Defense Communications

Mission and Organization of the Defense Information Systems Agency (DISA)

The mission and structure of the Defense Information Systems Agency
The worldwide digital systems architecture (WWDSA)

Composition of the Defense Communications System

Elements of the DCS
Responsibilities of DCS control facilities

In the early morning hours of 7 December 1941, the first wave of Japanese fighter aircraft began their attack on Pearl Harbor, Hawaii, launching the United States into World War II. The planes came in low and fast, striking their preselected targets with great accuracy. When the assault was completed, millions of dollars in damage had been done to key airstrips and other military installations, thousands of men were killed or injured, and our Pacific fleet was virtually destroyed.

The attack occurred while many of our soldiers and sailors were still sleeping and unaware of the impending danger. It did not have to be that way, though. Hours before the attack began, military authorities had drafted a message warning of possible hostile actions by the Japanese. Problems on the HF radio link from Washington to Hawaii that Sunday morning forced communications personnel to choose an alternate method for transmitting the message. Although several other Government communications links were available, the warning was sent by RCA commercial radio, arriving in Hawaii after the attack was already in progress.

This story gives some insight into the condition of our military communications structure as our country entered World War II. Since then, we have made tremendous advances in facilities, equipment, techniques, and organization. The organization gained momentum with the passing of the National Security Act of 1947. In that act, lawmakers included this declaration of purpose: To provide for the effective strategic direction and operation of the armed forces under unified command.

Effective strategic direction meant that efficient communications facilities would be needed. Moreover, they should be unified. In other words, what was needed was a common communications system that would link all defense activities together. The answer was the Defense Communications System (DCS).

To make sure the DCS became a reality, the Department of Defense (DOD) established the Defense Communications Agency (DISA) and gave it the task of creating and managing the worldwide military communications complex. In this unit, you will find information about the DISA in terms of its management of the DCS. Although we will be primarily discussing DISA, we cannot really separate *you* from the scene. In your job as a technical controller, you are part of the management team. You help manage the part of the DCS that passes through your Technical Control Facility (TCF). While doing so, you will be working within a framework of policies and procedures prescribed by DISA. Some of the most important of those managerial policies and procedures are covered in the sections that follow.

Mission and Organization of the Defense Information Systems Agency (DISA)

DISA was organized in May 1960 to make sure that an integrated communications system would be established, improved, and operated to meet DOD needs. Portions of the communications assets of the three military services were placed under the control of DISA and then combined to form the DCS. Before that time the Army, Navy, and Air Force had operated three separate strategic communications systems. Each was independent of the other, except for a few minor links that were often technically incompatible. DOD Directive 5105.19 gives DISA authority to direct the DCS. DISA is undergoing restructuring and renaming and eventually will be named the Defense Information Systems Agency, or DISA.

The mission and structure of the Defense Information Systems Agency

Mission of DISA

Managing a large and complex system, such as the DCS is by no means an easy task. The list of management responsibilities and functions of DISA are found in DISAC 640–45–21, *DISA Organization and Functions Manual.* Briefly, though, the mission of DISA is to:

a. Do systems engineering for the DCS.

b. Make sure the DCS is planned, improved, operated, maintained, and managed effectively, efficiently, and economically.

c. Meet the long-haul, point-to-point, and switched telecommunications needs of the National Command Authorities, DOD, and other Government agencies, as authorized and directed.

While DISA is responsible for the proper management of the DCS, the operation and maintenance of the various components of the DCS are the responsibility of the military departments through their operation and maintenance (O&M) agencies.

Even though you are in the Air Force and assigned to a major command, your working relationship with various elements of DISA will be close; so close, in fact, that at times you may think you are working for DISA. This misconception is caused by the fact that DISA retains the authority to direct the operation of the DCS. In the following paragraphs, we will see how DISA directs the daily operation of the system.

Organization (DISA Operations Control Complex)

The Director, DISA, exercises operational direction of the DCS through the Defense Communications Agency operations control complex (DOCC). The DOCC, as shown in figure 1–1, is composed of several levels of management centers that carryout the complex task of maintaining the DCS. The objectives of the DOCC are as follows:

a. Make sure of user-to-user communications support within the DCS.

b. Provide DCS status information in a useful form to let users and O&M agencies do their jobs and to prevent duplicate reporting.

c. Coordinate between the operating elements, user, commercial carriers, O&M agencies, military services, and other Government agencies, as directed, to identify communications problems quickly.

d. Make sure of restoration of the DCS under any adverse or catastrophic conditions.

e. Set up guidelines for transition to a wartime environment.

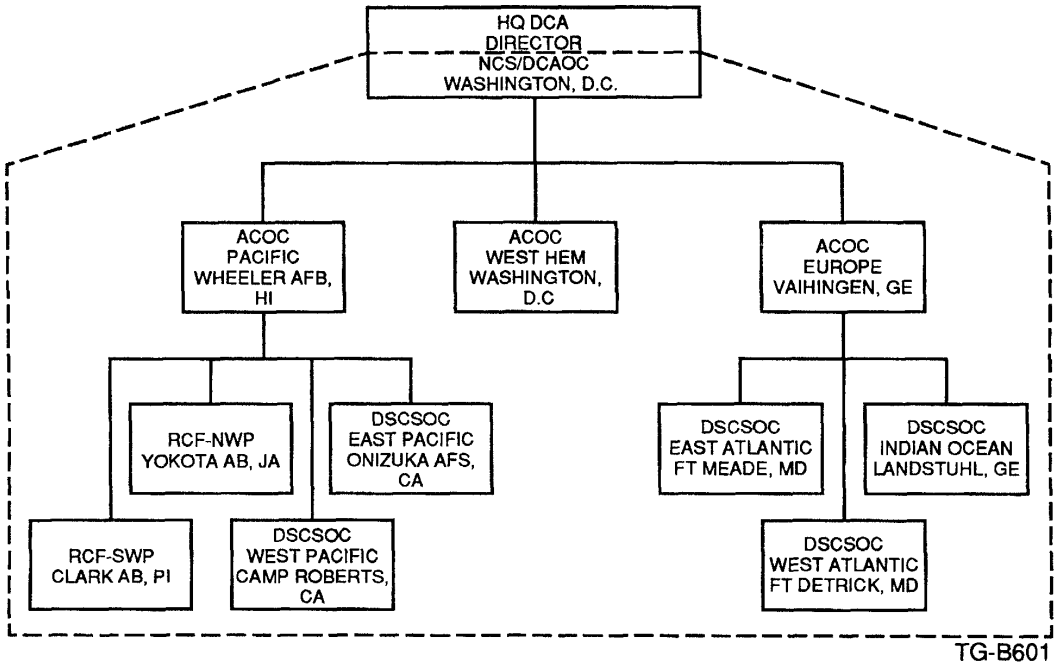

Figure 1-1. DCA operations control complex (DOCC).

[figure 1–1]

National Communications Agency Network Management Operations Center (NCANMOC)

The DISANMOC is the central controlling element of the DOCC. Located at Headquarters DISA, it is responsible for exercising day-to-day operational direction over the world-wide DCS operations elements.

Area Communications Operations Center (ACOC)

The ACOCs are responsible for the operational direction of a specific geographical area. There are three ACOCs: DISA Western Hemisphere, collocated with the DISANMOC at Headquarters/DISA; DISA Europe, located at Vaihingen, Germany; and DISA Pacific, located at Wheeler AFB, Hawaii. Current plans call for a fourth ACOC to be known as DISA Central.

Regional Control Facility (RCF)

Due to the large geographic area of the Pacific, DISA Pacific (PAC) is divided into two regions, each with an RCF responsible for its operational direction. DISA Northwest Pacific (NWP) is located at Yokota AB, Japan, and DISA Southwest Pacific (SWP) at Clark AB, Phillipines.

As a technical controller, you will work closely with controllers at either an area communications operations center (ACOC) or an RCF, depending on the location of your facility. Although you do not work for them, it is important that you maintain good relations with the controllers at the operations center you are working with. They are

responsible for ensuring that the policies of the director of DISA are carried out efficiently.

All DCS reporting stations (technical control facilities) within an area are connected to one of the operations centers by *critical control circuits*. These control circuits are special *order wires* used by the DOCC in exercising operational direction over the DCS and in receiving DCS status reports.

Each operations center has a communications status activity, whose personnel maintain 24-hour-a-day surveillance of the status of the DCS within their area of responsibility. They do this by collecting, processing, and analyzing the reports submitted by stations under their control. To make this work more efficiently, the larger operations centers use computers to collect and process the status information.

By analyzing the contents of incoming status reports, operations center personnel decide whether *operational direction actions* are needed. They also use technical controller requests on recommendations and user complaints. If action is necessary, they decide what it should be and then pass directions and information to the right DCS element—-your technical control facility, for example. Operations center personnel use the critical control circuits, on-call patches, and DSN calls to transmit directions. When situations are not urgent, they may use written messages sent through normal communications channels. Messages passed by any of the means we have just mentioned are known as *operational direction messages* (ODM).

An ODM is not merely an administrative message. On the contrary, it is usually a very important—-sometimes vital—-directive that normally requires immediate action by your technical control facility. While on duty, you may receive an ODM, perhaps passed over the critical control circuit or by DSN. Of course, it will not be addressed to you personally, but it might as well be. The person transmitting the ODM to your station will expect you to know what to do with it. If you receive a voice ODM, be certain to record the information exactly as given to you, then give it to your supervisor as soon as you can.

Your supervisor may prepare a reply to the ODM, called an *operational coordination message (OCM).* OCMs can also be used to send nonaction information to an area or regional operations center and are transmitted the same way as ODMs.

Defense Satellite Communications System Operations Center (DSCSOC)

The DSCSOCs are responsible for the operational direction of Defense Satellite Communications System Earth terminals in a given geographic area. The five DSCSOCs are located at Ft Meade and Ft Deterick, Maryland; Camp Roberts and Onizuka AFS, California; and Landstuhl, Germany. The DSCSOCs are manned by DISA personnel who report to the ACOCs as indicated in figure 1–1.

The worldwide digital systems architecture (WWDSA)

In May 1977, DOD tasked DISA, in coordination with the military departments, the TRI-TAC office, the National Security Agency, and other interested agencies and commands, to develop the WWDSA. The motivation for this effort stemmed from widespread concerns about the ability of DOD telecommunications systems to maintain acceptable levels of interoperability, survivability, and restorability on an end-to-end basis at a reasonable cost.

WWDSA was developed under DISAs leadership by the WWDSA working group; in December 1981, DISA issued the WWDSA final report, which documented the WWDSA goal architecture and the work done in its development. The report documents a transition strategy to achieve that architecture.

This transition strategy includes building on existing and planned programs, an enhanced command and control communications intelligence (C^3I) ability, an improved interoperability and standardization, exploitation of commercial developments, provision for continuity of service, incremental introduction of new services, and incremental improvements in management and control.

The improved systems will form an interoperable set of mutually supportive networks and facilities that are better able to cope with the challenges of supporting military operational needs throughout the full range of possible conflicts, including crises and contingencies, conventional warfare, limited nuclear warfare, and all phases of general nuclear warfare (preattack, transattack, postattack).

The WWDSA establishes evolutionary transition strategy for DODs telecommunications systems to achieve needed survivability and endurability that is affordable. The transition strategy incorporates 14 key objectives that are to be considered for incorporation in all DOD telecommunications systems as they are being planned or as improvements to existing systems are made. The key objectives of the WWDSA are:

(1) To obtain access to many sources of connectivity, including a variety of transmission media and switched networks, in order to achieve path and propagation diversity.

(2) To have the ability to use many sources of connectivity intelligently through improved routing strategies, processor augmentation, and extension of system capabilities closer to the users where possible.

(3) To have modularly expandable switches in capacity and features to allow low-startup cost. This composite switching ability is expandable to include such features as multilevel precedence and preemption (MLPP).

(4) To have interconnected voice and data (circuit-switched and packet-switched) networks for mutual support and improved reliability.

(5) To have improved internetwork systems control to improve call connect performance and system control responsiveness.

(6) To have a tandem switching ability to improve connectivity, provide a more distributed structure, and thereby increase survivability and responsiveness.

(7) To have a multirate ability (16 and 64 kbps) among switches for more effective use of digital transmission links. Tactical switches may be able to provide switching only at 15 kbps, but they should interface with 64 kbps switched networks. Secure voice at 2.4 kbps will be carried through the circuit switched network on 16 and 64 kbps channels through sub-multiplexing, multiple sampling, or bit-stuffing techniques. Trunking through HF radio will carry voice and data over 4-kHz analog channels.

(8) To enhance 2.4 kbps secure voice survivability through the use of packetized voice and the interconnection between circuit-switched and packet-switched networks.

(9) To have high-quality 16 kbps secure voice with an ability to tandem and conference with 2.4 kbps secure voice.

(10) To have a common proliferated survivability key distribution system for voice and data that will provide improved performance, security, and survivability of secure voice calls and secure data transfer.

(11) To have end-to-end encryption for classified data users over both circuit- and packet-switched networks.

(12) To have expanded and integrated use of satellite communications, including the use of small, extremely high-frequency/demand assignment multiple access (EHF/DAMA) satellite Earth terminals, both military and commercial, to supply wideband services and improve the mix of media at switching nodes.

(13) To have improved internetwork systems control between DCS, tactical, strategic, civil, commercial, and allied networks for normal operation, restoral, and reconstitution. Control will be made easier through the use of automated aids (network status indicators, facility reassignment algorithms, and data bases) useful to network management decisionmakers. Critical users will have a systems control ability to help in the step-by-step restoral of fragmented networks.

(14) To have common standards for all networks and equipment, where practical, for improved interoperability. Emphasis on use of commercial standards where suitable.

Most of the current major architectures, plans, and programs are generally consistent with WWDSA, and only minor refinements are needed, in most cases, to bring our telecommunications systems into full alignment. While the WWDSA final report offers only general guidelines for transition, DISA is issuing more specific recommendations as they are developed.

Composition of the Defense Communications System

As you know, the DCS is a composite of DOD-owned and -leased telecommunications systems, subsystems, and networks composed of facilities, personnel, and material and is managed by DISA. It provides the long-haul, point-to-point, and switched network telecommunications needed to satisfy the requirements of DOD and selected Government agencies.

You have already seen how the various elements of the DOCC direct the operation of the DCS. This section will provide an overview of the elements that make up the DCS and the facilities that have direct control responsibility over them.

Elements of the DCS

DCS facilities can be broken down into three general categories: fixed, transportable, and mobile.

Fixed

Most of the facilities in the DCS are fixed. These include, among other assets, switching facilities, such as the automatic digital network (AUTODIN), and automatic secure voice network (AUTOSEVOCOM), radio relay facilities, and most assets of the Defense Satellite Communications System (DSCS). These facilities are built permanently in place: in other words, they are not transportable or mobile. Some of these facilities will be discussed in detail in the remaining units of this volume.

Transportable

Some of the equipment in the DCS is transportable. This is equipment that can be moved by truck, rail, or other means. An example would be power generators used to support long-term, but not necessarily permanent, operations.

Mobile

Many technical controllers are assigned to mobile or tactical communications squadrons. The equipment these organizations use can be mounted on devices known as mobilizers or can be carried on trucks and trailers for rapid deployment in support of short-term military operations. Both mobile and transportable communications systems will be covered in Volume 3 of this course.

Also included in the DCS are the transmission media (including those commercially leased), circuits that provide user and subscriber connection to the switching and relay facilities of the DCS networks, and circuits that interconnect the switching and relay facilities of the DCS networks. All telecommunications required to interconnect the National Command Authority (NCA), the Joint Chiefs of Staff (JCS), and commanders of the unified and specified commands with the general purpose networks are DCS assets.

You should understand that some of the communications equipment and systems you encounter will not be part of the DCS. The communications networks for post, camp, or base operations are generally not considered part of the DCS, even though technical controllers who are assigned to a DCS facility help to maintain their proper operation. Also, the mobile and transportable communications facilities of the Army, Air Force, and Naval and Marine forces are not DCS assets. As you familiarize yourself with the particular facility you are assigned to, you should make it a point to know what your DCS assets are.

Responsibilities of DCS control facilities

In our discussion of the DOCC, we said that its various offices are responsible for the operational direction of the DCS. Understand that the DCS is a large and complex system that requires a wide dissemination of responsibilities to make sure of its proper management. For this reason, many TCFs are chosen as control facilities and given management responsibilities that are more specific than those of the elements of the DOCC. The control facilities in the following discussion report their status to the right DOCC elements in their geographical area.

Facility Control Office (FCO)/Subregional Control Facility (SRCF)

An FCO is assigned to supervise the operation and maintenance of communications links in given geographical areas. Certain TCFs will be assigned this responsibility based on their ability to access the systems and stations under their control. Essentially, the FCO is an added duty that some TCFs have. It should be noted that, at the time of this writing, DISA is undergoing a reorganization. The FCOs will slowly transition into SRCFs that will have responsibilities similar to those of the FCO.

Intermediate control office (ICO)

If the layout of a particular segment of a communications circuit or trunk is such that the FCO/SRCF or circuit control office (CCO) is not in the best position to test and coordinate with other TCFs, one or more of the other TCFs may be chosen as an ICO for that particular segment. Each ICO is responsible for the general service condition of its segment of a circuit or trunk.

Circuit control office

One TCF is named CCO for each circuit in the DCS. Generally, the CCO is responsible for coordinating the initial activation of a circuit by the telecommunications service order (TSO), which establishes the circuit. The CCO coordinates any realignment or deactivation of the circuit. The CCO also is responsible for end-to-end out-of-service (customer denied service) quality control testing and for coordinating troubleshooting efforts during circuit outages or to maintain the engineered value stated in the TSO.

An application of the CCO plan with one TCF at each end of a circuit is shown in figure 1–2. Both TCFs are referred to as serving TCFs as they provide users with access to the DCS.

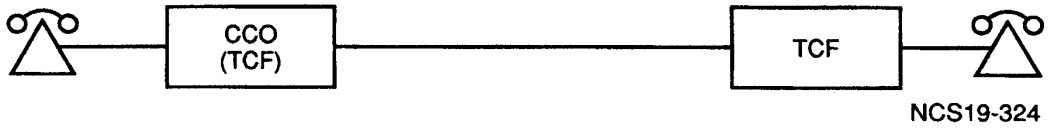

Figure 1-2. CCO assignment.

[figure 1–2]

Another application of the circuit control plan may require the assignment of an ICO to help the CCO in testing, coordination, and other required actions. A TCF may be assigned as an ICO on the path of long or complex circuits with the configuration as shown in figure 1–3.

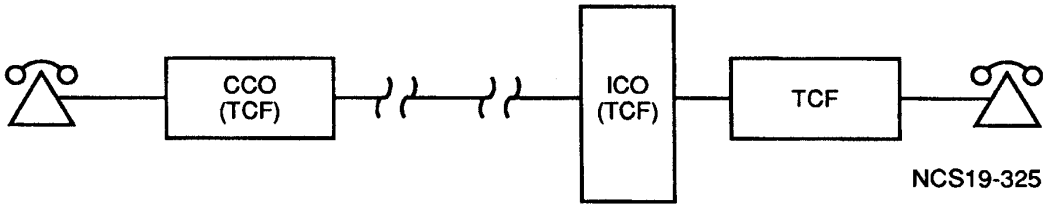

Figure 1-3. CCO assignment with ICO.

[figure 1–3]

The TCF to which you are assigned may be given FCO/SRCF, ICO, or CCO responsibilities, or any combination of the three. Elements of the DOCC decide which

TCFs fill these important positions, and they are named on the TSO for each circuit and system.