

CHAPTER 8

COMMUNICATIONS AND INFORMATION SYSTEMS

The MAGTF employs CIS to support the collection, processing, and exchange of information. CIS can accelerate and automate routine functions, freeing commanders and staffs to focus on those aspects of command and control that require experience, judgment, and intuition. In every phase of operations planning and execu-

tion, these systems assist the commander and his staff by enabling rapid, secure information flow, shared situational awareness, informed decision-making, and swift dissemination of decisions. The success of the MAGTF in the modern battlespace depends heavily on the effective employment of CIS.

SECTION I. MARINE AIR-GROUND TASK FORCE COMMUNICATIONS ARCHITECTURE

The design of the communications architecture to support a MAGTF is based on the nature of the operation, the physical environment, the commander's intent, the concept of operations, and the composition and task organization of the MAGTF and attached and supporting forces.

In the early stages of an operation, SCR normally provides the principal means of communications. As the operation evolves, LANs and a switched backbone are established to meet the information transfer requirements of command and control at higher echelons, and to connect to the Defense Information Systems Network (DISN). Maneuver battalions continue to depend on SCR throughout the operation with limited interfaces to the switched backbone. Special-purpose systems provide dedicated communications support for certain functions, such as position location, navigation, and intelligence.

The MAGTF communications architecture may be viewed as four subnetworks that interface with one another through the architecture provided by the tactical data network (TDN). Figure 8-1 depicts these four networks, which are described

in the following paragraphs. For a more detailed discussion of the MAGTF communications architecture, see MCWP 3-40.3.

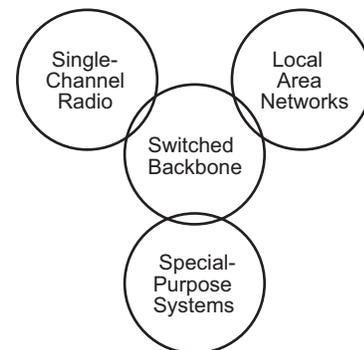


Figure 8-1. MAGTF Communications Architecture.

Single-Channel Radio

SCR equipment includes hand-held, manpack, vehicle-mounted, ground-mounted, and shelterized radios operating in the high frequency (HF), very high frequency (VHF), and ultrahigh

frequency (UHF) bands. It also includes TACSAT radios in the UHF band. The most widely employed tactical radios—the single-channel ground and airborne radio system (SINCGARS) family—provide built-in communications security (COMSEC) and electronic counter-countermeasures capabilities.

SCR equipment is easy to operate. SCR networks are easily established, rapidly reconfigured, and, most importantly, easily maintained on the move. They provide the principal means of communications support for maneuver units. SCR provides secure voice and data communications capability. However, data transfer rates (bandwidth) are limited. SCRs in the VHF and UHF bands are normally limited to line-of-sight ranges. In HF, SCR supports long-range communications, but not while on the move. SCR TACSAT communications combine mobility, flexibility, and ease of operation with unlimited range. However, TACSAT communications are restricted by the limited availability of satellite frequencies and channels.

In addition to a limited capability to support data transfer, other limitations are vulnerability to enemy electronic warfare, susceptibility to interference, and limited spectrum availability. The MAGTF employs TACSAT primarily in support of critical, long-range communications requirements; e.g., communications support for deep reconnaissance operations or ship-to-shore connectivity to the tactical echelon of a MEU(SOC) when deployed ashore.

Switched Backbone

The switched backbone consists of switching, routing, and wideband transmission systems that provide a high-capacity communications backbone for the MAGTF, and connectivity with the DISN. (See also section III.) The switched backbone is the tactical equivalent of commercial local and long-distance telephone networks. In some situations, it interfaces with and uses those

commercial networks. The switched backbone employs a mix of older equipment developed under the Tri-Service Tactical Communications System (TRI-TAC) program and newer equipment and technology. The TRI-TAC family of equipment was developed in the 1970s under a joint program by the Marine Corps, Air Force, and Army. TRI-TAC equipment, fielded beginning in the mid-1980s, provides the major components of the MAGTF switched backbone. This equipment was developed to provide interoperable, secure, and deployable voice and data digital switching and transmission systems for tactical forces operating in a joint environment.

The switched backbone is tailored to meet the requirements of a particular operation and has the flexibility to support the unfolding tactical situation and overall concept of operations. Planning, redesign, and adaptation are continuous as switched backbone equipment and personnel arrive in theater and the MAGTF transitions to operations ashore. Larger headquarters, rear areas, expeditionary airfields, and command and control centers at higher echelons are the principal subscribers to the switched backbone. Maneuver battalions cannot be constrained by the inherent lack of mobility of the switched backbone and normally link their voice and data systems through an SCR interface. The MAGTF switched backbone includes switches, IP routers, and wideband multichannel radio transmission systems.

Switches

Switches route traffic through a communications network. The three basic categories of switches are circuit, message, and packet. Circuit switches generally support telephone traffic. They range in size and capacity from man-portable switches that can support a few dozen subscribers to shelter-mounted switches that can handle traffic for over 100 users. They have an extensive built-in COMSEC capability. Message switches process formatted messages for storage and delivery. Packet switches process data into

standard packets for transmission and then reassemble the packets at the other end. The Marine Corps achieves a packet switching capability through the use of IP routers.

Internet Protocol Routers

The proliferation of information systems in the modern battlespace is driving an increased demand for data communications. Although circuit switches and message switches can support data communications, packet switching is far more efficient. The Marine Corps has developed a packet switching capability through the use of commercial IP routers. Routing protocol used with these routers provides for transmitting blocks of data called datagrams from sources to destinations, where the source and destination are identified within each packet by sets of 32 bits known as IP addresses. The router reads the network address of all data packets and forwards them to the addressee via the best available communications path. These IP routers form a data communications overlay on the switched backbone and serve as gateways to the IP router networks of the following:

- Other Services.
- JTF.
- DISN IP router networks: Joint Worldwide Intelligence Communications System (JWICS); Secret Internet Protocol Router Network (SIPRNET); and Nonsecure Internet Protocol Router Network (NIPRNET).

IP routers are an integral part of the TDN gateways and servers described in the following paragraphs.

Multichannel Radio

Multichannel radio provides the communications links for the switched backbone. It permits multiple users to access a single communications path and includes terrestrial and satellite radio

systems. Multichannel radio provides worldwide connectivity through links to the DISN and the links for long-distance communications within the theater and the MAGTF. Multichannel radio provides reliable, flexible, and high-capacity transmission paths for voice and data communications. Primary disadvantages are complexity and a lack of mobility. A multichannel radio network requires more time to set up and more expertise to operate and maintain than an SCR network. It cannot operate on the move due to the requirement for accuracy to transmit and receive a tightly-focused beam of radio energy. Consequently, maneuvering elements will rely primarily on SCR. Multichannel radio will be employed only down to the infantry regiment and artillery battalion levels in the GCE.

Local Area Networks

LANs are designed to support information exchange, collaboration, and resource sharing in a particular unit, agency, facility, center or cell in a confined geographic area. LANs can support high data throughput up to 1000 megabytes per second (Mbps), although 10 or 100 Mbps is more common. LANs include terminal equipment—usually computers—connected to a transmission medium such as wire or fiber optic cable. LAN media used in the MAGTF include copper-based coaxial and twisted-pair cable, and fiber optic cable used as a higher speed backbone that connects multiple facilities in a large headquarters complex. Optical networks are being employed at successively lower echelons. Initiatives such as the unit operations center (UOC)—described below—will continue that effort at regiment and lower headquarters. Fiber optic backbone LANs are also used aboard Navy ships with copper-based coaxial and twisted-pair LANs within an operational workspace such as the LFOC. MCWP 3-40.3 discusses how specific LAN media, access methods, technologies, proto-

cols, and equipment are employed to meet specific unit requirements.

Frequently, Marine Corps data networks are discussed using other terms, such as WAN or intranet. Table 8-1 provides a brief definition of these terms for clarification. Although all refer to an IP-based network, the differences are mainly issues of scale.

Table 8-1. Data Network Terms.

Term	Description
Local Area Network (LAN)	A LAN is a network confined to a relatively small area. It is generally limited to a single building or a small cluster of buildings. Rarely are LAN computers more than a mile apart.
Metropolitan Area Network (MAN)	A MAN covers more dispersed geographic areas, such as bases or larger deployed headquarters. By interconnecting LANs within a larger geographic area, information is easily disseminated throughout the network.
Wide Area Network (WAN)	A WAN connects larger geographic areas, such as states or countries. Dedicated trans-oceanic cabling or satellite uplinks may be used to connect this type of network.
Intranet	An intranet is a network based on transmission control protocol (TCP) and/or IP (just like the internet), belonging to an organization, which is accessible only by the organization's members or others with authorization. An intranet's web sites look and act just like any other web sites, but the security device (firewall) protecting an intranet prevents unauthorized access.

The UOC is a modular reconfigurable command and control system. It receives and transmits data and voice communications and provides the commander with a CTP to support staff planning and decisionmaking. Direction and control of unit operations can be accomplished through this center. It provides a centralized facility to host command and control functionality for CE, GCE, ACE, and CSSE. The UOC provides shelter/tent, power, cabling, LAN and processing systems to host mission application software. The UOC is scalable to support command echelons at the battalion level and above.

Special-Purpose Systems

Special-purpose communications systems support specific functions such as position location, navigation, and intelligence dissemination.

AN/PSN-11 Precise Lightweight Global Positioning System Receiver

The AN/PSN-11 precise lightweight global positioning system (GPS) receiver (PLGR) is small, hand-held, and weighs approximately 3 pounds. It provides precise positioning and timing solutions based on signals received from the GPS satellite constellation. It is important to understand the difference in capabilities between the PLGR and enhanced position location reporting system (EPLRS). The PLGR provides land navigation capability, but cannot provide the location of another unit. It does not have a communications capability beyond the passive receipt of location and time. Given the vulnerability of the GPS to interference and jamming, GPS should be viewed as a complement to, not a replacement for, EPLRS.

Enhanced Position Location Reporting System

EPLRS provides a dedicated data communications network and geodetic position location information to units below the regiment level. Its primary purpose is to provide data connectivity between the regiment and battalion. It provides the communication path to transfer data for Intelligence Operations Server version 1 (IOSv1), the data automated communications terminal (DACT), and the Advanced Field Artillery Tactical Data System (AFATDS).

The EPLRS radio set is normally vehicle-mounted, but may be removed and used in a man-pack configuration. EPLRS operates in the UHF spectrum, and provides a secure, robust communications architecture. This architecture supports the automated data distribution to

adjacent, senior, and subordinate commands and simultaneously provides unit position reports to automated command and control centers to update near-real-time tactical displays.

The network control station (NCS) provides the EPLRS control network, routes control net messages and queries, performs all calculations, and graphically displays the positions of all active EPLRS radio sets. The NCS provides over-the-air rekeying (OTAR) to radio sets that require keys for command, traffic, rekey or community of interest. Current plans call for fielding the EPLRS network manager (ENM) with EPLRS version 10. The ENM is a laptop-based system that will perform NCS functions and other planned network management functions. When fully fielded, the ENMs will allow network management functions to be performed at the battalion level.

Joint Tactical Information Distribution System

The Joint Tactical Information Distribution System (JTIDS) is an advanced radio system that provides information distribution, position location, and cooperative identification capabilities in an integrated form. The primary JTIDS role is in air defense coordination.

An initial JTIDS capability has been fielded. The AN/TYQ-JTIDS (modified AN/TSC-131 JM) does not currently have a JTIDS voice capability. It is normally fielded with a JTIDS tactical air operations module to provide an initial tactical digital information link-joint capability to the Fleet Marine Force. The Marine Corps implements the JTIDS terminal in the TAOC.

Integrated Broadcast Service

The integrated broadcast service (IBS) is the worldwide, Department of Defense (DOD) standard network for transmitting tactical and strategic intelligence and targeting data within a common format, which will migrate to a single family of joint tactical terminals (JTTs) for

improved operational jointness. The common IBS module is a totally integrated joint program (all Services and Special Operations Command) that was created to consolidate and replace existing IBS receiver functionality inherent with the duplicative existing systems with a common family of IBS modules (hardware and software).

Commander's Tactical Terminal

The commander's tactical terminals (CTTs) provide the warfighter with seamless, near-real-time intelligence and targeting information. They supply the critical data link to battle managers, intelligence centers, air defense, fire support, and aviation nodes across all Services. The CTT allows all Service users to exploit multiple intelligence broadcast networks.

Joint Tactical Terminal

The JTT, with its common IBS modules, can receive diverse broadcasts into terminals with common capabilities. These terminals use multiple transmission paths and sound information management to provide the ability for each user in the battlespace to view a COP/CTP. The modular feature of these terminals allows producers and users in the MAGTF to incorporate IBS into their existing information systems. Alternatively, users may also obtain completely configured tactical terminals. Employment of JTT/common IBS modules facilitates a seamless transition from current dissemination systems to the IBS without degrading the capabilities provided by current systems.

TROJAN SPIRIT II

TROJAN SPIRIT II is a mobile super high frequency (SHF) satellite communications system that receives, transmits, and processes multimedia products, including imagery and secure dial-up voice, data, facsimile, and video. It will be

deployed to provide GENSER and SCI communications for intelligence operations. TROJAN SPIRIT II supports two separate LANs (SCI and collateral secret) and provides entry to the SIPRNET and the JWICS.

Tactical Data Network

The Marine Corps is replacing interim, locally configured IP router-based data communications packages with the TDN. The TDN will augment the existing MAGTF communications infrastructure to provide an integrated data network—the MAGTF intranet. The TDN will connect the subnetworks of the MAGTF communications architecture and extend the MAGTF intranet down to battalion level. The data network established through the TDN will form the communications backbone for MAGTF information systems.

The TDN will consist of a network of gateways and servers interconnected with one another and their subscribers via a combination of common-

user long-haul transmission systems, LANs, SCRs, and the switched telephone system. It will provide subscribers with basic data transfer and switching services; access to strategic, supporting establishment, joint, and other Service component data networks; network management capabilities; and value-added services such as message handling, directory services, file sharing, and terminal emulation support.

The TDN gateway is mounted on a heavy-variant HMMWV. It will normally be employed with the digital technical control center and SHF- or extremely high frequency (EHF)-TACSAT to provide high bandwidth access to the DISN and/or the Marine Corps Enterprise Network (MCEN). TDN servers are being employed in several variants. The earliest of these are mounted in three man-portable transit cases. Newer variants are based on a laptop computer and are man-portable. TDN gateways will be employed at the MEF and MSCs. Servers will be fielded down to battalion/squadron level.

SECTION II. TACTICAL COMMUNICATIONS INFORMATION SYSTEMS

The Expeditionary Force Development System is being employed to develop new information systems-oriented warfighting capabilities. Experience gained by the operating forces is driving system modifications and changes in force structure. All staff sections require an organic capability to employ the information systems supporting their respective functional areas. Supported by CIS personnel under the cognizance and technical direction of the G-6/S-6, individual Marines, staff sections, and other activities now have an enhanced ability to support the commander's decisionmaking process.

To improve interoperability, increase efficiency, and reduce costs, the DOD has mandated that the

Services move to a common set of information systems and services. The Defense Information Systems Agency (DISA) is accomplishing this through the establishment of the common operating environment (COE), which includes the DISN, the Global Command and Control System (GCCS), and the Global Combat Support System (GCSS). These developments are having a profound effect on MAGTF CIS, doctrine, organization, training, and equipment.

The DISN provides the long-haul communications backbone for the MAGTF, both in garrison and deployed. The Marine Corps has implemented GCCS and is migrating its tactical information systems to comply with the COE. This migration began with the tactical

combat operations (TCO) and IAS command and control systems, now known as IOSv1 and IOSv2. COE compliance facilitates interoperability with the GCCS and other COE-compliant systems. MAGTF CIS must be viewed within the context of the COE.

Global Command and Control System

The GCCS implements the joint command, control, communications, computers, and intelligence (C4I) for the warrior concept. This concept calls for the capability to move a joint force anywhere on the globe at any time and to provide that force with the information necessary to accomplish its mission. The GCCS provides a fused and shared picture of the battlespace through its COP/CTP function. The GCCS also supports readiness assessment and reporting by the Services. The GCCS replaced the Worldwide Military Command and Control System, and is designed to resolve joint command and control interoperability issues by evolving incompatible, Service-specific command and control programs into a single integrated command and control system.

The GCCS employs a client-server architecture that uses both commercial and government-developed software. Through a DOD-mandated migration strategy, the GCCS will reduce the large number of information systems in use today. The GCCS is evolving from a baseline of existing or “legacy” command and control systems; as new GCCS versions are subsequently fielded, existing legacy systems will be replaced. The common functional, physical, and operational characteristics of the GCCS are based on a single COE. All future joint and Service/combatant commander-specific command and control systems must be compatible with this COE. The goal is to achieve a fully integrated, single GCCS in which all command and control functions are provided through GCCS application programs that have a common look and feel. The COE provides a standard environment, off-the-shelf software, and a set of programming standards

that describe in detail how mission applications will operate in the standard environment. Each mission application that is migrated to the common environment must comply with COE standards.

The first applications to be incorporated into the GCCS were mission-essential functions including the JOPES and the Status of Resources and Training System (SORTS). The GCCS also includes the infrastructure that supports sharing, displaying, and exchanging information and a COP/CTP. The GCCS infrastructure consists of UNIX-based servers and client terminals as well as personal computer (PC) workstations operating on a standardized LAN. The GCCS infrastructure supports data transfer among workstations and servers. Connectivity between GCCS nodes is achieved via SIPRNET.

Marine Air-Ground Task Force C4I

MAGTF C4I is the concept for the integration of Marine Corps tactical information systems and the migration of selected legacy systems to the COE. The MAGTF C4I concept is consistent with DOD mandates for COE compliance and designation of standard migration systems. MAGTF C4I is designed to support commanders and their staffs at all levels of the MAGTF. The MAGTF C4I migration strategy focuses on incorporating the software functionality of MAGTF tactical information systems into a MAGTF software baseline (MSBL). Standard software applications and the capability to support MAGTF command and control functions will be managed under the MSBL. The MSBL relies on the COE for its common software environment. This software environment, in addition to providing operating systems and application interfaces, provides users with common commercial-off-the-shelf (COTS) applications.

Command and control personal computer (C2PC) is a COTS-based software application designed to facilitate military command and control functions. C2PC applications are hosted on the

TCO and IAS. Laptops may be configured as IOSv1 workstations (maneuver client) and IOSv2 workstations (intelligence client).

IOSv1 and IOSv2 have already transitioned to support COTS. IOS servers and workstations have been fielded; in some instances, down to the regiment level.

Key Marine Air-Ground Task Force Information Systems

Key MAGTF information systems that support command and control are described below. The system descriptions focus on operational employment by functional area.

Maneuver

Information systems support maneuver by assisting commanders and staffs with shared situational awareness based on an integrated picture of the battlespace. This common picture is developed through the collection, processing, integration, and analysis of data from all functional areas. Through the COP/CTP, the commander and his staff gain an understanding of the situation and act on that understanding. Information systems support the planning process by facilitating the sharing of the commander's intent, the analysis of COAs, and the development and dissemination of OPLANs and OPORDs. Information systems then enable the commander and his staff to monitor execution, assess results, and act based on the changed situation.

IOSv1 is the primary information system supporting maneuver. As discussed above, IOSv1 has been incorporated into the MSBL and operates under the COE and in a PC client environment. IOSv1 processes tactical information from the GCCS track database manager (a UNIX server) to form a COP/CTP. Future enhancements to IOSv1 will provide automated support for the development of COAs and the preparation and

dissemination of OPLANs and OPORDs, including overlays that are geographically referenced to an electronic map.

IOSv1 supports the operations sections of all MAGTF units of battalion/squadron size and larger as well as planning sections at the MEF level. IOSv1 consists of computer workstations operating at the secret level on multiple LANs interconnected on the SIPRNET through MAGTF communications networks. The functional manager for IOSv1 is the G-3/S-3, and operations section personnel are responsible for setting up the IOSv1 equipment in the COC. CIS personnel are responsible for connecting IOSv1 terminals to the SIPRNET, providing them with IP network host addresses, and assisting the operations section in installing and maintaining the IOSv1.

Navy shipboard mission applications have been developed for operation in the same UNIX client-server COE as have the Marine Corps' IOSv1 and IOSv2. This permits embarked MAGTFs to "plug in" IOSv1 and IOSv2 to the shipboard client-server environment. Furthermore, like the Marine Corps, the Navy is currently rehosting some of these mission applications to a PC client environment. The Navy goal is the same as the Marine Corps: to transition away from UNIX to an all windows-based PC client-server environment.

Intelligence

Intelligence systems support the timely planning and direction, collection, processing and exploitation, production, dissemination, and use of all-source intelligence. IOSv2 is the principal Marine Corps intelligence information system. IOSv2 provides intelligence personnel with intelligence operations planning and direction, all-source processing and fusion, and dissemination capabilities. The G-2/S-2 is the functional manager for IOSv2. Intelligence personnel are responsible for setting up and employing IOSv2 equipment in their intelligence centers. MEF IOSv2 is a

sheltered, mobile system with multiple (scalable) analyst workstations in a UNIX-based client-server LAN configuration. IOSv2 suites for intermediate commands are configured in a four-workstation LAN. At the battalion/squadron level, a single intelligence/operations workstation with software developed as part of C2PC will provide IOSv2 capability. IOSv2 will host or integrate with a variety of MAGTF intelligence systems, to include:

- SIGINT—technical control and analysis center (TCAC).
- IMINT—tactical exploitation group, secondary imagery dissemination system.
- CI/HUMINT Automated Tool Set.
- Measurement and signature intelligence tactical remote sensor systems.
- GEOINT—topographic set, topographic production capability.

Additionally, it will be interoperable with other intelligence systems at the national, theater, joint, and other Services levels.

Aviation Operations

The MACCS provides the tactical air commander with the automated support required to exercise control over MAGTF air operations. The MACCS supports both tactical air command and the control of aircraft and missiles. The control of aircraft and missiles is a highly specialized function addressed in MCWP 3-25. MACG personnel support the installation, operation, and maintenance of the MACCS. The Marine wing communications squadron (MWCS) provides CIS connectivity.

Theater battle management core systems (TBMCS) is a battle management system used for planning and executing air operations. TBMCS provides a complete tool kit to manage, plan, and execute the ATO. TBMCS is an Air Force-developed program formed by the consoli-

dation of several existing segments: Contingency theater automated planning system (CTAPS), combat intelligence system, and the wing command and control system. Some of the functions provided by TBMCS are the following:

- Build the target nomination list, the air battle plan, and the ATO.
- Monitor the execution of the air battle and re-plans, as required.
- Plan routes, ensure airspace deconfliction.
- Build the airspace control order.
- Provide weather support.
- Manage resources; e.g., aircraft, weapons, fuel, logistics.
- Display information on the enemy, battle results, and friendly forces.
- Analyze information to determine strategies and constraints.
- Identify potential targets and propose an optimal weapons mix.
- Provide for support and protection of ground forces.
- Plan countermeasures and frequency assignments.

Tactical air command systems provide the tactical air commander with support for planning, controlling, and coordinating overall MAGTF air operations through the execution of the air tasking cycle. Functions supported include determination of operational requirements, allocation of aircraft, processing of ATOs and airspace control orders, planning and monitoring of air operations, and coordination with naval and joint agencies. TBMCS runs at the secret level on UNIX-based servers on the TACC LAN. The MWCS provides each TBMCS workstation with an IP host address and connects the TACC LAN to remote airfields, the DASC, the TAOC, and other-Service command centers over the SIPRNET by using IP routers and organic transmission assets. TBMCS replaces the CTAPS.

Fires

The Initial Fire Support Automated System provides automated support for technical artillery fire control and limited automated support for fire planning and tactical fire direction. AFATDS fully automates support of fire planning, tactical and technical fire direction, and fire support coordination. AFATDS is employed at FDCs down through the firing battery level, at FSCCs down through the battalion level, at the SACC, and by the MAGTF CE. AFATDS assists the commander in improving tactical planning and control of supporting arms operations. Supporting arms fires, including rocket and tube artillery, mortar, and naval surface fires support, are planned and coordinated within the MAGTF by AFATDS. AFATDS provides the ability to integrate supporting arms assets into maneuver plans, provide battlefield information, target analysis, and unit status, while coordinating target damage assessment and sensor operations.

The AFATDS workstation, the main component of AFATDS, receives, transmits, edits, displays, and processes fire support requests, and stores data to facilitate artillery fire support directions and coordination. It displays a full range of fire support, maneuver control, coordination measures, and geometry data for fire support at the workstation. AFATDS operates within the current and planned communications architecture, using wire and tactical radio, and assists the commander with automated message delivery for coordination of supporting arms fires.

Logistics

Logisticians employ information systems to plan, coordinate, and direct logistic operations and to maintain visibility of logistic status. Currently fielded logistic information systems include the Asset Tracking Logistics and Supply System

(ATLASS) and the MAGTF II/Logistics Automated Information System (LOGAIS) family of systems. The MAGTF II/LOGAIS family of systems includes MAGTF II, the MAGTF Deployment Support System (MDSS) II, the computer-aided embarkation management system (CAEMS), and the Transportation Coordinator's Automated Information for Movement System (TC-AIMS).

ATLASS provides automated support for supply and maintenance. It is replacing two mainframe-based systems, the Marine Corps Integrated Maintenance Management System and the Supported Activities Supply System (SASSY), with a client-server system running on PCs. ATLASS is being implemented through phased development, with the current phase focusing on integrating user-unit supply and shop-level maintenance functions.

MAGTF II is a system that allows planners to select and tailor MAGTF force structures, estimate sustainment, and estimate airlift requirements for plan feasibility analysis. MAGTF II serves as the bridge between the MAGTF II/LOGAIS family of systems and JOPES, permitting MAGTF commanders to submit TPFDD refinements to JOPES. Additionally, MAGTF II has the capability to download plans from JOPES. MAGTF II runs on PCs. It includes TC-AIMS and MDSS II. (TC-AIMS II, a joint system, will eventually replace TC-AIMS and MDSS II). TC-AIMS and ATLASS will be the primary systems to provide functional logistic management for sustainment and distribution.

TC-AIMS provides the MAGTF commander and staff with an automated capability to plan, coordinate, manage, and execute MAGTF movement from the point of origin to the air and sea port of embarkation and from the port of debarkation to the final destination. TC-AIMS runs on PCs.

MDSS II enables planners at various echelons of a MAGTF to build and maintain a database that contains force and equipment data reflecting how a MAGTF is configured for deployment. This data can be updated during plan development and execution. Extracted MDSS II data is passed through MAGTF II to JOPES to provide an accurate picture of MAGTF composition, including the lift requirement. MDSS II runs on PCs.

CAEMS is an interactive database/graphics tool for producing amphibious, MPF, and MSC ship load plans and associated reports. CAEMS employs linked computer-aided design (CAD) and database systems to recognize ship and cargo characteristics, to conduct cargo loading and offloading flowpath analysis, to allocate cargoes to stowage spaces, and to ensure that stowage compatibility requirements are met. Additionally, CAEMS provides input to trim, stability, and stress calculations and produces accurate "as-loaded" ship load plans and reports. During the planning and execution phases of an operation, CAEMS updates MDSS II. CAEMS runs on PCs.

Communications and Information Systems

The Systems Planning, Engineering, and Evaluation Device (SPEED), with its associated software, is the primary information system supporting the planning and employment of MAGTF CIS. SPEED provides the Marine Corps with the capability to rapidly engineer tactical communications systems by using automated radio propagation and network planning tools on a PC-based system. SPEED can also be used to evaluate system performance before installation. SPEED supports radio path profiling and area coverage analysis, HF propagation analysis, network planning (line of sight and position location information studies), and unit level circuit switch (ULCS) network planning. SPEED incorporates the Revised Battlefield Electronic Communications-Electronics Operating Instruction System (RBECS), which is the software required to operate the SINCGARS in a frequency hopping mode. SPEED is fielded down to the infantry regiment level with a database that includes the technical profiles of communications-electronics equipment and a set of National Imagery and Mapping Agency digital terrain maps.

SECTION III. DEFENSE COMMUNICATIONS ARCHITECTURE

DISA is responsible for implementing, as the information transfer segment of the COE, a single, integrated, common-user, global communications network. This network, the DISN, will provide support for the exchange of voice, data, imagery, and video from strategic to tactical levels, at all echelons, in garrison or when deployed. The DOD and the Services are implementing the DISN in an evolutionary manner by interfacing and integrating existing communications networks and making maximum use of commercial services and standards.

The Marine Corps has combined its private enterprise network, the MCEN, with the DISN. Just as the GCCS and the COE are shaping the development of MAGTF information systems, DISN implementation is shaping the MAGTF communications architecture. For the near term, the communications networks supporting the MAGTF will include the current MAGTF tactical communications networks: the switched backbone, SCR, LANs, and special-purpose networks with an interface to the DISN for long-haul communications. However, change is

occurring rapidly with the introduction of IP router-based data communications systems and equipment augmenting the switched backbone and providing enhanced connectivity among tactical networks and between tactical networks and the DISN.

It is these IP router-based systems, combined with COTS software, that allow the MAGTF to establish an intranet. That intranet rides on the backbone provided by the MAGTF communications architecture, and the data communications overlay provided by the TDN. This MAGTF intranet should be designed and employed based on a well-thought-out information management plan.

Defense Information Systems Network

The DISN is evolving toward a single, integrated telecommunications infrastructure that will provide end-to-end communications connectivity in support of military operations worldwide. Ongoing efforts include upgrades to switching and transmission centers around the world and consolidating and integrating satellite and terrestrial communications networks. The DISN currently provides long-haul, common-user, dedicated, secure and nonsecure, voice, data, and video service through a mix of DOD-dedicated and standard commercial communications services.

The DISN provides the communications backbone for DOD-wide subnetworks including the following:

- The Defense Switched Network (DSN).
- The Secure Voice System.
- The Defense Data Transport Network (NIPRNET and SIPRNET).
- The JWICS.
- Separate systems and networks serving the combatant commanders, Services, and agencies.

Deployed forces access the DISN through 14 DISA standardized tactical entry points (STEPs), commonly referred to as STEP sites. MAGTFs use these STEP sites to access the DISN to support training, exercises, and operations. When ashore, the primary means available to the MAGTF to access the STEP sites is through TACSAT communications over the Defense Satellite Communications System (DSCS). Shipboard access is provided through the Navy Tactical Network. Five entry points with Navy-unique configurations are located at Naval Computer and Telecommunications Area Master Stations (NCTAMSs) to provide ship-to-shore and ship-to-ship communications.

The services provided to the deployed MAGTF through the DISN STEP sites include voice, data, and video.

Defense Switched Network

Each STEP provides one T1 (1.544 Mbps) circuit supporting 44 interswitch trunks to a DSN multi-function switch. These 32 kilobits per second (kbps) interswitch trunks allow tactical users to place nonsecure or secure telephone unit-III (STU-III) calls to a DSN subscriber.

Defense Red Switch Network

A single STEP accommodates up to four 56 kbps circuits to the Defense Red Switch Network switch. Each circuit provides two interswitch trunks between the tactical and Defense Red Switch Network switches. These eight interswitch trunks allow tactical users to place secure red switch calls from the field.

Nonsecure Internet Protocol Router Network

The NIPRNET is an information network that is based on IP routers and Integrated Digital Network Exchange (IDNX) smart multiplexers.

NIPRNET is designed for sensitive but unclassified information transfer. It supports unclassified networks such as the MCEN and the Tactical Automated Weather Distribution System. Under the Integrated Tactical-Strategic Data Network program, 10 of the 14 STEP sites were configured with NIPRNET routers. MAGTFs use the NIPRNET in garrison and when deployed, and aboard ship and during operations ashore to transfer administrative data.

Secure Internet Protocol Router Network

The SIPRNET is an information network based on IP routers and IDNX smart multiplexers, and is designed for exchange of classified information up to and including the secret level. It supports the exchange of classified data between the GCCS, Defense Message System (DMS), TBMCS, IOSv1, IOSv2, and other tactical information systems. SIPRNET routers are collocated with NIPRNET routers at 10 STEP sites. MAGTFs use the SIPRNET in garrison and when deployed, aboard ship and during operations ashore to transfer operational data.

Joint Worldwide Intelligence Communications System

JWICS is an information network based on IP routers and IDNX smart multiplexers. It is designed for exchange of SCI-level video and data information. It supports the MAGTF's use of intelligence link (INTELINK) and other services accessed by using joint deployable intelligence support system (JDISS) and TCAC. MAGTFs use JWICS in garrison and when deployed, aboard ship and during operations ashore to exchange SCI data.

Video Teleconferencing

VTC is used at MSC and higher echelons with increasing frequency. When deployed, it is primarily used for MAGTF-to-component/JTF/ combatant commander coordination.

Defense Message System

The DMS is a secure X.500 and X.400 based e-mail system developed by the USG with industry partners to ensure safety for critical operations. Essentially an enhanced version of various commercial e-mail products, DMS was developed for the DOD as a replacement for the automatic digital network (AUTODIN).

At the user level, DMS looks like a typical e-mail application and is designed to feature familiar user-friendly functionality, such as global directory service and transmission support for digital files of various types and sizes. Security and delivery assurance mechanisms are approved by the National Security Agency for information classified at all levels, up to and including Top Secret. DMS policies require that all messages be signed and encrypted with Class IV Public Key Infrastructure protection through Fortezza, the National Security Agency's trademarked security products suite.

DMS was designed to incorporate components from a variety of leading hardware and software vendors and to leverage the best current and emerging messaging technologies within the defense information infrastructure, a worldwide connectivity transport infrastructure. The DMS development program began in response to joint staff requirements for an integrated messaging service that could be accessed from any DOD location in the world and by designated government users or contractors.

DMS uses the DISN IP router-based network and supports messaging in garrison or in the tactical environment. DMS, once fully implemented, will eliminate AUTODIN.

Marine Corps Enterprise Network

The Marine Corps is provided global computer network communications through the MCEN. The MCEN is connected to the DISN, which provides

access to the NIPRNET and SIPRNET networks. MCEN connectivity to the commercial internet is accomplished via its links to the NIPRNET.

Overall management of daily operations and security of the MCEN is accomplished by the mutually supporting efforts of the Marine Forces Integrated Network Operations (MARFOR-INO) and the Marine Corps Information Technology and Network Operations Center (MITNOC). These two organizations are collocated in Quantico, Virginia. Both fall under the direct cognizance of the Director, C4 Department, Headquarters Marine Corps.

The MARFOR-INO is the Marine Corps' Service component to the US Space Command's Joint Task Force-Computer Network Operations (JTF-CNO). The JTF-CNO is responsible for coordinating and directing DOD efforts to secure and defend the DISN. The Commandant of the Marine Corps has vested authority in the MARFOR-INO to direct network defensive actions across the Marine Corps and to fulfill Service responsibilities assigned by JTF-CNO and higher authority.

The MITNOC is responsible for the overall management of the global MCEN. The MITNOC controls the network connection points between Marine Corps installations (base-to-base communication links) and to external networks, such as the NIPRNET and SIPRNET. It is also responsible for maintaining enterprise-wide network services, to include the global e-mail address directory. The MITNOC provides the highest echelon of technical support in the Marine Corps for computer problem resolution.

The MCEN is a global network with over 100,000 users located at 30 geographically separate locations around the world. Although the MITNOC has overall responsibility for the daily operation of the MCEN, there is an underlying network management and computer technical support structure based on a hierarchy of four mutually supporting echelons.

First Echelon

The ISC is the central point of contact within a small unit or work section. Technical problems beyond the ISC's capabilities or authority are referred to the second echelon of support.

Second Echelon

The LAN manager is normally located within the G-6 at an operational command or the information technology division at a base/station. The LAN manager is responsible for all LANs operating within subordinate or tenant organizations and units. LAN managers are specifically tasked to provide technical support to ISCs under their cognizance. Technical problems beyond the scope of the LAN manager's capabilities or authority are referred to the third echelon of support.

Third Echelon

Each base/station network manager serves as a third echelon organization. Base/station network control centers provide technical guidance and support to LAN managers within their geographic area of concern. Technical problems beyond the scope of the base/station network control center are referred to the fourth echelon for resolution. Third echelon organizations house the connection point between the internal base/station network and the rest of the MCEN and to the DISN and other external networks. Although these connection points are housed by third echelon organizations, management and control of these are exercised centrally by the MITNOC.

Fourth Echelon

The MITNOC manages the overall operation of the MCEN and is the fourth and highest echelon of network and computer technical support within the Marine Corps.

Deployed Units

The senior command in an operating force that has established a tactical network is temporarily designated a third echelon organization while deployed and may receive support directly from the fourth echelon. Unlike the supporting establishment network environment, the connection point between the tactical network and external networks is not centrally managed by the MITNOC. The operating forces maintain these tactical network connection points.

Many management issues are involved in deployed network support; i.e., effecting a communications shift when switching between NCTAMS or when the MAGTF transitions from

ship-to-shore. While afloat, MAGTFs will be supported by the ship's technical communications center with reachback to the Navy Network Operations Center or NCTAMS site. When a MAGTF is deployed as part of a JTF, a joint communications control center will provide network management throughout the JTF area of responsibility. The MITNOC has a deployed support section. Its mission is to provide network technical advice and assistance during all phases of a deployment and coordinate the timely resolution of technical problems. It works in partnership with DISA, NCTAMS, the Marine Corps Tactical Systems Support Activity, and operating force commands to provide coordinated support to deploying units.

SECTION IV. ROLES AND RESPONSIBILITIES

Responsibilities *must* be understood to establish and maintain an effective communications network. Failure of any single individual, unit or activity to carry out assigned responsibilities can have catastrophic results.

Commander

The commander has the responsibility to establish communications within his unit, and to higher, adjacent, and subordinate units according to his mission and organic capabilities. Although the authority to plan and employ communications systems may be delegated, ultimate responsibility for communications planning and employment remains with the commander. The commander must provide adequate guidance, including necessary assumptions and constraints, to support the development of communications estimates, plans, and orders.

Communications Officer/G-6/S-6

The communications officer is responsible to the commander for all matters on the planning and employment of communications within the command. As a general/executive staff officer, the G-6/S-6 serves as an advisor, planner, supervisor, and coordinator. Specific responsibilities include the following:

- Provides the commander and other staff officers with—
 - Estimates of the supportability of COAs.
 - Estimates of requirements for communications resources (personnel, equipment, supplies, and facilities).
 - Recommendations for the allocation and use of communications resources.
 - Recommendations for communications training for the command.

- Recommendations on the location, echelonment, and displacement of the command post and other command and control facilities.
- Advice on operational aspects of INFOSEC.
- Prepares communications plans, orders, and SOPs to implement the commander's policies and decisions on communications employment.
- Assists the staff with communications to prepare studies, estimates, plans, orders, instructions, and reports.
- Complies with the commander's orders and instructions by supervising the following:
 - Employment of communications personnel.
 - Installation, operation, and maintenance of communications networks.
 - LAN and WAN management, including IP address and routing management.
 - Technical support for functional users in the installation, operation, and maintenance of information systems hardware and common user software.
 - Communications systems training and, in coordination with functional users, information systems administration training.
 - Supply and maintenance of communications systems and equipment.
 - Compliance with SOPs and interoperability standards.
 - COMSEC in coordination with other staff sections.
- Coordinates communications matters with cognizant staff sections and with staffs of other units.
- Establishes communications liaison with senior, subordinate, adjacent, supported, and supporting units.

Supported Unit/Agency

Communications support is more and more frequently considered a service, much like electricity or water service delivered to a household. Responsibilities of the service recipient—whether an entire unit, a small agency or an

individual—are an important factor in successful employment of the service delivered.

No longer is the bulk of information processing done through a batch job on a faraway mainframe computer, staffed with specialists, and delivered in hard copy to the requester. Today, users within staff sections administer and use information systems that deliver specialized information that permits unparalleled effectiveness. Most of it is done in an information-pull environment. The user employs his system to obtain information over the communications network to accomplish a specific goal or mission. This relatively new power comes at a cost, namely that of individual knowledge and training.

On the modern battlefield, it is essential that functional users of information be able to configure and operate the information systems supporting their functional area. Such ability increases the speed and effectiveness that a distributed network can be established and employed. It also ensures functional area users are able to best exploit and control the capabilities of systems that support their needs. Functional users include every staff section supported by communications systems. Consequently, all staff principals have functional user responsibilities for the function-specific systems under their staff cognizance; e.g., the G-3/S-3 has functional user responsibilities for IOSv1.

Functional user responsibilities include the following:

- Serves as the primary point of contact—internal and external to the command—for issues affecting information systems supporting the functional area.
- Serves as the configuration manager for information systems supporting the functional area.
- Conducts routine information system administration (assigning user identification, passwords, and privileges; performing data/file storage and management; conducting system backups of functional area information systems).

- Coordinates with the G-6/S-6 to ensure that adequate hardware, software, trained personnel, and procedures are in place before implementing or modifying a new system.
- Coordinates with the G-6/S-6 to develop and maintain user training programs for communications.
- Identifies information system support requirements to the G-6/S-6.
- Identifies specific communications requirements, including requirements to interface with other information systems and potential interface problems, to the G-6/S-6.
- Complies with applicable COMSEC measures.
- Reports malfunctions and outages and coordinates with the G-6/S-6 to restore service.
- Designates an IMO for the staff section.