, overall scheme of maneuver and fire, and intelligence collection plan to effectively employ his IEW assets. The MI commander may be frequently absent from his command post to coordinate with the G2 (S2) and personally oversee the IEW operations of subordinates. He therefore relies on his S3 to supervise the TOC and execute asset management of unit IEW assets to include supporting or reinforcing assets. The S3 works closely with the ACE to ensure IEW assets are effectively employed and provided ACE technical support needed to execute the mission.

ACE Chief. The ACE chief focuses and prioritizes work, supervises interaction between sections, and task organizes the ACE resources to meet analytic demands. He is responsible to the G2 (S2) for producing timely, relevant, accurate, and predictive intelligence which answers the commander's PIR. The ACE chief accomplishes his mission by evaluating and tracking requirements, focusing the collection and analysis effort, and reviewing ACE products for quality and timeliness. He is supported by a staff of officers, warrant officers (WOs), and noncommissioned officers (NCOs) who supervise the production and dissemination of intelligence, targeting information, and technical data. Along with his collection manager, the ACE chief interacts with the G2 (S2) and MI commander to ensure synchronization of IEW support with the commander's operation.

ACE Collection Manager. The ACE collection manager supervises the requirements and mission management portions of the collection management and synchronization process. This requires close working relationships with the G3 (S3) section, the MI unit, and other ACE teams to ensure the collection and synchronization plan is dynamic and linked to the fire support and operations plans. Figure 2-2 shows the basic steps of the collection management process used to control and synchronize IEW operations. Some of the collection manager's responsibilities include—

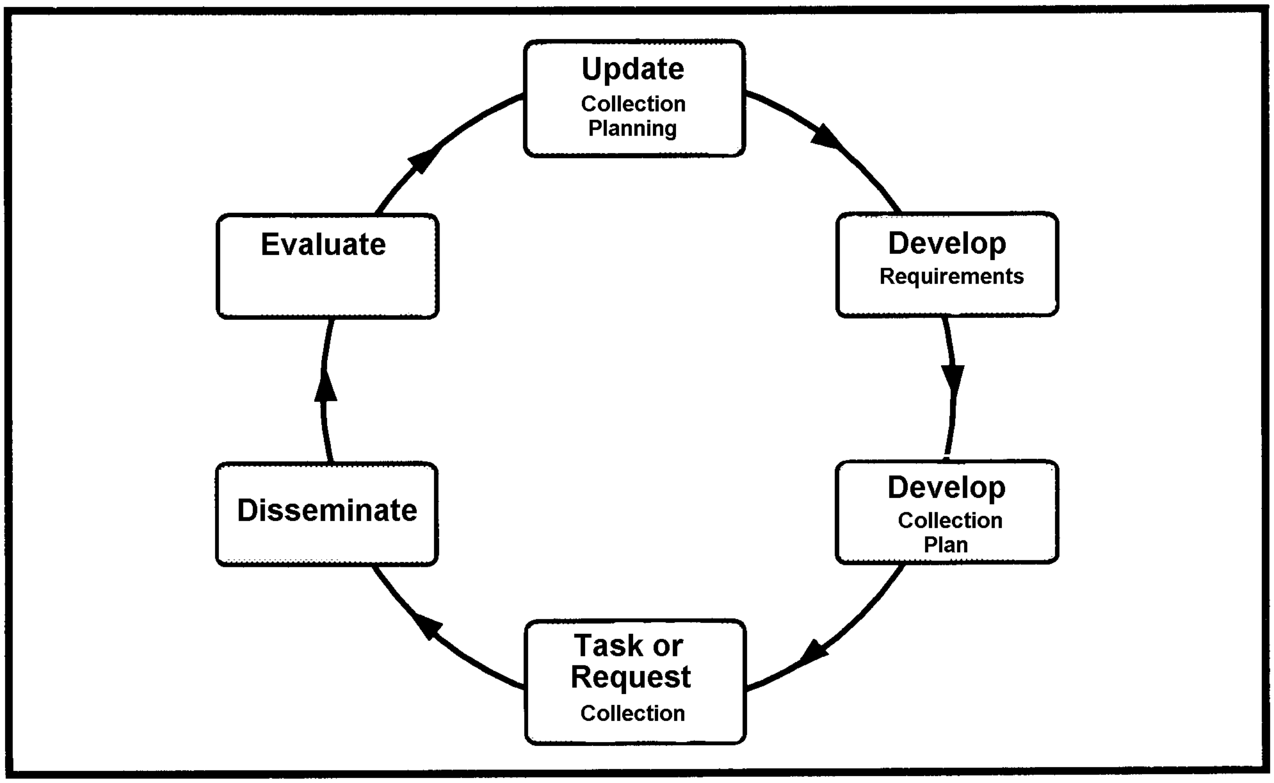


Figure 2-2. Collection management process.

- Identifying the specific information requirements (SIR) necessary to satisfy each PIR and to support subordinate unit reconnaissance and surveillance (R&S) plan.

- Using the SIR to develop the collection plan and specific orders and requests (SOR).
- Working with the MI unit and other collection managers to determine the availability and capability of IEW assets to execute the collection plan.
- Using the intelligence synchronization matrix (ISM) to ensure collection, processing, analysis, and dissemination are in concert with the commander's operation.

See FM 34-1, FM 34-2, and FM 101-5 for information on staff and command intelligence responsibilities, collection management, and synchronization.

INTELLIGENCE PRODUCTION:

All-source intelligence production is the heart of the ACE. In the ACE, production is a single, integrated system that merges often separated activities of single-discipline analysis, all-source analysis, database development, and technical control. Within the ACE, the "battle captain" keeps supervisors and analysts focused on the commander's PIR and the IEW effort synchronized with the commander's operations. The analysis elements gather information from multiple echelons and sources to produce intelligence products and technical data that meet the commander's maneuver, targeting, BDA, and other IEW support requirements. Figure 2-3 depicts the basic steps of the all source intelligence production process.

Battle Captain. The battle captain supervises the ACE analysis, target nomination, collection management, technical control, and dissemination operations during his shift. As a key leader within the ACE, the battle captain ensures subordinate supervisors and analysts are focused on the commander's PIR and synchronized with the command's operations. He accomplishes his duties by retaining personal mobility within the ACE, communicating with ACE personnel and other staff elements, and maintaining situational awareness within the ACE. His ability to move freely within the ACE helps him to focus the ACE and apply his knowledge and experience where it can be most beneficial.

All-Source Intelligence Section Chief. The all-source intelligence section chief oversees the all-source intelligence fusion, target nomination, collection management, and dissemination responsibilities of the ACE. He coordinates the efforts of his section with other elements such as the engineer terrain team and the Air Force weather team. During operations,

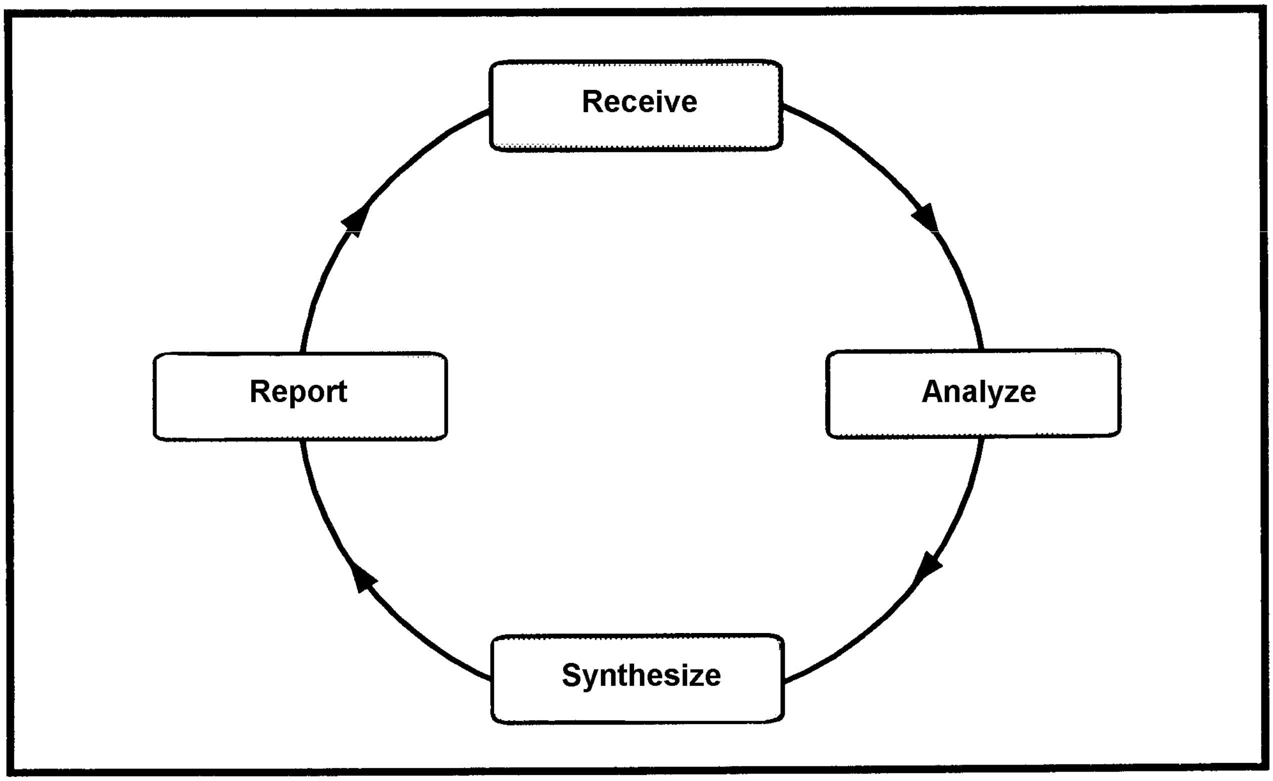


Figure 2-3. Production process.

the section chief serves as a shift supervisor and, in that capacity, is referred to as the ACE battle captain.

Technical Control and Processing Section Chief. The technical control and processing section chief supervises single-discipline intelligence production and technical supped to SIGINT and EW operations. He works closely with the all-source intelligence section to maintain situational awareness and to ensure availability of single-discipline products and technical support. During operations, the section chief serves as a shift supervisor on the shift opposite the all-source intelligence section chief and executes those battle captain duties described above.

See FM 34-3 and FM 34-130 for additional information on analysis and IPB.

TARGETING:

Key players in IEW support to targeting and target development are the G2 (S2), the FAIO, and the EWO. Supported by the ACE target nomination team, they work with other ACE sections and staff elements of the command to support the targeting process. Interaction by the ACE with the fire support cell and deep operations coordination cell (DOCC) is essential to effective IEW support to targeting for both lethal and nonlethal fires.

G2 (S2). As a member of the targeting team, the G2 (S2) or his representative uses intelligence, particularly IPB products, to identify decisive points and enemy high-value targets (HVTs). These HVTs are reduced during the targeting process shown in Figure 2-4 to a set of high-payoff targets (HPTs). The G2 (S2) works with the G3 (S3) and fire support officer (FSO) to develop a BDA methodology that evaluates the success of the commander's operational and targeting actions. He advises the commander and FSO on the capability of IEW assets to acquire and track HPTs as well as evaluate battle damage information on HPTs previously designated as PIR.

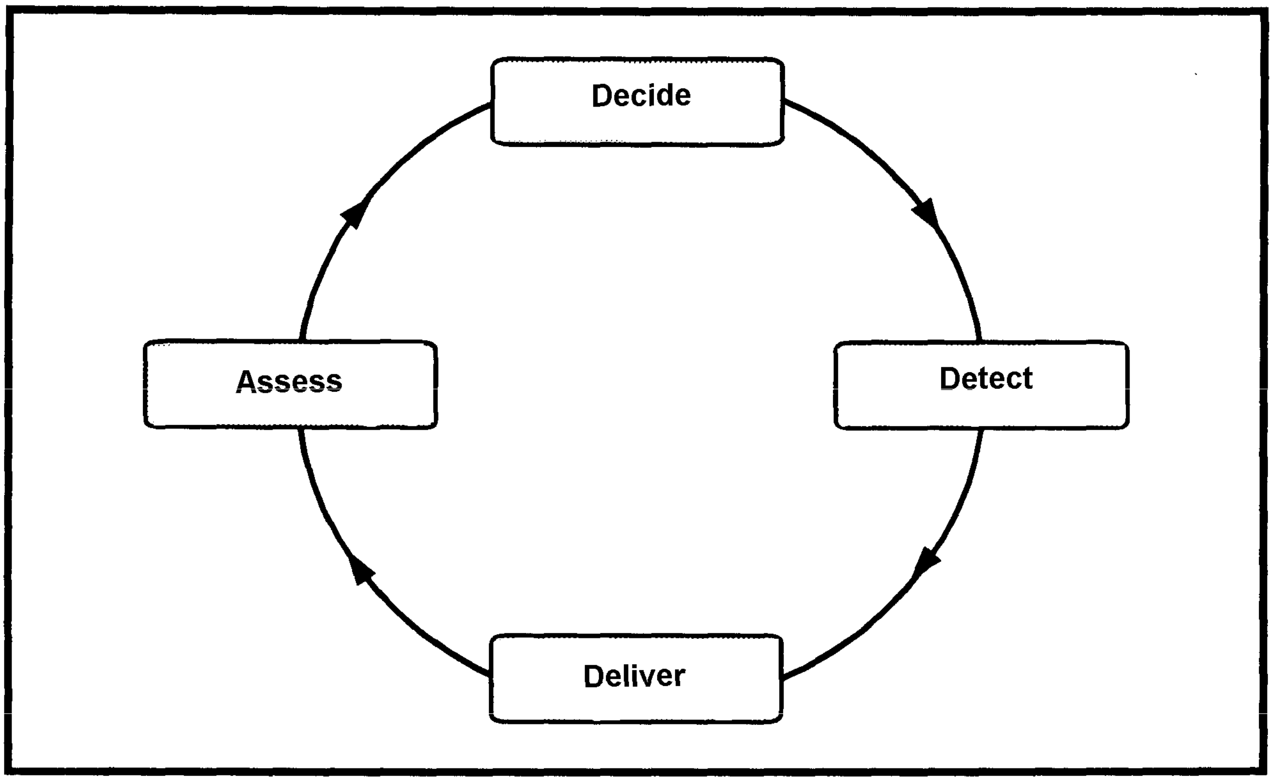


Figure 2-4. Targeting process.

Field Artillery Intelligence Officer. The FAIO is an important liaison between the ACE and the fire support cell. He provides the ACE with a detailed understanding of the targeting process, attack system information requirements and target acquisition system capabilities. The FAIO works with the ACE to develop an intelligence collection plan that supports targeting and BDA related PIR. During operations, the FAIO helps the ACE identify and nominate potential targets to the fire support cell.

Electronic Warfare Officer. The EWO is the focal point for planning and managing EW operations. He works closely with the G3 (S3), FSE, and

DOCC to ensure EW assets are properly allocated and synchronized with the scheme of fire and maneuver. The EWO works with the ACE, specifically the collection manager, to develop EW tasking for subordinate or nonorganic EW assets capable of executing his EW plan. He also works with the command's signal officer to reduce the possibility of electronic fratricide.

See FM 34-2, FM 34-3, FM 34-40-7, and FM 6-20-10 for additional information on IEW support to targeting and the targeting process.

FORCE PROJECTION OPERATIONS

The G2 (S2) and the ACE capitalize on the flexibility and power of the ASAS to support the commander's IEW requirements in peace, war, and OOTW. The ACE chief configures the ACE and components of the ASAS to provide seamless uninterrupted intelligence support from predeployment through redeployment stages of a force projection operation. Throughout the operation, the ACE uses its ASAS to update databases, develop intelligence products, disseminate intelligence, and control IEW operations.

MOBILIZATION AND PREDEPLOYMENT:

After alert or activation of the contingency plan, the G2 (S2) surges the intelligence effort to support the commander's decision making, fill information voids, refine intelligence products, and prepare the initial entry IEW support. During mobilization and predeployment stages, the ACE exchanges information and databases with other intelligence organizations at higher and lower echelons. In particular, the ACE draws on the resources and databases of the theater Army ACE. If not already in place, the ACE establishes connectivity and database access with other service, joint, national, and RC intelligence activities that collect against or possess information on the contingency area. ***The connectivity and database access established or refined during this stage is essential to the success of initial top-down intelligence support and split-based intelligence operations.*** At all echelons, the ACE operates from garrison sites and maintains communications with higher and subordinate units. This stage includes the detailed planning, RC integration, mission-focused training, and initial tactical tailoring that will lead to successful IEW support to the force projection operation.

DEPLOYMENT:

During the deployment stage, key intelligence personnel and equipment are placed into the deployment flow early. The ACE of the next higher echelon to the deploying force normally forms the intelligence support base. This allows the deploying force to send a Deployable Intelligence Support Element (DISE) with the initial entry force and to continue preparing the remainder of its ACE for movement without compromising intelligence support to the commander. The DISE provides immediate split-based intelligence support to the assault command post. The remainder of the deploying G2 (S2) staff and ACE locate with the rest of the primary staff at the staging base. Throughout the deployment stage, the DISE and units in movement receive continuous support from the intelligence support base.

Intelligence Support Base. An ACE normally forms the intelligence support base of a split-based operation. The intelligence support base allows the deployed commander to pull from his habitual peacetime sources and complements support from in-theater joint intelligence elements. During the early stages of force projection, split-based operations reduce the possibility of intelligence shortfalls which could arise from reliance on deploying intelligence organizations and evolving communications architectures. The support base is responsive to the needs of the deployed commander and G2 (S2) yet is not intended to circumvent the joint intelligence channels or levy taskings beyond its organic assets. The extent and duration of split-based intelligence support must be consistent with and supportive of the theater or JTF J2's overall intelligence plan. As the JTF commander's senior intelligence officer, the J2 is responsible for theater or JTF intelligence operations and support to subordinate forces.

Deployable Intelligence Support Element. A DISE is an integral part of IEW support to force projection operations. it is not a permanent organization, specific unit, or quantity of equipment but a tactically tailored support team, uniquely configured for each operation. It provides the deployed commander with assured intelligence support by augmenting his intelligence staff with the communications, automated intelligence processing, and broadcast downlink systems needed to execute split-based intelligence operations. Split-based operations provide the commander with access from his forward deployed command post to his intelligence support base outside the area of operation (AO). As the forward element of the ACE, the DISE is normally the foundation on which a full ACE is formed after the lodgement is secured and follow-on operations begin.

When using the split-based configuration, planning for communications connectivity and early deployment of a DISE are essential. The DISE is kept small enough to allow its deployment with the initial entry force. Once alerted, DISE personnel upload appropriate databases and map products needed to support the entry force. This material comes from the intelligence support base, theater Army ACE, or, if necessary, directly from national databases for short notice deployments.

One possible configuration for the DISE accompanying the entry force consists of a TROJAN SPIRIT to provide a long haul communications capability, an ASAS workstation for automated intelligence fusion, and a Joint STARS GSM for collateral broadcast intelligence capability. In another configuration, the DISE could consist of a manportable tactical satellite terminal, a laptop computer running ASAS software, and a UAV remote video terminal (RVT). The exact configuration of a DISE is tactically tailored based on METT-T.

ENTRY OPERATIONS:

Deploying forces will make either an unopposed or forcible entry. The commander will rely heavily on intelligence to support the initial lodgement during entry into the AO. He must know what his forces will encounter upon arrival and on the way to achieving initial objectives. If a brigade is the initial entry force, the S2, the battlefield information control center (BICC), and the ACT should deploy with the brigade command element. The S2 and BICC are essential to planning and directing the brigade's IEW support. The ACT from the brigade's DS Ml company is equipped with ASAS workstations needed to provide seamless intelligence support to the brigade commander. In the lodgement, the brigade ACT works closely with the DISE of the division assault command post to support IEW operations and facilitate enemy situation development. The brigade commander receives intelligence from the ACT through ASAS workstations in his TOC or mounted in brigade command vehicles.

OPERATIONS:

During combat operations, the ACE is located with the main command post and, if possible, adjacent to the G2 (S2) cell. Connectivity can be established between the ACE and the command post through MSE and local area networks (LANs). Once the ACE becomes operational, the DISE is melded back into the ACE. It is also during this stage that intelligence reaches a crossover point where dependency on top-down intelligence is reduced by intelligence derived from in-theater tactical IEW assets. This transition increases the demands on ACE collection management and technical control as organic collectors become operational.

In OOTW, the ACE may not deploy to the AO. Its deployment is based on METT-T and the ability of split-based intelligence operations to support the commander. The IEW resources provided for an OOTW, such as humanitarian relief, could consist of a maneuver brigade, Cl and HUMINT teams from the DS Ml company, and an ACT augmented with a TROJAN SPIRIT. In larger operations such as peacekeeping, a division may deploy a DISE to support a division forward command post.

WAR TERMINATION AND POSTCONFLICT OPERATIONS:

During termination and postconflict operations, the ACE adapts to the changing intelligence requirements of the commander. Because of the possibility of renewed hostilities or other action which could jeopardize military personnel, the commander may place emphasis on indications and warnings (I&W) and force protection products. The ACE must also remain prepared to provide immediate support if combat resumes. ACE readiness includes file maintenance to eliminate unwanted or outdated material accumulated during the operation, and analyst cross-training. The priority for ACE intelligence production efforts may also shift to support postconflict operations such as rebuilding infrastructure, providing medical assistance, and clearing obstacles.

REDEPLOYMENT AND RECONSTITUTION:

During this stage, the G2 (S2), MI commander, and ACE chief determine the sequence and composition of redeployment. In general, ACE personnel and equipment redeploy in reverse order to which they deployed. A DISE or scaled-down ACE will remain in theater until all forces are withdrawn. As the quantity and availability of IEW resources decrease, the G2 (S2) and ACE must remain proactive in coordinating and planning IEW support to meet the commander's mission. The G2 (S2) and MI commander should also use this time to record lessons learned from the operation and incorporate them into standing operating procedures (SOPs).

DEMOBILIZATION:

During demobilization, RC personnel supporting the ACE are released from active duty. The ACE reestablishes its normal peacetime relationship with RC units.

See FM 34-1, FM 100-5, FM 100-17 for additional information on force projection operations, mobilization, deployment, redeployment, and demobilization.

Chapter 3

EQUIPMENT

The ASAS consists of government-furnished equipment (GFE) and nondevelopment items. These components support the execution of IEW tasks, collection management, analysis, and dissemination. The ASAS hardware and software also provide compatible interfaces between the ASAS and other automated information systems.

ASAS BLOCK I

The ASAS Block I consists of six major groups of equipment: remote workstations (RWSs), all-source workstations (ASWs), single-source workstations (SSWs), CCSs, DPSs, and supplementary equipment, electronic (SEE) sets. Together, these groups form an integrated system capable of supporting G2 (S2) and ACE operations. Figure 3-1 shows all the major components of the ASAS Block I, except the SEE.

REMOTE WORKSTATION:

The ASAS Block I is an integrated assembly equipped with two ASAS-RWSs. Each workstation, as shown in Figure 3-2, is a portable, ABCS CHS computer workstation. Non-ACE intelligence organizations use the ASAS-RWS to maintain collateral security level databases and threat situational awareness. The workstation also provides the primary interface between ASAS and the other systems of the ABCS. It can send, receive, and modify products to support dissemination and use by other staff elements. The ASAS-RWS supports wargaming, planning, and situation development. It provides—

- The IEW interface between the sensitive compartmented information (SCI) ASAS workstations in the ACE and the collateral security level ABCS.

- Access to automatic updates from the collateral security level ASCDB of the ASAS-ASW in the ACE.

- An automated interface between the ACE and staff elements in the command post, to include maintaining IEW, enemy, and related portions of the force level information database.

System Software. The system software provides the UNIX operating system, security and control mechanisms, system services,

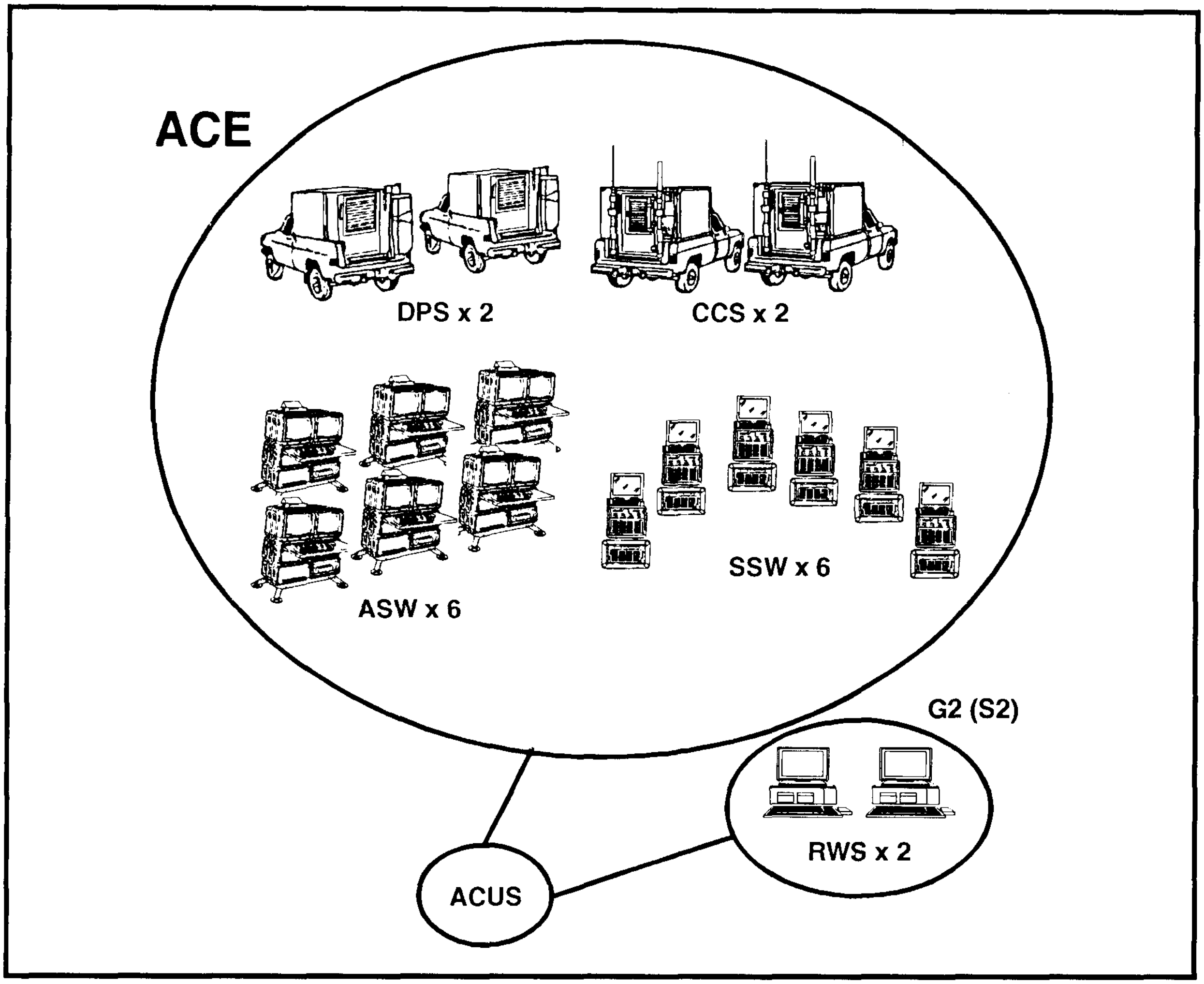
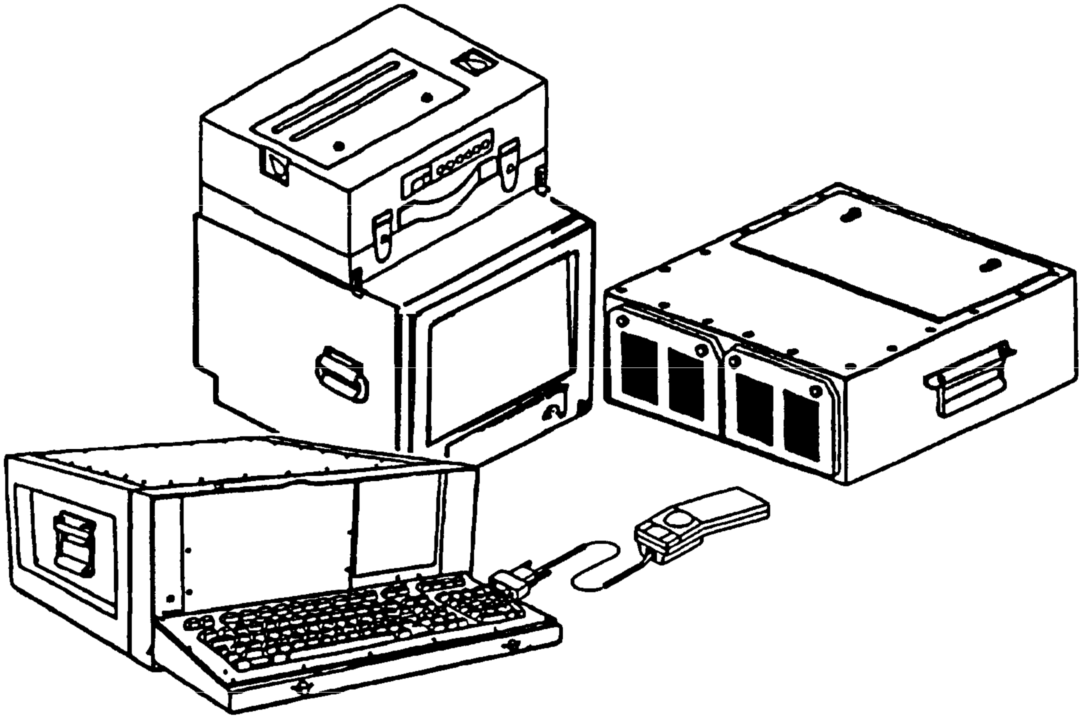


Figure 3-1. ASAS Block I.

human-machine interface, and system utilities required to support the use of the applications and communications software.

Communications Software. The communications software provides the message level interface with other ABCS workstations and systems. It provides a set of functions to create, modify, transmit, receive, and archive messages. It uses standard formats, such as the United States Message Text Format (USMTF) for the exchange of databases or graphics. The software supports LAN and wide area network (WAN) connectivity.

Applications Software. The applications software provides an automated planning tool and a database of current threat information. These support the development of intelligence products and information used in the decision making and targeting processes. Its strength is its ability to create,



Components:
- 1.44 MB floppy disk drive
- 200 MB removable HDD
- CD-ROM drive
- Magneto optical drive
- Mouse
- Keyboard
- Color monitor
- Processor
- Printer

Characteristics:
- Uses UNIX operating system
- Interfaces via ethernet LAN or communications port

Figure 3-2. Block I RWS.

manipulate, and plot graphics, to include IPB templates and COA overlays developed during wargaming. The applications software—

- Provides the G2 (S2) automation support to planning and current operations.
- Maintains the collateral version of the ASCDB maintained in the ACE.

- Maintains IEW partitions of the force level information database and performs force level coordination between other elements of the ABCS.

- Supports the presentation and dissemination of secondary imagery.

ALL-SOURCE WORKSTATION:

The ASAS Block I is equipped with six AN/TYQ-37(V)5, ASAS-ASWs. The ASAS-ASW shown in Figure 3-3 is a ruggedized, portable, dual-screen computer workstation. Its design supports multidiscipline intelligence fusion. The strength of the ASAS-ASW is its ability to correlate and combine multiple reports about the same target, unit, or activity. The all-source analyst sets system parameters that automatically correlate information based on time, location, and level of identification.

The ASAS-ASW stores current threat data in a single relational database, the ASCDB. Many types of messages can automatically update the ASCDB which the ASAS-ASW can then graphically display. It can automatically transmit these updates on a recurring basis to other ASAS workstations including those in other units. Analysts can also set various types of event alarms so critical information comes to their attention immediately.

System Software. The system software provides the Virtual Address Extension (VAX) operating system, system services, human-machine interface, and operating supervision needed to link the applications and communications software to the host processors. System software functional identities (FIs) include—

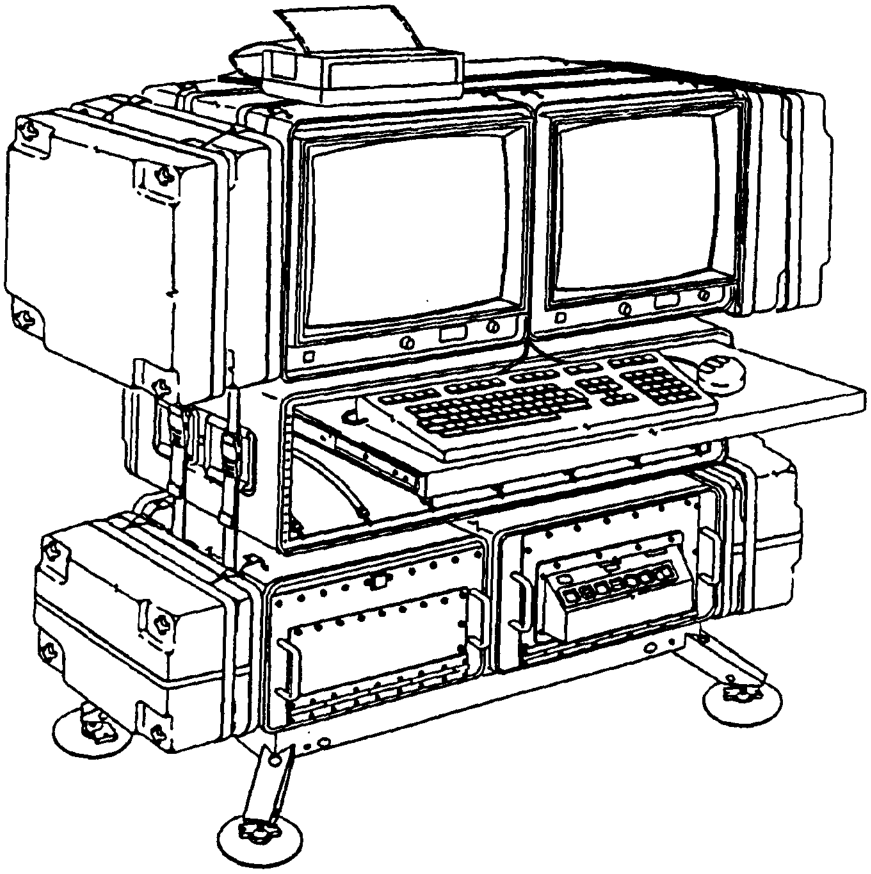
- **Automatic data processing (ADP):** ADP enables periodic backups and restores the backups if an online system is lost.

- **Functional manager (FMR):** FMR provides message routing, normalization of terms, communications monitoring, reference databases loading, and parsing table maintenance.

- **Operational diagnostics (OPR):** OPR provides an online diagnostic check of the system during operations. OPR is designed to verify operational readiness of the hardware and isolate failures in the ASAS.

- **Security audit trail (SAT):** SAT provides a mechanism to back up and store transaction information to an optical disk for security audit purposes.

- **System supervisor (SPV):** SPV configures, initializes, and monitors the system; establishes communications patterns; and maintains analyst accounts.



Components:
512 per side ODD
Mouse
Keyboard
Two high resolution color monitors
Processor
Printer
Five two-person lift components in transit cases

Characteristics:
Uses VAX operating system
Interfaces via fiber-optics LAN or synchronous communications ports
Output to large screen displays and large format map plotter
Uses optical disk cartridge or HDD for map image retrieval media
Act as an intelligent terminal for the DPS

Figure 3-3. Block I ASW.

Communications Software. The communications software provides message interfaces between applications software, analyst functions, external data sources, and users. It is capable of receiving and distributing messages within the ASAS, and distributing and supporting security release of messages leaving the ASAS.

Applications Software. The applications software supports the analysis and processing of intelligence data. It includes machine functions and operator machine-assisted functions for processing and collecting intelligence data. Applications software FIs include—

- **All-source analysis (ALL):** ALL supports message parsing and correlation, all-source processing and analysis, and all-source database maintenance.

- **Intelligence collection management (lCM):** ICM supports unique collection management message parsing, asset tracking, creation or deletion of requirements, requirements consolidations, requirements database maintenance, and generation of tasking messages.

- **Message release authority (MRA):** MRA provides a final check of message format, addressees, and security compliance before release of messages.

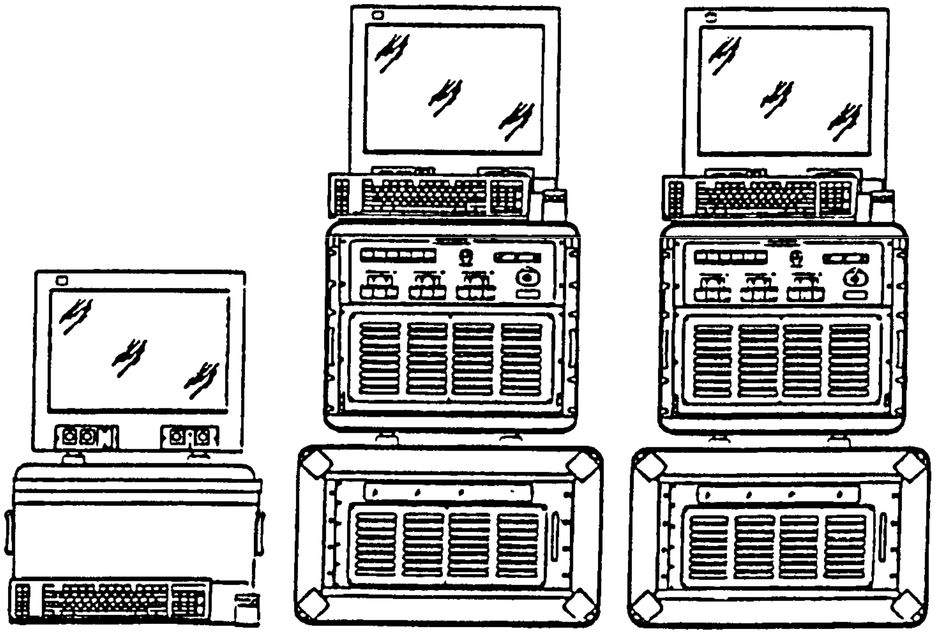
- **Situation analysis (SIT):** SIT supports situation development, alarms processing, and graphic display of IPB products.

- **Target analysis (TGT):** TGT supports target development, alarms processing, and the rapid turnaround of potential targets to the FSE.

The system supervisor can authorize each analyst access to all available FIs or selected FIs based on ability and mission. Up to eight FIs can be concurrently activated on each ASAS-ASW based on the authorization of the analyst who is logged on to the equipment. The system supervisor can assign the same FIs, except for the SPV, to more than one analyst for concurrent processing. The SPV must be active on one station to maintain an operational state. In addition to these software FIs, there are additional common functions available to each analyst that assist processing by providing graphics capabilities, inter-ACE coordination, time and distance calculations, and coordinate conversions.

SINGLE-SOURCE WORKSTATION:

The ASAS Block I is equipped with six AN/TYQ-52(V). The ASAS-SSW shown in Figure 3-4 is a ruggedized, portable computer workstation that supports single-discipline analysis and technical control. The ASAS-SSWs UNIX operating system and windows environment allow the configuration of each station based on mission requirements or analyst proficiency.



Components:
- 1.44 MB floppy disk drive
- 1.2 GB removable HDD
- CD-ROM drive
- Mouse
- Keyboard
- High resolution color monitor
- Central processing unit
- Seven four-person lift components in transit cases

Characteristics:
- Uses UNIX operating system
- Interface via ethernet LAN or synchronous communications port
- Output to large screen displays and large format map plotters
- Uses optical disk cartridge of HDD for map image retrieval media
- Operates in a modular cluster of three workstations

Figure 3-4. Block I SSW.

System Software. The system software provides the UNIX operating system, security and control mechanisms, system services, and system utilities required to support the applications and communications software.

Communications Software. The communications software provides message interfaces between applications software, analyst functions, external data sources, and users. It is capable of receiving and distributing messages within the ASAS, and distributing and supporting security release of messages leaving the ASAS.

Applications Software. The applications software allows the operator and the SPV to process incoming messages, distribute data to the appropriate analysts, generate intelligence products, and send messages. It consists of three categories:

- **Intelligence analysis:** Generic database interface, template builder, terrain evaluation tools, and situation maps.

- **Message handling:** Message review, message generator, and communications interface.

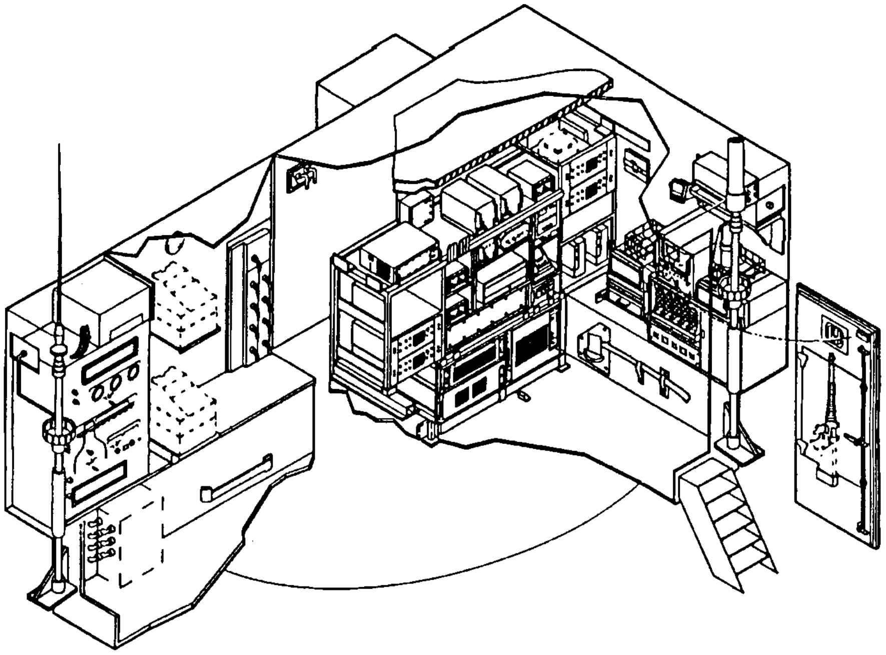
- **Analysis utilities:** Analysis support tools and utilities.

COMMUNICATIONS CONTROL SET:

The ASAS Block I is equipped with two AN/TYQ-40(V)2, CCS. The CCS is the communications center for the ASAS. It supports collateral and SCI level communications processing, and relay; it interfaces with ACUS, CNR, and special purpose intelligence communications systems. The CCS provides secure voice and data communications through MSE, SINCGARS, and the JTT. The CCS equipment provides capabilities for automatic message routing, operator message review, and manual message routing. The CCS shown in Figure 3-5 consists of the major systems discussed below.

Communications Processing Subsystem (CPS). The CPS performs message protocol translation, message processing, and detailed auditing of system activity. It has a variety of tools to help operators distribute message traffic automatically. The CPS retains messages on disk packs for temporary storage. The system is capable of processing a number of communications protocols. This capability establishes the basic ASAS compatibility and interoperability with other systems. All data handling internal to the ASAS uses Full Duplex Message Protocol (FDMP)/Digital Data Communications Message Protocol (DDCMP). Outgoing message traffic is translated from FDMP/DDCMP; incoming traffic is translated to it. The CPS provides protocol translation for Automatic Digital Network (AUTODIN), digital communications terminal (DCT), net radio protocol (NRP), and External Digital Data Communications Message Protocol (XDDCMP).

Computer Operator Terminal (COT). The COT allows the CCS operator to initialize and control the CPS.



Components:
- Two removable HDDs
- Communications processing subsystem
- Computer Operator Terminal
- Six TSEC/KY-68
- One AN/ARC-164A
- One AN/PSC-2
- Four AN/VRC-92A
- One TSEC/KG-84A
- UHF and VHF antenna assemblies

Characteristics:
- Installed in TEMPEST, EMI, and EMP protected S-250 shelter
- Interface via fiber-optic LAN

Figure 3-5. Block I CCS (internal).

TSEC/KY-68 Terminal and Data Adapter. The CCS is equipped with six TSEC/KY-68 Digital Subscriber Voice Terminals (DSVTs) and data adapters for communication into the MSE network. It provides non-secure voice, secure voice, and secure data communications within the MSE network. The data adapter is a carry-in microprocessor based communications controller capable of protocol tasks.

AN/ARC-164A. The CCS has one AN/ARC-164A ultra high frequency (UHF) radio. It provides secure voice or data communications when used with the TSEC/KY-57 for voice, AN/PSC-2 and TSEC/KY-57 for data, and the TSEC/KG-84A for NRP. The combination of the system's RT-1288A with NRP, a datalink processor, and encryption device provide data communications with NRP capable sensors and relays such as the AN/TSQ-138 TRAILBLAZER, AN/TRQ-32(V)2 TEAMMATE, and AN/TSQ-175 TIGER.

AN/PSC-2. The CCS is equipped with one AN/PSC-2, DCT. The AN/PSC-2 DCT is used to prepare, send, receive, and display reformatted IEW Character Oriented Message Catalog (COMCAT) messages and free-text messages. The CNR systems in the ASAS Block I CCS support secure data communications when used with the AN/PSC-2. It supports the exchange of SCI tasking and reporting messages between the ACE and AN/PSC-2 equipped IEW assets. The ACE also uses the system to exchange collateral messages with Cl teams, interrogation teams, and long-range surveillance teams.

AN/VRC-92A. The CCS has four AN/VRC-92A, SINCGARS, very high frequency (VHF) frequency radios that are frequency modulation (FM) with integrated COMSEC module (lCOM). Operated in the secure non-hopping mode, these systems provide secure voice and data communications.

DATA PROCESSOR SET (DPS):

The DPS, AN/TYQ-36(V)3 shown in Figure 3-6 is a mobile, self-monitoring, unmanned data processing station for the Block I ASAS-ASW. Each ASAS Block I has two DPSs. The ASAS-ASW applications software and databases reside within the DPSs. They provide the communications connectivity between the CCS and ASAS-ASW. The shelter provides environmental control, intrusion protection, fire protection, and secure storage for the ASAS main processors.

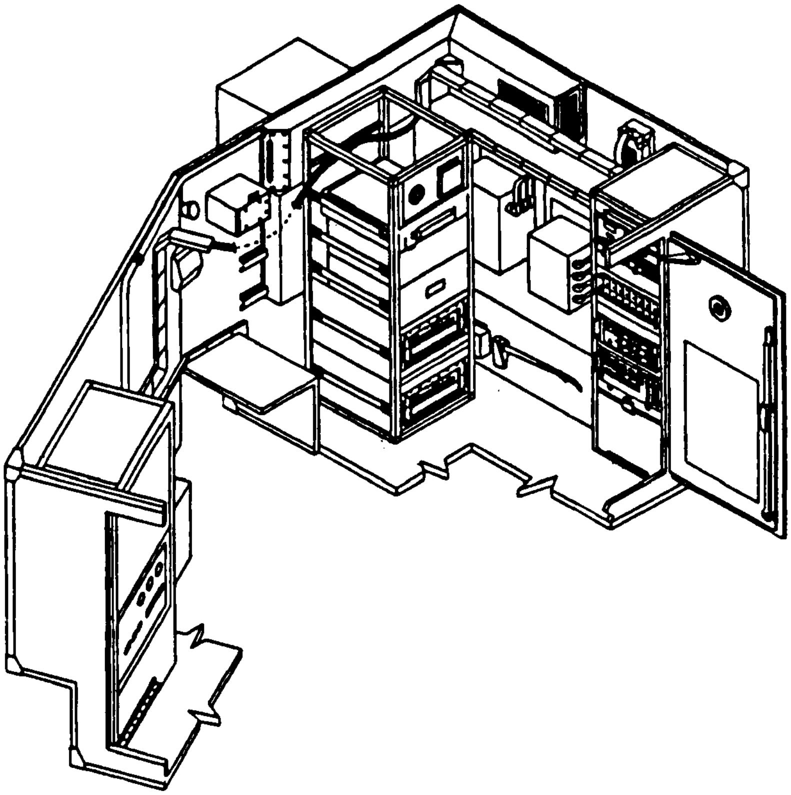
SUPPLEMENTARY EQUIPMENT, ELECTRONIC:

The SEE, AN/TYQ-42(V), consists of ancillary equipment for power generation and distribution, communications, and transportation. It consists of three distinct groups:

- **Power Group.** The power group generates and distributes power. It includes 10 kW or 30 kW generator sets, M40 or M200 power distribution systems, power cable assemblies, and distribution boxes.

- **Signal Group.** The signal group supports communications connectivity. It includes thirteen TSEC/KY-68, one TA-838, and communications cable assemblies.

- **Transport Group.** The transport group consists of M35A2, M925, or high mobility multipurpose wheeled vehicles (HMMWV) with cargo trailers.



Components:
- Two removable HDDs
- Optical disk drive
- Two TSEC/KG-84A
- Up to eight full duplex modems
- Communications Protocol Processor (four remotely programmable processors)

Characteristics:
- Installed in TEMPEST, EMI, and EMP protected S-250 shelter mounted
- Interface via fiber-optic LAN
- Operates in conjunction with the CCS to provide communications for the Block I ASW

Figure 3-6. Block I DPS (internal).

ASAS-EXTENDED

The ASAS-Extended uses commercial hardware and ASAS Block II prototype software. It provides units not issued the ASAS Block I standard hardware with an automated intelligence capability and full ASAS interoperability. The ASAS-Extended communications subsystem can exchange information with ASAS systems, other battlefield automation systems, and EAC systems. Figure 3-7 shows the major components of the ASAS-Extended.

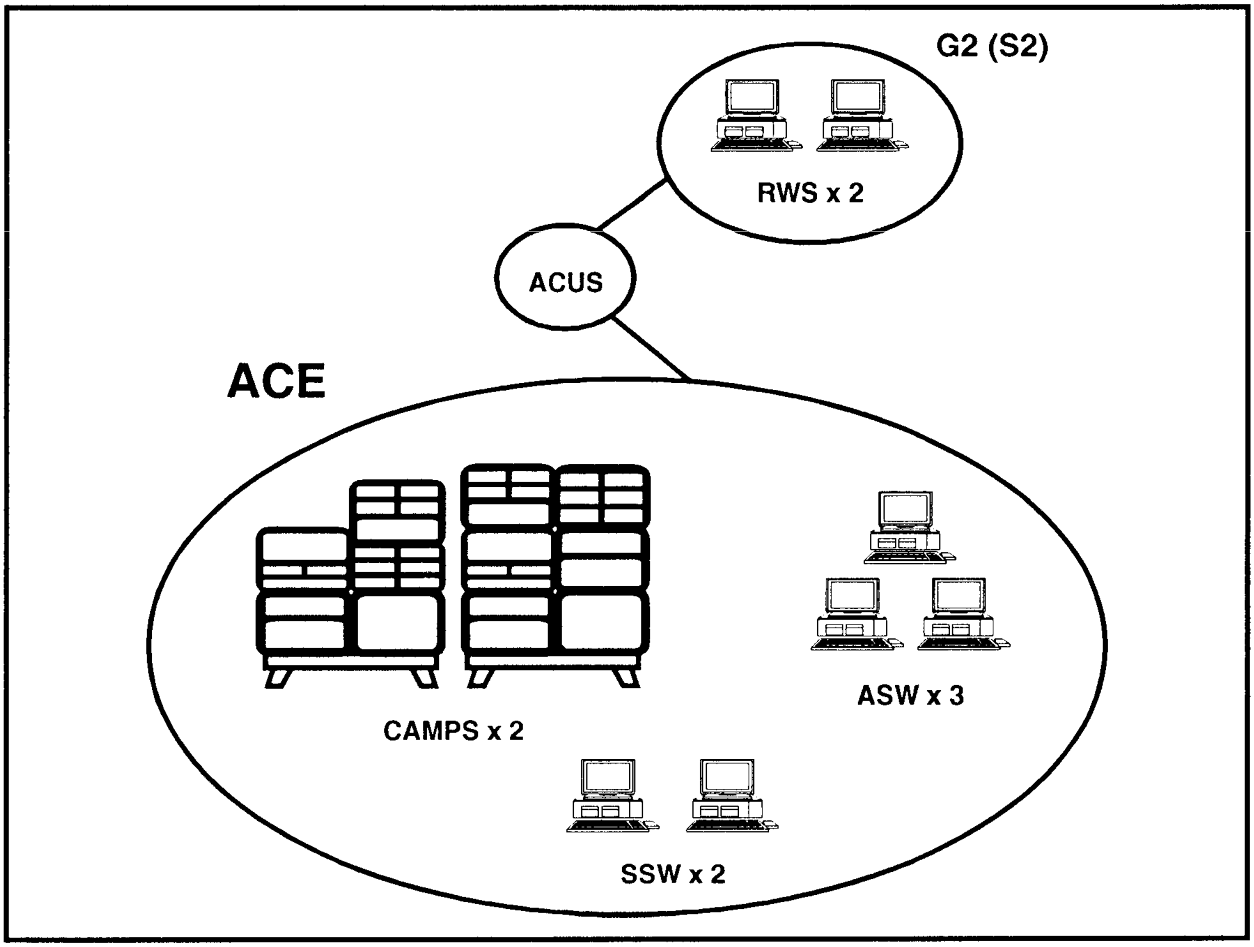


Figure 3-7. ASAS-Extended.

EXTENDED REMOTE WORKSTATION:

The ASAS-Extended RWS is a commercial workstation with a Virtual Memory System (VMS) operating system in a windows environment. The ASAS-Extended normally has two RWSs. Each workstation has a 2.0 gigabyte (GB) extended hard drive. Both workstations share a laser printer.

EXTENDED ALL-SOURCE WORKSTATION:

The ASAS-Extended ASW uses the Alpha-RISC processor and Virtual Memory System (VMS) operating system in a commercial computer. A minimum of three workstations linked by a LAN support the ACE all-source intelligence section. The Alpha-RISC processor and 288 megabytes (MB) of random access memory (RAM) significantly improve processing time over the initially fielded ASAS Block I VAX processors. Its storage units of 2.2 GB of capacity also eliminate the need for the two ASAS Block I DPSs. Other hardware supporting this workstation includes one magnetic tape drive, one compact disk-read-only memory (CD-ROM) reader, one laser printer, and one communications modem per terminal.

EXTENDED SINGLE SOURCE WORKSTATION:

The ASAS-Extended SSW is a commercial workstation using a UNIX operating system in a windows environment. A minimum of two workstations linked by a LAN support the ACE technical control and processing section. Each workstation has 64 MB of RAM, one 1.2 GB external disk drives, one CD-ROM reader, one tape reader, and one laser printer. The workstations use baseline ASAS-SSW software with one workstation also loaded with Joint Deployable Intelligence Support System (JDISS) software.

COMPARTMENTED ASAS MESSAGE PROCESSING SYSTEM (CAMPS):

The CAMPS is an intregal component of the ASAS-Extended and is used in lieu of the ASAS Block I CCS. In air assualt, airborne, and light infantry divisions, the CAMPS and only one ASAS Block I CCS form the ASAS communications center. It is a modular, transportable communications processing system consisting of a Communications Gateway System-100 central processing unit (CPU) controlling Secure Telephone Unit (STU)-III and TSEC/KY-68 DSVT phones; generic gateways; tactical switch processors; and TSEC/KIV-7 COMSEC equipment. It supports the receipt, processing, and dissemination of SCI and collateral information. The CAMPS also provides an interface capability for the TROJAN SPIRIT II and tactical satellite. Figure 3-8 and the following summarize the CAMPS features:

- Lighter, smaller, and more modular than the ASAS Block I CCS.
- Supports multiple protocols and interfaces (AUTODIN Modes I, II, and VI; DDN x .25/(MPN) x .25; (IEEE) 802.3 LAN Transmission Control Protocol/Internet Protocol (TCP/IP) (Fiber-optic or Thin Net; and E-mail)).
- Mirrors CCS functions.
- Lightweight and smaller than a CCS.
- Modular.
- Adds flexibility to ASAS deployments (supports tiered deployment; supports forward deployed G2 workstation).

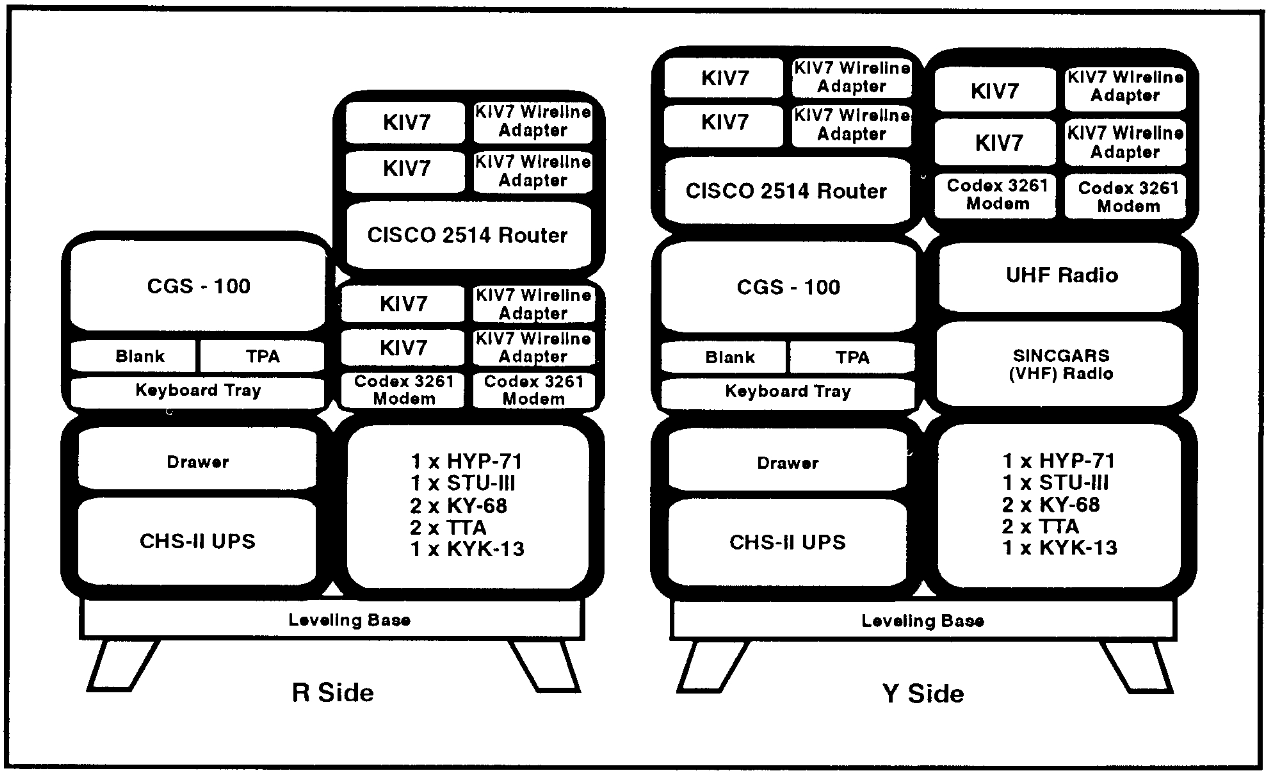


Figure 3-8. Compartmented ASAS Message Processing System.

- Multiple protocols and interfaces (Dial Up Circuit; connects to TROJAN network).
- Joint development effort.
- Possesses VHF and UHF communications equipment.

ASAS BLOCK II

The ASAS Block II will use ABCS CHS II workstations and comply with joint common operating environment requirements. The ASAS Block II builds upon the ASAS Block I and prototyping initiatives. As shown in Figure 3-9, ASAS Block II will consist of 8 to 24 reconfigurable SCI workstations, a CCS or CAMPS, and two remote workstations. These components (along with enhancements in communications interfaces, data handling, and common applications) will improve the joint interoperability of the system.

Most hardware will consist of integrated GFE and CHS II workstations mounted in standard shelters or in transit cases. The ASAS Block II

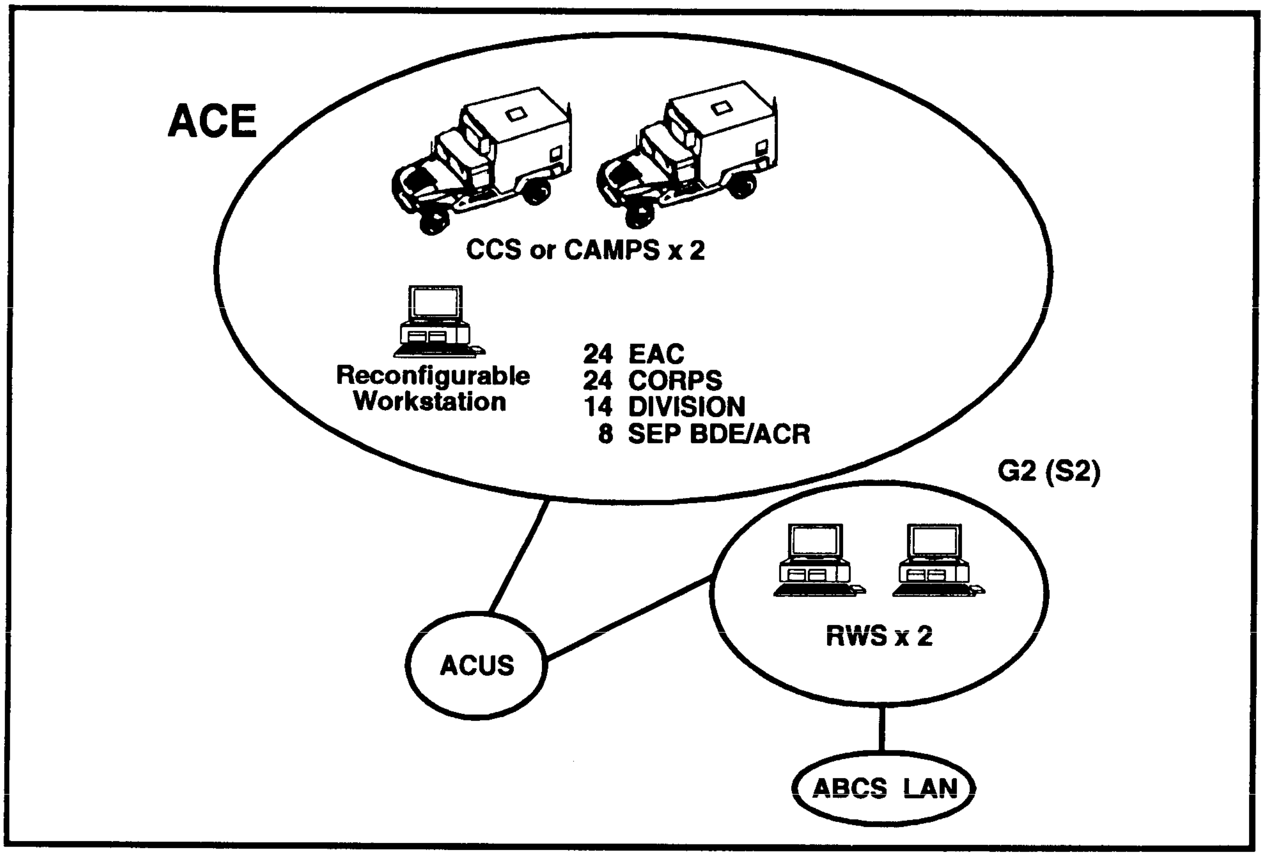


Figure 3-9. ASAS Block II.

software will use a UNIX-based, POSIX compliant secure operating system. Software will include an extensive package of system service software consistent with common ABCS support software architecture and the joint common operating environment. The use of CHS II will simplify equipment maintenance and allow greater interoperability among ABCS.

The ASAS Block II will significantly improve the ACE's ability to exchange data outside the SCI environment by building in a multilevel security capability for automatic sanitization and collateral release. Other features of the ASAS Block II are—

- Military Intelligence Integrated Database System (MIIDS) and Integrated Database (IDB) automation that expands the number of available databases.

- Communications upgrades that provide four additional channels, satellite communications, Improved High Frequency Radio (IHFR), Defense Secure Network 3 (DSNET3), MSE packet switch, and SINCGARS frequency hopping, and an integrated JTT interface.

- Common applications enhancements that provide additional message parsing and improved alert and alarm services; better display support functions for map operations, digital terrain, and weather products; and faster data output.
- Secondary imagery capability that supports receipt, display, storage, and forwarding of softcopy imagery products.
- Integration of the Joint Collection Management Tools (JCMT) software to improve collection management tasks support.
- Enhanced correlation ability for SIGINT.
- JDISS and Defense Intelligence Threat Data System (DITDS) software applications that improve interoperability with the Joint Worldwide Intelligence Communications System (JWICS).
- Addition of CI and HUMINT specific processing capability.

ASAS BLOCK III

The ASAS Block III is the objective system for the ASAS program. The ASAS Block III, scheduled for fielding at the turn of the century, will meet the requirements of the Army of the 21st century. The system will use an open architecture system that incorporates the results of baseline system performance and prototyping. The ASAS Block III will use CHS to ensure interoperability and seamless flow of intelligence between ABCS control systems and echelons.

Chapter 4

INFORMATION SYSTEMS

The ASAS communications equipment provides essential connectivity and interface capabilities with a variety of Army and joint information systems. These information systems provide the G2 (S2) and ACE access into joint intelligence systems and gateways into allied systems in multinational operations. The combination of Army, joint, and special purpose intelligence communications systems provide interoperability between intelligence organizations and users at multiple echelons.

AREA NETWORKS

ASAS workstations are linked locally through a LAN and outside the ACE by a WAN. The SCI security level LAN allows workstations to exchange information and to share common communications interfaces. The WAN provides the ACE access to IEW organizations throughout the AO and theater long-haul communications systems.

LOCAL AREA NETWORK:

ASAS workstations and the CCS or CAMPS are linked through a combination of a LAN and direct data exchange. The LAN allows workstations to exchange information with other workstations and to share a common database and communications interfaces. The ACE LAN operates at the SCI level. ASAS-RWS outside the ACE may be operated independently or on other collateral LANs.

WIDE AREA NETWORK:

The ASAS is interoperable with a wide range of Army and Joint communications systems. These systems form the WAN that underpins the intelligence architecture that the ACE uses to gather and disseminate intelligence. The networks that make up the WAN include multichannel, single-channel tactical radios, wire, and satellite systems. All are integrated to provide voice, data, and packet switch communications to the intelligence users and producers at multiple echelons. Most importantly, these communications systems allow the ASAS to exchange information with Army and Joint automated intelligence processors.

ARMY COMMUNICATIONS

This section is an overview of the principal systems of the ACUS, CNR, and ADDS. These systems provide the Army communications support to the ABCS. Together with the joint communications systems discussed later in this chapter, they provide the framework for joint and Army split-based intelligence support to forward deployed Army forces.

ARMY COMMON USER SYSTEM (ACUS):

The ACUS is a multi-user, common-user area system for high volume C^2, operations, intelligence, administrative, and logistics communications. It consists of a series of nodal switching centers in a grid-like network connected primarily by terrestrial line of sight (LOS) multichannel radio systems. The system provides an integrated switching system from battalion through theater Army. The ACUS also provides interface points with access to strategic and sustaining base environments. Figure 4-1 is an example of a division MSE network.

Mobile Subscriber Equipment (MSE). MSE is the backbone of the ACUS communications system at corps and division. it is the primary system supporting ACE operations and ASAS connectivity. By providing digital communications from the corps rear area forward to the maneuver battalion, MSE extends the ASAS interoperability from theater Army to forward information collectors. These communications include telephone, facsimile, mobile radiotelephone, data transmission, and CNR network access. MSE secures transmissions to the collateral SECRET level. Protection of SCI requires use of an additional COMSEC variable applied from a DSVT by the subscriber before it is released to the MSE.

MSE provides both functional point-to point communications and geographic support to the designated units. Geographic support is provided through a gridded network of nodes and node centers to all elements requiring communications within a designated area. These nodes are interconnected by terrestrial LOS multichannel radios. Where terrain is restrictive or extended range is desired, troposcatter or satellite radio systems can be used. Each corps interfaces with other corps' through the switching nodes. The system is normally established and maintained by the corps' signal brigade based on the area communications plan.

The ASAS connectivity to the MSE is provided by the CCS or CAMPS through force entry switch, small extension nodes (SEN), or large extension nodes (LEN). Network access is established from a DSVT via wireline through a J-1077 junction box at the CCS or CAMPS. The incoming MSE signal is initially routed into the CCS or CAMPS where communications software converts it into a compatible protocol format. After conversion, all messages are automatically routed to the appropriate workstation or database based on plain language address (PLA) and routing indicators applied to each message. COMSEC protection and MSE on hook service is provided through the "S" variable in the DSVT for voice and data transmissions.

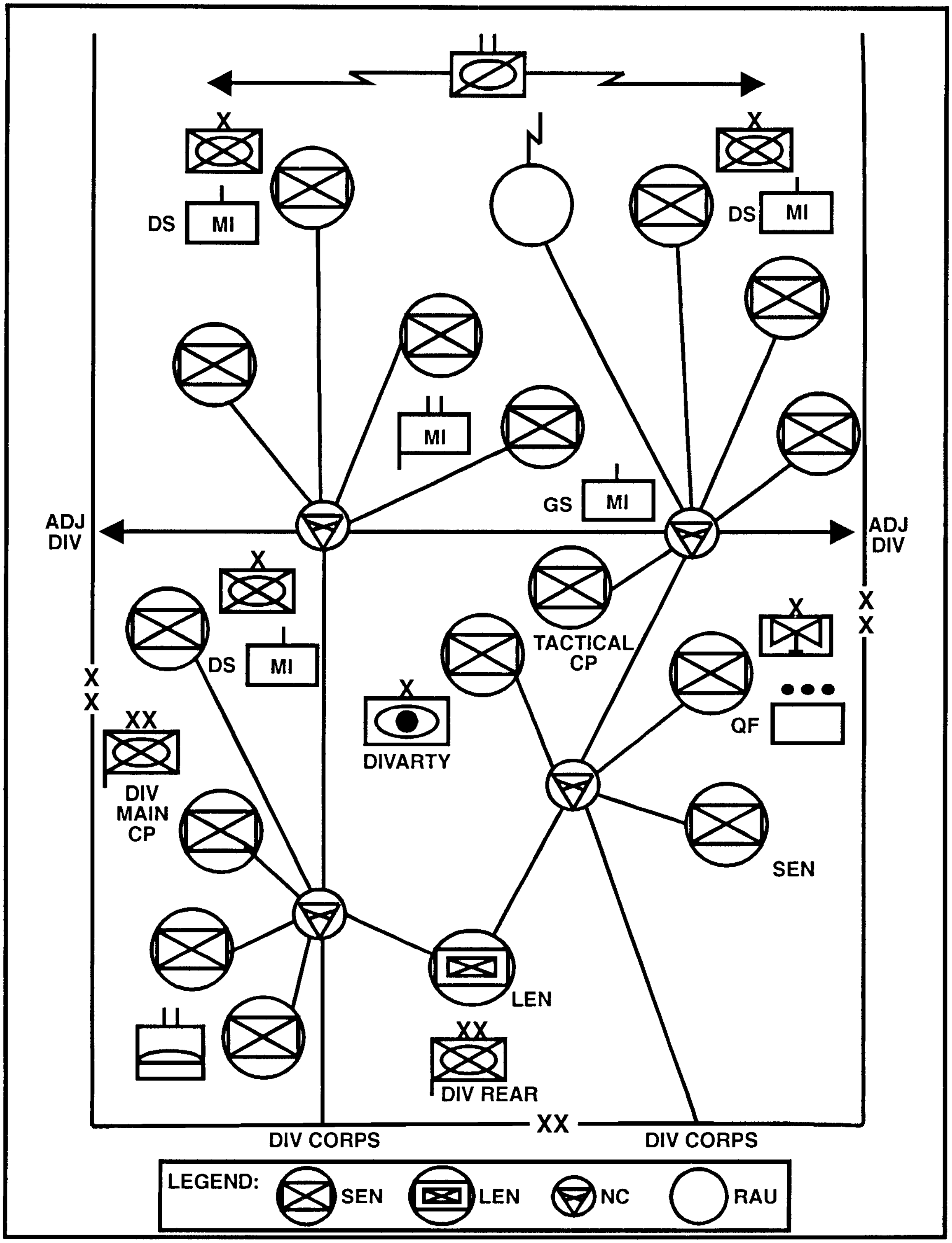


Figure 4-1. Typical division ACUS.

See FM 11-30, FM 11-37, and FM 11-38 for more information about the MSE.

COMBAT NET RADIO (CNR):

The CNR provides a secondary means of data communications for the ASAS. It covers a broad spectrum of single-channel radio systems used for immediate C^2. The CNR architecture consists of VHF FM radios, high frequency (HF) amplitude modulation (AM) radios, and UHF tactical satellite systems. The CNR systems are designed to meet the requirements of speed, reliability, and security on the battlefield.

Improved High Frequency Radio (IHFR). IHFR is the new family of secure tactical HF AM radios replacing systems such as the AN/PRC-7, AN/GRC-165, and AN/GRC-106. The IHFR extends and complements VHF FM communications networks in the corps and division. The IHFR is configured as the AN/GRC-193A (vehicular), AN/GRC-213 (manpack or vehicular), and the AN/PRC-104 (manpack). Beginning with ASAS Block II, the ASAS will be capable of IHFR communications.

Single-Channel Ground and Airborne Radio System (SINCGARS). SINCGARS is the new family of VHF FM radios replacing older FM equipment on a one-for-one basis. It provides secure voice and data transmission, a broad frequency spectrum, and a frequency-hopping capability. With an ICOM capability, it secures data to the SECRET level and provides low probability of intercept when operated in the frequency-hopping mode. However, when overlaid with a special “S” variable security device, frequency-hopping modes are voided. The ASAS CCS contains four SINCGARS transceivers operated in the single-channel mode for both voice and data communications. These radios are used primarily for voice and data communications with supporting IEW assets. If necessary, they can provide access to the MSE network or, if the MSE is not available, provide an alternate means of ASAS data communications.

Tactical Satellite (TACSAT). The TACSAT (AN/TSC-85B and AN/TSC-936) provides secure long-haul Super High Frequency (SHF) voice and data satellite communications. It can interface and provide an internodal link between widely separated MSE node centers (NCs) or a gateway link between net control stations (NCSs). The system provides ASAS a communications link with higher echelon intelligence centers or forward elements during split-based operations.

See FM 11-30 and FM 24-1 for additional information on CNR operations.

ARMY DATA DISTRIBUTION SYSTEM (ADDS):

The ADDS is an integrated C^2 communications system providing NRT transmission capabilities to support high volume data networks. Additionally, it provides precise position, location, navigation, identification, time of day, and reporting information for units on the battlefield. ADDS meets the needs of users for a high speed, high volume, secure communications system to convey sensor traffic for evaluation and firing data for target engagement. The combination of time division multiple access (TDMA), frequency-hopping, and spread spectrum technologies provides resistance to enemy jamming. The system automatically relays data from the origin to the destination transparently to the user. The Enhanced Position Location Reporting System (EPLRS), MSE Packet Switch Network (MPN), and Tactical Fire Direction System (TACFIRE) are examples of ADDSs.

Enhanced Position Location Reporting System (EPLRS). The ASAS Block II and follow-on versions will possess an EPLRS capability. The EPLRS is a computer-based communications system designed to provide secure, jam-resistant, contention free, NRT data transmission and distribution to subscribers. Additionally, it provides unit identification, navigational aids, and automatic location reporting of tactical combat and combat support units. The EPLRS uses integral dual level (CONFIDENTIAL and SECRET) COMSEC with over-the-air rekeying, frequency-hopping, and error correction encoding as protection from electronic attack.

See FM 11-30 and FM 24-1 for additional information on ADDS.

JOINT COMMUNICATIONS

This section is an overview of the primary joint communications systems through which intelligence flows. These systems support the daily maintenance of intelligence readiness and provide the communications foundation for split-based intelligence operations.

DEFENSE COMMUNICATIONS SYSTEM (DCS):

The DCS is a composite of certain Department of Defense (DOD) communications systems and networks. The system provides long-haul, point-to-point, and switched network telecommunications. The Defense Information Systems Agency (DISA) provides centralized management and command, control, communications, computers, and intelligence (C^4) systems of the DCS. The US Army Information Systems Command is the Army's executive agent for the DISA. The communications networks of the DISA are discussed below.

Defense Switching Network (DSN). The DSN is the principal common user, switched, nonsecure voice communications network within the DCS. It consist of a worldwide network of commercial leased and government-owned facilities. Tactical DSN subscribers normally gain access through the Theater Communications System (TCS) using the AN/TTC-39 circuit switch. The TCS provides circuit or message switches and direct access to many worldwide DOD networks.

Defense Information Systems Network (DISN). DISA integrated the Defense Data Network (DDN) packet switching networks under the DISN. DISN provides DOD worldwide packet switched data communications through four physically separate networks. These networks were implemented with technology developed by the Advanced Research Projects Agency (ARPA) using packet switch nodes (PSNs). These PSNs accept inputs using the international standard x .25 set of protocols. Until completely replaced by DISN, the four networks are managed together as the DDN:

- Military Network (MILNET) UNCLASSIFIED network.
- Defense Secure Network 1 (DSNET1) SECRET network.
- Defense Secure Network 2 (DSNET2) TOP SECRET network.
- Defense Secure Network 3 (DSNET3) TOP SECRET/SCI network.

Under DISN, the four DDNs will remain physically separate and the x .25 PSNs replaced with commercially available Internet Protocol (IP) routers. Each network will employ IP routers to perform switching and routing functions. The trunk circuits that interconnect the routers may be shared by multiplexing the encrypted outputs of the routers. DIA will transition DSNET3 to an IP router network under the auspices of the JWICS program.

Automatic Digital Network (AUTODIN).DISA operates the AUTODIN system. AUTODIN is the DOD common user store-and-forward message switching network for all record message traffic. It consists of a network of fixed and mobile AUTODIN switching centers (ASCs) and AUTODIN communications centers. The current AUTODIN system evolved from the consolidation of the Defense Special Security Communications System (DSSCS) with the General Services (GENSER) AUTODIN system in the mid-1970s. While the two independent systems have been merged, each system has retained its own identity and mission function. GENSER AUTODIN (referred to as the “R” side) handles UNCLASSIFIED through TOP SECRET record message traffic including special category (SPECAT) type messages. DSSCS AUTODIN (referred to as the “Y” side) handles record message traffic containing SCI information. DISA is replacing the aged and inefficient AUTODIN with the modern E-mail based Defense Message System (DMS).

Each ASAS requires an AUTODIN routing indicator to exchange information. Router indicators identify the relationship of subscribers to their parent message switching center. As stated above, the “R” routers access the collateral security level record message traffic of the worldwide GENSER AUTODIN network, and the “Y” routers access the DSSCS for SCI AUTODIN message traffic. The ASAS CAMPS is discussed in terms of the “Y” and the “R” sides. Figure 4-2 is an example of intelligence use of AUTODIN communications between a deployed corps ACE and its CMISE at the corps garrison.

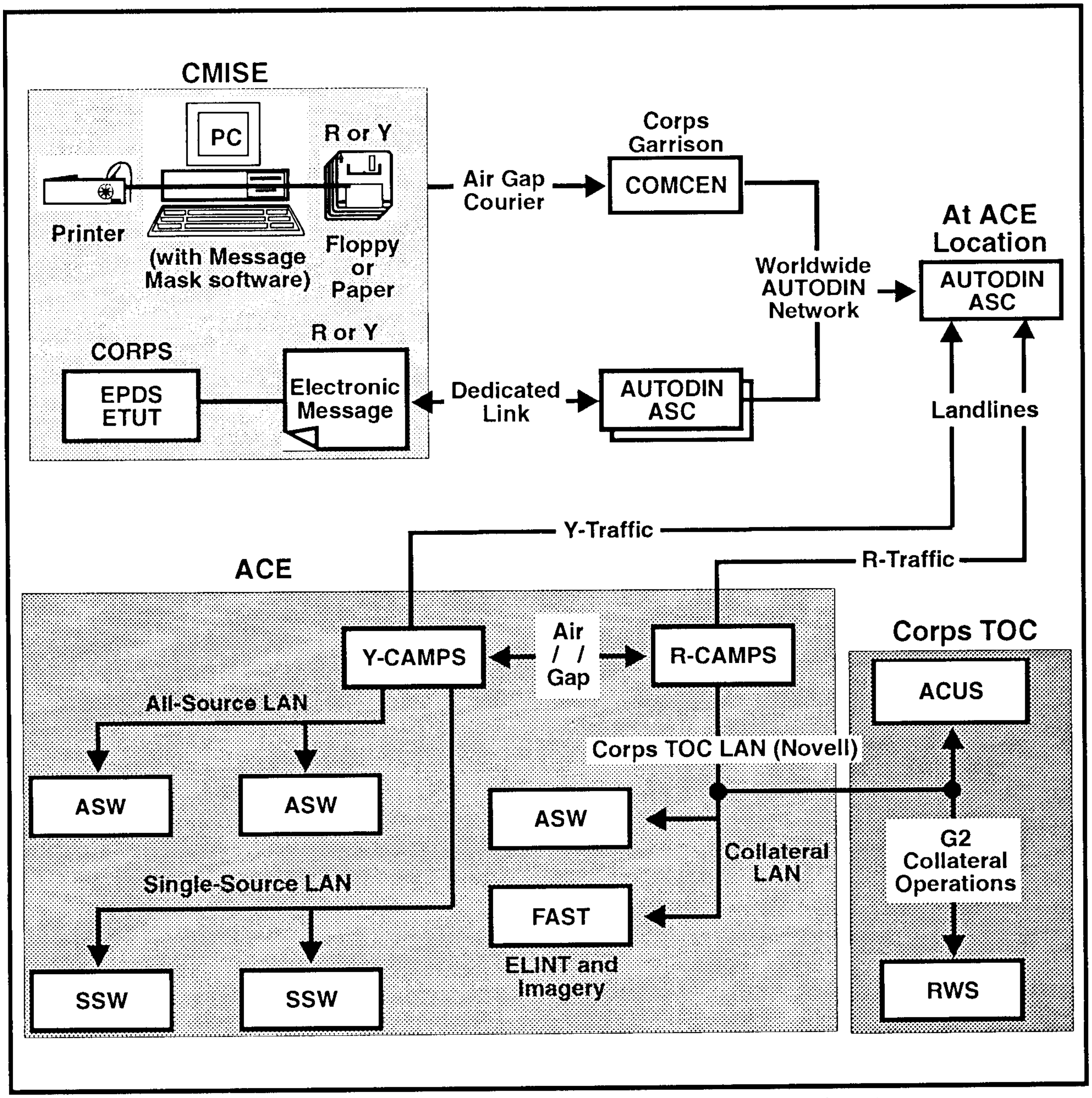


Figure 4-2. Corps CMISE to ACE communications (AUTODIN).

Defense Message System (DMS). While the DMS is a system in the sense that its components work together to provide message services, it is and will continue to be the composite result of many coordinated service and agency development and acquisition projects. DMS supports two classes of messages: organizational messages (formal record messages) and individual messages (informal E-mail). Its distributed message system supports on-line message preparation, coordination, and release of organizational messages. The DMS will replace the centralized AUTODIN message system, the DDN E-mail components, and the formats and procedures of the current message distribution baseline.

DEPARTMENT OF DEFENSE INTELLIGENCE INFORMATION SYSTEM (DODIIS): DODIIS is the DIA managed program that incorporates the DISN secure networks under a single architecture. The system defines the standards for intelligence systems and applications interoperability. The DODIIS provides, within limits, an integrated strategic to tactical user environment for performing identical intelligence functions on compatible systems. The system's primary components include the SECRET Internet Protocol Router Network (SIPRNET), the JWICS, and the JDISS.

Secret Internet Protocol Router Network (SIPRNET). SIPRNET replaces the DDN DSNET1 as the SECRET portion of DISN. Its complete architecture will be achieved by constructing a new worldwide backbone router system. Various DOD router services and systems will migrate onto the SIPRNET backbone router network to serve the long-haul data transmission needs of the users. Transmission services will use smart multiplexer and 512 kilobytes per second (kbps) channels. Other transmission services will be acquired or leased as needed. Future expansion will progress to the T1 circuit data rate of 1.544 megabytes (mbps) and potentially to the T3 data rate of 45 mbps. High speed packet switched service will be provided through the use of IP routers. This SECRET router layer of the DISN is intended to support national defense C^3I requirements.

JWICS. JWICS replaces the DDN DSNET3 as the SCI portion of DISN. It provides DODIIS users a SCI level high-speed multimedia network using high-capacity communications to handle data, voice, imagery, and graphics. The system uses JDISS as its primary means of operator interface and display. In much the same way as ASAS, JWICS is an evolutionary system. The JWICS program initial or pilot phase established a hub and spoke circuit switched T1 backbone for point-to-point and multi-point video teleconferences (VTCS), broadcast of the Defense Intelligence Network (DIN), and variable bandwidth packet switched data communications. The Hybrid JWICS phase removed the DSNET3 PSNS, re-homed the lines to JWICS IP routers, and extended the JWICS to additional sites to form a mesh network. Some sites will have video and data capability on T1 lines, and some sites will have strictly data capability

(64 kbps lines). The final phase–Goal JWICS–will replace Hybrid JWICS with a single commercially available technology that can accommodate data, voice, and video. This technology is expected to be asynchronous transfer mode (ATM). JWICS will ride the DISN as an overlay when the DISN acquires T3 lines.

SPECIAL PURPOSE INTELLIGENCE COMMUNICATIONS

This section describes the special purpose intelligence communications systems supporting Army IEW operations. These systems provide intelligence organizations the dedicated and flexible intelligence communications needed to support commanders across the range of military operations.

BROADCAST SYSTEMS:

A number of broadcast systems support the dissemination of tactical intelligence to commanders at multiple echelons. These systems are usually designed to “push” formatted time-sensitive information to tactical forces. This information includes multi-sensor national and theater electronic intelligence (ELINT) and imagery-derived data, and multisource fused tactical force disposition information.

One system, the Tactical Related Applications (TRAP) broadcast system provides worldwide dissemination of ELINT, contact reports, and parametric information at the SECRET level. This information is broadcast from one of nine gateways, using Tactical Data Information Exchange System-Broadcast (TADIXS-B) message format over a shared sideband of the UHF satellite communications channel used for the Navy’s Fleet Secure Voice communications. Selected Air Force units receive the TRAP broadcast using their CONSTANT SOURCE terminals; Army units use the Synthesized UHF Computer Controlled Equipment Substation (SUCCESS) radio; and Navy and Marine Corps use Tactical Receive Equipment (TRE) terminals. Other common broadcast systems are—

- Tactical Information Broadcast System (TIBS).
- Tactical Reconnaissance Exchange System (TRIXS).
- Fleet Intelligence Broadcast.

See Joint Pub 2-0 and Joint Pub 6-0 for more information on joint communications support to intelligence operations. Figure 4-3 illustrates UHF broadcast dissemination coverage.

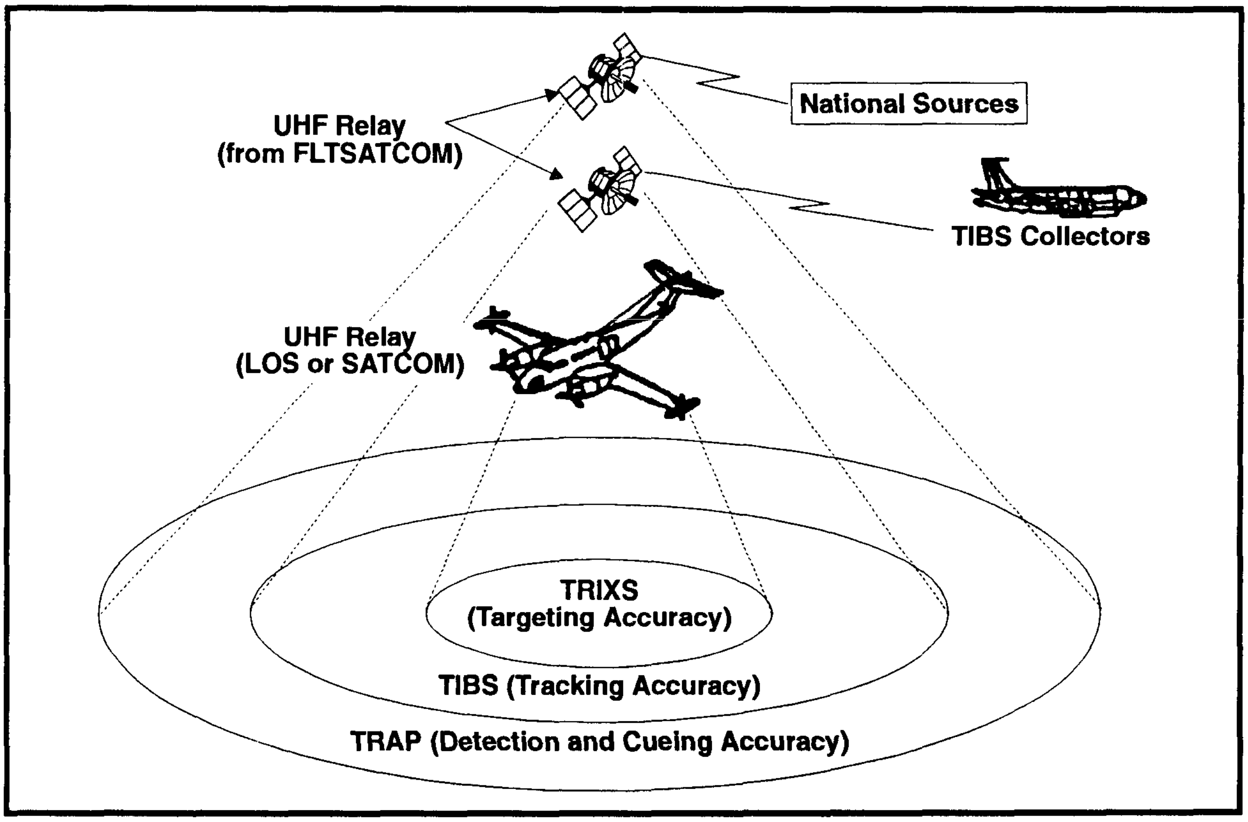


Figure 4-3. Intelligence coverage for UHF broadcast dissemination.

JOINT TACTICAL TERMINAL:

The Joint Tactical Terminal (JTT), formerly the Commanders Tactical Terminal (CTT), is a family of special application UHF tactical intelligence terminals which provide the capability to disseminate time sensitive Command, Control, Communications, Computer, and Intelligence (C^41), and battlefield targeting information to tactical commanders-and intelligence nodes. This information is provided in near-real-time and allows selected collection managers at all echelons a full-duplex capability to dynamically adjust pre-planned tasking. The JTT has the capability of operating in the following intelligence dissemination networks: TRIXS, TIBS, TRAP, and TADIXS-B. The ASAS CCS will receive the AN/USR-55, a full duplex data/half duplex voice version of the JTT Hybrid (JTT/H3), and the Joint STARS GSM will integrate the AN/USR-6, a receive only version of Hybrid (JTT/H-R3). Currently, the CTT/Hybrid Receive-Only (CTT/H-R) 2 channel system (AN/USR-5) is being fielded with the GSM; however, these systems will ultimately be replaced by the JTT. The United States Air Force (USAF) Contingency Airborne Reconnaissance System (CARS), the Army GUARDRAIL IPF, and tactical units in the TRIXS net use the JTT/H-R to disseminate information. The JTT/H-R also provides the commander access to theater and national intelligence through the TIBS and TRAP.

SYNTHESIZED UHF COMPUTER-CONTROLLED EQUIPMENT SUBSYSTEM:

The SUCCESS UHF radio is a fully automated microprocessor based, computer-controlled UHF radio. Data may be transmitted and received simultaneously over its one transmit and three receive channels. Two SUCCESS radios may be stacked to provide an integrated, fully redundant, two transmit and six receive channel capability. The radio is designed to communicate with selected airborne, terrestrial, and satellite systems. It contains a TRE processor and can process all TRAP and TADIXS-B formatted transmissions. The system is designed for ground or mobile sheltered environments. The DIA accredited communication subsystem is compatible with TROJAN, MSE, DIN or DSSCS, as well as all Tactical Exploitation of National Capabilities (TENCAP) systems.

TACTICAL INTELLIGENCE GENERATION AND EVALUATION RELAY (TIGER):

The AN/TSQ-175 TIGER consist of an RT-1288A, KG-84A, and laptop commercial processing system. It supports data communications relay using NRP between forward deployed IEW sensors and the ASAS CCS.

TROJAN DATA NETWORK (TDN):

The TDN is a router, TCP or IP based network. It is overlaid on the communications network that links the AN/FSQ-144(V) TROJAN Classic central operating facilities and switch extensions at various US bases with remote collection facilities worldwide. The TDN is subdivided into three electronically and physically separated networks that correspond to the three security levels required of the system. As with the TROJAN Classic architecture, the TDN has a TROJAN Network Control Center in the TROJAN Switch Center at Fort Belvoir, VA, to provide configuration control and network management. The three networks of the TDN are—

TROJAN Data Network-1 (TDN-1). The TDN-1 operates at the SECRET security level and is the gateway to DSNET1. It provides data exchange between TROJAN Classic facilities, switch extensions, and Special Purpose Intelligence Remote Integrated Terminals (SPIRITS).

TROJAN Data Network-2 (TDN-2). The TDN-2 operates at the TOP SECRET/SCI level. It provides data exchange between selected TROJAN sites requiring access to the NSA network.

TROJAN Data Network-3 (TDN-3). The TDN-3 operates at the TOP SECRET/SCI security level and is the gateway to JWICS. It provides data exchange between TROJAN Classic facilities, switch extensions, and SPIRITS.

TROJAN SPECIAL PURPOSE INTELLIGENCE REMOTE INTEGRATED TERMINAL (SPIRIT) II:

The AN/TSQ-190(V), TROJAN SPIRIT II, provides worldwide secure voice, data, facsimile, video, and secondary imagery dissemination capabilities.

The TROJAN SPIRIT II is a corps and division asset that provides dedicated intelligence communications. The system's SATCOM system supports up to 14 circuits (8 SCI and 6 collateral) using variable baud rates from 4.8 to 512 kbps per channel on C, Ku, or X frequency bands. System connectivity capability includes DSNET1 and DSNET3, MSE, and TPN interfaces, as well as LAN connectivity. The TROJAN SPIRIT II is shelter mounted on two HMMWVs. It ties into TDN as a mobile switch extension from tactical. The system's two workstations also allow the operators to receive and disseminate secondary imagery, SIGINT databases and reports, and UAV video. This capability allows the TROJAN SPIRIT to serve as a temporary communications set for the ACE during redeployment or split-based operations. Figure 4-4 shows TROJAN SPIRIT's connectivity potential.

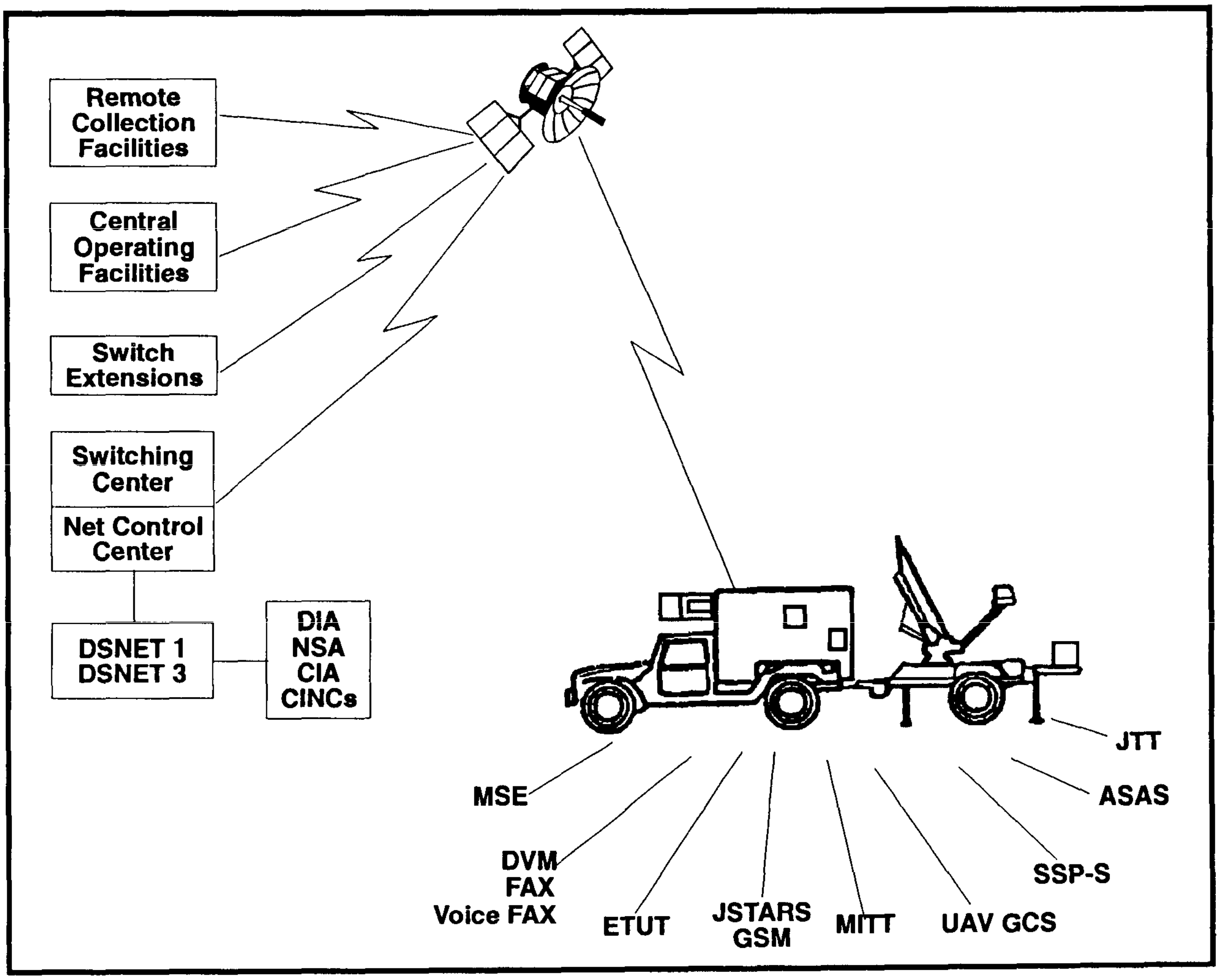


Figure 4-4. TROJAN data network connectivity.

See FM 34-10-2 for additional information on Army special purpose intelligence communications systems.

ARMY INTELLIGENCE PROCESSORS

The ASAS is not the only processing system found in the ACE or supporting IEW operations. Other systems provide the ACE access to broadcast intelligence or support missions not envisioned for ASAS Block I. The systems described below are found in the ACE at theater Army, corps, division, brigade, separate brigade, and ACR. Some of these systems will be eliminated and their missions assumed by the ASAS Block II and GCS when those systems are fielded.

ENHANCED TACTICAL USERS TERMINAL (ETUT):

The ETUT is a theater Army and corps asset. It is an intermediate processing system that receives TENCAP digital secondary imagery and correlated ELINT via ACUS or SUCCESS radio. Equipped with three analyst workstations, the ETUT provides secondary imagery for use in targeting and NRT ELINT data to the SIGINT team of the ACE technical control and processing section. The system is designed as the interface between the EPDS for SIGINT data and the Imagery Processing and Dissemination System (IPDS) or Mobile Imagery Exploitation System (MIES) for imagery data. It also provides an automated collection management capability.

ETUT communications consists of a SUCCESS radio which provides simultaneous connectivity with multiple airborne and spaceborne platforms as well as the TRAP and TADIXS-B interface. The ELINT position maintains a database which is a reflection of the data manipulated in the EPDS. The imagery management position interfaces with a variety of corps, theater, and national imagery systems to provide softcopy manipulatable imagery, as well as a database of exploited imagery reports.

FORCES COMMAND AUTOMATED INTELLIGENCE SUPPORT SYSTEM (FAISS):

The AN/UYK-71A, FAISS, is a corps and division Disk Operating System (DOS) compatible processing and dissemination system. The system was one of the first desktop computers fielded to corps through ACR TCAEs in the continental United States (CONUS). The system allows analysts to import, export, and manage SIGINT, topographic, collateral, and national systems databases and messages. Any database records, such as unit position or topographic indicators, can be plotted on maps displayed on the system’s video monitors. The FAISS will be retained in some units to provide a minimum automation capability until ASAS is fully fielded.

JOINT STARS GROUND STATION MODULE (GSM):

The primary mission of the GSM is to receive and process Joint STARS imagery data to support targeting, situation development, and battle command. It can also receive UAV video and, via its built-in JTT, collateral broadcast intelligence. The GSM is found at each echelon from theater

Army to brigade and ACR. In addition to the main and forward command posts at corps, division, brigade, and ACR, a GSM is normally located with the main command posts of aviation and artillery brigades. There are two operator positions in the GSM and a remote terminal that can be positioned in the supported unit's command post or ACE. The prototype system was the Interim GSM (IGSM). Production versions are the Medium GSM (MGSM) and Light GSM (LGSM). The objective system is the common ground station (CGS). The LGSM is projected to evolve into the CGS.

MOBILE INTEGRATED TACTICAL TERMINAL (MITT):

The MITT is the downsized version of the Tactical High Mobility Terminal (THMT) and replaces the THMT in the force structure. The MITT is a division ACE asset. It is an intermediate processing system that receives TENCAP digital secondary imagery and correlated ELINT via ACUS or SUCCESS radio. It receives, annotates, and transmits secondary imagery. It can also receive, process, and disseminate SIGINT data and maintain a correlated database.

The MITT is equipped with the SUCCESS radio for stand-alone secure communications capable of receiving TRAP, UHF SATCOM, and point-to-point terrestrial communications. The MITT is accredited for and compatible with the TROJAN network, MSE, DIN, and DSSCS, as well as all TENCAP systems. By positioning the MITT remote terminal with the target nomination team, it provides secondary imagery for use in targeting. The system provides NRT ELINT data to the SIGINT team of the ACE technical control and processing section.

SINGLE SOURCE PROCESSOR-SIGINT (SSP-S) PRODUCT IMPROVEMENT (PI):

The AN/TSQ-163, Top Graphic SSP-S PI, is a transportable, downsized, lightweight addition to the SSP-S found in the theater Army MI brigade. The SSP-S PI provides enhanced communications and SIGINT processing to the current SSP-S. Communications software permits the system to interface with theater and communications systems. The SIGINT processing system uses ASAS-SSW and Core Analyst Tool System (CATS) applications software. The SSP-S PI communications subsystem supports secure character-oriented messages using COMCAT, USMTF, and USSID message formats.

WARRIOR WORKSTATION (ASAS-W):

The WARRIOR workstation is an ASAS prototype system originally developed as a joint effort of the Project Manager-intelligence Fusion and United States Army, Europe (USAEUR). Designated as ASAS-W, it is a highly effective stand-alone intelligence processor that can be used in place of or to complement the ASAS-RWS in the G2 (S2). Employing a UNIX operating system and commercial hardware, the WARRIOR can receive, store, process, and display data, graphics, and imagery products. The system's communications software supports LAN and WAN connectivity. Lessons learned from units which have used the system in CONUS, Europe, Korea, and Southwest Asia have been incorporated into the WARLORD applications software resident on ASAS-RWS of ASAS-Extended.

See FM 34-10-2 for additional information on Army intelligence processors.

JOINT AND SERVICE INTELLIGENCE PROCESSORS

The ASAS is not the only processing system supporting military operations. Joint and service component intelligence processing systems directly and indirectly contribute to the IEW operations of the ACE. The systems described below are found in joint and service component intelligence organizations that may support Army operations.

DEFENSE INTELLIGENCE THREAT DATA SYSTEM (DITDS): DITDS is a message handling system with specialized software tools designed to support and facilitate the unique data handling requirements of the intelligence community. These tools allow the operator to receive incoming message traffic and create, manage, and manipulate databases. DIA is the proponent agency for DITDS. A number of government and military organizations use DITDS-format systems under different names. Other names for DITDS include—

- Naval Intelligence Threat Evaluation System (NITES) used by the US Navy.
- Special Operations Intelligence System (SOIS) used by Joint Special Operations Command (JSOC).
- USAREUR Defense Intelligence Threat Data System (UDITDS).
- US Southern Command (SOUTHCOM) Information Management System (SIMS).
- National Center for the Analysis of Violent Crimes Computer Assisted Security Investigative Analysis Tool (CASIAT) of the Federal Bureau of Investigation (FBI).
- US Special Operations Command (SOCOM) Command Research and Threat Evaluation System (SOCRATES).
- Expert Analysis System for Intelligence (EASI) used by Special Operations Intelligence Command (SOIC).

The types of databases that fall under each of these DITDS-format systems varies by organization, but are all manipulated using the same DITDS software tools.

JOINT DEPLOYABLE INTELLIGENCE SUPPORT SYSTEM (JDISS):

The JDISS is a deployable laptop or desktop workstation that can operate where there is space for a computer and access to JWICS. It is a multimedia system supporting a broad range of peripheral equipment including CD-ROM, scanners, digital cameras, mensuration modules, Tactical Communications-2 (TACO-2) and a variety of printers. The system is an integrated set of commercial off-the-shelf hardware and UNIX-based software applications. Its applications software includes word processing, E-mail, CHATTER, presentation graphics, spreadsheets, database management, imagery manipulation and dissemination, mapping, and remote access. Communications interfaces can be configured to meet specific user requirements for interoperability between JDISS users at strategic, operational, and tactical levels. JDISS can be installed on ASAS Block I SSWS and will be resident on all follow-on ASAS versions.

JOINT MANAGEMENT SUPPORT TOOLS (JMST):

The JMST, formerly known as Collection Management Support Tools, is a UNIX based system that provides a collection manager with an automated means of tasking national, theater, and organic collection assets in support of operations. Rapidly accessible databases allow the user to review asset capabilities, ensure efficient tasking of assets, and track the status of asset tasking. JMST supports collection management through the use of platform and target area coverage, along with timelines for planned missions. System functions include asset capability and availability analysis, message processing of over 30 message types and formats, full-duplex accredited communications, database management of an interactive operation with over 20 databases (target, contact, references, and symbology), and system security administration.

UNITED STATES AIR FORCE:

Typically, the intelligence architecture calls for data flow from national sources such as DIA into a Theater Distribution Host. The theater JIC flows intelligence data down to the Air Operations Center (AOC) via the Combat Intelligence System's Data Management (CIS-DM) server. CIS-DM feeds the Contingency Theater Automated Planning System (CTAPS) by correlating the integrated database (IDB) and the automatic associator (from Constant Source) data. The CIS Targeting Module (TM), formerly Rapid Application of Air Power, uses this data to generate the Target Nomination List (TNL) and associated weaponeering loads. CIS then passes the TNL to the Advanced Planning System (APS) to support the Air Tasking Order (ATO) build. (Note: APS has been adopted as the Joint ATO build system.) The unit mission planning cell (MPC) and squadron operations use CIS to—

- Do threat anlaysis for flight mission routes with the Improved-Many-On-Many (IMOM) module.
- Determine enemy force composition and deployment with the Data Manipulation module.
- Asssess real-time threat status and location with the automatic associator.
- Submit, receive, and evaluate GENSER messages with the Message Analysis module.
- Transmit, receive, search, and manipulate imagery via the Electronic Light Table 3000 and Demand Driven Direct Digital Dissemination.
- Perform data and product searches of Intelink-S servers using Mosaic.
- Emulate full JDLSS functionality.
- Perform office automation and presentation functions with Applixware.

Hardware included with the system allows the user to print color maps and full-size map overlays, print color or black and white briefing slides, scan images, and print hardcopy photographs.

UNITED STATES NAVY:

Intelligence support functions have been incorporated into the Joint Maritime Command Information System (JMCIS), the Navy's primary C^2 system afloat. This includes those functions previously found in the Naval Intelligence Processing System (NIPS), and the JDISS functions now being fielded. For example, on an aircraft carrier the JDISS functions will be available on the SCI-level Navy Tactical Command System-Afloat workstation on a LAN linking the Carrier Intelligence Center (CVIC), the Ship Signal Exploitation Space (SSES), and the Supplementary Plot (SUPPLOT). The SUPPLOT is the SCI area to the Flag Command Center. However, fleet units will still rely on support from centers ashore, especially the maritime JICS (Atlantic and Pacific), for processing high volume data from non-organic sensors, and for the picture of the battle space beyond the range of the afloat force's organic sensors. Shipboard JDISS, connected to the ship's SHF communications system, is extremely bandwidth limited and consequently slow. NISTs are increasingly deploying to JTFs embarked aboard command ships at sea and are bringing their own portable JDISS. Planning must also include reserved bandwidth, stabilized antennas, and a 360-degree field of view (FOV) of the COMSATs, because of a rolling sea state and heading changes of the ship.

UNITED STATES MARINE CORPS:

The Intelligence Analysis System (IAS) is the Marine Corps' primary intelligence processing system supporting Marine IEW operations. It is a UNIX-based modular, three tiered, ADP system which provides multisource intelligence support to the Marine Component and Marine Air-Ground Task Force (MAGTF). JDISS communications functionality is incorporated into the IAS. This provides interoperability with theater and JTF JICs and access to DSNET3 and JWICS. IAS may operate at either the collateral GENSER or DSSCS SCI-level, and it incorporates a secondary imagery dissemination capability.

SPECIAL OPERATIONS COMMAND:

Intelligence support to Special Operations Forces (SOF) is provided via SOCRATES. SOCRATES encompasses total intelligence support for SOF mission activities, including computers, databases, intelligence communications systems, secure phones, facsimile equipment, imagery processing, and secondary imagery dissemination equipment. SOCRATES integrated existing Intelligence Data Handling System (IDHS) and the DITDS, which hosts a database specifically focused on terrorism and OOTW into a LAN-based, multi-functional intelligence support system. This capability (including ADP, secure voice, open source and classified message traffic, video mapping, softcopy imagery processing, and secondary imagery dissemination) is extended to USSOCOM forces using the USSOCOM SCAMPI, a leased line communications link. SOCRATES also provides full access to national intelligence systems and databases. Future SOCRATES will focus on providing on-line connectivity to operational units and theater SOF, and development of a rugged, portable SOCRATES workstation. Additionally, SOCRATES will transition into a UNIX environment employing the JDISS architecture, and then will evolve into a client server environment.

JOINT AND SERVICE INTELLIGENCE DATABASES

Databases of information are maintained by all government agencies and services, to include ASAS-equipped Army units down to the brigade level. Access to databases will generally be given on a need-to-know basis and with the permission of the database's proponent agency. Protocol to enter these databases differs with each one and each is subject to change.

MILITARY INTELLIGENCE INTEGRATED DATA SYSTEM (MIIDS):

The IDB resides on the MIIDS architecture and supports general MI production. The IDB is the primary DIA intelligence database providing integrated data on foreign military organizations worldwide. The IDB data and structure supersedes the Defense Intelligence Order of Battle System (DIOBS), the Automated Intelligence Installation File (AIIF), and the

Defense Intelligence Equipment Index (DIEQP). DIA is the proponent agency for MIIDS and IDB.

In CONUS, the US Army Forces Command (FORSCOM) Automated Intelligence Support Activity (FAISA) at Fort Bragg, NC, has access to the MIIDS and IDB by tactical users of the ASAS. They maintain a complete copy of DIAs MIIDS and IDB and update file transactions in order to support the tactical user. This section discusses how to obtain files containing MIIDS data sets and updates.

Obtaining MIIDS. There are currently three methods of obtaining MIIDS base loads and updates.

- The tactical unit downloads MIIDS and IDB data sets using file transfer protocol (FTP) via DSNET3 communications to user's host on a SCI LAN in an accredited sensitive compartmented information facility (SCIF).

- FAISA downloads MIIDS and IDB data sets to produce an optical disk, which is couriered to the tactical unit via Defense Courier Service and is put into the unit's ASAS IDP optical drive.

- FAISA downloads MIIDS and IDB data sets to optical disk, and they are couriered to the tactical unit by two cleared personnel from the requesting unit.

The initial ASAS Block I software does not allow for direct access from ASAS to the FAISA System to accomplish file transfer of MIIDS and IDB files. To get to the data, the unit will need an intermediate host on the LAN that will do the job. In most cases, field service support personnel will accomplish all the file transfers for the unit.

IDB File Types. There are two types of IDB files on the FAISA System:

- **Base loads.** To populate the ASAS ASCDB, the tactical unit must first submit a request for an IDB base load to FAISA, specifying country codes (in priority). There are 20 base load files required for each country to make a full set of data set files needed to build the database. Users will need to download all files for a particular country.

- **Updates.** The updates are also in a different file format than the IDB base load files. They are in transaction file format. For each update, the ASAS needs four transaction files. FAISA produces the updates by country codes for the unit to download.

OTHER AVAILABLE DATABASES:

The database listing in Table 4-1 is not all-inclusive. Access to databases and files is based on mission and justification.

Table 4-1. Other databases.

Database Title	Acronym	Type of Database	Proponent
Intelligence Collection Requirement File	ICR	HUMINT	DIA
Intelligence Defector Source File	IDSF	HUMINT	DIA
Evaluation File	EVAL	HUMINT	DIA
Intelligence Information Reports and Index Summary	IRISA	HUMINT	DIA
Imagery Reconnaissance Objective File	IROF	IMINT	DIA
Imagery Reconnaissance Objective File Justification	IROFJUS	IMINT	DIA
Advanced Imagery Requirements and Exploitation System	AIRPIN	IMINT	DIA
AIRES Preliminary Imagery Nomination	AIRES	IMINT	DIA
All-Source Document Index Summary	ASDIA	All-Source	DIA
Foreign Military Assistance	FOMA	All-Source	DIA
Foreign Broadcast Information Service	FBIS	Open-source	NSA
National Photographic Interpretation Center	NPIC	IMINT	CIA
ANCHORY (formerly SIGINT On-Line Intelligence System)	ANCHORY	SIGINT	NSA
WRANGLER	None	ELINT	NSA
Central Information Resource and Control	CIRC	All-Source	DIA (Air Force)
Telecommunications Equipment Automated Retrieval System	TEARS	SIGINT	DOD (Army)
CONSTANT WEB	CW	SIGINT	Air Force

Chapter 5

OPERATIONS

The Ml Corps, like the Army it supports, is largely based in CONUS with a relatively small forward presence in selected areas of the world. During peacetime, MI uses ASAS to maintain intelligence readiness by supporting contingency planning, mission-essential task list (METL) based training, and real-world intelligence operations. In war and OOTW, Ml uses the ASAS to support force projection operations, defeat of the enemy in war, and accomplishment of OOTW.

INTELLIGENCE READINESS

In garrison, the G2 (S2) and ACE maintain intelligence readiness in part by using the ASAS to support exercises, real-world intelligence operations, and contingency planning. These actions in turn support the development of the METL and battle-focused training for combat, combat support (CS), and CSS units. In addition, the intelligence databases developed by Active Component (AC) units for contingency areas aids training and mobilization of RC units with similar or supporting contingency missions. When a crisis arises, these databases and relationships established during their development will facilitate effective intelligence support of the force projection operation.

The G2 (S2) and ACE use the ASAS daily in garrison to develop contingency specific intelligence databases, IPB products, working aids, and operational procedures. The commander directs the intelligence effort through his PIR and IR on his most likely contingency operations. The G2 (S2) uses his ASAS equipment to develop and distribute intelligence estimates, plans, and other products which support contingency planning, wargaming, and decision making. Based on the commander’s guidance and G2 (S2) direction, the ACE establishes databases, intelligence support relationships, access to higher echelon databases, and internal ASAS procedures for each potential contingency. The MI unit commander uses the guidance and products mentioned above to examine his force, requirements for each contingency, and to execute battle-focused training.

SITE SELECTION

Mission, support relationships, communications, logistics, and security are some of the factors which must be considered when determining the location, configuration, and connectivity requirements of ASAS equipment. When not part of a larger command post, ACE leaders must ensure the site provides concealment, cover, and security for ACE personnel and equipment. When possible, the ACE should optimize the use of existing structures such as warehouses, hangers, bunkers, and barns. Some specific site selection considerations for the ACE and its ASAS equipment include—

- Type of operation (conventional offensive, forcible entry, humanitarian assistance, etc).
- Tactical situation (hostile OOTW environments like that in Somalia or a full-scale military operation such as Operation DESERT STORM).
- Terrain (drainage, slope, trafficability, vegetation, and routes of ingress and egress).
- Connectivity with IEW sensors and communications systems (transmitter LOS and access to MSE nodes).
- Sources of reliable tactical and commercial power.

Site reconnaissance is essential to choosing and occupying a good position. The ACE site reconnaissance team must be very familiar with the ASAS equipment's physical and mission requirements. The team should evaluate potential sites based on the guidance of the G2 (S2) and the considerations addressed above. After selecting a site, they should develop a site sketch showing routes to the site, significant terrain features, and the location of major systems. The ACE chief uses the reconnaissance team's sketch and briefing to make his decision on the final site selection.

PREDEPLOYMENT

Prior to deployment, G2 (S2) and ACE personnel must ensure that the ASAS databases contain up-to-date and relevant information. Analysts and database managers should continuously update and refine contingency databases while in garrison. This effort must include close coordination and an in-depth database deconfliction at all levels. Database maintenance should also ensure sufficient space on electronic storage media to handle the volume of information that will be generated during the operation. Backup files should be available in case of a system failure or the operational loss of an ASAS component during deployment.

G2 (S2) and ACE must plan and, if possible, test communications connectivity before deploying. The level of predeployment coordination should include information on the distribution of IP addresses, router allocations, message addresses, database passwords, and frequencies, to name just a few. In a force projection operation, this would include determining how the intelligence support base will communicate with forces enroute and the DISE from predeployment through completion of the initial entry operation. In conventional offensive operations, G2 (S2) and ACE planning would identify how to maintain contact with the tactical command post and forward deployed IEW assets. The end state of this planning and coordination should be seamless, uninterrupted intelligence support to the commander.

DEPLOYMENT

After securing the site, the ACE advance party uses the site sketch to identify and mark the location of ASAS equipment prior to the arrival of the ACE into the site. Upon arrival of the ACE main body, the advance team first positions the CCS, DPS, and additional communications systems such as the TROJAN SPIRIT II to immediately establish external communications.

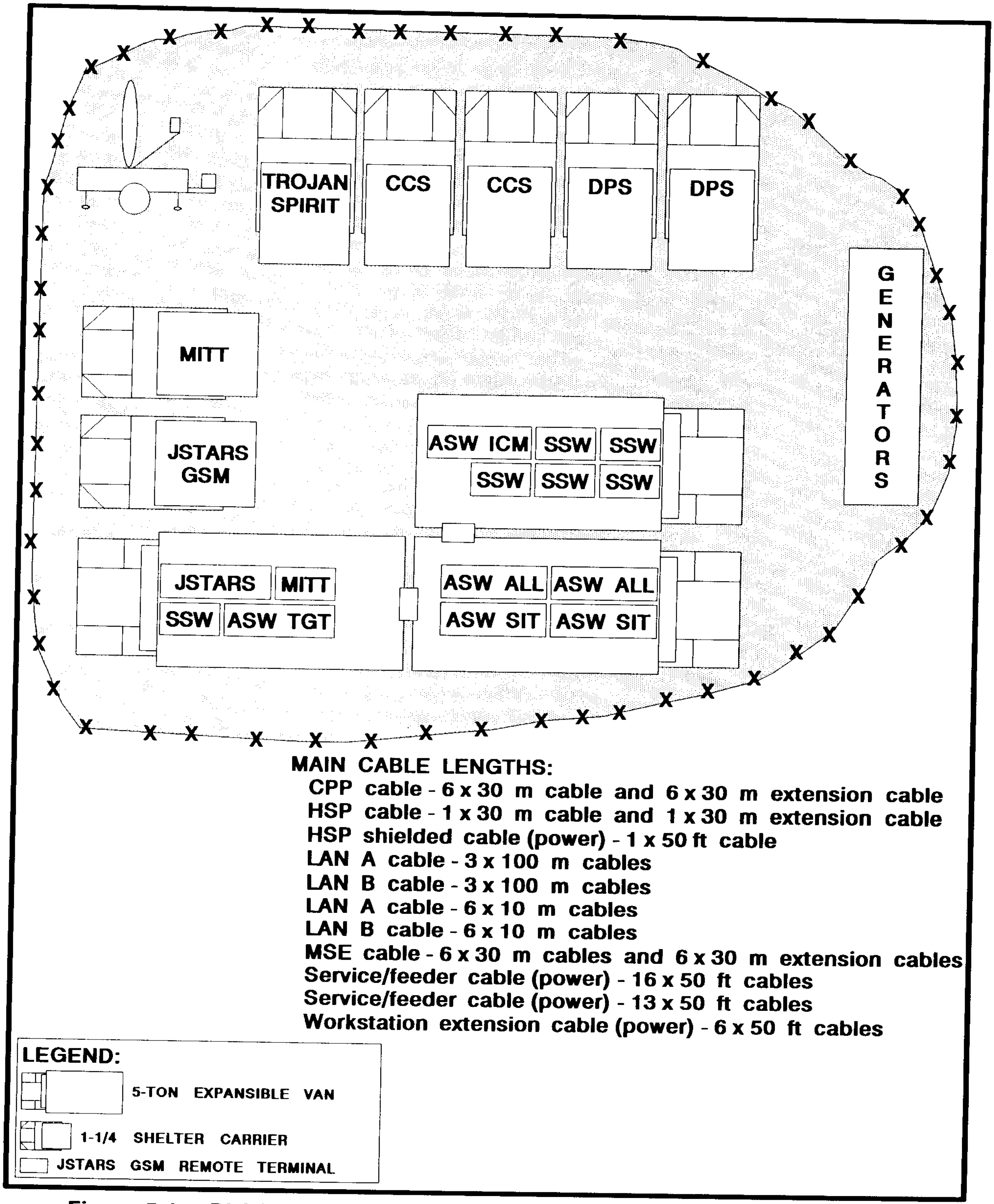
Next, the team positions the vehicles or tentage in which the ASAS workstations are operated. ACE personnel then establish ASAS workstations configuration, internal connectivity between the ASAS components, and physical security using triple strand concertina wire. When positioning the ASAS, ACE personnel must keep in mind the limits imposed on the location of workstations, CCS, DPS, and SEE by power distribution requirements and communications cable lengths. Figure 5-1 is an example of an armored or mechanized division ACE. The final responsibility of the advance party is to identify the location of the life support area to ACE leaders for subsequent occupation. The ACE personnel continue to improve the site throughout its occupation. These improvements include—

- Incorporating non-ASAS terminals and systems into the ACE.
- Constructing fighting positions for both individual and crew-served weapons.
- Sandbagging generators to improve noise discipline.
- Burying power and communications cables.

WORKSTATION CONFIGURATION

The ASAS workstations are configured based on the factors of METT-T. Tactical tailoring takes into account both the configuration of SCI ASAS and non-ASAS workstations in the ACE and the allocation of the ASAS-RWSs. There is no single “right way” to configure the ASAS. However, the ACE chief must determine and specify the configuration to the G2, ACE, and other staff personnel before deployment. The ACE chief should base the configuration on a specific methodology. A hedge-podge mix of configurations, poorly explained to those concerned, risks intelligence failure and compromise of effective battle command.

REMOTE WORKSTATION:
The ASAS-RWS is the G2 (S2) principal tool for maintaining situational awareness and developing estimates of future enemy operations. As the IEW component of the ABCS, the ASAS-RWS is also an important conduit for intelligence and targeting information outside the Intelligence BOS. The



MAIN CABLE LENGTHS:

CPP cable - 6 x 30 m cable and 6 x 30 m extension cable
HSP cable - 1 x 30 m cable and 1 x 30 m extension cable
HSP shielded cable (power) - 1 x 50 ft cable
LAN A cable - 3 x 100 m cables
LAN B cable - 3 x 100 m cables
LAN A cable - 6 x 10 m cables
LAN B cable - 6 x 10 m cables
MSE cable - 6 x 30 m cables and 6 x 30 m extension cables
Service/feeder cable (power) - 16 x 50 ft cables
Service/feeder cable (power) - 13 x 50 ft cables
Workstation extension cable (power) - 6 x 50 ft cables

Figure 5-1. Division ACE massed configuration (armored and mechanized).

G2 (S2) organizes his workstations to support battle command and future operations. He could position one ASAS-RWS in the G2 (S2) operations section at the main command post and one ASAS-RWSs in the G2 (S2) section of the forward command post. If available, the G2 (S2) can allocate ASAS-RWSs to the G2 (S2) plans section and other cells within the main command post. He may at times be directed to provide ASAS-RWS to subordinate non-ASAS equipped units such as the aviation brigade or an attached allied or coalition unit. In force projection operations, the ASAS-RWS is the most likely automated intelligence processing system used by the G2 (S2) at the port of debarkation and in the assault command post within the lodgement.

ALL-SOURCE WORKSTATION:

The ASAS-ASW is the primary fusion point within the ACE. It aids the ACE in turning combat information and single-discipline intelligence into all-source intelligence products and targeting information. The all-source intelligence section organizes its workstations to support the execution of six IEW tasks (discussed later in the Operations paragraph of this chapter), collection management, and dissemination. The ASAS-ASW configuration should be tailored based on the METT-T factors and unit capabilities. Figure 5-2 is an example of a divisional ACE tailored for a SIGINT intensive environment. The base ASAS-ASW configuration should consist of the following workstations and software application FIs:

Database. The database workstation uses “ALL” and “FMR” FIs to support database management and all-source fusion analysis. The analyst at this workstation ensures the ASCDB is accurate and current. Two ASAS-ASWs are normally designated as database workstations.

Situation. The situation workstation uses the “SIT” FI to support I&W, situation development, and IPB. This workstation is critical to developing and graphically portraying the common picture of the enemy situation.

Targeting. The targeting workstation uses the “TGT” FI to support rapid detection, tracking, and nomination of targets to the FSE. The targeting analyst also relies on products developed on the situation workstation to perform target development and BDA.

Analysts can use additional FIs such as “ICM” and “MRA” on these three workstations on a shared or dynamically allocated basis. The base ASAS-ASW configuration provides essential automation support needed for minimum ACE operations and split-based operations where the full ACE may not be deployed. Beyond the base structure, the ACE should allocate workstations to enhance the control and synchronization of IEW operations as well as intelligence production and dissemination. The following workstation designations are examples of allocations that support these objectives:

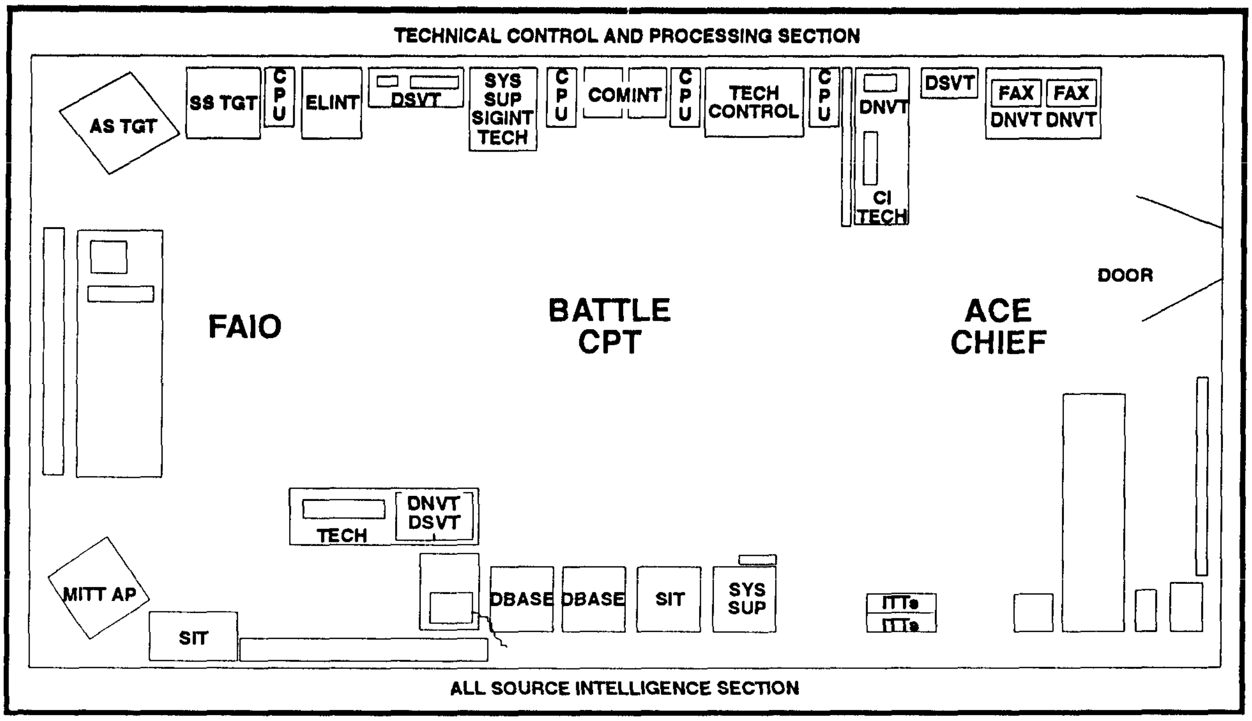


Figure 5-2. Division ACE configuration (airborne).

Collection Management. The collection management workstation uses the “ICM” FI to support requirements management, mission management and intelligence synchronization, and technical control. In addition to collection management, the “ICM” FI can also be used on other ASAS workstations to support multidiscipline counterintelligence (MDCI) analysis.

System Supervisor. The system supervisor workstation uses FIs “SPV” and “OPR” to establish communications patterns, configure workstation capabilities, and monitor system operations. The system supervisor can also use “FMR,” “SAT,” and “MRA” FIs to distribute intelligence products and serve as the ACE message release authority.

The ASAS-ASW can also be tailored to support new tasks or those not normally designated as a separate task in the ACE such as intelligence support to command and control warfare (C^2W), A C^2W workstation could use “ALL” and “SIT” FIs to develop information system specific IPB products and to identify critical enemy C^2centers of gravity. The C^2W workstation could be the focal point within the ACE for integrating ACE support to the four areas of C^2W (deception, EW, operations security [OPSEC], and targeting).

SINGLE-SOURCE WORKSTATION:

The ASAS-SSW processes the bulk of single discipline combat information and intelligence entering the ACE. The technical control and processing section organizes the ASAS-SSWs to support single discipline analysis, workstation configuration is therefore driven by the mission and nature of the threat rather than a fixed organizationally based allocation of processors. In a SIGINT intensive environment, this may require the section to increase the number of workstations performing communications intelligence (COMINT) and ELINT analysis. These COMINT and ELINT workstations can in turn be organized to look at activity within specific portions of the battlefield framework. This type of configuration helps the section process enormous amounts of message traffic while still providing timely intelligence support to decision making and targeting. Figure 5-2 and the lessons learned example at the end of this section illustrate the flexibility of the ASAS and one possible configuration.

COMINT. The COMINT workstation focuses on the analysis of COMINT reports and maintenance of supporting technical databases. This workstation can also receive tactical electronic intelligence (TACELINT) data and correlate these products for a complete SIGINT product. The results of COMINT analysis are forwarded to the all-source intelligence section as input to all-source analysis and targeting.

ELINT. The ELINT workstation is responsible for assembling the electronic order of battle (EOB) and maintaining the ELINT database. The operator provides results of ELINT analysis to the COMINT workstation and the all-source intelligence section.

SIGINT. The SIGINT workstation supports SIGINT fusion analysis and reporting. It can serve an additional function as a SIGINT or single discipline targeting workstation. In this role, the SIGINT workstation analyst works closely with the target nomination team to ensure timely analysis and reporting of targeting information. The workstation uses COMINT and ELINT reporting to develop EOB and C^2 node overlays. These products support C^2W and the targeting effort of the all-source intelligence section.

IMINT. The IMINT workstation processes narrative IMINT products such as reconnaissance exploitation report (RECCEXREP). Narrative imagery products are automatically parsed and placed in the ASCDB. The IMINT analyst works with the operators of intermediate processing systems like the MITT, GSM, and UAV GCS to provide imagery support to targeting and IPB. If equipped with a JDISS, the IMINT workstation can interface directly with theater and national imagery sources. The TROJAN SPIRIT II also can be used to access theater and national level sources. The IMINT analyst maintains the IMINT database for use by the ACE in producing all-source intelligence and targeting products.

HUMINT and MDCI. This workstation is responsible for analyzing and reporting HUMINT and MDCI. The analysts produce a fused SCI product that supports all-source intelligence production, force protection, and target development. Most HUMINT data will be provided via hardcopy reports which are handcarried to the HUMINT workstation. This information can development. Most HUMINT data will be provided via hardcopy reports which are handcarried to the HUMINT workstation. This information can also be provided via of the collateral interface to subordinate units that have the capability to report electronically. Size, activity, location, unit, time, and enemy (SALUTE) report data from subordinate units are the most frequently generated HUMINT and will be the primary source of information used for this production mission. CI and SALUTE reports can be received and disseminated automatically.

Lessons Learned

ASAS Single-Source Workstation Configuration
82d Airborne Division Warfighter Exercise
Battle Command Training Program 94-05
6 to 10 March 1994

Based on a Warfighter scenario of OOTW in a high SIGINT environment, the technical control and processing section organized its six Block I ASAS-SSWs to facilitate coverage of the battlefield framework and control MI battalion assets. The resulting configuration consisted of workstations for system supervisor, targeting or deep COMINT, ELINT, close battle COMINT, rear area COMINT, and HUMINT and Cl workstations.

The targeting or deep COMINT workstation simultaneously supported targeting and monitored deep battle COMINT activity. It was positioned adjacent to the ELINT workstation. The ELINT workstation covered the entire AO and AI. The deep battle was a critical fight and, consequently, occupied most of the focus for the ACE, The targeting and ELINT analysts developed techniques to cross-analyze data between work-stations. Based on the “pictures” on their ASAS-SSW screens, these analysts conducted EOB analysis. They associated ELINT reporting with COMINT reporting to identify and validate HPTs for the FAIO.

The close battle COMINT workstation monitored the area from the corps deep battle hand-over line to the division close battle area. The rear area COMINT workstation covered the close battle area to the division rear boundary, The overlapping coverage of the workstations ensured continuity of coverage and effective hand of of targets. It also forced analysts to exchange analytic conclusions and validate their analysis.

The remaining ASAS-SSW was dedicated to HUMINT and CI. The HUMINT and CI workstation supported MDCI analysis and the counter-reconnaissance fight, ASAS alarms set for the HUMINT and CI workstation were specific to the counterreconnaissance HPT list developed by the FAIO and the FSE.

In summary, the COMINT and ELINT workstations provided the division commander with indicators of enemy actions. They also gave the commander an idea of the effectiveness of the division deception plans. The division FSE had direct access to SIGINT via the FAIO and the single discipline targeting NCO. The division’s Air Force liaison officer, aviation officer, and aviation brigade S2 could coordinate with the ELINT workstation NCO for analyzed EOB radar data for deep attacks, They also received information on remnant and stay-behind forces from the close and rear battle COMINT workstations. The HUMINT and CI team along with information from the division support command (DISCOM) S2 and the rear command post greatly assisted the division in its rear area fight. The commander personally reviewed ASAS-SSW products and grilled analysts for Interpretation. The commander was able to interpret these products on his own and grew to trust the capabilities of both ASAS and the ACE.

OPERATIONS

The ACE uses the ASAS to support the commander's plan and direct operations during war and OOTW. The ASAS supports both target and situation development in the deep battle by using ASAS time-saving processing functions. ASAS supports the close battle by developing the enemy situation portion of the common picture of the battlefield for use in the planning, preparation, and execution of missions. This common picture and integration of both the friendly and enemy situation in ASAS assists analysts in assessing friendly vulnerabilities and potential enemy targets. Intelligence collection requirements and indicators of enemy activity in the rear area, developed through a thorough IPB of the rear area, are entered into ASAS in the same way as requirements for the deep and close battle. The six IEW tasks described below are the basis for the ACE support in deep, close, and rear area battles.

INDICATIONS AND WARNINGS:

I&W, as a distinct function, is performed routinely at the EAC level. The I&W analyst uses the ASAS-ASW or ASAS-RWS to develop critical alarms that automatically alert analysts to sensor data or reports that meet established I&W criteria.

SITUATION DEVELOPMENT:

From IPB products and participation in the battle staff wargaming process, the ACE develops the collection plan and intelligence synchronization matrix (ISM). These products focus on the commander's PIR and targeting priorities within the AO and AI. Using the ASAS, the ACE records and transmits collection management data electronically to appropriate agencies and assets. Individual ACE analysts develop alarms, and database queries to filter information needed to answer these PIR. These filters and the ASAS capability to automatically correlate reports assist in the analysis and synthesis of large volumes of information. As information is received, ASAS automatically posts, logs, and correlates reports. From this information, the ACE develops a picture of the enemy situation derived from multiple sources and disciplines. The G2 (S2) can then use his ASAS-RWS to rapidly distribute this picture of the enemy situation to subordinate, adjacent, and higher units. Figure 5-3 shows the information flow between the ACE and the G2.

Development. Situation development begins at the situation workstation in the all-source intelligence section. Using the ASAS-ASW, the analyst develops the enemy situation by querying and displaying the requested ASCDB holdings on an electronic SITMAP overlay. The information displayed on the SITMAP is sanitized then disseminated to the ASAS-RWS as an external database coordination (EDC) message. This EDC represents a sanitized version of the holdings of the ASCDB. The ACE analyst creates the sanitized EDC message and coordinates with the CCS or CAMPS operator for its release to the G2 (S2) ASAS-RWS. The ASAS-RWS can then display the same situation data as it appears on the

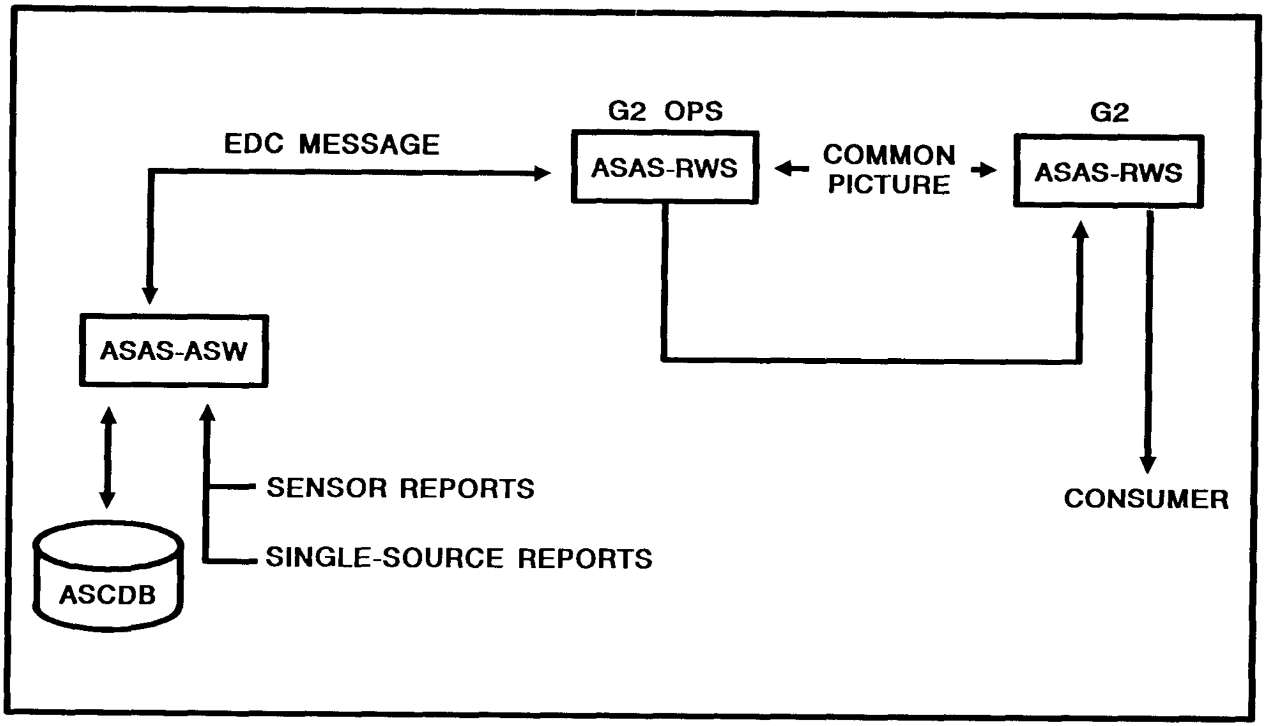


Figure 5-3. Flow between the G2 and ACE for collateral situation development.

situation workstation. The situation analyst uses the latest information developed by ACE single-discipline analysts and reporting from IEW assets to keep the enemy situation graphics updated.

Graphic Production and Dissemination. The ACE situation analyst can create collateral text and graphic intelligence summaries (INTSUMs) of the current situation. The analyst compares this picture with the SCI-level electronic SITMAP and modifies features of the picture to create the most informative INTSUM. Using his ASAS-RWS, the G2 (S2) can modify the INTSUM to reflect the latest friendly situation or tailor it to specific user information requirement. The G2 (S2) then disseminates the graphic INTSUM via LAN to elements within the command post and WAN to subordinate units.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD:

The IPB process and resultant products are the foundation of the decision making process and wargaming. The G2 (S2) improves his ability to perform IPB by integrating the automation capabilities of the ASAS system into IPB development. Optimal use of ASAS depends heavily on the analyst automating the IPB process through the use of database queries. The analyst uses these applications to develop templates, record information, and support IPB products. OB information can be stored in shared databases and electronically updated. Digitized terrain and elevation data in the ASAS-SSW assist in developing and refining electronic templates. Figure 5-4 illustrates the information flow within the ACE for all-source intelligence production.

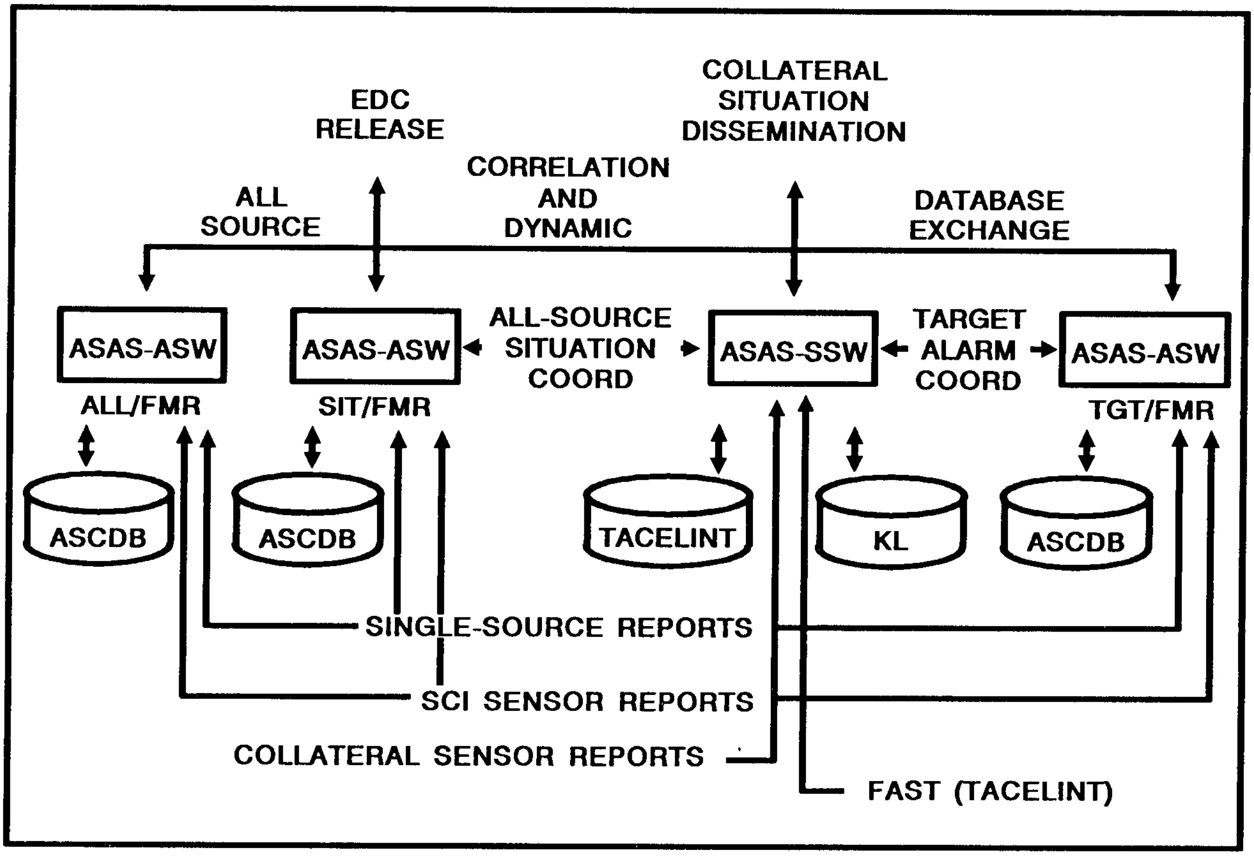


Figure 5-4. Information flow within the ACE for all-source production.

Development. Essential to providing IPB input to the decision making process is an understanding of how manual production techniques are integrated and interpreted by ASAS. For example, the event template graphically portrays named areas of interest (NAIs). In order for ASAS to key on these areas, analysts must interpret and then establish database queries. These actions provide the analyst with confirmation of the threat's present COA and indications of future plans. Taking this collated data, the G2 (S2) can then project the adversaries' future COAs and make adjustments to the event template or other IPB overlay products. Adjustments and recommendations to the HPT list and attack guidance matrix (AGM) are also made.

Dissemination. The ACE is connected to the G2 (S2) and the G2 plans section through the ASAS-RWS. This allows the ACE to electronically transfer databases to the G2 (S2) for planning. The G2 plans officer can use the electronic templates, overlays, and supporting text to determine threat COAs and plan future IEW operations. The ASAS-RWS allows the G2 plans analyst to modify IPB products based on the latest planning information from higher echelon intelligence organizations. The G2 (S2) cell can distribute collateral IPB, wargaming, and planning material within the command post via LAN or to subordinates over MSE. The following provides an example of how ASAS supports the decision making process.

See FM 101-5 and FM 34-130 for information on decision making and IPB.

Lessons Learned

ASAS-RWS and the Decision Making Process 2d AD Warfighter Exercise
Battle Command Training Program Rotation 94-06,27 to 31 March 1994

Normally, in wargaming, the G2 plans officer maneuvers enemy icons down the avenue of approach, or puts them into the defense. The G2 plans officer identifies various phases of threat fire support and locations of reconnaissance, first and second echelon forces, and reserve forces at different H-hours Simultaneously, the G3 plans officer maneuvers friendly icons. Representatives from fire support, aviation, chemical, service support, engineers, EW, PSYOP, deception, air defense, and MP identify their probable activities at various hours. The scribe tries to capture this information plus the outcome of each engagement on a BOS synchronization matrix.

The BOS matrix is valuable, but not perfect, Previously, the G3 plans section said that after wargaming, when they attempted to build the COA decision briefing. It was hard to recall how they maneuvered icons during the wargame. They pointed out that the BOS synchronization matrix did not provide enough detail to reconstruct the fight. Using ASAS workstations helps solve this problem.

During the Warfighter Exercise, the wargaming worked about the same as during earner exercises, The analyst posted the map board with the projected locations of enemy and friendly units. The G2 and G3 stood at the map and conducted engagements between their icons. Representatives from various BOSs waited to contribute to the wargaming. The scribe recorded the results on the synchronization matrix. There was, however, one difference. Sitting off to one side of the map was an ASAS-RWS that also contained the templated initial locations of enemy and friendly units. As G2 and G3 plans officers moved their icons on the map; the ASAS-RWS operator moved the icons on the computer screen. As each side destroyed units, the operator deleted the icon while the G2 and G3 plans officers removed them from the map.

One advantage of the ASAS-RWS over the map was the ability to save a screen as an overlay. When G2 and G3 plans officers finished wargaming an H-hour, the ASAS-RWS operator labeled the hour on the screen and displayed the major activities, The operator saved the overlay to show the situation at that point. The operator removed the labels from the screen and continued the process until the G2 and G3 plans officers established the final set of locations for the next hour.

When the wargame was over, the operator could go to the overlays list and recall any hour of the battle. On the workstation, the operator saved the icons exactly where they were at that point in the wargame; whereas, the map merely displayed the end state. Without the ASAS-RWS, the flow of the battle at each critical event was lost in the pile of removed enemy and friendly stickers.

The ASAS-RWS operator further helped the planning process by printing a hardcopy of each H-hour. This allowed the G3 plans officer to examine each hour or critical wargame event and use the prints as snapshots in the COA decision brief. The G2 plans officer used the hard copies to help create a timeline of enemy activities The operator could also recall each overlay in the database and create a digitized slide from the screen, Once the operator created the slides, he animated them chronologically. This resulted in a moving picture of the battle as icons moved and engagements occurred. This provided a clear, concise picture of how the G2 and G plans officers executed the battle. The workstation operators then sent the digitized slides to subordinate units electronically. This allowed planners at all levels to call them up and discuss planning assumptions.

The ASAS-RWS was valuable in the G2 plans section during the division Warfighter Exercise. It increased efficiency and effectiveness, allowed the G2 and the ACE to focus on analysis, and most important, developed a common picture of the battlefield for every level.

SUPPORT TO TARGETING AND TARGET DEVELOPMENT:

The ACE uses the ASAS to identify, track, and report targets developed during the targeting process. The ACE targeting nomination team can produce and compare target overlays to IPB templates and incoming reports. The analyst can develop target alarm criteria to ensure incoming reports are prioritized based on the targeting priority. Targets determined to be valid, accurate, and timely are sent electronically to the FSE using a target intelligence data (TIDAT) report. Figure 5-5 shows the information flow between the ACE and the FSE.

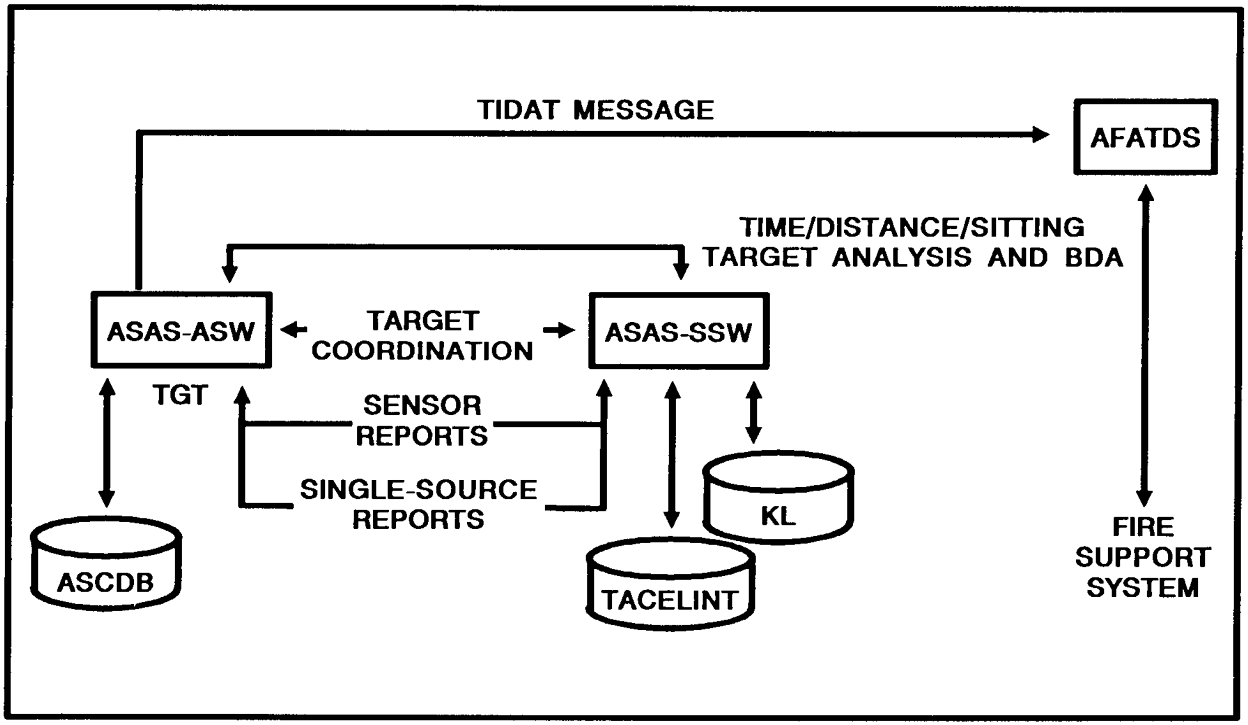


Figure 5-5. Information flow between ACE and FSE for target development.

Development. The ASAS is an important tool for support to targeting and target development. The ACE targeting analyst can load IPB, maneuver, and fire support products into the ASAS targeting workstation and display them graphically when needed. The analyst uses products developed during the DECIDE phase of the targeting process to assist identifying, tracking, and nominating targets. Some examples of these targeting products are HVT and HPT lists, AGM, and the EW target list. The AGM is a key product for determining priorities and targets for engagement. The targeting analyst, for example, can move a report regarding HPTs to the top of a message cue, even if it was the last report received, according to priorities set in the AGM. The analyst cannot, however, decide when to change priorities. These decisions must come from the FSE, G2 (S2), and ACE leaders who are thoroughly familiar with both enemy and friendly situations as well as the commander’s targeting requirements.

Dissemination. The targeting workstation analyst sends a TIDAT message to the CCS or CAMPS. The TIDAT is then forwarded to the AFATDS for action.

See FM 6-20 and FM 6-20-10 for additional information on targeting and target development.

FORCE PROTECTION:

Automated access to databases and collectors aids the ACE in identifying, assessing, and developing countermeasures for threats throughout the AO. CI information can be disseminated and specific CI tasks issued from ASAS. Indicators of unconventional warfare activity can be entered into ASAS as threat alerts and alarms. The integration of multidiscipline collection management and analysis in the ACE facilitates MDCI analysis.

See FM 34-1 and FM 34-60 for additional information on Cl support to force protection.

BATTLE DAMAGE ASSESSMENT:

The ACE links collection management, targeting, and situation development into a single synchronized intelligence effort. ASAS supports tracking of requirements, technical control, analysis, and dynamic tasking of IEW assets. These capabilities allow the ACE to provide both immediate feedback on BDA-related PIR and conduct long-term threat assessments.

See FM 34-1, FM 34-2 and FM 6-20-10 for additional information on BDA and intelligence support to BDA.

DEGRADED OPERATIONS

The ASAS, like any other system, is subject to hardware and software failures that impact on its ability to execute some or all of the operations it is designed to perform. ASAS may also be unavailable due to deployment, enemy action, accident, or redeployment. The system has no redundant equipment to allow for continued fully automated operations in the event of a major system failure or loss. ACE supervisors and analysts must be prepared to use the ASAS in a degraded operational state that may require a mixture of manual and automated IEW operations for a limited time. Because of the systems complexity and the diverse missions of the ACE, there are no set solutions for any specific degraded condition.

It is essential that units train personnel to identify and perform critical tasks under difficult or degraded conditions in order to complete the mission. Manual procedures must be incorporated into unit METL and standing operating procedures (SOPs) as well as practiced in exercises and training. Once ASAS operators identify a defective component or software process, the ACE chief or section supervisor must decide whether to continue the mission with degraded automation capability or implement manual procedures. ACE personnel should consult unit maintenance personnel and system technical manuals to determine the extent of system reconfiguration and limitations during the degraded state.

REDEPLOYMENT

During redeployment of the ACE, one or two ASAS-SSWs and one ASAS CCS must remain operational and connected to an MSE node or other data communications means. The remainder of the ACE moves, including the second CCS; the first CCS remains stationary and continues to receive automated message traffic. The first CCS operator monitors message traffic to identify and report critical intelligence. These reports can be printed in hardcopy and verbally disseminated via MSE, SINCGARS, or messenger. Once the ACE is in place and the second CCS is operational, the first CCS transmits its stored data to the new location. The first CCS moves to join the ACE and updates its databases. The download and update choices are last in, first out (LIFO); first in, first out (FIFO); or by precedence (FLASH, PRIORITY).

Chapter 6

SURVIVABILITY AND SECURITY

ASAS can deploy anywhere the commander needs it, from garrison or an intelligence support base to tactical command posts on the battlefield. Commanders and MI personnel must take proactive measures to protect the system, recognize and counter threats to the system's survivability, and provide security to protect its operations.

SURVIVABILITY

The ASAS like most systems is vulnerable to a variety of threats. The type and degree of threat to ASAS is influenced by the type of unit in which the system operates and its proximity to hostile forces. Another factor is the capability of the threat to identify, locate, and target the ASAS or, more accurately, the unit that the ASAS supports. The most common battlefield threat to ASAS will be from lethal and nonlethal fires. Figure 6-1 shows some of the survivability measures that could be taken by a division ACE.

LETHAL FIRES:

Positioning the ASAS to take advantage of concealment and cover reduces the vulnerability to direct and indirect fire. Conducting split-based operations where the bulk of ASAS equipment remains outside the AO can also dramatically reduce the risks poised by threat weapon systems. ACE personnel must be proficient in the use of camouflage to supplement natural concealment and cover in order to reduce the possibility of detection and attack by the enemy.

NONLETHAL FIRES:

Using correct COMSEC procedures helps reduce ASAS vulnerability to nonlethal fires from EW systems. Reliance on MSE rather than the CCS's UHF or VHF radios reduces susceptibility to intercept, direction finding, and electronic attack. When use of UHF and VHF communications is necessary, the enforcement of COMSEC procedures can reduce the risks of enemy EW to these radio and ASAS.

SECURITY

Most of the information the ASAS processes is classified defense information. ACE personnel must protect this information in accordance with Director of Central Intelligence Directives (DCIDs), DOD Manuals (DODMs), DIA Manuals (DIAMs), NSA United States Signals Intelligence Directives (USSIDs), and Army Regulations (ARs). These directives provide guidance and requirements on how to collect, process, produce, disseminate, store, and discuss classified information both in garrison and at field locations (see Figure 6-l).

PERSONNEL SECURITY:

Access to ASAS equipment processing SCI data located within a SCIF is limited to personnel with proper clearances and the need to know. DCID 1/14 and AR 380-67 provide guidance on personnel security. All personnel with access to SCI data, equipment, and work areas must be properly indoctrinated, cleared to the level of intelligence being processed or stored, possess a need to know, and be listed on a current security access roster. Personnel operating ASAS workstations must have individually assigned system user names and passwords.

PHYSICAL SECURITY:

Security standards for garrison operations are based on the guidance for use of SCIFS (as defined in DCID 1/21 and AR 380-28) in a semi-permanent configuration such as a motor pool or similar area. These standards are similar to those for field training and combat operations in that they can only prescribe the minimum requirements, since each situation differs. Situation and time permitting, personnel must improve on the minimum standards using the security considerations and requirements for permanent secure facilities as an ultimate goal. ACE personnel will use permanent facilities if available. The following SCIF requirements should be met while operating ASAS in garrison, field training, combat operations, or OOTW:

- The SCIF must be located within a controlled area with the perimeter conspicuously marked by a physical barrier. In a field environment, this barrier should be of triple-strand concertina wire (See Figure 6-1).

- The perimeter must be guarded by walking or fixed guards to provide observation of the entire controlled area (See Figure 6-1).

- Access into the controlled area must be restricted to a single entrance.

- Material must be stored in General Services Administration (GSA)-approved security containers.

- Emergency destruction and evacuation plans must be kept current.

In field training, G2 (S2) or ACE personnel must request accreditation for a tactical field SCIF according to DCID 1/21. Temporary SCIFs are evaluated and accredited on a case-by-case basis due to the many variables in use, configuration, guard response, location, construction, and type of storage.

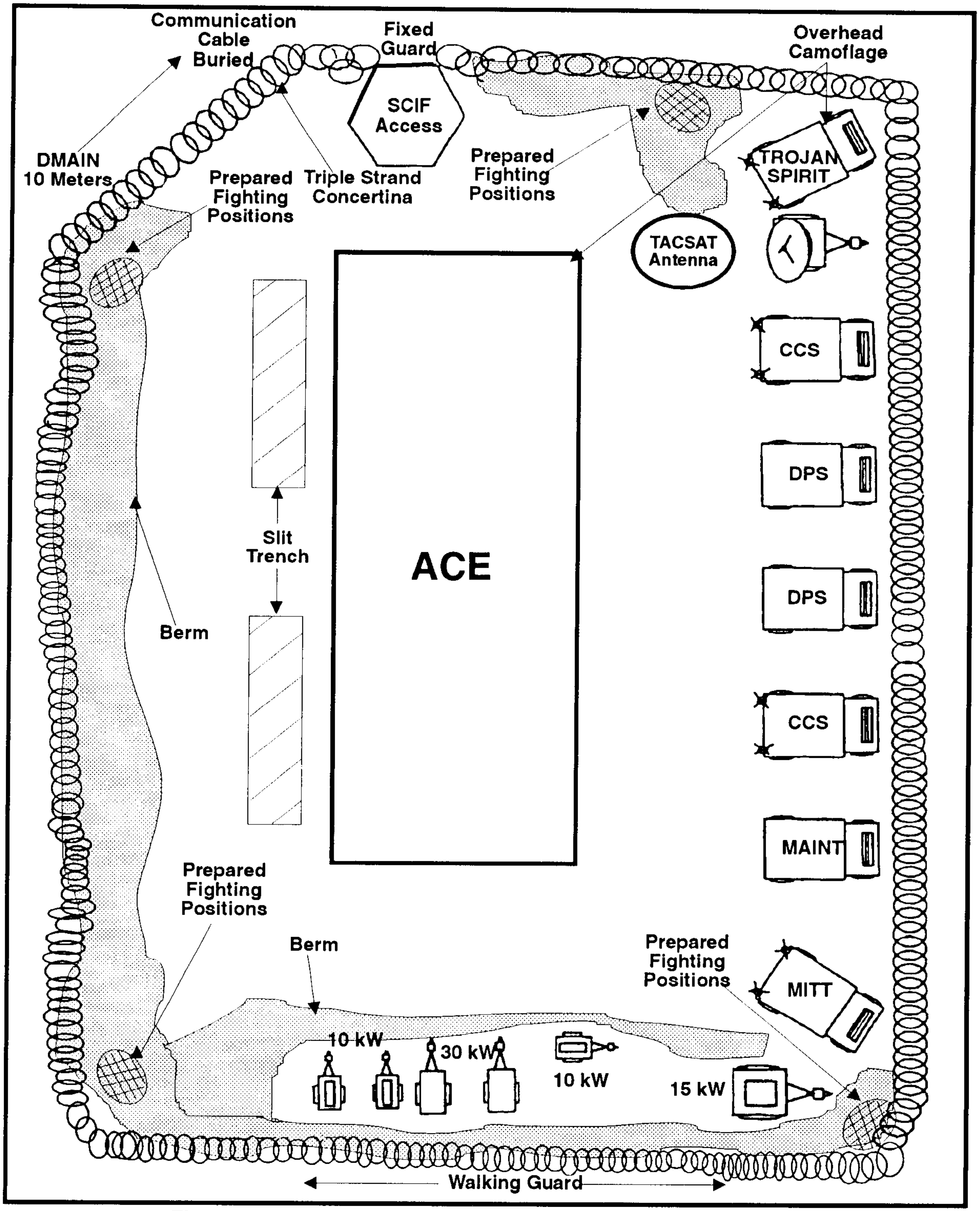


Figure 6-1. Division ACE survivability and security (airborne).

INFORMATION SECURITY:

ASAS operators must have individual user names with assigned passwords protected by appropriate security measures. In garrison, ASAS operators must store all removable storage media and hardcopy products in approved containers. They must place the storage media in a locked container that the special security office (SSO) has authorized, and must remove and store the following components in accordance with regulations and unit SOPs:

- Hard disk drives (HDDs).
- Cartridges from the optical disk drive (ODD).
- Hardcopy products from the printer.

COMMUNICATIONS SECURITY:

ASAS COMSEC has the same requirements as other communications facilities processing SCI. COMSEC procedures must follow AR 380-5, AR 380-28, and AR 380-40. Personnel are not to operate nonsecure communications systems within the restricted classified discussion area. The ASAS-RWSs operate at the SECRET security level. Each workstation has its own signal address and interfaces with ASAS SCI workstations using the Version 2 Data Adapter (V2DA). Other local workstations interface with the ASAS-RWSs via a collateral LAN. The following security requirements include—

- All cryptographic equipment and keying material are safeguarded according to regulations and unit SOP.
- All cable and field wire entering the SCIF are authorized by the unit SS0 and are pad of the system.
- Unencrypted classified data and voice lines are identified by tags at the communications panel and show classification level.
- Protective radio frequency interference gaskets and shielding are intact and complete.

SANITIZATION AND DESTRUCTION PROCEDURES:

The following ASAS sanitization and destruction procedures should be incorporated into the ACE operations and unit SOP:

- Conduct training to ensure all personnel are familiar with sanitization and destruction procedures.
- Sanitize all devices containing classified material before maintenance by uncleared personnel.

- Incorporate incendiary methods into emergency destruction measures to ensure the total destruction of SCI material.

- Sanitize all devices in accordance with DODM 5200.M2 and appropriate technical manuals.

Chapter 7

MAINTENANCE

A mixture of Army soldiers, civilians, and contractors maintain the ASAS. The most important ASAS maintainer is the system operator. The ASAS operator preventive maintenance checks and services (PMCS) keep the system combat ready and ensure early detection of potential problems. Trained ASAS maintenance personnel, both military and contractor, support the operator when hardware or software components fails. Together, operators and maintenance personnel keep the ASAS operational and ready to support the unit's IEW mission.

RESPONSIBILITIES

Operators, unit maintenance personnel, and contractor logistics support (CLS) perform most maintenance for ASAS unique equipment. The exception are those line replaceable units (LRUs) and shop replaceable units (SRUs) having test program set (TPS) support. CLS provides maintenance on contractor-furnished equipment (CFE). Corps and division support commands base shop test facilities (BSTFs) perform maintenance on TPS supported items. Established Army logistics procedures and organizations support ASAS GFE. ASAS maintenance responsibilities can be broken down into the following areas.

OPERATOR:

ASAS operators perform PMCS and limited corrective maintenance of ASAS GFE and CFE. Operator PMCS consists primarily of running built-in-tests (BITs), checking cable connections, and observing normal functions of equipment. The ASAS operator performs PMCS (visual inspection, test, cleaning, tightening, and minor adjustments); limited corrective maintenance (such as replacing filters); and calibration checks (using BIT diagnostics). Operators use system software alarms, notices, and operational diagnostic subsystems to fault-isolate equipment malfunctions. Operators may also reinstall the component after repairs by maintenance personnel.

UNIT MAINTENANCE PERSONNEL:

Unit maintenance personnel use BITs to fault-isolate equipment malfunctions to the defective LRU. They remove the defective LRU and install spares to return the system to operational status. Authorized repairs are limited to items that are easily replaceable and do not require complex adjustment or system alignment after replacement such as knobs, exterior cable assemblies, and expendable antennas.

CONTRACTOR PERSONNEL:

Contractor personnel perform troubleshooting and maintenance on all CFE LRUs and SRUs not supported by TPS. Army maintenance personnel are responsible for direct support level maintenance of ACE equipment (CCS, DPS, workstations, and SEE).

SUSTAINMENT LEVEL ACTIVITIES:

Repairs beyond field level maintenance (unit or contractor personnel at the Ml unit) capabilities for the equipment supported by TPS are evacuated to a designated Army maintenance activity at the sustainment level. Contractors will support single-source hardware at these facilities. Sustainment level maintenance support includes the rebuilding or overhaul of major assemblies and subassemblies. Maintenance personnel will sanitize and evacuate for repair or disposition any LRU or SRU that is not repairable at the field level in accordance with source maintenance recoverability (SMR) codes. These codes can be found on the unit authorized parts list.

HARDWARE MAINTENANCE

ASAS maintenance has separate channels for hardware and software maintenance. To ease hardware maintenance planning at each level, all spare parts are categorized as LRU or SRU. LRUs are major items that maintenance personnel can easily replace onsite. Examples are keyboards, monitors, printers, cables, and removable hard drives. SRUs are items internal to an LRU and are sent to a shop for replacement or repair. Examples are printed circuit boards, internal power supplies, and internal wiring. ASAS hardware maintenance covers two categories of equipment: GFE and CFE.

GOVERNMENT-FURNISHED EQUIPMENT:

GFE is standard Army equipment that is not ASAS specific. The operator does PMCS according to the applicable manuals which should already be familiar to equipment operators.

CONTRACTOR-FURNISHED EQUIPMENT:

CFE is equipment that is ASAS specific. The operator still does PMCS. Unit and higher level maintenance requirements are handled as previously described in this chapter under **Responsibilities.**

SOFTWARE MAINTENANCE

ASAS software maintenance is critical to effective unit operations. Under Army Maintenance Policies, software maintenance is considered a sustainment function within the responsibilities of unit maintenance. This sustainment function is performed for all ASAS equipment by the on-site FSSS personnel and the unit operators. The CECOM Software Engineering Directorate (SED), located at Fort Huachuca, AZ, is responsible for making ASAS software baseline changes which affect the operational capability of the system software. The CECOM SED maintains overall responsibility for managing, quality controlling, and configuration management (CM). CECOM SED also ensures that the multiple versions of software developed for the various subsystems of ASAS located worldwide meet the warfighters' critical mission requirements.

If during normal system operations the operator experiences a system failure. The operator will first attempt to eliminate any possibility of hardware problems. If system diagnostic procedures in the Operator Users Manual eliminate hardware as the related failure, the operator will attempt to focus the problem to a specific application of the software. If the failure can be corrected, the mission continues; if not, the operator will contact the on-site FSSS representative for assistance. Together they will attempt to recreate and verify the problem. If the problem cannot be corrected using standard system keystrokes, then a Software Problem Report (SPR) will be generated. This SPR is logged, then forwarded through the Regional Software Support Activity (RSSA), back to CECOM SED for action. If the unit decides that the software does not provide adequate functionality or capability, the unit must submit an SPR recommending what changes or enhancements should be made.

FIELD SOFTWARE SERVICES SUPPORT (FSSS)

This section will discuss the FSSS concept implemented by CECOM SED. CECOM SED is responsible for providing Life Cycle Software Support (LCSS) for all IEW Mission Critical Defense Systems (MCDS) of which the ASAS program is a part. The concept for FSSS is implemented during the Post Deployment Software Support phase of the project's life. SED's mission is to provide dedicated on-site software support as well as to manage an RSSA for all ASAS equipment fielded. The primary role of FSSS is centralized around performing tasks which will sustain computer processing operations, both in garrison and field environments. The FSSS function is maintained until such time as Army personnel are routinely trained to perform those tasks which are executed by the FSSS representatives or until the system leaves the Army inventory.

FSSS LEVELS:

FSSS is provided at two levels. The first level consists of dedicated on-site support at each ASAS fielded unit. For a specific period of time, two FSSS representatives are present to support the unit during the New Equipment Training Team (NETT) phase for equipment fielding until approximately 90 days following the departure of the NETT instruction. The primary purpose for the augmentation by FSSS personnel is to verify system operation during the initial fielding activities and to ensure operational effectiveness. At the end of the 90-day post-NETT period, the FSSS on-site support is reduced to one individual. The second level of support consists of augmentation from a regional base, the RSSA.

On-Site FSSS. SED has the mission to provide on-site contractor FSSS for each MI unit equipped with an ASAS. On-site FSSS personnel perform their functions using the supported unit's operational equipment. FSSS personnel serve as the liaison between the supported unit, the RSSA, and SED. A memorandum of agreement (MOA) between the unit and SED TFS provides a description of each organization's responsibilities in areas such as FSSS, security, logistical support, and administrative support. Agreements between the ASAS project manager, the US Army Training and Doctrine Command (TRADOC) system manager (TSM)-ASAS, and SED resulted in similar support being provided to the ASAS-Extended.

Regional FSSS. The RSSAs are at centrally located sites worldwide to augment and provide additional support to the FSSS site representative. Centralized support, as required, will provide—

- Telephonic assistance.
- Emergency site response.
- On-call response to unit problems.
- Periodic site assistance visits to system locations.
- A central point for SPR processing.
- Support to exercises.

The RSSA is staffed with FSSS representatives who have expert knowledge of each of the ASAS systems. The RSSA staff will also provide additional support for exercises and assist the on-site FSSS representative during vacation, sick leave, and emergency absences. Any exercise or contingency support will require as much prior notification and coordination with SED as possible.

RSSA facilities are located at the following five cities; Uijonjbu, Korea; Fort Huachuca, Arizona; Fort Hood, Texas; Fort Bragg, North Carolina; and Heidelberg, Germany. These sites focus their support on 20 field service sites. As additional units are fielded ASAS equipment, they will be assigned to an RSSA for the same regional support.

FSSS RESPONSIBILITIES:

FSSS personnel will prepare and maintain backup media for system-specific databases and system executable disks. They will perform periodic file maintenance, to include purging, archiving, and restoring data. FSSS personnel will run various system and diagnostic routines to ensure proper system operations. If a system's media is determined to be corrupted or unusable, FSSS personnel follow established procedures to recover the media and correct the fault or will reinstall the baseline media having difficulty.

FSSS for the ASAS requires periodic (routine), emergency, and nonroutine tasks. Periodic tasks include file maintenance, table and database maintenance, periodic database backup and restoration, and system initialization. Emergency tasks involve operations to identify, isolate, and correct operating system failures or other perceived software faults. Nonroutine tasks may include reconfiguring hardware and software, in the event that nodes within the enclave are inoperable due to a power failure, disk failure, or other causes. Other tasks entail listing file and disk directories, executing operating system software diagnostics, and viewing file contents to assess system problems. FSSS personnel responsibilities are discussed below:

New Software Version Release and Upgrade Installation. For any release of software, whether initial, upgrade or corrective, the FSSS personnel will be primarily responsible to load the software and run verification and parameter checks prior to being loaded on any unit's operational equipment. The software will arrive at the unit as a package containing, as a minimum, the following:

- Appropriate media with the operational software.
- Installation instructions.
- Change pages for SED supported documents such as operators manuals, software users manuals (SUMs), and a version description document (VDD) detailing changes in the latest version of software.

User-Reported Problems Investigation. FSSS personnel will assist each unit in identifying and resolving operational software problems. FSSS personnel will verify faults identified by first ensuring the problem is not related to operator or hardware error. FSSS personnel will try to replicate the problem encountered by the operator to determine if a work-around is possible. If not, the FSSS field representative will contact the supporting RSSA and ask if the same problem has occurred with other unit locations. If so, the RSSA will instruct the FSSS field representative on how to fix the error. Only the RSSA is authorized to call other regional sites to inquire about the identified error, unless the problem is time critical to the unit mission. If the problem is new, and the RSSA is unable to find an immediate work-around, the unit, assisted by the FSSS field representative, will generate an SPR. Only the unit commander will determine how critical the problem is to the unit operational mission requirements. Based upon this decision, a level of priority will be given to the SPR and forwarded to the supporting RSSA. The RSSA will review the SPR for completeness and accuracy. The SPR will be logged in at the RSSA before being forwarded to SED, Fort Huachuca. (NOTE: No SPR will be forwarded through the system until the security classification of the SPR is determined. If the FSS or unit is not sure, the local SSO will make the call.) Once received by SED, Fort Huachuca, it will be placed within the SPR or CM process, from which a technical bulletin will be produced, if necessary.

Site-Specific Requirements. FSSS personnel will load site-specific databases such as TEXTA, electronic parameter listing (EPL), or MIIDS and IDB which are provided to the FSSS personnel by the unit. FSSS personnel will also assist each unit in developing, loading, and maintaining site-specific files, tables, and exercise data. FSSS personnel will also assist the unit operators when necessary in maintaining and preparing backup database copies in the event of database corruption or other catastrophic failures.

Exercise Support. FSSS personnel will support garrison and field activities on a scheduled, preapproved basis. During field exercises, assigned FSSS personnel will accompany the unit to the field, work a normal duty day, and return to private quarters; however, they will be expected to remain on-call during the remainder of the duty day in the event a problem occurs with the supported software. Supported commands will be furnished with telephone and beeper numbers for FSSS personnel to facilitate recall procedures. Each unit exercise is unique. FSSS support operations span the globe from Southeast Asia to Europe. Prior planning and coordination with the FSS representative is critical to ensuring that the RSSA and FSSS Operations Center (Fort Huachuca, AZ) can identify and commit the necessary personnel and create the support estimates required by the unit to plan resourcing. The FSSS Operations Plan maintained within the unit identifies specific unit and FSSS personnel responsibilities for exercise support.

Operator Training Assistance. FSSS personnel will assist the NETT, as necessary, during initial unit training. The FSSS personnel provide new software release training to unit personnel, addressing any functional or operational changes necessitated by software updates, software releases, or the issuance of a technical bulletin. FSSS personnel can be asked to assist with a unit's established sustainment training program. Commitment of the FSSS representative for this requirement will be based upon a time available basis and coordination with the RSSA for resource commitment.

Map Data Conversion. Map data requests are processed and currently requested for specific systems through specific agencies. For map data requests concerning the ASAS-ASW and the ASAS-RWS, requests must be sent to the Program Management Office-Integration Fusion (formerly PM ASAS). This office is located at HQDA, PM-intelligence Fusion, 1616 Anderson Road, McLean, VA 22102-1616. For requests for ASAS-SSW, requests must be sent directly to SED, Fort Huachuca. In the future, all map requests will be centralized, and new request procedures will be published. Once the new map data is received, the FSSS representative will load the data onto the respective ASAS system.

FSSS CONFIGURATION MANAGEMENT:

CM is a process for ensuring that development and changes to system software is managed, edited, enhanced, and delivered under close control. The control factor is required to facilitate universal development and to handle required changes. For this reason, system operators are given only limited access to the system software files affecting the operational use, while the FSSS representatives have access to a full range of system applications via a special code word. Within ASAS equipment, numerous standard VAX and UNIX management utilities and tool sets are not made available to the user but are to the FSSS representative. Improper access to the operating system or improper use of the tool sets can result in lost or destroyed files, modified or lost functionality, or complete system failure. Only trained personnel are permitted access into these operating environments. Such capability requires extensive knowledge of the hardware, the operating system architecture, and capabilities of the tool sets. For these reasons and security (DIA requirements), system integrity, and CM, unit operators are not granted privileges which permit access.

Application Software. New ASAS application software deliveries will be made to FSSS personnel at RSSA locations and, as appropriate, to ASAS systems at field locations. Each RSSA maintains a master copy of the baseline software under configuration control. RSSA personnel use the master copy to replace executable files which may become corrupted at unit sites and to attempt to replicate problem areas.

Data Files. Some default ASAS data files and tables are field-modifiable. The contents of those tables, files, and databases in the fielded system may not remain the same as those initially installed. The database files altered by the user will reflect actual unit requirements as the user makes adaptive changes based on daily operational activities. The FSSS personnel maintain the default configuration-controlled entities and field-modified entities, thus providing both system and site-specific configuration-protected files. The capability to provide either an initial release version or a site-adapted version of files and databases will be provided as a service for each unit.

FSSS SOFTWARE PROBLEM REPORTING:

Problems associated with ASAS operations, software functionality, or data and message processing are identified via an SPR. The SPR is the vehicle through which system anomalies and enhancements for SED maintained systems are implemented into the software baseline. The on-site FSSS personnel will be responsible for assisting military operators in reporting these problems and providing recommendations to resolve discrepancies. This process includes verifying the SPRS for accuracy and completeness, attempting to recreate the problem on the local system, and forwarding the SPR to SED's CM group at Fort Huachuca, AZ.

SPR Process. The process for all SPRs related to the ASAS program will follow the steps outlined within Figure 7-1. Unit personnel will generate an SPR by using the SPR Originator Form to report software problems, desired enhancements, or discrepancies between user documentation and the user operational software. Completed SPR forms are provided to the FSSS representative for verification and completeness. The FSSS representative will coordinate with the RSSA concerning the SPR and have it forwarded to SED Fort Huachuca, AZ.

The CM group at SED will assign a system specific CM SPR control number and log the SPR into the SPR tracking database. Software technical personnel review the SPR and submit an assessment for resolution to a Configuration Control Board (CCB) review. Periodic CCB meetings are conducted to review and prioritize each SPR. Emergency SPRs (those that have been identified by the unit commander as "seriously impacting mission accomplishment") are resolved first to ensure prompt action. SED chairs and is a voting member at the ASAS CCB, with voting members from the PMO IF, and a user representative (either the Intelligence Center [USAICS&FH] or the Intelligence and Security Command [INSCOM]).

When resolved, the SPR is integrated into the next scheduled software version release of the software system. If an immediate work-around for the SPR can be created, a technical bulletin is forwarded to the user unit for immediate implementation until a new software release is dropped. Timely and accurate feedback to users regarding the status of their SPRs, or other user problems, is of significant importance to SED. Each unit FSSS representative must be able to brief the unit commander or his designated representative on the SPR status for the unit. Software related information on technical bulletins, CCB meeting minutes, and user group meeting minutes are supplied to the unit (monthly) through the FSSS representative.

Technical Bulletin. Should an SPR identify a problem for which a temporary work-around can be implemented, a technical bulletin (TB) will be generated and issued. TBs may address training, documentation, and operational and functional issues. A technical bulletin will be developed,

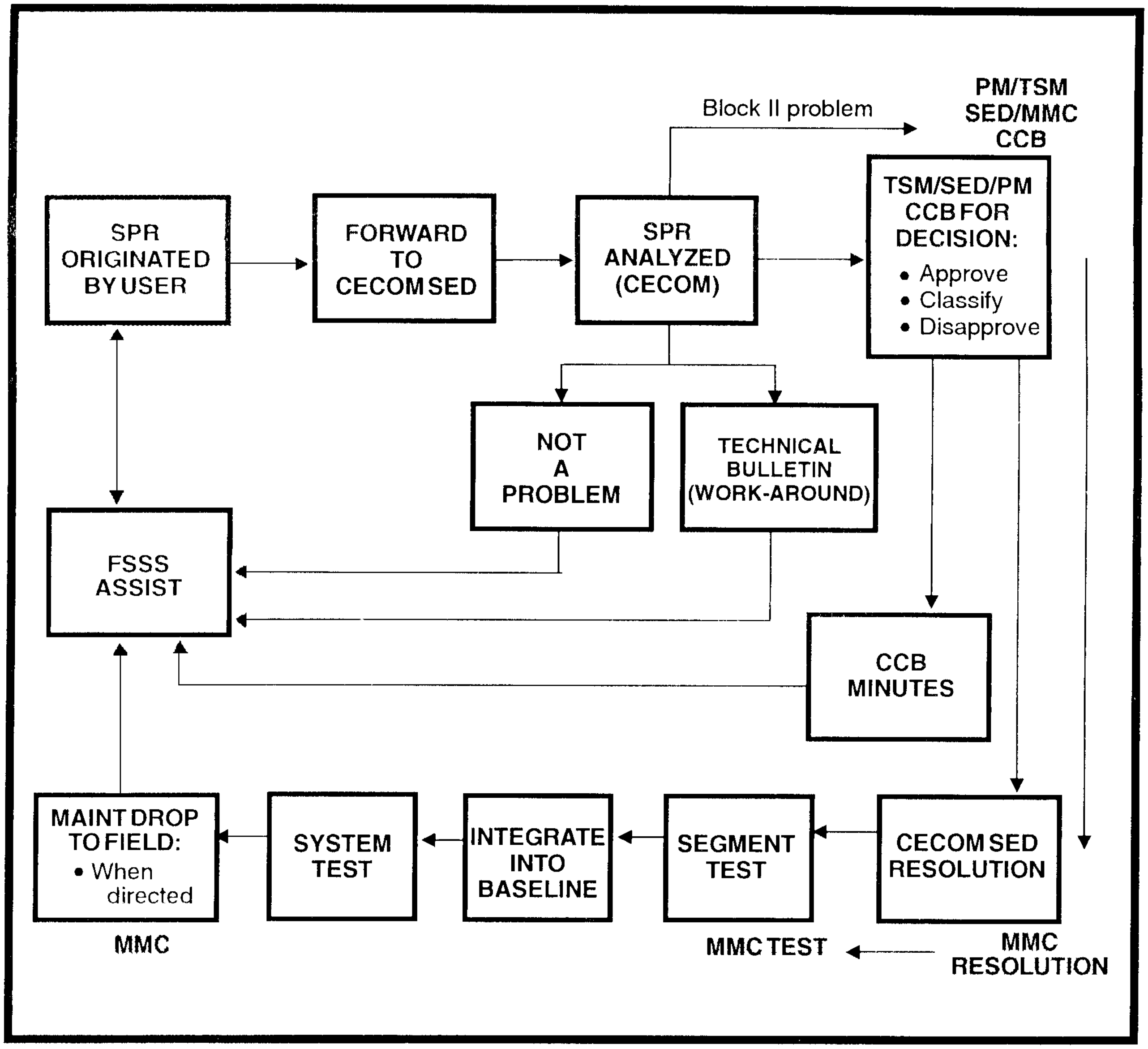


Figure 7-1. Software problem report (SPR) process.

documented, and issued by the SED CM group, then forwarded to the FSSS Operations Center for distribution to each FSSS site for immediate loading.

FSSS EQUIPMENT:

FSSS personnel use the supported unit's ruggedized equipment to perform FSSS tasks. FSSS personnel perform routine, emergency, and nonroutine tasks using selected equipment or, if necessary, the unit's equipment in a nonoperational state. All equipment usage by FSSS personnel will be coordinated with the unit.

Chapter 8

TRAINING

Training is fundamental to building and maintaining intelligence readiness. Leaders and operators within the G2(S2) and ACE must be competent in their military leadership, tactical skills, and military occupational specialty (MOS) before they can fully exploit the capabilities of automation intelligence processing systems like the ASAS. Once mastered, individual skills must be further refined through participation in battle focused collective training, mission-oriented exercises, and real world operations. Effective training produces a combat ready intelligence organization capable of satisfying the commander’s requirements in peace, war, or OOTW.

NEW EQUIPMENT TRAINING

During the initial fielding of ASAS, the US Army Intelligence Center provided eight weeks of ASAS Block I new equipment training (NET) at the gaining units. The ASAS Block I NET “Train-the-Trainer” is the foundation for NET for the ASAS-Extended and follow-on versions of ASAS. The Block I NET consisted of operator, supervisor, and leader training with a separate CCS operator course given by USAIC&FH, Fort Huachuca. Figure 8-1 shows the ASAS Block I NET described below.

OPERATOR TRAINING:

Operator training includes technical and mission-oriented training. Technical training consists of hardware skills such as cabling, configuring LANs, calling up software applications, and operator level maintenance. Mission-oriented training addresses MOS tasks, IEW tasks, and unit specific requirements.

LEADER TRAINING:

Leader training covers system operation and supervision. This training provides the skills and knowledge necessary to understand workstation allocations, message release, system interface, communications, file maintenance, database loading, security controls, alarms, and other supervisory processes and tasks.

MAINTENANCE TRAINING:

Maintenance training is oriented toward organizational maintenance for all ASAS equipment. The maintainer performs fault isolation and removes or replaces LRUs. Training will also include the operation and maintenance of special test equipment for associated components.

COLLECTIVE TRAINING:

Collective training brings leaders and operators together as the G2 and ACE. Using a “crawl—walk—run” approach, the NET instructors help the

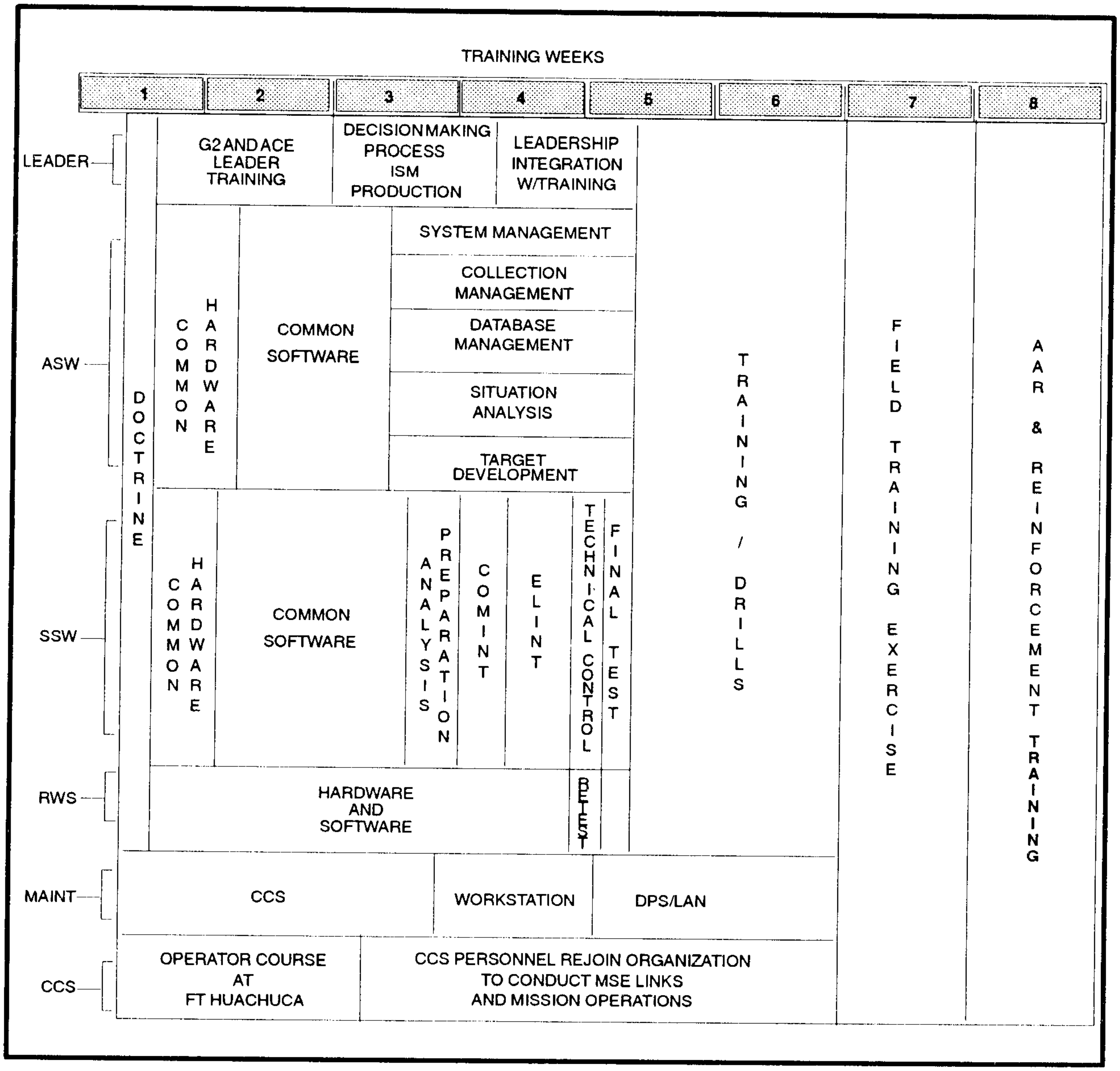


Figure 8-1. ASAS BlockI NET.

unit blend leader and operator ASAS tasks into a successful ACE collective training event. The “crawl” phase begins with instructors reviewing and demonstrating of each ASAS component. The review is followed by unit leaders briefing the SOPs and operations orders (OPORDs) they developed during leader training. This phase ends with instructors feeding messages into the ASAS to stimulate the G2 and ACE operations in a classroom environment. In the “walk” phase, the unit deploys its ASAS to a local training area and conducts an FTX. Instructors evaluate the training to verify that the unit has been trained to NET standards and identify areas requiring retraining. The NET ends with the unit entering the “run” or sustainment phase of ASAS training.

INSTITUTIONAL TRAINING

The USAIC&FH provides institutional training for ASAS operators, supervisors, and maintenance personnel. The Intelligence Center integrates ASAS training into enlisted, WO, and officer courses as course length allows. These courses include initial entry training for MOSs 96B, 98C, and 98J. ASAS training is provided to supervisors attending basic and advanced NCO, WO, and officer courses. MOS 33T soldiers train under a separate ASAS maintenance training course.

SUSTAINMENT TRAINING

The ASAS is a crew-served system and requires continuous operation and training to be effectively employed. The MI commander is responsible for individual and collective ASAS training. The G2 (S2) provides the battle focus and performance standards. Together, the G2 (S2) and MI commander establish measurable training standards, provide training time, and allocate resources for ACE and ASAS training. The ACE requires regular and challenging proficiency training. The ACE chief is the focal point for planning and executing this training. He and his subordinate leaders ensure ACE soldiers are trained and cross-trained on ASAS hardware and software. They also ensure that ACE soldiers are trained to standard as a team on battle focused objectives. The following describes this training in the context of the intelligence training principles outlined in FM 34-1.

EXECUTE REAL-WORLD OPERATIONS:

The G2 (S2) and the ACE should use the ASAS in daily operations and contingency planning. The upkeeping of databases and processing of reports on unit contingency areas are actions which provide minimal sustainment training. Producing and disseminating graphic INTSUMs on contingency or emerging regional hot spots is another way of incorporating ASAS training into day-to-day intelligence operations. The ASAS can also support remote collection operations of the TROJAN Classic.

INTEGRATE INTELLIGENCE:

ACE soldiers operate in teams to perform specific functions and missions. Each team must understand its relationship to the other and to those elements outside the ACE which they support. For example, the collection management team must understand the capabilities and limitations of all the IEW assets that normally support the command. These assets include non-MI personnel and units that are sources of information on the battlefield because of their proximity to the enemy, target acquisition capabilities, or access to the local population. The collection management team must understand that intelligence is not “one size fits all.” Combat, CS, and CSS commanders require intelligence in different levels of detail, timeliness, and format. By participating in staff wargaming, non-Ml unit training events, and asking questions, the collection management team can develop an appreciation of the needs of intelligence users. This same approach to training applies equally to other sections and teams within the ACE and G2 (S2).

UNDERSTAND THE BATTLEFIELD:

ACE soldiers must understand how the friendly combat, CS, and CSS forces are employed on the battlefield. Their knowledge should include an understanding of the tactics and equipment of their command; the capability and targeting requirements of friendly weapon systems; and the commander’s expectations of the intelligence system. The performance of ACE leaders and analysts is directly proportional to their understanding of the battlefield dynamics and the needs of their command.

APPLY STANDARDS:

The soldiers who make up the ACE must receive periodic training to ensure they meet Army and unit standards for individual proficiency. This training must include familiarization with unit, G2 (S2), and ACE SOPs. Leaders at all levels should also ensure an effective reception and integration program is in place. This will assist soldiers in understanding their role in the ACE and the standards required to provide IEW support to the commander.

MAINTAIN PROFICIENCY:

The ASAS requires frequent collective training events to maintain crew proficiency and improve essential ACE tasks. Collective training should strive for the full integration of ACE leaders and operators into a combat ready intelligence team. Crew drills and simulations provide opportunities for gaining this objective. Crew drills teach soldiers how to employ the entire system in accordance with established doctrine; techniques, tactics, procedures (TTP); and unit specific SOPs. Crew drills can and should be incorporated into the train-up for major exercises and training at the Combat Training Centers.

Exercise Support. The ACE may remain in garrison or deploy to field SCIFs to support training and exercises. The location of the ACE depends on the scenario, communications architecture, and objectives of the exercise. The ACE uses its ASAS equipment to process exercise data and maintain exercise databases during FTXs or command post exercises (CPXs). When preparing for an exercise, the ACE must develop a plan for downloading and storing real-world intelligence databases, loading exercise information, and building analytic support databases. During exercises, incoming real-world message traffic should be routed to the higher echelon ACE or the CMISE, while the ACE is participating in the FTX. If available, the ACE could use separate hard drive storage devices as an alternative means of separating exercise and real-world data.

Simulations and Interactive Training. ASAS requires high message volume (across a range of message types) for a variety of contingency areas to support sustainment training. The day-to-day message flow of real-world data during peacetime operations is not sufficient to train ACE personnel to a wartime standard. The USAIC&FH can support ASAS proficiency training at unit garrison or field sites through the TROJAN communications network and a Tactical Simulation (TACSIM) System driver at Fort Huachuca.

Tactical Simulation System. The TACSIM System stimulates the ASAS and stresses the analysts with a realistic volume of intelligence reports using the correct format. From a scripted scenario database, TACSIM performs intelligence missions against enemy forces and generates reports in USMTF. TACSIM then provides ASAS with the reports at multiple classification levels forming the perceived picture of a conflict in progress. Using USMTF reports allows the model to transmit simulated intelligence directly into the same assets that process real-world intelligence. TACSIM reports can be processed without modification or manual intervention using the message parsers of the ASAS as well as other processing systems. This translates into more realistic training through the use of systems the way they will be used in actual combat. The TACSIM includes a standard communication support processor (CSP). The CSP can transmit data to training or exercise participants at multiple security levels. This real-world communication connection enables the transmission of TACSIM reports across AUTODIN and local transmission lines.

FM 22-102, FM 25-100, and FM 25-101 provide guidance on team development and battle focused training, and FM 34-1 describes the intelligence training principles.

Glossary

SECTION I. ABBREVIATIONS AND ACRONYMS

A

AA	avenue of approach
ABCS	Army Battle Command System
AB^2	Army Brigade and Below
A^2C^2	Army Airspace Command and Control
AC	Active Component
ACE	analysis and control element
ACR	Armored Cavalry Regiment
ACT	analysis and control team
ACUS	Area Common User System
AD	air defense
ADA	air defense artillery
ADDS	Army Data Distribution System
adj	adjacent
ADP	automatic data processing
AES	Army Experiment Site
AFATDS	Advanced Field Artillery Tactical Data System
AGCCS	Army Global Command and Control System
AGM	attack guidance matrix
AI	area of interest
AIIF	Automated Intelligence Installation File
AIRES	Preliminary Imagery Nomination
ALL	all-source analysis
AM	amplitude modulation
AO	area of operation
AOC	Air Operations Center
APS	Advanced Planning System
AR	Army regulation
ARFOR	Army force
ARPA	Advanced Research Projects Agency
arty	artillery
ASAS	AH-Source Analysis System
ASAS-ASW	all-work station
ASAS-RWS	remote workstation
ASAS-SSW	single-source workstation
ASC	AUTODIN switching center
ASCDB	all source correlated database
ASDIA	All-Source Document Index Summary
ASW	all-source workstation
ATCCS	Army Tactical Command and Control System
ATM	asynchronous transfer mode
ATO	air tasking order
AUTODIN	automatic digital network
AWACS	Airborne Warning and Control System
AWLS	Army World Wide Military Command and Control

B

BDA	battle damage assessment
BFACS	Battlefield Functional Area Control System
BICC	battlefield information control center
BIT	built-in-test
BOS	Battlefield Operating System
BSC	Battlefield Simulation Center
BSTF	base shop test facility
BTU/hr	British thermal unit per hour

C

C	frequency band
C^2	command and control
C^2W	command and control warfare
C^3I	command, control, communications, and intelligence
C^4	command, control, communications, and computers
C^4I	command, control, communications, computer, and intelligence

CAMPS	Compartmented ASAS Message Processing System
CARS	Contingency Airborne Reconnaissance System
CASIAT	National Center for the Analysis of Violent Crimes Computer Assisted Security Investigative Analysis Tool
CATS	Core Analyst Tool System
CCB	Configuration Control Board
CCIR	commander's critical information requirements
CCs	communications control set
CD-ROM	compact disc-read-only memory
CECOM	US Army Communications-Electronics Command
CFE	contractor-furnished equipment
CGS	common ground station
CGS	Communications Gateway System
CHS	common hardware and software
CI	counterintelligence
CIA	Central Intelligence Agency
CINC	Commander in Chief
CIS	Combat Intelligence System
CIS-DM	CIS data management
CLS	contractor logistics support
CMISE	Corps Ml Support Element
CNR	combat net radio
CA	course of action
COMCAT	Character Oriented Message Catalog
COMINT	communications intelligence
COMSEC	communications security
CONUS	continental United States
COT	computer operator terminal
CPU	central processing unit
CPS	Communications Processing Subsystem
CS	combat support
CSP	communications support processor
CSS	combat service support
CSSCS	Combat Service Support Control System
CSSCS-EAC	CSSCS Echelon Above Corps
CTAPS	Contingency Theater Automated Planning System
CTT	commanders tactical terminal
CPX	command post exercise
CVIC	Carrier Intelligence Center
CW	CONSTANT WEB

D

DCS	Defense Communications System
DCT	Digital Communications Terminal
DCID	Director of Central Intelligence Directive
DDN	Defense Data Network
DEA	Drug Enforcement Agency
DIA	Defense Intelligence Agency
DIAM	Defense Intelligence Agency Manual
DIEQP	Defense Intelligence Equipment index
DIN	Defense Intelligence Network
DIOBS	Defense Intelligence Order of Battle System
DISA	Defense Information Systems Agency
DISCOM	division support command
DISE	Deployable Intelligence Support Element
DLSN	Defense Information Systems Network
DITDS	Defense Intelligence Threat Data System
DIVARTY	division artillery
DMS	Defense Message System
DOCC	deep operations coordination cell
DOD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DODM	Department of Defense Manual
DOS	Disk Operating System

DPS	data processor set
DREAR	
DS	direct support
DSN	Defense Switching Network
DSNET	Defense Secure Network
DSSCS	Defense Special Security Communications System
DSVT	Digital Subscriber Voice Terminal
DVM	Digital Voice Module

E

EA	engagement area
EAC	echelons above corps
EACIC	Echelons Above Corps Intelligence Center
EASI	Expert Analysis System for Intelligence
ECB	echelons corps and below
ECU	environmental control unit
EDC	external database coordination
ELINT	electronic intelligence
EMI	electromagnetic interference
EMP	electromagnetic pulse
EOB	electronic order of battle
EPDS	Electronic Processing and Dissemination System
EPL	electronic parameter listing
EPLRS	Enhanced Position Location Reporting System
ETUT	enhanced tactical users terminal
EVAL	Evaluation File
EW	electronic warfare
EWO	electronic warfare officer

F

FAADC^{3}I	Forward Area Air Defense Command, Control, Communications, and Intelligence
FAIO	field artillery intelligence officer
FBIS	Foreign Broadcast Information Service
FAISA	FORSCOM Automated Intelligence Support Activity
FAISS	Forces Command Automated Intelligence Support System
FAST	Forward Area SIDS and TRE
FAX	facsimile
FBI	Federal Bureau of Investigation
FDMP/ DDCMP	Full Duplex Message Protocol/Digital Data Communications Message Protocol
FI	functional identity
FIFO	first in, first out
FLTSATCOM	fleet satellite communications
FMR	functional manager
FOMA	Foreign-Military Assistance
FORSCOM	US Army Forces Command
FOV	field of view
FSCOORD	fire support coordinator
FSSS	field software services support
Ft	Fort
FTP	file transfer protocol
FTX	field training exercise
FM	frequency modulation
FMR	functional manager
FSE	fire support element
FSO	fire support officer

G

G2	Assistant Chief of Staff, G2
G3	Assistant Chief of Staff, G3
GB	gigabyte
GBCS	ground-based common sensor
GCCS	Global Command and Control System
GCS	ground control station
GCS	ground control system
GENSER	general services
GFE	government-furnished equipment
GRCS	GUARDRAIL Common Sensor
GS	general support
GSM	ground station module
GSR	ground surveillance radar
GUARDRAIL	AN/USD-9A or 9B

H

HDD	hard disk drive
HF	high frequency

HHOC	Headquarters, Headquarters and Operations Company
HMMWV	high mobility multipurpose wheeled vehicle
HPT	high-payoff target
HUMINT	human intelligence
HVT	high-value target

I

IAS	Intelligence Analysis System
I&W	indications and warnings
ICM	intelligence collection management
ICOM	integrated COMSEC module
ICR	Intelligence Collection Requirement File
IDB	integrated database
IDHS	Intelligence Data Handling System
IDSF	Intelligence Defector Source File
IEW	intelligence and electronic warfare
IEWSE	IEW Support Element
IGSM	Interim Ground Station Module
IHFR	Improved High Frequency Radio
IMETS	Integrated Meteorological System
IMINT	imagery intelligence
IMOM	improved-many-on-many
INMARSAT	International Maritime Satellite
INTSUM	intelligence summary
I/O	input/output
IOF	
IP	internet protocol
IPB	intelligence preparation of the battlefield
IPDS	Imagery Processing and Dissemination System
IPF	integrated processing facility
IPF	Intelligence Processing Facility
IR	information requirements
IRISA	Intelligence Information Index Summary
IROF	Imagery Reconnaissance Objective File
IROFJUS	Imagery Reconnaissance Objective File Justification
ISE	intelligence support element
ISM	intelligence synchronization matrix

J

J2	Intelligence Directorate
JCMT	Joint Collection Management Tools
JMST	Joint Management Support Tools
JDISS	Joint Deployable Intelligence Support System
JIC	Joint Intelligence Center
JMCIS	Joint Maritime Command Information System
Joint STARS	Joint Surveillance Target Attack Radar System
JSOC	Joint Special Operations Command
JTF	joint task force
JTT	joint tactical terminal
JTTM3	joint tactical terminal hybrid
JTT/H-R3	joint tactical terminal hybrid-receive-only
JWICS	Joint Worldwide Intelligence Communications System

K

kbps	kilobytes per second
KISS	Korea Intelligence Support System
KL	Klieglight
Ku	frequency band
kW	kilowatt

L

LAN	local area network
LCSS	Life Cycle Software Support
LEN	large extension nodes
LGSM	Light Ground Station Module
LIFO	last in, first out
LOS	line of sight
LRS	long-range surveillance

LRU	line replaceable unit

M

m	meter
MAGTF	Marine Air-Ground Task Force
Mb	megabyte
mbps	megabytes per second
MCDS	Mission Critical Defense Systems
MCS	Mneuver Cotrol System
MDCI	multidiscipline counterintelligence
METL	Mission-essential task list
METT-T	mission, enemy, troops, terrain and weather, and time available
MGSM	Medium Ground Station Module
MI	military intelligence
MIIDS	Military Intelligence Integrated Data System
MIES	Mobile Imagery Exploitation System
MILNET	Military Network
min	minutes
MITT	Mobile Integrated Tactical Terminal
MOA	memorandum of agreement
MOS	military occupational specialty
MP	military police
MPC	mission planning cell
MPN	mission packet switch network
MRA	message release authority
MSE	mobile subscriber equipment
msg	message
MTI	moving target indicator

N

NAI	named area of interest
NATO	North Atlantic Treaty Organization
NC	node center
NCS	net control station
NCA	national command authority
NCO	noncommissioned officer
NET	new equipment training
NETT	New Equipment Training Team
NIPS	Naval Intelligence Processing System
NITES	Naval Intelligence Threat Evaluation System
NPIC	National Photographic Interpretation Center
NRP	net radio protocol
NRT	near-real time
NSA	National Security Agency
NTCS-A	Navy Tactical Command System-Afloat

O

OB	order of battle
ODD	optical disk drive
OOTW	operations other than war
OPCON	operational control
OPLAN	operations plan
OPORD	operation order
OPR	operational diagnostics

P

PC	personal computer
PI	product improvement
PIR	priority intelligence requirements
PLA	plain language address
PMCS	preventive maintenance checks and services
PSN	packet switch node
PSYOP	psychological operations

Q

QF	QUICKFIX
QSTAG	Quadripartite Standardization Agreement
QUICKFIXIIB	AN/ALQ-151 (V)2

R

RAM	random access memory
RC	Reserve Components
RDEC	Research, Development, and Engineering Center
RDS	remote display screen
RECCEXREP	reconnaissance exploitation report

RELROK	Releasable ROK
RISC	Reduced Instruction Set Computing
ROK	Republic of Korea
ROKUS	Republic of Korea/United States
RRSA	Regional Software Support Activity
R&S	reconnaissance and surveillance
RSOC	Regional SIGINT Operations Facility
RWS	remote workstation
RVT	remote video terminal

S

S2	Intelligence Officer (US Army)
S3	Operations and Training Officer (US Army)
SALUTE	size, activity, location, unit, time, and enemy
SAT	security audit trail
SCAMPI	leased line communications link
SCCB	Software Configuration Control Board
SCI	sensitive compartmented information
SCIF	sensitive compartmented information center
SE	southeast
sec	seconds
SED	Software Engineering Directorate
SEE	supplementary equipment, electronic
SEN	small extension nodes
SF	Special Forces
SHF	super high frequency
SIGINT	signals intelligence
SIMS	SOUTHCOM Information Management System
SINCGARS	Single-Channel Ground and Airborne Radio System
SIPRNET	SECRET Internet Protocol Router Network
SIR	specific information requirements
SIT	situation analysis
SITMAP	situation map
SMR	source maintenance recoverability
SOCOM	US Special Operations Command
SOCRATES	SOCOM Command Research and Threat Evaluaton System
SOF	special operations forces
SOIC	Operations Intelligence Command
SOIS	Special Operations Intelligence System
SOP	standing operating procedures
SOR	specific orders and requests
SOUTHCOM	US Southern Command
SPECAT	special category
SPIRIT	Special Purpose Intelligence Remote Integrated Terminal
SPR	software problem report
SPV	system supervisor
SRF	SIGINT readiness facility
SRU	shop replaceable unit
SSES	Ship Signal Exploitation Space
SSP-S	single source processor-SIGINT
SSO	special security office
SSW	single-source workstation
STACCS	Standard Theater Army Command and Control System
STU	Secure Telephone Unit
SUCCESS	Synthesized UHF Computer-Controlled Equipment Subsystem
SUM	software users manual
SUPPLOT	Supplementary Plot
SW	southwest

T

TACELINT	tactical electronic intelligence
TACO	tactical communications
TACSAT	Tactical Satellite
TACSIM	tactical simulation
TADIXS-B	Tactical Data Information Exchange System-Broadcast
TAI	target area of interest
TB	technical bulletin
TBP	to be published

TC	training circular
TCP	Transmission Control Protocol
TCS	Theater Communications System
TDMA	time division multiple access
TDN	TROJAN Data Network
TEARS	Telecommunications Equipment Retrieval System
TECHINT	technical intelligence
TEMPEST	compromising emanations
TENCAP	Tactical Exploitation of National Capabilities
TEXTA	database
TFS	Tactical Fusion Systems
TGT	target analysis
THMT	Tactical High Mobility Terminal
TIBS	Tactical Information Broadcast System
TIDAT	Target Intelligence Data
TIGER	Tactical Intelligence Gathering and Exploitation Relay
TM	targeting module
TNL	target nomination list
TOC	tactical operations center
TOCSE	TOC support element
TO&E	table of organization and equipment
TOPS	tactical operations
TPS	test program set
TRACKWOLF	AN/TRQ-152
TRADOC	United States Army Training and Doctrine Command
TRAP	Tactical Related Applications
TRE	Tactical Receive Equipment
TRITAC	Tri-Service Tactical Communications
TRIXS	Tactical Reconnaissance Exchange System Relay
TSM	TRADOC system manager
TTP	tactics, techniques, and procedures

U

UAV	unmanned aerial vehicle
UDITDS	Defense Intelligence Threat Data System
UHF	ultra high frequency
US	United States (of America)
USAF	United States Air Force
USAIC&FH	United States Army Intelligence Center and Fort Hucahuca
USAREUR	United States Army, Europe
USMTF	United States Message Text Format
USSID	United States Signal Intelligence Directive

V

V2DA	Version 2 Data Adapter
VAX	Virtual Address Extension
VDD	version description document
VHF	very high frequency
VTC	video teleconference

W

WAN	wide area network
WO	warrant officer

X

X	frequency band
XDDCMP	external digital data communications message protocol

REFERENCES

REQUIRED PUBLICATIONS

Required publications are sources which users must read in order to understand or to comply with this publication.

Field Manuals (FMs)

6-20-10 *Tactics, Techniques, and Procedures for the Targeting Process.* 29 March 1990.
11-30 *MSE Communications in the Corps/Division.* 27 February 1991.
34-1 *Intelligence and Electronic Warfare Operations.* 27 September 94.
34-2 *Collection Management and Synchronization Planning.* 8 March 1994.
34-3 *Intelligence Analysis.* 15 March 1990.
34-40(S) *Electronic Warfare Operations (U).* 9 October 1987.
34-130 *Intelligence Preparation of the Battlefield.* 8 July 1994.
100-5 *Operations.* 19 June 1993.

RELATED PUBLICATIONS

Related publications are sources of additional information. They are not required in order to understand this publication.

Army Regulations (ARs)

34-1 *International Military Rationalization, Standardization, and Interoperability.* 15 February 1989.
190-13 *The Army Physical Security Program.*
380-5 *Department of the Army Information Security Program.* 25 February 1988.
380-19 *Information Systems Security.*
380-28 *Department of the Army Special Security Systems.*
380-40 *Policy for Safeguarding and Controlling Communications Security (COMSEC) Material.*
380-67 *The Department of the Army Personnel Security Program.* 9 September 1988.
381-1 *Security Controls on the Dissemination of Intelligence Information,* 12 February 1990.
381-10 US *Army Intelligence Activities.* 1 July 1984.
381-20 US *Army Counterintelligence Activities.* 26 September 1986.
381-47(S) *US Army Offensive Counterespionage Operations (U).* 30 July 1990.

Director of Central Intelligence Directives (DCIDs)

1/14 *Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information.*
1/21 *Physical Security Standards for Sensitive Compartmented Information Facilities.*

Field Manuals (FMs)

11-37 *MSE Primer for Small-Unit Leaders.* 14 November 1990.
11-38 *MSE System Management and Control.* 4 April 1991.
11-50 *Combat Communications within the Division (Heavy and Light).* 4 April 1991.
17-95 *Cavalry Operations.* 19 September 1991.
17-95-10 *The Armored Cavalry Regiment and Squadron.* 22 September 1993.

22-102 *Soldier Team Development.* 2 March 1987.
25-100 *Training the Force.* 15 November 1988.
25-101 *Battle Focused Training.* 30 September 1990.
24-1 *Signal Support in the Airland Battle,* 15 October 1990.
24-7 *Army Battle Command System (ABCS) Systems Management Techniques* (TBP FY96).
34-2-1 *Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and intelligence Support to Counterreconnaissance.* 19 June 1991.
34-5(s) *Human Intelligence and Related Counterintelligence Operations (U).*10 January 1994.
34-7 *Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations.* 18 May 1993.
34-8 *Combat Commander's Handbook on Intelligence.* 28 September 1992.
34-10 *Division Intelligence and Electronics Warfare Operations.* 25 November 1986.
34-10-2 *IEW Equipment Handbook,* 13 July 1993
34-25 *Corps Intelligence and Electronic Warfare Operations.* 30 September 1987.
34-25-1 Joint Surveillance and Target Attack Radar System. (TBP, 1995.)
34-25-2 *Unmanned Aerial Vehicle* (TBP).
34-35 *Armored Cavalry Regiment (ACR) and Separate Brigade Intelligence and Electronic Warfare (IEW).* 12 December 1990.
34-36 *Special Operations Forces Intelligence and Electronic Warfare Operations.* 30 September 1991.
34-37 *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations,* 15 January 1991.
34-40-7 *Communications Jamming Handbook.* 23 November 1992.
34-60 *Counterintelligence.* 5 February 1990.
34-80 *Brigade and Battalion Intelligence and Electronic Warfare Operations.* 15 April 1986.
71-3 *Armored and Mechanized Infantry Brigade.* 11 May 1988.
71-100 *Division Operations. 16*June 1990.
100-7 *Decisive Force: The Army in Theater Operations,* April 1994.
100-15 *Corps Operation.* 13 September 1989.
100-16 *Support Operations: Echelons Above Corps.* 16 April 1985.
100-17 *Mobilization, Deployment, Redeployment, Demobilization.* 28 October 1992.
101-5 *Staff Organization and Operations.* 25 May 1984.
101-5-1 *Operational Terms and Symbols.* 21 October 1985.

Joint and Multiservice Publications

Joint Pub 1-02 *DOD Dictionary of Military and Associated Terms.* 23 March 1994.
Joint Pub 2-0 *Joint Doctrine for Intelligence Support to Operations.* 5 May 1995.
Joint Pub 2-01 *Intelligence Tactics, Techniques, and Procedures for Joint Operations.* 15 July 1992.
Joint Pub 6-0 *Doctrine for Command, Control, Communications, and Computers (C4) Systems Support to Joint Operations.* 30 May 1995.

Professional Bulletin (PB)

34-94-3 *24th ID(M) ACE in Operation Desert Capture II,* MIPB, Volume 20, Number 3, July-September 1994.
34-94-3 *The MI Revolution,* MIPB, Volume 20, Number 3, July-September 1994.

34-94-4 *TACSIM: Intelligence Training for Tomorrow's Battlefield*, MIPB, Volume 20, Number 4, October-December 1994.

34-95-1 *ASAS and 1st Cavalry Division*, MIPB, Volume 21, Number 1, January-March 1995.

34-95-1 *ASAS* Arrives, MIPB, Volume 21, Number 1, January-March 1995.

34-95-1 *Wargarning With the ASAS-W*, MIPB, Volume 21, Number 1, January-March 1995.

34-95-2 *XVIII Airborne Corps Intelligence Architecture in Haiti*, MIPB, Volume 21, Number 2, April-June 1995.

34-95-2 *Division Ready Brigade IEW: Don't Leave Home Without It*, MIPB, Volume 21, Number 2, April-June 1995.

Technical Bulletin (TB)

380-5(C) *Security, Use, and Dissemination of Sensitive Compartmented Information (SCI) (U).*

Technical Manuals (TMs)

11-5865-303-10 *Data Processor Set, AN/TYQ-36(V)3*, 1 March 1993.

11-5865-304-13 *Supplementary Equipment, Electronic, AN/TYQ-42(V) 10, 11, 12, 13, and System Manual for LCC.* 1 March 1993.

11-5895-1497-10-1 *Communications Control Set, AN/TYQ-40(V)2.* 1 March 1993.

11-7010-255-10 *Workstation, Computer Graphics, AN/TYQ-37(V)5.* 1 March 1993.

Training Circulars (TCs)

34-10-20 *Military Intelligence Combat* Assessment *Tables (MICAT).* 7 May 1993.

34-10-20-1 *Military Intelligence Collective Training Standards Document Volume I.* 14 December 1992.

34-10-20-2 Military *Intelligence Collective Training Standards Document Volume II.* 14 December 1992.

Forms

DA Form 2028 *Recommended Changes to Publications and Blank Forms*

INDEX

A

AUTODIN, 3-8, 3-13, 4-6, 4-7, 4-8, 8-5

ACE Chief responsibilities, 2-6, 2-7, 2-11, 2-14, 5-2, 5-3, 5-15, 8-3

ACT, 1-19, 2-1, 2-3, 2-13

Advanced Field Artillery Tactical Data System (AFATDS), 1-5

All-Source Analysis System (ASAS), iii
Block I, 1-1
Block II, 1-1
Block III, 1-2
ASAS-ASW, 1-1, 3-1, 3-4
ASAS-RWS, 1-1
ASAS-SSW, 1-1, 4-14
CCS, 2-4, 3-1, 3-8, 3-9
Extended, 1-2, 3-11, 3-12, 3-13, 4-15

all-source correlated database (ASCDB), 1-10

All-Source Intelligence Section Chief, 2-8, 2-9

All-Source Intelligence Section, 2-4, 2-8, 2-9, 3-12, 5-5, 5-7, 5-9

Alpha Reduced Instruction Set Computing (RISC), 1-2

AN/FSQ-144(V) TROJAN Classic, 4-11

AN/TYQ-36(V)3, 1-2

analysis and control element (ACE), iii

Area Common User System (ACUS), 1-4

armored cavalry regiment (ACR), iii

Army Data Distribution System (ADDS), 1-4

Army Force (ARFOR), 2-1

Army Battle Command System (ABCS), iii
common hardware and software II, 1-1

Army World Wide Military Command and Control (WWMCC) Information System (AWIS), 1-3

Army Common User System (ACUS), 4-2

Army Data Distribution System (ADDS), 4-4

Army Global Command and Control System (AGCCS), 1-3

Army Brigade and Below (AB^2), 1-6

Army Tactical Command and Control System (ATCCS), 1-4

B

battle damage assessment (BDA), 2-4

Battle Captain, 2-8, 2-9

battlefield functional area control systems (BFACS), 1-4

battlefield information control center (BICC), 2-13

brigade S2, 2-3

broadcast systems, 4-9

C

CECOM, 7-3

counterintelligence, 2-1

Collection Manager, 2-6, 2-7, 2-8, 2-11, 4-10, 4-16

combat net radio (CNR) systems, 1-4, 4-4

Combat Service Support Control System (CSSCS), 1-4

Combat Service Support Control System-Echelon Above Corps (CSSCS-EAC), 1-4

command and control warfare (C^2W), 5-6

Commanders Tactical Terminal (CTT). *See* JTT

communications systems, 1-1, 1-3, 1-6, 1-8, 1-9, 3-8, 4-1, 4-5, 4-9, 4-12, 4-14, 4-18, 5-2, 6-4

communications intelligence (COMINT), 5-7

Communications Processing Subsystem (CPS), 3-8

Communications Security, 6-4

Compartmented ASAS Message Processing System (CAMPS), 3-14

Computer Operator Terminal (COT), 3-8

corps
  ACE, 2-2, 4-7
  MI brigade, 2-2, 2-4
  G2, 2-2

Corps Military Intelligence Support Element (CMISE), 2-2

D

Data Processing Sets (DPSs), 1-2, 3-1

deep operations coordination cell (DOCC), 2-9

Defense Intelligence Threat Data System (DITDS), 3-16

Defense Intelligence Network (DIN), 4-8

Defense Message System (DMS), 4-6, 4-8

Defense Information Systems Network (DISN), 4-6

Defense Data Network (DDN), 4-6

Defense Information Systems Agency (DISA), 4-5

Defense Switching Network (DSN), 4-5

Defense Message System (DMS), 4-8

Defense Intelligence Threat Data System (DITDS), 4-15

Defense Communications System (DCS), 4-5

Defense Special Security Communications System, 4-6

Department of Defense Intelligence Information System (DODIIS), 4-8

Deployable Intelligence Support Element (DISE), 2-11

DS MI company, 2-3

division, iii
  G2, 2-2, 2-3
  ACE, 2-3

E

echelons above corps (EAC), 1-3

Echelons Above Corps Intelligence Center (EACIC), 2-1

electronic warfare officer (EWO), 2-5

electronic intelligence (ELINT), 4-9

Electronic Processing and Dissemination System (EPDS), 1-8

Enhanced Position Location Reporting System (EPLRS), 4-5

Enhanced Tactical Users Terminal (ETUT), 4-13

external database coordination (EDC), 5-11

F

field artillery intelligence officer, 2-9, 2-10

Field Software Services Support (FSSS), 7-3

Forces Command Automated Intelligence Support System (FAISS), 4-13

Forward Area Air Defense Command, Control, Communications, and Intelligence (FAADC^{3}I), 1-4

functional identities (FIs)
- ADP, 3-4
- ALL, 3-6, 5-5
- FMR, 3-4, 5-5
- ICM, 3-6, 5-5
- MRA, 3-6
- OPR, 3-4, 5-6
- SAT, 3-4
- SIT, 3-6, 5-5
- SPV, 3-4
- TGT, 3-6, 5-5

G

G2 (S2), iii

GENSER, 4-6

Global Command and Control System (GCCS), 1-3

ground station module (GSM), 2-4

GUARDRAIL, 1-8

H

human intelligence (HUMINT), 2-1

I

IEW support element (IEWSE), 2-1

Imagery Processing and Dissemination System (IPDS), 4-13

IMINT, 2-1, 2-3, 2-4, 4-20, 5-7

Improved High Frequency Radio (IHFR), 3-16

Information Security, 6-4

Integrated Processing Facility (IPF), 1-8

Intelligence Battlefield Operating system (BOS), 1-1

Intelligence Analysis System (IAS), 4-18

Intelligence processing system
- USAF, 4-16
- USN, 4-17
- USMC, 4-18

Internet Protocol (IP), 4-6

IPB, 2-4, 2-9, 2-10, 3-3, 3-6

J

Joint Collection Management Tools (JCMT), 3-16

Joint Deployable Intelligence Support System (JDISS), 3-13

Joint Intelligence Center (JIC), 2-1

Joint Management Support Tools (JMST), 4-16

Joint Prototyping Office, 1-2

Joint Surveillance Target Attack Radar System (Joint STARS), 2-4

Joint Tactical Terminal (JTT), 4-10, 4-13

Joint Tactical Terminal-Hybrid Receive Only (JTT-HR), 1-8

joint task force (JTF), 2-2

Joint Worldwide Intelligence Communications System (JWICS), 3-16

L

Lessons Learned, 5-8

M

Maintenance, 7-1

Maneuver Control System (MCS), 1-4

military intelligence (MI)
  battalion, 2-2, 2-3, 2-4, 5-8
  brigade, 2-1
  company, 2-3, 2-4, 2-13

Military Intelligence Integrated Database System (MIIDS) and IDB, 3-15

Mobile Integrated Tactical Terminal (MITT), 1-8, 4-14

Mobile Imagery Exploitation System (MIES), 4-13

Mobile Subscriber Equipment (MSE), 4-2

N

net radio protocol (NRP), 3-8, 3-10

new equipment training, 8-1

P

processors, 1-3, 1-6, 1-8, 2-2, 3-4, 3-10, 3-13, 4-1, 4-13, 4-15, 5-7

R

remote workstations (RWSs), 3-1. *See also* ASAS

Reserve Components (RC), iii

S

SECRET Internet Protocol Router Network (SIPRNET), 4-8

Security, 6-1

sensors, 1-3, 1-6, 1-8, 3-10, 4-11, 4-17, 5-2

separate brigade, iii

SIGINT, 2-1

Single Source Processor-Sigint (SSP-S), 4-14

Single-Channel Ground Airborne Radio System (SINCGARS), 1-8, 4-4

SOCRATES, 4-18

Software Problem Report, 7-3

Standard Theater Army Command and Control System (STACCS), 1-4

supplementary equipment, electronic (SEE), 3-1

Synthesized UHF Computer Controlled Equipment Substation (SUCCESS), 4-9

T

Tactical Related Applications (TRAP), 4-9

Tactical Data Information Exchange System-Broadcast (TADIXS-B), 4-9

Tactical Satellite (TACSAT), 4-4

Tactical Receive Equipment (TRE), 4-9

Tactical Simulation (TACSIM) System, 8-5

Tactical Intelligence Gathering and Exploitation Relay (TIGER), 1-8

Tactical Reconnaissance Exchange System (TRIXS), 4-9

Tactical Information Broadcast System (TIBS), 4-9

Tactical High Mobility Terminal (THMT), 4-14

Targeting, 2-9

technical control and analysis element (TCAE). *See* ACE

Technical Control and Processing Section, 2-4, 2-9

theater Army, iii, 2-1

theater Army ACE, 2-1

TOC support element (TOCSE), 2-1

Training, 8-1

TROJAN Data Network, 4-11

TROJAN SPIRIT II, 1-8, 4-11

U

UAV ground control station (GCS), 1-8

United States Air Force, 4-16

United States Navy, 4-17

United States Marine Corps, 4-18

UNIX operating system, 3-6, 4-16

V

Virtual Memory System (VMS), 3-12

Virtual Address Extension (VAX) operating system, 3-4

W

WARRIOR, 1-3

FM 34-25-3
3 OCTOBER 1995

By Order of the Secretary of the Army:

DENNIS J. REIMER
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Acting Administrative Assistant to the
Secretary of the Army
00726

DISTRIBUTION:

Active Army, USAR, and ARNG: To be distributed in accordance with DA Form 12-1lE, requirements for FM 34-25-3, *All Source Analysis System and the Analysis and Control Element* (Qty rqr block no. 5370)

***U.S. Government Printing Office: 1995—628-027/40051**