REF ID:A58489

~~RESTRICTED~~

DEPARTMENT OF THE ARMY TECHNICAL MANUAL TM 32-250

DEPARTMENT OF THE AIR FORCE MANUAL AFM 100-80

FUNDAMENTALS OF TRAFFIC ANALYSIS (RADIO-TELEGRAPH)

RESTRICTED. DISSEMINATION OF RESTRICTED MATTER.—No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also AR 380–5.)

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
OCTOBER 1948

~~RESTRICTED~~

Declassified and approved for release by NSA on 12-24-2013 pursuant to E.O. 13526

REF ID:A58489

WARNING

Authority for release of this document to a foreign government must be secured from the Assistant Chief of Staff, G–2.

When this document is released to a foreign government, it is released subject to the following conditions: This information is furnished with the understanding that it will not be released to another nation without specific approval of the United States of America, Department of the Army; that it will not be used for other than military purposes; that individual or corporation rights originating in the information whether patented or not will be respected; and that the information will be afforded substantially the same degree of security as afforded by the United States of America, Department of the Army.

REF ID:A58489

TM 32–250—AFM 100–80

FUNDAMENTALS OF TRAFFIC ANALYSIS (RADIO-TELEGRAPH)

RESTRICTED. ***DISSEMINATION OF RESTRICTED MATTER.***—**No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also AR 380–5.)**

United States Government Printing Office
Washington; 1948

REF ID:A58489

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
Washington 25, D C, 1 October 1948

TM 32-250—AFM 100-80, Fundamentals of Traffic Analysis (Radio Telegraph) is published for the information and guidance of all concerned

[AG 300.7 (9 Jun 48)]

BY ORDER OF THE SECRETARIES OF THE ARMY AND THE AIR FORCE

OFFICIAL
EDWARD F WITSELL
Major General
The Adjutant General

OMAR N BRADLEY
Chief of Staff, United States Army

OFFICIAL
L L JUDGE
Colonel, USAF
Air Adjutant General

HOYT S VANDENBERG
Chief of Staff, United States Air Force

DISTRIBUTION

Army

GSUSA (1), Arm & Sv Bd (2), AFF (15), OS Maj Comd (5), Base Comd (2), MDW (16), A (ZI) (30), (Overseas) (15), CHQ (5), D (3), USMA (20), Sch (10) except Ground Gen and 11 (25), ROTC (1), T/O & E 32-952 (20), 32-1027 (20)

Air Force

USAF (10), USAF Maj Comds (5), USAF Sub Comds (3), Div (Air) (2)

For explanation of distribution formula, see TM 38-405

REF ID:A58489

CONTENTS

REF ID:A58489

CHAPTER 1

INTRODUCTION

Section I. GENERAL

1. Purpose

The purpose of this manual is to present a standard approach to traffic analysis problems of the military type in order to furnish signal intelligence personnel with a knowledge of traffic analysis techniques, capabilities, and applications. It is to be recognized that no text on analytic techniques can be definitive because techniques are subject to continual improvement and change in order to meet changing problems. This text is intended merely as a guide. Specific application is dependent on the ability and ingenuity of the analyst.

2. Scope

This manual is concerned only with traffic analysis of military radio communications, but the techniques covered will also be found of value in the analysis of other kinds of communication networks. Discussion of other means of communication, such as wire or cable, has not been included; in the reconstruction of the radio communication system it should be remembered that often these other means will account for missing portions of the system. Further, the scope is limited to the study of Morse transmissions. Non-Morse transmissions, such as radio-teletype and radio-telephone, are not discussed. The differences, however, are largely technical and procedural and involve the material transmitted only to a limited extent. It is thought, therefore, that this text will serve as a basis for all traffic analysis and that, with some minor modification, the methodology described will be found applicable to all types of transmission.

REF ID:A58489

3. References

A general knowledge of radio theory, Morse code, and radio procedure is assumed. For reference purposes the field and technical manuals listed in the appendix will be found useful.

4. Definition of Traffic Analysis

Traffic analysis is that branch of signal intelligence analysis which deals with the study of the external characteristics of signal communications and related materials for the purpose of obtaining information concerning the organization and operation of a communication system. This information is used (1) as a guide to efficient intercept operation, (2) as an aid to cryptanalysis, and (3) as a basis for drawing deductions and inferences of value as intelligence even in the absence of specific knowledge of the contents of the message.

5. Objectives

To achieve planned and coordinated action, it is necessary for the components of a military force to communicate with each other from the highest headquarters through all intermediary channels to the individual man in the field or the airplane in the air. Much of this communication, for reason of speed and efficiency, is conducted by radio, and radio is vulnerable to intercept. Therefore, disguises are devised to conceal both the traffic passed and the structure of the communication network. Traffic is disguised through the employment of codes and ciphers, and it is the task of cryptanalysis to solve these codes and ciphers. The communications net work is disguised through the use of a number of techniques which relate, for example, to the use of call signs and frequencies, the method of routing messages, and the use of secret procedure signs. These techniques, the means for attacking them, and the resulting reconstruction of the network are the study of traffic analysis. The responsibility of the traffic analyst, however, does not stop with the reconstruction of the communication network. It is also part of his mission to discover practical applications for his knowledge in the associated fields of intercept, cryptanalysis, intelligence, and security. The objectives of traffic analysis, then, fall into two main groups:

a. The acquisition of a detailed knowledge and a complete understanding of a communications network. This involves the reconstruction of the nets, the determination of the features of their operation, the solution of call sign and routing systems, analysis of the components of the message externals, the interpretation of radio procedure, and the use of the various cryptographic systems passed; in

REF ID:A58489

other words, everything about communications except the actual cryptanalysis of the text.

b. The application of this knowledge to—

(1) *Intercept operations.* Traffic analysis contributes to three aspects of the intercept problem. First, by providing the intercept station with certain necessary information, such as call sign and frequency lists, target locations, schedules, etc., it assists the station in the accomplishment of its mission and encourages the best possible results. Second, in coordination with cryptanalytic and intelligence interests, it determines the priorities governing the interception of individual circuits. Third, through a study of intercept, it checks the performance of the station in relation to its mission.

(2) *Cryptanalysis.* Aid to cryptanalysis is furnished in a great variety of ways, largely dependent on the cryptanalytic and traffic analytic peculiarities of the communications under study. *In most instances, traffic analysis and cryptanalysis become so interrelated that it is impossible to determine where one begins and the other leaves off, and it is necessary to set an arbitrary dividing line.* In general, however, assistance takes the following forms: the solution of the routing systems, where disguised, and the placing of the routings in the clear on traffic; the study of the uses of the various cryptographic systems; the reading of chatter for items of cryptanalytic interest; the discovery of crib, or stereotype, texts from message externals; the location of isolog messages; and the application of other traffic analysis data, such as message serial numbers, which may be of value in specific cryptanalytic problems.

(3) *Intelligence.* Military communications, including both the organization of the nets and the traffic passed, reflect the disposition of troops and the intentions for movements and operations. A careful analysis, therefore, of net structure, traffic contacts and patterns, traffic volumes, and similar signals features, assists in the building of the final intelligence picture. The exact techniques to be used are, again, dependent on the individual problem and involve the recruitment, training, organization, and order of battle of the military forces under study as well as characteristics of communications.

(4) *Security.* Because the traffic analyst becomes skilled in probing the weaknesses of communication systems, he is in an ideal position to assist in maintaining high standards of security within our own communication networks. This function of traffic analysis is mentioned merely in passing. It will not be discussed further in this text.

REF ID:A58489

Section II. GENERAL APPROACH

6. The Raw Material

The traffic analyst begins his study of a communications network with three types of raw (basic) data:

a. INTERCEPT DATA. This is the information supplied by the intercept operator. It consists of the frequencies to which he is listening, the times during which he hears signals, and occasional comments such as notes on the quality of the signal or the characteristics of the radio operator.

b. THE TRANSMISSION. The transmission is the sum total of everything sent by the radio operators. It includes the initial call-up, the exchange of call signs, the traffic, servicing, miscellaneous chatter, and signing off. Traffic may be divided into two parts: the message externals (preamble and postamble) and the text. The externals generally contain radio station and message center numbers of a variety of types, routing instructions, addresses, precedence indicators, and file times, all of value in traffic analysis. The text usually exhibits a number of cryptographic features in the clear which are likewise of use.

c. COLLATERAL INFORMATION. Besides the above material, there is a large amount of data which is available or which can be made available for traffic analysis purposes. Some of these are directly related to intercept, such as goniometric bearings. Other items are message decodes, captured documents, and intelligence reports.

7. The Analytic Approach

a. Traffic analysis is partly analytic, partly synthetic. Analysis is performed on each feature of the communications network and then, through exploiting the relationships between these features or within them, traffic analysis synthesizes them into a unified whole. In other words, the types of raw data noted in paragraph 6 are first analyzed until everything possible is known about each item independently, after which, though often seemingly unrelated, they can be pieced together to produce a complete picture of the radio nets. This means that the analyst must pay particular attention to detail and must carry much of this detail in his mind so that he can readily perceive the relationships between discrete items and integrate them to form the whole.

b. The actual approach to a traffic analysis problem is broadly determined by the stage of development of the problem. These stages of development are threefold, but it should be understood that what is represented are not clear-cut divisions in operation, but rather, gradual shiftings of emphasis as the problem matures.

REF ID:A58489

(1) *Initial attack.* (*a*) In the initial period, little is known about the problem and it may first be necessary to identify the radio nets and traffic involved so that they can be distinguished from all other types. When this has been accomplished, the characteristics are furnished to the intercept station which embarks on a large-scale search mission, scanning the entire range of frequencies for transmissions of the desired nature. During this time, it is the task of the traffic analyst to give direction to this mission and to evolve from it a definite assignment. It should be noted here that the search mission, in reduced scale, should always continue until the problem has ceased to exist, in order to cover new net developments.

(*b*) As soon as material begins to accumulate, an elementary study may be conducted on the elements of the transmission, particularly the message externals. The functions of the various preamble components should be observed, the method of routing noted, and in general, the significance of each component determined.

(2) *Development.* During the second period, emphasis is placed on the study of the communications system with a view to learning all its details of organization, operation, and procedure. There are usually two phases to this: the research phase, which involves thorough analysis of every item, such as call signs, procedure signs, message numbers, routing codes, and cryptographic features; and the actual net reconstruction, consisting of the building of the entire radio net complete with call signs, frequencies, schedules, and station locations.

(3) *Application.* When this knowledge has been gained, and even while it is being gained, it can be put to use in the three related fields of control, cryptanalysis, and intelligence. From the very first moment that traffic analysis is performed, it begins contributing to these phases of communications intelligence, but it is not until a substantial amount of information has been gathered that these applications receive full emphasis. The final goal of traffic analysis operations is the reconstruction of the complete radio network against its cryptographic and order of battle background, and the production on a day-to-day basis of items of cryptanalytic application and intelligence importance.

REF ID:A58489

CHAPTER 2

RADIO OPERATIONS

Section I. INTRODUCTION

8. Radio Operations

a. The operation of a radio network requires a set of fixed rules and regulations which define the manner and form of communications. These rules are in part subject to the laws of nature, in part to the necessities of communication itself, and in part to the whim and ingenuity of the personnel formulating them. The first two factors impose some degree of uniformity on radio networks, no matter what the type or nationality. This makes it possible to set down the basic features of communications, e.g., call signs, frequencies, message numbers, and routing instructions. However, the third factor acts to vary those features by determining the way that they are used. This chapter outlines what these basic features are and some of the ways in which they may be manipulated. It is, of course, not possible to include all the types which may be encountered, but it is hoped that what is given will serve to indicate the general patterns the traffic analyst is likely to meet in studying radio operations and will serve to set up general lines of traffic analysis thinking.

9. Phases of Radio Operations

Radio operations for purposes of study may be divided into four main phases:

a. Operating Data. The first considerations in the creation of a communication net relate to the structure or form of the net, the use of frequencies and call signs, and the system of schedules. These are the basic operating data of the net and involve its mechanical functioning. In the case of some nets, the military for instance, attempts are made to conceal these data; in other cases, such as commercial, they can be determined with little effort.

b. The Radio Transmission. Once the operating data have been determined, the next step is to devise the form and language of radio transmission. There must be regulations governing the Morse code to be used (largely dependent on the alphabet concerned), the pro-

REF ID:A58489

cedure signals which make for brevity and speed and which may be encoded for reasons of security, the order of elements in the transmission, the plain-language chatter of the radio operators, and the plain-language and simple cipher messages usually considered part of the traffic analysis task.

c. THE MESSAGE EXTERNALS. The message externals are actually a part of the radio transmission and belong under *b* above, but because of their importance a separate section (sec. IV, this ch.) is devoted to them. They include the preamble and postamble and generally contain serial numbers of various types, group check, file date and time, precedence indicators, and routing instructions.

d. TEXTUAL FEATURES. Some of the cryptographic aspects of the text are in the clear to make possible proper handling of the traffic by message center personnel and to permit decrypting. These features in the clear are often of great assistance to the traffic analyst. They may merely involve whether the text is in letters or numbers, or the length of the code groups, or they may be somewhat more complex as discriminants, indicators, or pad numbers.

Section II. OPERATING DATA

10. General

The operating data enable the network to function. They consist of the frequencies, call signs, and schedules used in communication. Traffic analysis is interested not only in the operating data as used by the network, but also in the general system on which the allocation of operating data to specific nets and radio stations is based. This section is devoted to a discussion of radio nets and of the ways in which the operating data are used and assigned.

11. Definitions

a. A radio network is composed of radio stations organized for the purpose of intercommunication. This organization is not haphazard but follows very definite and detailed patterns. These patterns are based on the order of battle since the lines of communication themselves must coincide with the echelon of command and the military requirements. Before it is possible to enter into a discussion of these patterns, however, it is necessary to define some of the terminology to be used.

(1) *Link:* Any system of telecommunication between two points.

(2) *Group:* One or more links whose stations work together as a communication entity under a common operating control.

REF ID:A58489

(3) *Net:* One group or a number of groups assembled on the basis of common operating characteristics, presumably under the administrative direction of an immediate common superior headquarters.

(4) *Network:* The radio system of a service of a nationality, as United States Army network, United States Naval network, United States Air Force network.

b. These definitions may appear somewhat obscure to the student for the moment, but it should be kept in mind that they are formulated from a traffic analysis point of view, that is, from the outside looking in. These terms must be so categorized in order to be of value analytically and, therefore, they represent the situation as it appears rather than as it actually is. Figure 1 will help to clarify these terms, and it is suggested that the student study the diagram from time to time as its understanding is essential to the proper approach to net reconstruction.

c. Figure 1 illustrates the general organization of the military network, proceeding from Department of the Army Headquarters through theater, army group, army, corps, and division. The equivalent Department of the Air Force organizations are shown in figure 2. (The following pertains equally to the Department of the Air Force.) Each line or connection represents a radio link within the terms of the definition in *a*(1) above—any telecommunication system between two points. It is to be emphasized that only *two* stations are involved in a link, never any more. Thus, the line from Department of the Army HQ to Theater "A" is a link; the line from Department of the Army HQ to Theater "B" is another; the line from 2d Corps to 1st Division is one; as is the connection from 1st Division to 2d Division. The links which form the triangle, 2d Corps, 1st Division, 2d Division, constitute a group; those forming the triangle, 2d Corps, 3d Division, 4th Division, constitute another. These links are placed in groups because they work together as a communication entity under a common operating control (the group control being at the highest headquarters of the group, here the 2d corps), yet do not, in themselves, comprise the complete net. The net is made up of the two groups together and is, in this instance, the 2d Corps net with the 2d Corps headquarters as net control. It should be observed that very often the link and the group may be the same thing, or the link, group, and net may be the same. Each definition of the larger unit enfolds the lesser. For example, the line from Department of the Army HQ to Theater "A" may be termed a link, for it is composed of only two stations, or a group because its stations work as a communication entity under the control of the Department of the Army station; the three links, or groups, however, running out from Department of the Army HQ form the Department of the Army net.

REF ID:A58489

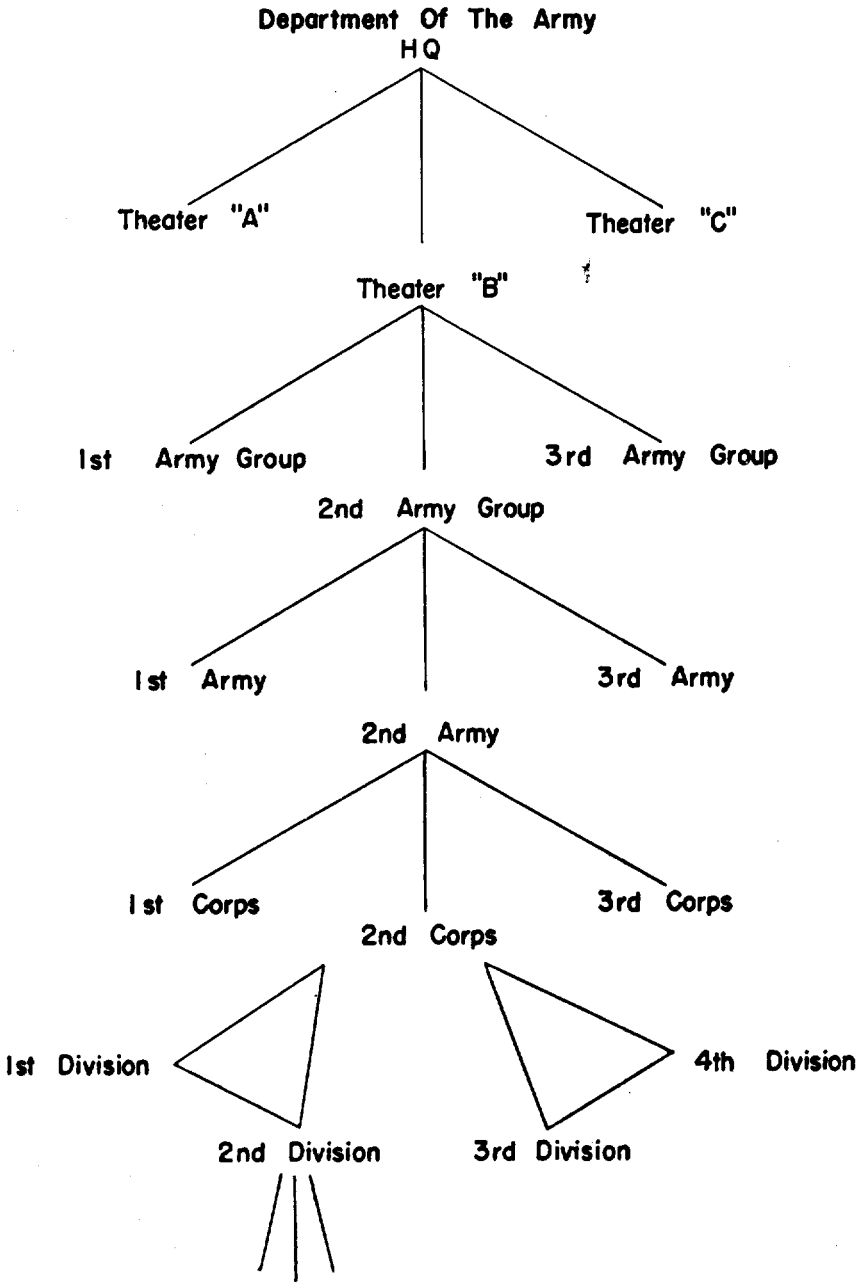


Figure 1. General organization of military network—United States Army.

REF ID:A58489

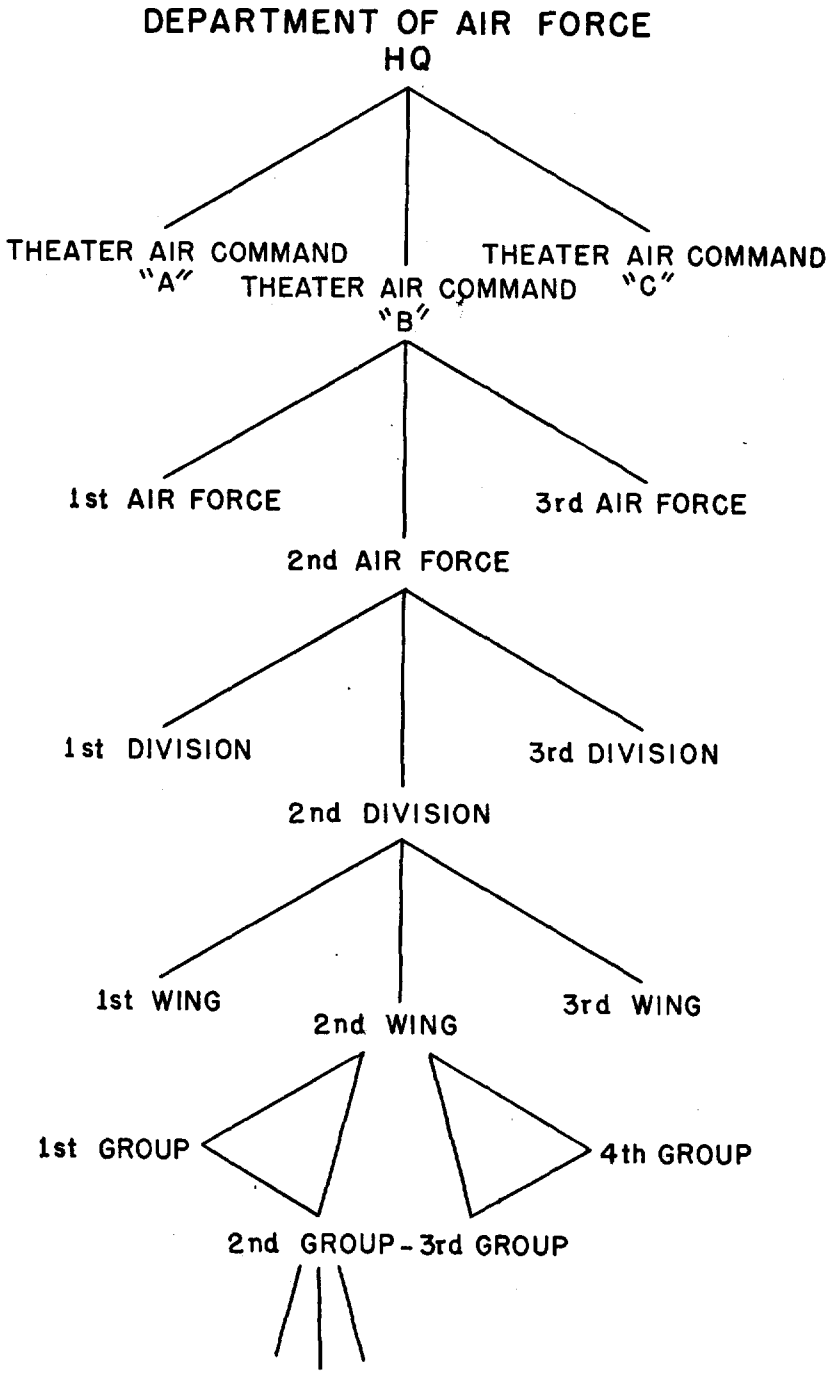


Figure 2. General organization of military network—United States Air Force.

REF ID:A58489

d. It will be recalled that, in discussing these definitions in *b* above, it was stated that they were formulated from an analytic point of view. This is particularly true of the definition of the net. In the reconstruction of the radio network, one of the first problems is the organizing of a number of radio links into groups and nets. In the case of the group, this is fairly simple to accomplish for the group is a communication entity, that is, all of its stations either work each other or have contact with a central operating control. The net, on the other hand, often does not exhibit such cohesive characteristics. A number of groups, apparently unrelated, may eventually fall into a single net when the order of battle is finally derived. There are two touchstones for the association of groups into nets:

(1) *Common operating characteristics.* Since the links and groups of the net all have a common superior headquarters, it may be assumed that certain rules of procedure and operation will be promulgated by this superior and that, therefore, all links and groups of the net will exhibit these in common.

(2) *Administrative direction of an immediate superior headquarters.* When the order of battle is known, it is often possible to associate groups and links through the knowledge that they are controlled by the same unit.

e. The net, the group, and the link, then, are merely units of organization in the radio network, just as armies are broken down into corps, divisions, regiments, companies, and platoons. Likewise, air forces are broken down into divisions, wings, groups, squadrons, and flights. And these nets, groups, and links may be characterized by the unit served and the function performed. For instance, figure 1 represents command channels so that there is a Department of the Army command net, a Theater "B" command net, a 2d Army Group command net, and so on. Radio, however, serves many other military functions than that of command. Military nets, for example, may be organized to contain an antiaircraft artillery group, an artillery air-ground group, an artillery observation group, a reconnaissance group, an air warning group, and others beside the command group.

12. Examples of Radio Nets

Figures 3 through 9 illustrate some of the type nets which may be encountered. These types will vary in individual instances; they serve, however, to indicate some of the possibilities.

REF ID:A58489

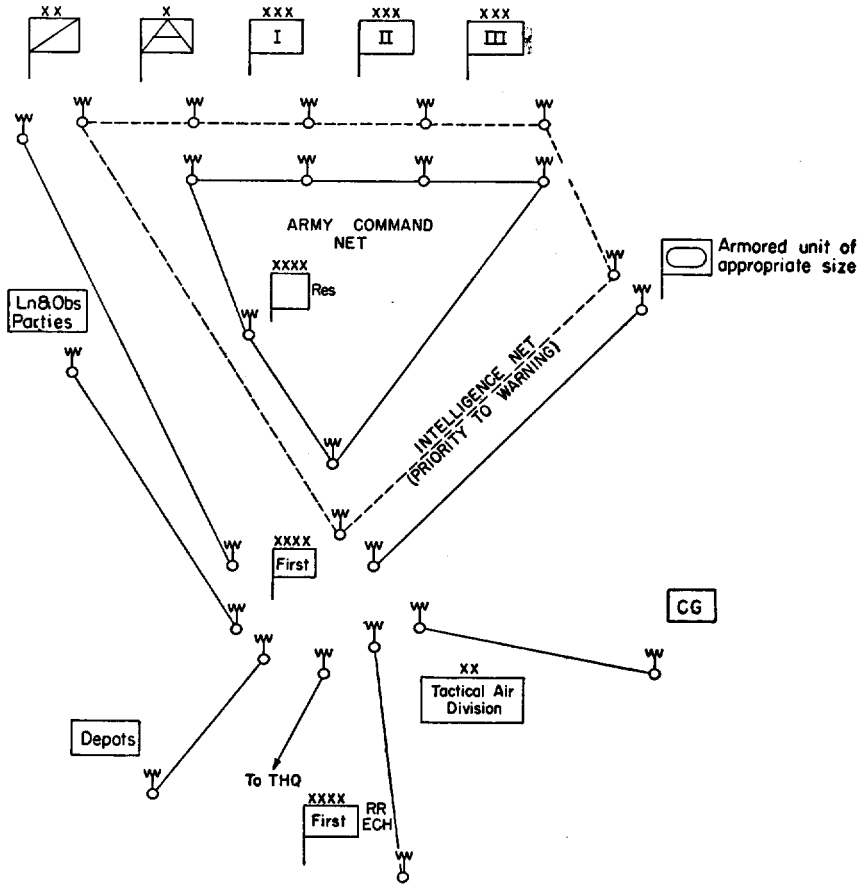


Figure 3. Type radio nets, Army.

REF ID:A58489

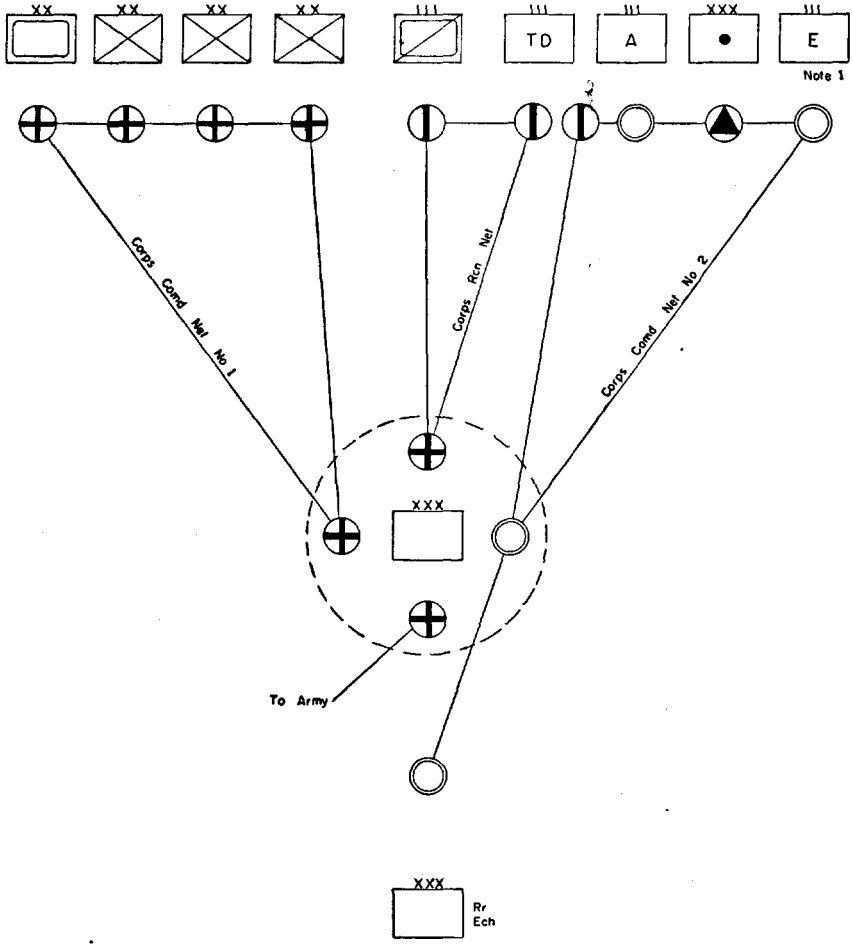


Figure 4. Type radio nets, corps.

REF ID: A684682

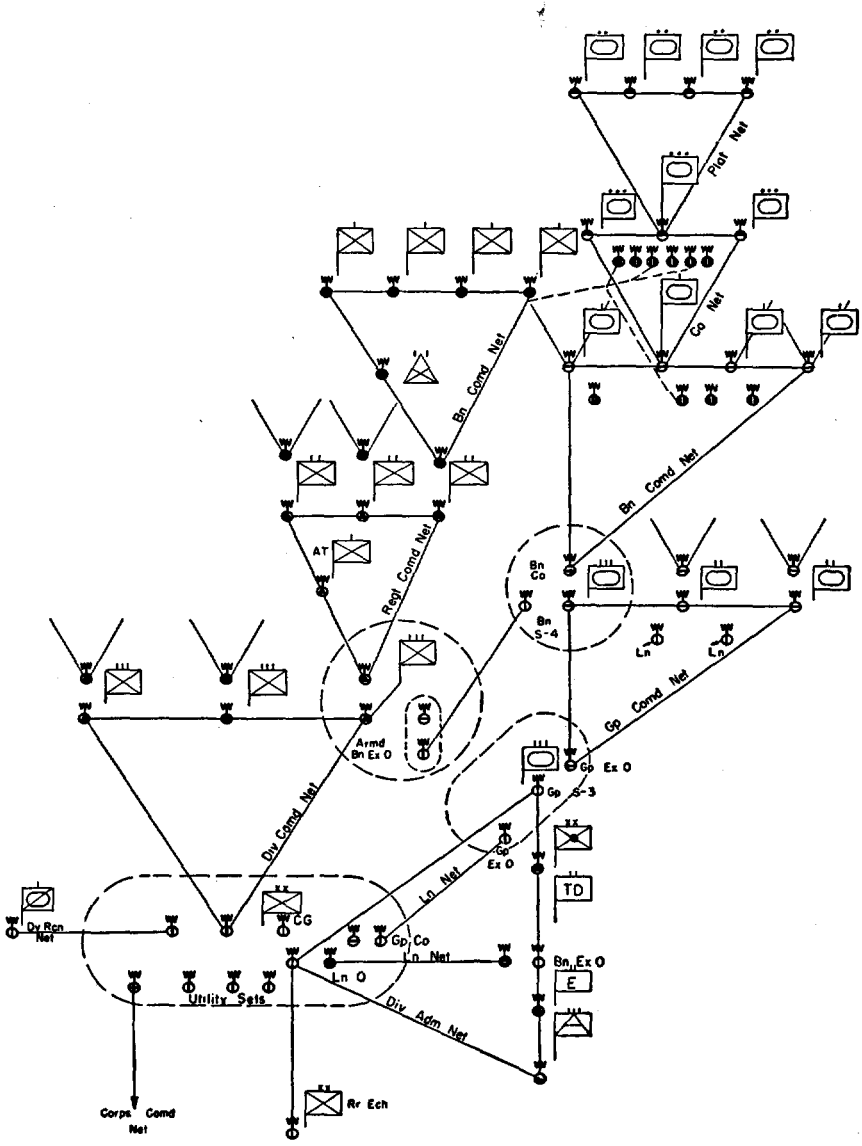


Figure 5. Type radio nets, infantry division, with attached units.

REF ID: A684682

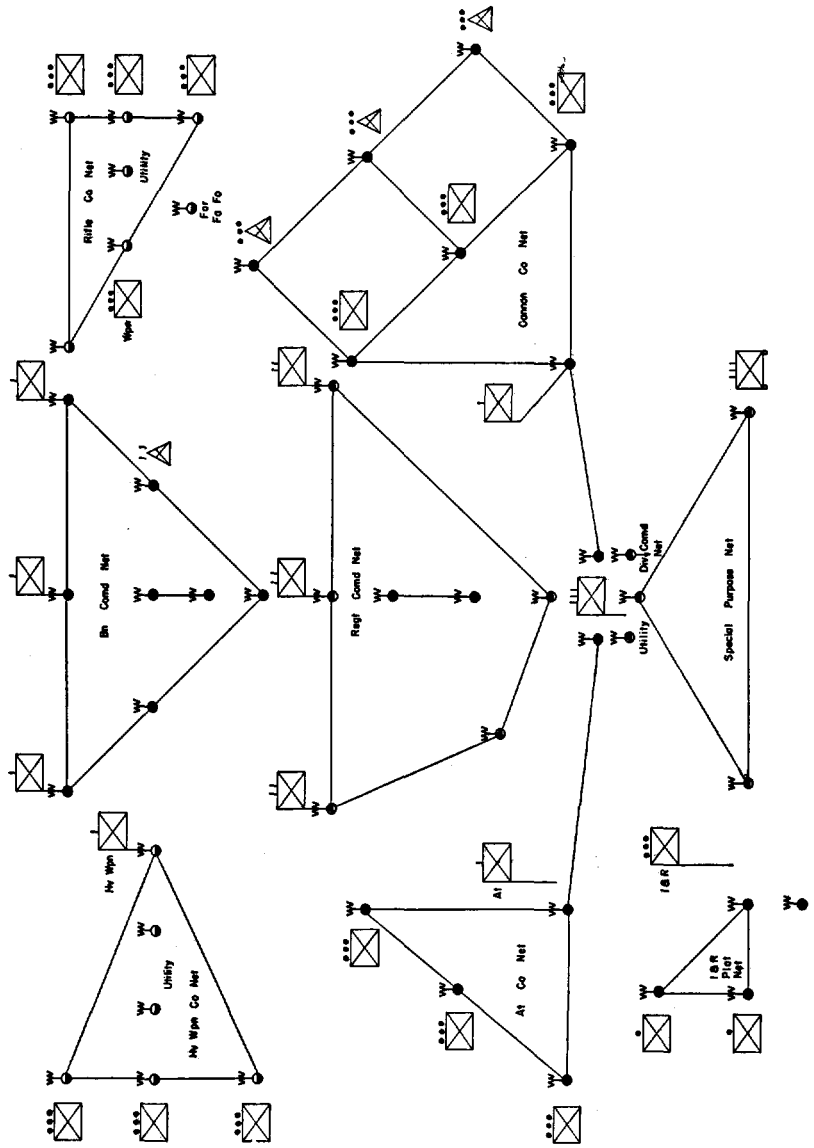


Figure 6. Various radio nets in an infantry regiment.

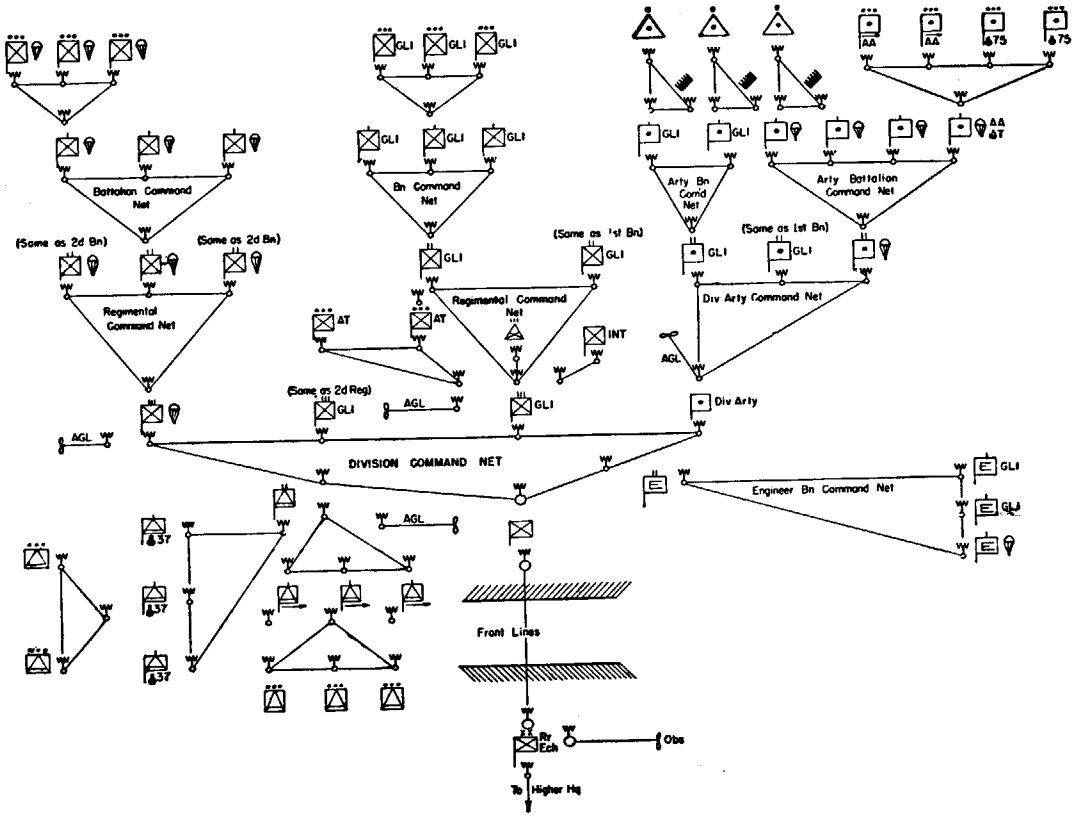


Figure 7. Type radio nets, airborne division.

REF ID:A584489

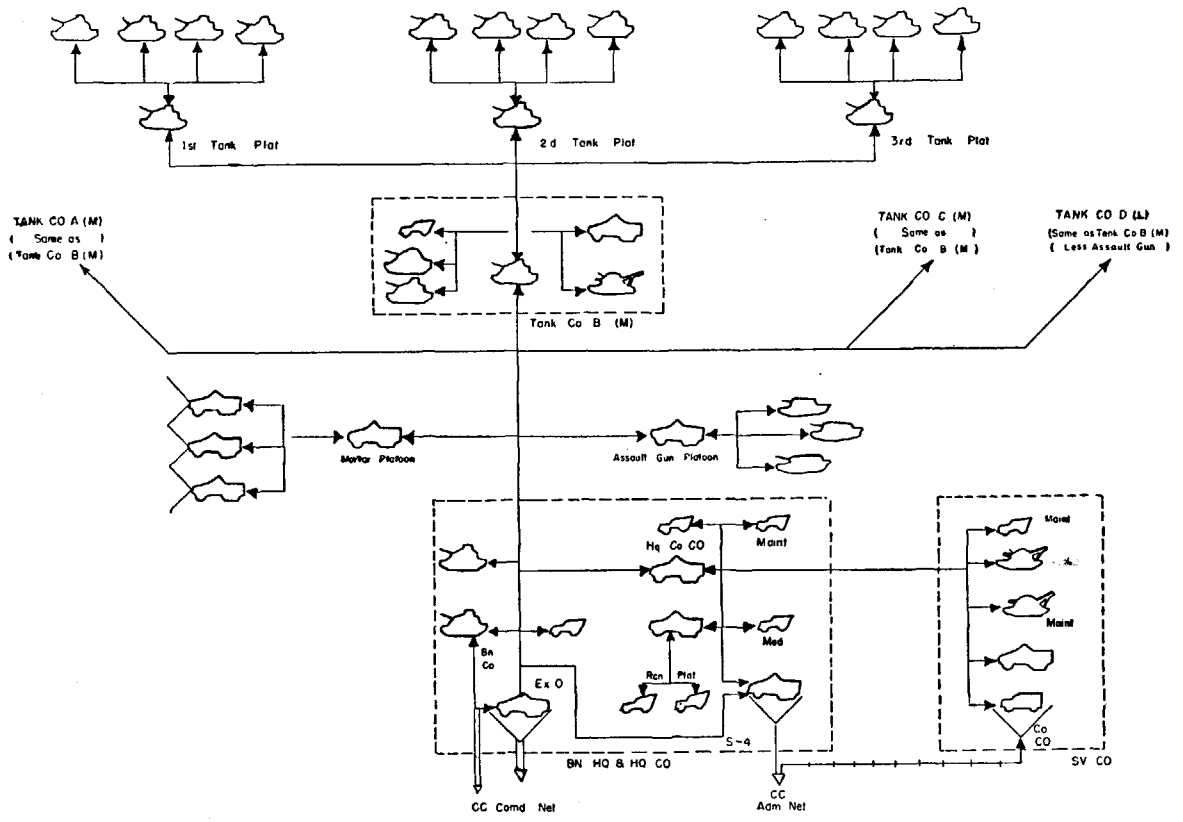


Figure 8. Type radio nets, tank battalion.

REF ID:A58489

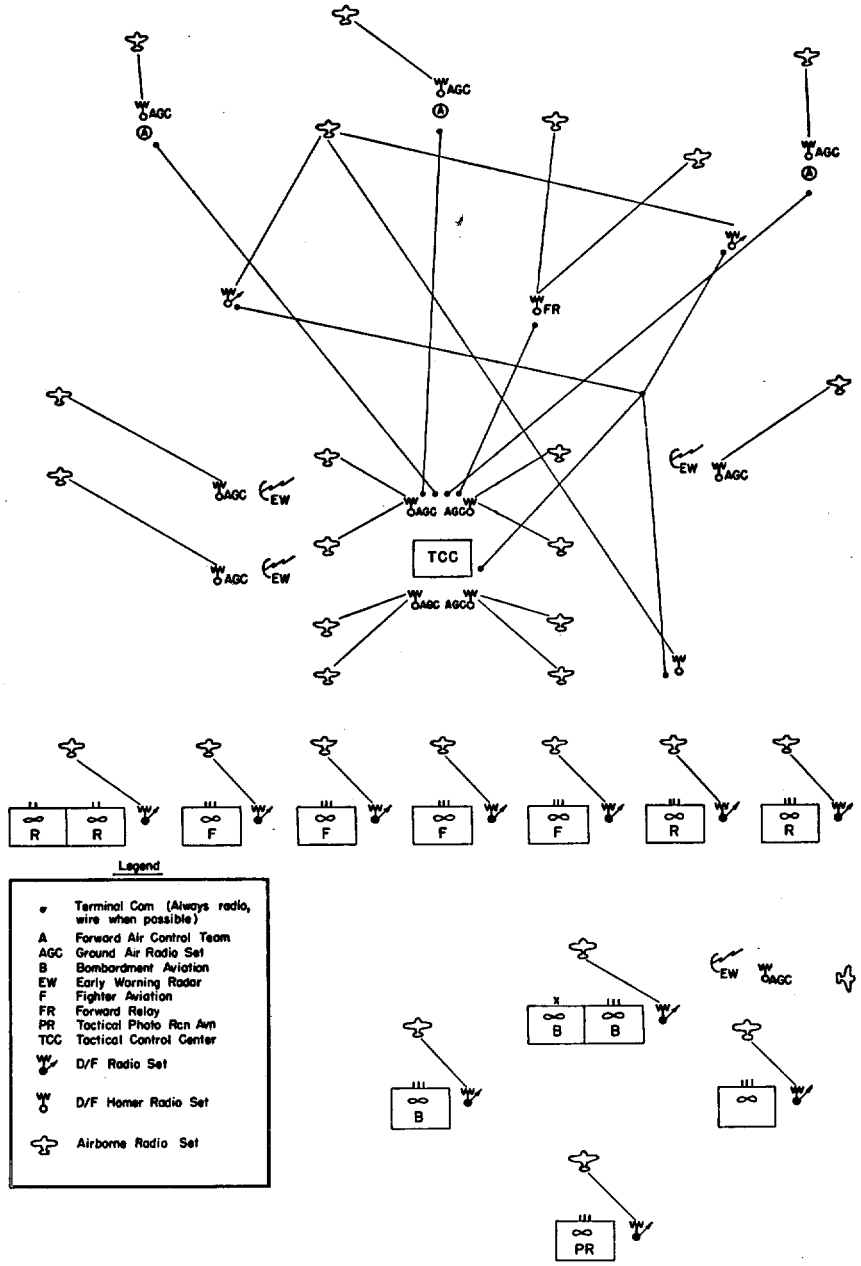


Figure 9. Tactical Air Force control channels.

REF ID:A58489

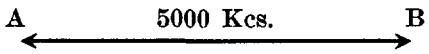
13. Frequencies

a. GENERAL. The analysis of the use of frequencies on a network may be divided into two parts:

(1) *Systems of use.* The system of use is concerned with the manner in which frequencies are employed on the net, i.e., whether the entire net uses one frequency, whether each station sends on an individual frequency, etc.

(2) *Systems of allocation.* The system of allocation is the method used to assign specific frequencies for communications so that different stations will not interfere with each other. It also involves the rotation of frequencies for security purposes.

b. SYSTEMS OF USE. (1) *Simplex:* Two stations intercommunicating on the same frequency.



(*a*) A sends to B on 5,000 Kcs.

(*b*) B sends to A on 5,000 Kcs.

(2) *Complex sending* (fig. 10): Two or more stations on different sending frequencies. A different frequency is assigned to each radio transmitter in the net, and each transmitter uses its assigned frequency to contact the other stations.

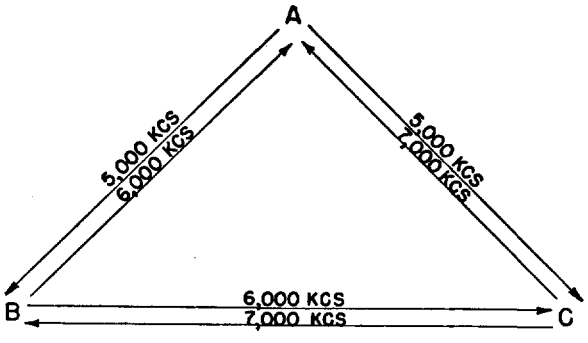


Figure 10.

(*a*) A sends to B and C on 5,000 Kcs.

(*b*) B sends to A and C on 6,000 Kcs.

(*c*) C sends to A and B on 7,000 Kcs.

(3) *Complex receiving* (fig. 11): Two or more stations on different receiving frequencies. A frequency is assigned to each station for receiving transmissions. All stations in the net when sending to a particular station will use the frequency assigned to the receiving station.

REF ID:A58489

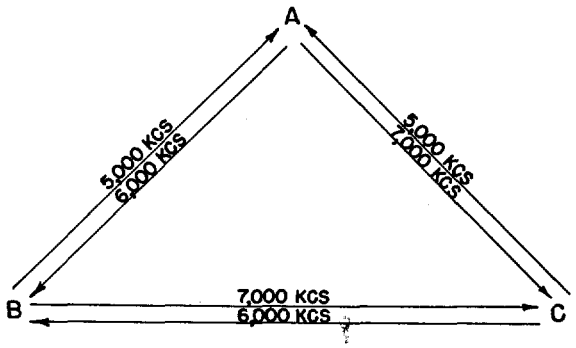


Figure 11.

(*a*) B and C send to A on 5,000 Kcs.

(*b*) A and C send to B on 6,000 Kcs.

(*c*) A and B send to C on 7,000 Kcs.

(4) *Star* (fig. 12): A number of stations on the same frequency with no normal lateral working. This is an extension of the simplex system, as the latter involves only two stations on the same frequency. In the star form, if one outstation wishes to contact another, it must obtain permission from control.

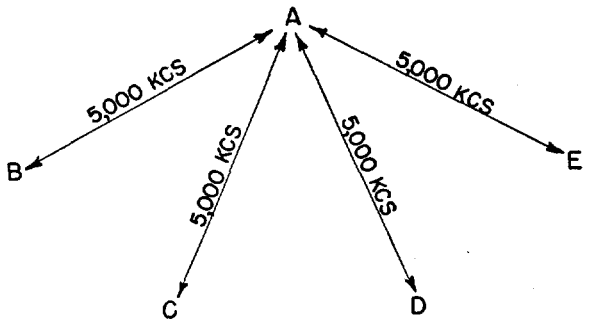


Figure 12.

(*a*) A sends to B, C, D, and E on 5,000 Kcs.

(*b*) B, C, D, and E send to A on 5,000 Kcs. B, C, D, and E may not intercommunicate without express authorization from A. Normally, messages between outstations will be relayed through A (control).

(5) *Star with lateral* (fig. 13): Number of stations on the same frequency with some lateral working. In many of the star nets, lateral working will be a regular procedure between some, but not all, of the outstations.

REF ID:A58489

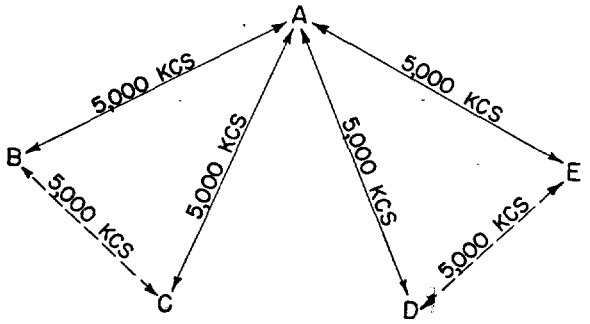


Figure 13.

(*a*) A sends to B, C, D, and E on 5,000 Kcs.
(*b*) B, C, D, and E send to A on 5,000 Kcs.
(*c*) B sends to C on 5,000 Kcs. and C to B on 5,000 Kcs.
(*d*) D sends to E on 5,000 Kcs. and E to D on 5,000 Kcs.

(6) *Free star* (fig. 14): Number of stations on the same frequency with free operation. One frequency is assigned to the entire net and any station in the net may contact any other on the assigned frequency.

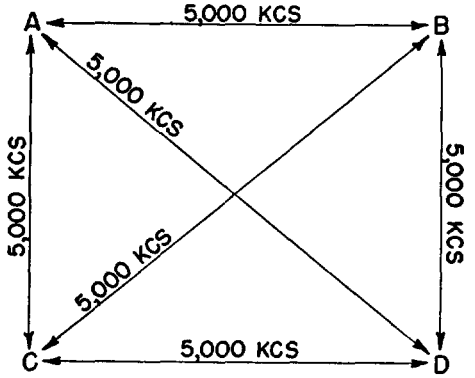


Figure 14.

(*a*) A sends to B, C, and D on 5,000 Kcs.
(*b*) B sends to A, C, and D on 5,000 Kcs.
(*c*) C sends to A, B, and D on 5,000 Kcs.
(*d*) D sends to A, B, and C on 5,000 Kcs.

(7) *Complex star* (fig. 15): Number of stations with control on one frequency, outstations on others. This is similar to the star in its form, but it uses several frequencies instead of only one. Often, a number of the outstations will operate on one frequency, others on another.

REF ID:A58489

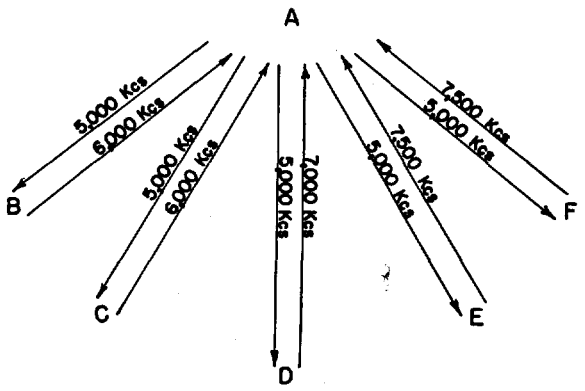


Figure 15.

(*a*) A sends to B, C, D, E, and F on 5,000 Kcs.
(*b*) B and C send to A on 6,000 Kcs.
(*c*) D sends to A on 7,000 Kcs.
(*d*) E and F send to A on 7,500 Kcs.

(8) *Broadcast* (fig. 16): A frequency is assigned to the broadcasting station. Usually no frequency is assigned to the outstations for reply.

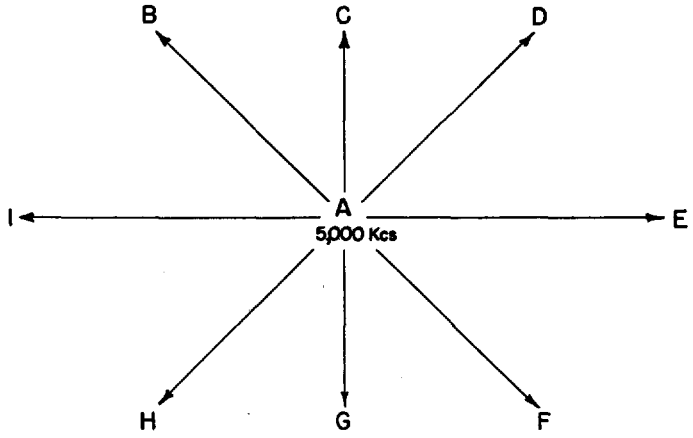


Figure 16.

(*a*) A sends to all stations simultaneously on 5,000 Kcs.

(*b*) Because a broadcast must be heard at so many scattered places, care must be taken in the selection of a frequency in order to choose one that will be heard by all stations. Sometimes, where this has not proved possible, double-keying is resorted to, i.e., the broadcasting station sends on two or more different frequencies at the

REF ID:A58489

same time. Outstations may receipt for traffic on regularly assigned frequencies in the net. In many such nets, however, no receipt is given.

c. SYSTEMS OF ALLOCATION. (1) *General.* Several factors enter into the selection of specific frequencies for use. These involve two basic considerations: readability (the ability of the receiving station to hear) and security. A number of miscellaneous factors, such as the type of power supply available, the nature of the transmitting and receiving equipment, and military and operational requirements, also affect the choice.

(2) *Readability.* The readability of a frequency is dependent on certain factors of wave propagation. These factors involve consideration of the distances between stations, ionospheric conditions, including night and day effects which usually make it necessary to allocate several frequencies to each radio station or net for night and day use, seasonal changes, and the type of terrain, e.g., water, high mountains, and jungle. Furthermore, the possibility of interference between transmitters on approximately the same frequency in the same area must be borne in mind and care taken to avoid such conflict. In any allotment of frequencies, therefore, central control must be established and an over-all plan of allocation devised.

(3) *Security.* One of the methods of attaining security against communications analysis is to hinder the act of intercept. This may be accomplished by changing frequency so that the intercept operator will be forced to "search" the entire frequency range for the desired transmissions. A second effect achieved by these changes is to increase the difficulty of identifying stations or units with frequencies. Maximum effectiveness is obtained by changing call signs along with the frequency. Plans for changes of frequency may operate in a patterned or random fashion, but in any event, such plans must take into consideration the factors noted under (2) above; thus these plans are usually rather detailed and complex.

(4) *Range of frequencies.* Frequencies may range from very low to ultra-high. The latter are not usable for long distance operation and find their chief applications in low echelon, air-ground, and plane to plane communication. Many of the applications of ultra-high frequency transmissions are still in the experimental stage. Low frequencies, such as 300 or 400 kilocycles, may be used for close field contact or air-ground and plane to plane nets. However, the major portion of military transmissions presently falls between 1,500 and 20,000 kcs. In passing, mention should also be made of the use of frequency modulation. FM has found its main application in tank, air, and small combat units where distances are not great and a minimum of noise level is desired for reception.

(5) *Secret frequencies.* As a countermeasure to possible jamming

REF ID: A58489

operations, some nets are provided with secret reserve frequencies These frequencies are not employed except in the case of jamming of the usual frequencies and circumstances demand that communication be kept open The secret frequency, of course, only remains secret for as long as it takes intercept to scan the bands and pick it up, but this interval may be sufficient to complete the transmission

(6) *Example of allocation of frequencies* The following chart illustrates a system which might be used for the allocation and rotation of frequencies

	Jan	*Feb*	*Mar*	*Apr*	*May*	*Jun*	*Jul*	*Aug*		*Dec*
A	1955	2035	2150	1910						
	2035	2150	1910	2305						
	2150	1910	2305	2070						
B	1910	2305	2070	2190						
	2305	2070	2190	2210						
	2070	2190	2210	1940						
C	2190	2210	1940	2350						
	2210	1940	2350	1925						
	1940	2350	1925	2240						
D	2350	1925	2240	1955						
	1925	2240	1955	2035						
	2240	1955	2035							

The months are listed across the top of the chart The squares are divided into three portions representing ten day periods within each month, 1–10, 11–20, 21–31 Each station of the net is assigned a letter and finds its frequency for each period in the square opposite the letter The frequencies which have been selected on the basis of their operational characteristics can be inscribed in the squares at random, in this instance, they are moved up one each month For example, on 1–10 January, A uses 1955 kilocycles, B, 1910 kilocycles, C, 2190 kilocycles On 11–20 January, A uses 2035 kilocycles, B, 2305 kilocycles, C, 2210 kilocycles

14. Call Signs

a GENERAL Call signs are actually names for the correspondents in a radio net They are usually composed of letters, numbers, or combinations of both and serve as a convenient means of identification The analysis of call signs falls into the same categories as does the study of frequencies systems of use, and systems of allocation

b SYSTEMS OF USE (1) *Single station call* One call only is nor-

REF ID:A58489

mally used by the calling station This call may be either the sending station's or the receiving station's call

1 (ABC) _____ 2 (DEF)

Call up	1 to 2	DEF DEF DEF
	2 to 1	DEF DEF DEF
	or	
	1 to 2	DEF DEF DEF
	2 to 1	ABC ABC ABC

Note in this last instance that only one call was used by the calling station This makes the procedure single call even though the reply used a second call

(2) *Double-station call* Both the sending station s and the receiving station's calls are normally used by the calling station

1 (ABC) _____ 2 (DEF)

Call-up	1 to 2	DEF DEF DEF de ABC ABC ABC
	2 to 1	ABC ABC ABC de DEF DEF DEF

(3) *Link call* (fig 17) A common call sign is used for intercommunications between two stations Unlike the previous two types, here the call sign does not belong to an individual station but to a link

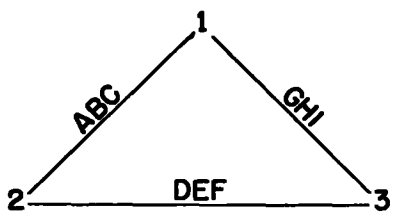


Figure 17

Call up	1 to 2	ABC ABC ABC
	2 to 1	ABC ABC ABC
	1 to 3	GHI GHI GHI
	3 to 1	GHI GHI GHI

(4) *Collective call* In addition to one of the above assignments, a collective call may also be allocated This call is used to alert all stations in the net preparatory to the transmission of broadcast traffic There are also some nets which are maintained only for broadcast purposes and this type of call is usually assigned to such groups The use of "CQ" may be classified under this heading

(5) *Split call working* Usually a single call is assigned to a transmitter or receiver position or to a link However, the use of separate calls for each frequency, one for day, one for night, is also valid This variation may be applied to any of the systems enumer-

REF ID: A684682

ated above and is known as split call working. It has the advantage of dissociating the night and day frequencies, but requires the use of twice as many calls.

(6) *Secondary calls.* In some systems of communication a secondary call is employed in conjunction with link call procedure. These secondary calls are of the station call type and serve as a more definite identification of each station than is supplied by the link call.

(7) *Authenticators.* In order to prevent outside stations from entering a net and confusing its operations, authenticators are sometimes used. They generally consist of a word or a combination of letters and/or digits to which there is a secret, prearranged reply.

c. SYSTEMS OF ALLOCATION. (1) *Composition.* Call signs may be composed of any combination of letters and/or numbers. Usually they are kept as brief as possible and the general range is from 2 to 5 characters. Calls may be composed at random or in some methodical fashion, such as the use of sliding alphabets. An example is included in *d* (2) below.

(2) *Methods of assignment.* Since calls are used as identifying marks, it is necessary to assign them so that two stations operating in proximity or in the same net do not have the same call. Otherwise, confusion would result on call-ups and the passage of traffic hindered. This necessitates some form of over-all control of call sign allocation. This control may be of a very tight nature in which every call is allotted from headquarters down to the smallest unit, or it may be rather loose with considerable discretion left to major subordinate groups whose commands are sufficiently separated geographically to prevent the possibility of confusion. A second consideration in the assignment of calls involves the problem of security since calls are identifications and thereby, if unchanged, furnish continuities for intercept and analysis. Most systems, therefore, cover not only the allotment of calls, but also provisions for change or rotation. These changes may be made daily, weekly, monthly, or at any other interval thought desirable. Calls which change frequently are called "changing calls", those which remain constant for some length of time, are called "fixed".

d. In general, call-sign systems may be divided into two basic groups:

(1) *Book systems.* These systems are founded on a call-sign book from which all calls are taken. These books will usually contain thousands of call signs and some method is provided for the allocation of calls from the book to individual radio stations. The recovery of these books often requires traffic intercept for a period of a year or more.

(2) *Cipher systems.* Call signs may be generated by the use of simple cipher devices such as sliding alphabets and square tables.

REF ID:A58489

The number of call signs available through such systems is usually limited and the method of assigning the call signs to individual radio stations is often bound up with the method for generating the calls. Figure 18 illustrates the use of a cipher system for the allocation and rotation of calls.

1	B	M	A	K	D
2	R	W	C	T	I
3	Z	G	N	O	U
4	H	L	S	X	E
5	V	J	P	F	Y

Figure 18.

The square is filled in random fashion. Station 1 begins with the letter "B" and takes off its calls in diagonal fashion, moving over one diagonal each day. At the end of each line, it drops down one line. Station 2 begins with "R", 3 with "Z", etc. Every 25 days, the calls repeat.

	Station No. ( )				
Date	1	2	3	4	5
1	BWN	RGS	ZLP	HJA	VMC
2	MCO	WNX	GSF	LPK	JAT
3	ATU	COE	NXY	SFD	PKI
4	KIZ	TUH	OEV	XYB	FDR
5	DRG	IZL	UHJ	EVM	YBW
6	RGS	ZLP	HJA	VMC	BWN
7	WNX	GSF	LPK	JAT	MCO
to					
25					

15. Times of Communication

a. GENERAL. An integral part of the operating data of the net is the setting of the times for communication. There are two main systems for accomplishing this: Unrestricted signaling and restricted signaling.

b. UNRESTRICTED SIGNALING. Under the system of unrestricted signaling, the stations of a net are free to contact each other at any time they choose. This method may be implemented either by the stations setting the time for the next schedule at the close of the

REF ID:A58489

previous one or by "alert" operating. In alert operating, which finds its greatest use in tactical and warning nets, all stations are always tuned to receive on certain assigned frequencies.

c. RESTRICTED SIGNALING. Restricted signaling limits the time at which contacts may be made between two radio stations. It is divided into two types: period signaling and priority signaling.

(1) *Period signaling.* The times of communication are assigned by definite schedule and contacts are made only at those specific times.

(2) *Priority signaling.* Priority signaling sets down a definite order in which the stations of a net will send traffic. It differs from unrestricted signaling in that one station may not call another at any time; and from period signaling in that no particular time is set aside for one station to call another. An example of priority signaling is shown in figure 19.

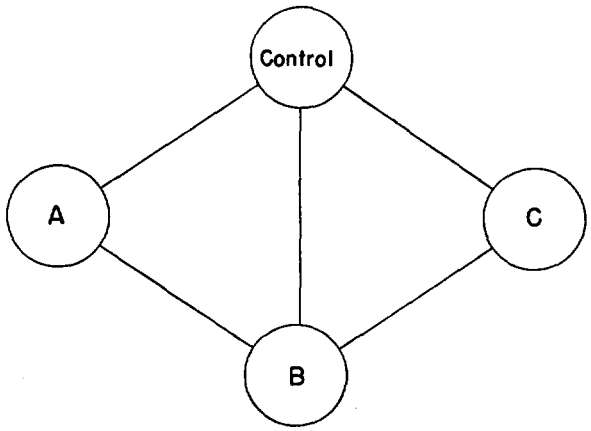


Figure 19.

In this net, "control" is permitted to send first, then stations A, B, and C in order. Schedules may be set up for the hours at which "control" comes on the air.

Section III. ELEMENTS OF RADIO PROCEDURE

16. Morse Code

Morse code is a system of dots and dashes used to transmit letters and numbers by electrical means. In the case of the English alphabet the Morse code is standardized by international convention, is used the world over, and is known as International Morse. In the instance of some nations whose alphabets differ from the English, however, special combinations of dots and dashes have been devised. For

REF ID:A58489

example, in German Morse, the German letters which correspond to the English follow the International, but the umlauted letters and "ch", for which there are no equivalents, are designated by new combinations:

A .—.—
O ———.
U ..——
CH ————

Morse code may be transmitted automatically or manually. In lower-echelon communications, the latter is usually employed, in the higher echelons sending is often automatic. Automatic transmission permits of speeds as high as 400 or 500 words per minute, though generally it averages somewhere between 75 and 200. Manual sending of coded traffic rarely rises above 35 words per minute. Atmospheric conditions, operator abilities, equipment, and similar items are, of course, limiting factors.

17. Procedure Signals

a. In order to facilitate conversation between radio operators, certain signals and signs have been composed. The most common sets of such signals used internationally, are made up of three-letter combinations beginning with "Q" or "Z", and are called "Q Signals" and "Z Signals". The use of these signals saves considerable time and simplifies transmission. Examples are—

QSV Send V's.
QRN I am troubled by atmospherics.
QSA? What is my signal strength?
QSA 4 Your signal strength is 4.

b. Beside these signals, there are a number of standard signs called prosigns which are likewise considered part of international procedure. Some of these are—

AA all after
R received
K go ahead

c. Another type of standard signal is the International Service Code. These signals are made up of five letters in pronounceable form:

UPBAG—for your information

d. Since much information may be derived from a study of chatter, military nets often make up sets of secret procedure signals and, in some cases, may encipher these signals on a periodic basis. For instance, the standard Q signal list may be used, but the last two letters of the signal enciphered by means of a daily changing alphabet.

899152 O - 50 - 5

REF ID:A58489

18. Elements of the Transmission

a. GENERAL. Just as a definite procedure is followed in making a telephone call, so in the normal radio transmission there is also a more or less fixed procedure which covers the basic elements involved. These elements are—

(1) *The call-up.* This embodies the rules of procedure by which one station makes contact with another and prepares for the transmissions of traffic.

(2) *The order of traffic.* After contact has been established, it is necessary to determine which station is to send traffic first.

(3) *Transmission of traffic.* The traffic is transmitted according to a prescribed form.

(4) *Receipting for traffic.* The receiving station acknowledges receipt of the message.

(5) *Corrections and services.* Messages are frequently garbled because of reception difficulties or operators' errors. Thus methods are provided for the efficient and speedy correction of these garbles.

(6) *Signing off.* At the conclusion of the schedule, the two stations follow certain procedures in signing off.

b. If allowance is made for differences in language and procedure signs and signals, it will be found that the above elements are generally standard for most communication systems. The detail, however, may vary somewhat between countries and also within the military of any one country. For instance, different units may observe different rules relative to the transmission of the call or the method of servicing. This often stems from individual requirements arising from strategic or tactical situations, e.g., an air unit as against an infantry unit. Furthermore, the echelon will also alter procedures. The lower echelons will usually abbreviate their procedures as much as possible because of the necessities of time and because they do not require all the data and detail that higher echelons do. Similarly, transmissions on low-echelon nets are liable to be confusing since a number of stations are often on the air at the same time and on approximately the same frequency.

c. THE CALL-UP. The calling station usually comes on the air with a series of V's sent for tuning purposes and the appropriate calls. The calls are generally sent three times, though this number may vary. The called station replies with a series of V's and calls. If the contact between the two stations is quickly made, readability reports are exchanged. Should these reports be unsatisfactory, transmitters and receivers will be adjusted, frequencies changed, etc., until signals are readable. If contact cannot be made, the calling station may hold its traffic for a later schedule, relay it through a third station, or send it blind. In sending blind, messages are generally

REF ID:A58489

transmitted twice and at a slow speed in the hope that the called station can hear although it cannot be heard.

d. THE ORDER OF TRAFFIC. Once contact has been successfully established, it becomes necessary to determine who will send traffic first. Various methods are employed. It may be ordered, for example, that the station of higher echelon send first, or that the calling station have this privilege, or that the highest priority traffic be cleared before all else regardless of which station is involved. One-for-one procedure may be used; i.e., the calling station is permitted one message, then the called station sends one, thus alternating back and forth until one of the stations has cleared all its traffic. Duplex working may be employed when the stations have the available operators and equipment and there is a large amount of traffic to be passed by both. Four operators are required in this type of working. For example, in figure 20, Operator No. 1 at station A sends

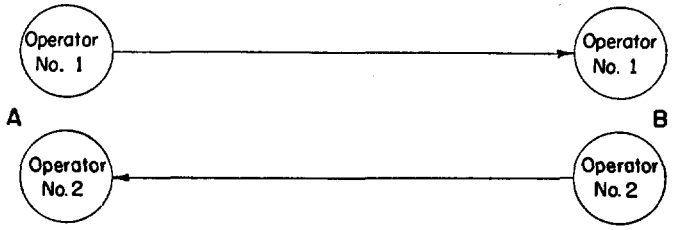


Figure 20

to Operator No. 1 at station B, at the same time that Operator No. 2 at B is sending to No. 2 at A. The chief difficulty with this sort of sending arises when No. 1 at B requires a service on a message from A. Since No. 1 at B is then using the frequency channel of the station, No. 2 at B must stop his transmission.

e. THE TRANSMISSION OF TRAFFIC. Traffic is usually preceded by a commence signal indicating that a message is about to be sent. The traffic itself is composed of the message externals and the text. The message externals contain such items as message numbers, file date and time, group count, addresses, routing instructions, precedences, and similar data. These externals may either precede or follow the text (preamble and postamble) or may be split between the two locations. Most commonly, however, these data appear in the preamble position. The text may be transmitted in code groups of letters, numbers, or both, or in plain text. In the case of coded traffic there are often signals indicating the end of a line and page of text as a check for the receiving operator. Signals usually appear preceding and following the text, the former separating the preamble from the text, the latter indicating the end of the message.

f. RECEIPTING FOR TRAFFIC. After the transmission of a message,

REF ID:A58489

the sending operator waits for a receipt from the receiving operator. This is generally rendered as simply "R". There are also procedures for provisional receipts and other special forms. In some cases, time of receipt may be given following the receipt sign.

g. Corrections and Services. A variety of methods are employed for the servicing of traffic depending on the nature and magnitude of the difficulty. A missed digit, for instance, may be serviced immediately; on the other hand, if a group were omitted this would not be known until the conclusion of the message and might be serviced at that time or might be held until all traffic has been sent. This latter procedure is fairly common, since it is convenient to transmit all traffic without interruption and then to take care of all necessary servicing. Some methods of servicing follow:

(1) *Break-in procedure.* When reception between two stations is good, "break-in" procedure may be used for quick servicing. It is useful only for minor corrections such as garbles caused by a moment of static, is very fast, and calls for alert operating.

A.	6403	3661	9626 - - -	
B.	2			B sends "2" as it is the last number he received correctly.
A.	26	8139	5560	A picks it up from 2.
or:				
A.	6403	3661	9826 - - -	
B.	(Merely depresses his key)			
A.	9826	8139	5560	A re-sends the last group and continues.

(2) *Correction of error (U. S. Army procedure).*

A.	QXTU SRV SRWP TSTL	EEEEEEEE	Actually eight or more dots indicating that "V" is in error.

(3) *Repetitions (U. S. Army procedure):*

A.	IMI 3–6 to 8	K	Repeat groups 3 and 6 to 8 of last message.
B.	3–LAJY–6 to 8–MUCU KAWC GUXO	K	

(4) *Verifications and corrections (U. S. Army procedure).*

A.	J 271545 Z 3–6 to 8	K	Verify and repeat groups 3 and 6 to 8 of message filed at 271545 Z.
B.	C 271545 Z 3–LAJY–6 to 8–MUCU KAWC GUXO	K	

(5) *RQ's and BQ's.* Services which are more complex than the types noted above are usually sent as short messages. A request for

REF ID:A58489

service in international procedure is preceded by the sign "RQ", the reply by "BQ". Services which relate to cryptographic features, however, are generally sent as regular encrypted messages.

h. SIGNING OFF. When there is no further traffic to be transmitted, or at the end of the schedule time, the two stations will sign off. Usually, each station sends the "I have no more traffic" signal and then the "sign-off" signal. In many nets, the time of the next schedule is included just prior to the sign-off. These times may be enciphered for security purposes. Stations in lower-echelon nets will often sign off in order. An example from U. S. Army procedure follows:

A.	2SN	V	6F2	QNW	K	"2SN" is net call. QNW is the "close down" signal.
B.	6F2	V	G94	R	AR	
C.	6F2	V	KFR	R	AR	

19. Chatter

Radio operators, particularly the lesser-trained and on the lower echelons, exhibit a disposition to chatter amongst themselves. This chatter is the source of much information of value. It does not fall into the categories discussed above as it may relate to anything from discussions of personal problems to mentions of units or cryptographic features. This sort of talk is forbidden since it represents not only idling but a serious breach of security. Nevertheless, depending on the degree of discipline, it will occur in some volume in almost every radio net.

20. Plain-language and Low-grade Cipher Messages

Very often the error is made of transmitting, in plain language or low-grade cipher, messages which are apparently of no analysis value, yet when properly used prove of enormous assistance in the traffic analysis processes. Such messages may involve personal items or routine affairs which serve to reveal such important data as personalities, units, and locations. This type of traffic is particularly prevalent in the lower units where speed may be of the essence and where it is cumbersome to use complex cryptographic devices. Radio station personnel also indulge in this practice for exchange of technical data. They often find it necessary to ask, or reply to, questions of a semi-secret nature relative to their own operations. For this purpose, they may not use a standard system which would involve the delay of the code room and message center, but instead devise their own relatively simple ciphers.

REF ID:A58489

Section IV. THE MESSAGE EXTERNALS

21. Usual Components

a. In order to insure the proper handling of messages in both the message center and the radio station, some information must be sent in the clear or in simple code relative to message routing and accounting. This information is usually embodied in the preamble or postamble although, in some instances, it may be buried in the text. It may include any or all of the following items:

(1) Serial numbers, such as radio station numbers, message center numbers, etc.

(2) Group count.

(3) File date and time.

(4) Routing systems which serve to indicate message centers or units of origin, destination, and sometimes relay points of traffic. Distinction is also often made as to action and informational destinations. Routings may be in plain language, code, and/or cipher.

(5) Addresses and signatures, either in clear or cryptographed.

(6) Priorities, indicating the transmission and delivery precedence of traffic.

(7) Special instructions, as "time of receipt requested," "personal," "service," "repeated message," "relay message."

b. As a general rule, high-echelon traffic will contain most of these items, low-echelon traffic will cut them to a minimum. Their uses, positions, and surrounding procedure vary considerably according to communication system.

22. Serial Numbers

a. Serial numbers appearing on traffic may be enciphered or unenciphered and may represent any of the various stages through which the message passes before it is actually transmitted. The serial number acts as a reference to the message, and generally there are as many numbers in the externals as are necessary for convenient reference. The points at which such numbers may be attached to the message are—

(1) *The writer.* The writer of the message may have a personal series of numbers allotted for his use. Usually, however, numbers of this type, if present, will be included in the text.

(2) *Message center.* The message center of the unit in which the message originates generally assigns it a number. A number of this nature, if used, will usually remain constant through various relays of the traffic as it is the basic reference.

(3) *Signal center.* At large locations, several unit message centers often forward their traffic to a central signal center. The signal

REF ID:A58489

center also gives a number to the message. This number may appear in place of the message center number, along with it (though this is rare), or it may not be included at all. It is often difficult, where only one number is transmitted, to determine whether it is a message center or a signal center number.

(4) *Code room.* The code room, whether located in the message or signal center, may add a number to the traffic. Again this number may replace, or be used along with, the other types.

(5) *Radio station in-desk.* Each radio station maintains some form of in-desk for the handling of incoming messages and their routing to the proper radio positions for transmission. Here, too, a number may be put on the message. There may be several such desks for the forwarding of different types of traffic and this may result in several different series of numbers. In relayed traffic, these numbers (as well as the type included in (6), (7), and (8), below) may accumulate on the message, or a new one may be substituted for the old on each retransmission so that only the latest number appears.

(6) *Transmitter.* A number is often put directly on traffic by the radio operator as his reference. This number may be assigned in different ways. One method is to allot a series of numbers to a transmitter position and regardless of the receiving station this series is continued.

(7) *Link.* A second method is the employment of a link number, i.e., separate series are allocated for each station worked.

(8) *Operator.* A third system is the allocation of a personal series of numbers to each operator. A diagram of the above possibilities is given in figure 21.

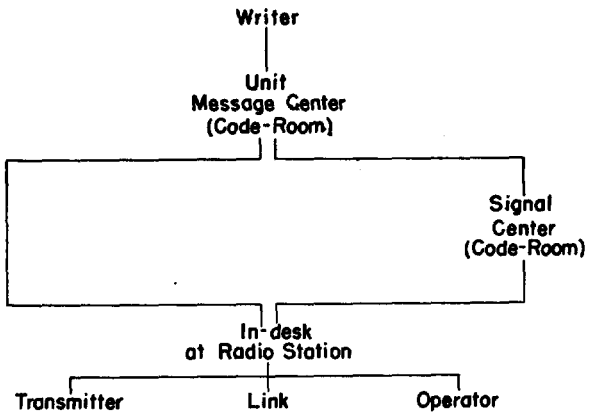


Figure 21

b. As a general rule, not more than two numbers will appear in the message externals, one representing some stage of the message or signal center phase, the other the radio station phase. In the lower

REF ID:A684682

echelons often only one number is used since the whole operation is usually so small that these fine distinctions lose much of their significance.

c. Series of numbers are allotted in some organized fashion, though this fashion may differ from net to net and from unit to unit. The series may be allocated in block form, e.g., 1 to 100 or 501 to 1000, etc. The blocks may be used until completed and then started over again; or the series may begin over on a periodic, such as a daily, basis, but if the prescribed limit is reached within the period, it is likewise recommenced. The series, on the other hand, may be open-end and repeat only at the close of a fixed period as a week, a month, or a year. In some types of series, the date or similar feature may be incorporated in the number.

d. These numbers may be enciphered in order to conceal the volume of traffic passed. It is not likely that this would be done with any of the radio station numbers because of the complexity of the operation, but it may be done at message center or signal center level. In this procedure, the plain text numbers run in serial order and messages are filed in the sending center by it. Another center referring to a specific message would do so by the enciphered number, the sending unit would then decipher same and locate the traffic. Thus, it is not necessary for the receiving center to know the system of encipherment and this permits considerable latitude in the employment of enciphering methods between the various centers.

23. Group Count

The group count may cover only the text of the message or it may include both externals and text. In some types of preamble separate counts are given for each. The group count may represent either the number of cryptographic groups, number of plain language words, or the number of individual letters and/or digits according to the method used.

24. Date Time Group

The date time group appears in the message externals and is expressed in six digits followed by a time zone suffix. It is intended to indicate the time the message was authorized for transmission, but may be used to indicate the time the message was filed at the message center, signal center, or at the radio station for transmission. Time is expressed in terms of the 24-hour clock and may be based on Greenwich Mean Time or on some local time zone. Whatever the base, it is generally kept standard for the entire net, if not for the entire communication system, regardless of the geographical area covered.

RECD 10 : AD684682

25. Routing Systems

a. GENERAL. Some method is required on radio traffic to indicate points of origin and destination and, in many cases, relay points. These methods must be relatively simple as they are designed chiefly as an aid to radio station personnel in the routing of messages. In this respect, it is necessary to understand the distinction between the routing designations and the addresses when both appear. The routing designations usually refer to message or signal centers, the addresses to specific units or persons. (There is nothing to bar the use of routing designations for specific persons but this is not generally the case.) It may be compared with the address on a letter, the routing designation representing the city of address, the address representing the company or person. On high-echelon traffic this difference is generally made, but in low-echelon traffic the routing designation often suffices for both purposes since message centers are small and traffic is almost always intended for the commanding officer. Thus, addresses as such do not usually appear on messages at this level. This distinction similarly holds true for routing designations used to indicate origin and signature.

b. The discussion of routing systems has been divided into two portions, the first dealing with the composition of routing systems, the second with their use.

(1) *Composition of routing systems.* Routing systems may be divided into three main types, plain text, call sign, and code. Plain text is seldom used on military nets because of its insecurity. Thus, generally, either the call signs of the stations are used for routing or a separate code is set up for this purpose. A routing code usually consists of two parts: code and syllabary. The code is composed of short number and/or letter combinations which may represent a location, message center, or unit. The syllabary provides code equivalents for the spelling out of place names or units not provided for in the regular code. These codes are usually rather simple, often being one-part in nature so as to be convenient for application. In some cases they are not used for security reasons, but rather for brevity. Generally, however, they serve both purposes and an encipherment of the code may be a feature of a few of these systems.

(2) *Use of routing systems.* Methods of using routing designations and the placement of these designations on traffic vary to a considerable extent. It may be set forth as a cardinal principle, however, that in most systems routing designations are used only when absolutely necessary. This increases their security and also makes it more difficult for the traffic analyst to determine the origin and destination of a message. On traffic which is point-to-point in nature, therefore, there are usually no routings at all. For example, in figure 22, A has a message for B. This message will be transmitted over

Approved for Public Release: IAW 190-1 Distribution Unlimited

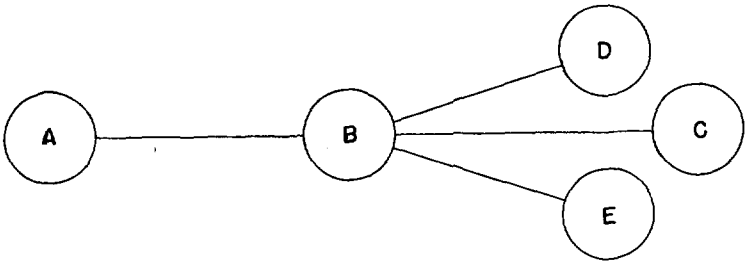


Figure 22

the A-B link and since it has originated with A and is destined for B, routing designations are not required. On the other hand, if A has a message for C, this is generally indicated in the externals so that B knows that it is to be forwarded. (It should be remembered that it is always possible to bury routing instructions in the text, but this is, as a rule, not done since it would necessitate the decoding of the message at each stage of the transmission.) This may be handled in two ways. The message may carry the routing "A to C," or it may only carry "to C" with the originator omitted. When the message is relayed from B to C, it may state "A to C," "from A," or have no routing at all. In some systems the relay point is noted, as "A to C through B."

c. Messages to several addressees can be indicated in several ways. For instance, in figure 22, A may originate a message for B, C, D, and E. All of these destinations could be incorporated in one preamble, "A to B, C, D, and E," or a separate preamble could be added at the end of the message for each location. Thus, the preamble preceding the message may carry no routing since it is being forwarded direct from A to B, but each of the preambles following the text would note "A to C," "A to D," "A to E." When this message reached B, B would transmit a copy with the proper preamble to each of the stations indicated. In this manner each copy would be numbered separately; in the single preamble method, only one message number would appear for all the recipients. It is further to be observed that if various specific addresses at one location, or routing designation, were involved, it would be possible to handle it in either of these ways or to indicate the addresses internally.

d. Distinction also may be made externally as to information and action destinations by the use of appropriate procedure. For example, in U. S. Army procedure, "W" is used to separate action from information addresses, e.g., "ABC W XQR" where ABC is the action addressee, XQR the information.

REF ID:A58489

26. Addresses and Signatures

Addresses and signatures may or may not appear externally on messages. Very often it is standard procedure to conceal them as part of the text. When they do appear externally, however, they are usually encoded and/or enciphered by means of complex cryptographic systems since they contain the specific names of units and persons and thereby are of high intelligence value. The address, unless it is in simple cipher or plain text, is usually considered a cryptanalytic, rather than a traffic analytic problem. Nevertheless, there are some features of the address and signature, such as length and manner of encipherment, which are of interest and use to traffic analysis.

27. Precedence Indicators

a. In order to insure the most expeditious handling of important traffic in both message center and radio station, some means of designating such traffic through the use of precedence indicators is usually devised. The precedences may be in the form of plain text, abbreviations of plain-text words, or number or letter code groups. Furthermore, in some military systems, these code groups may be enciphered.

b. The number of precedences used varies considerably from one nation to another and may range through several classifications of high priority to routine and deferred. There is, very often, no precedence designated "routine" and messages in this category, which are generally the most numerous, carry no marking at all.

28. Special Items

There are a great number of special items which are often included in the message externals. Some of the more common follow.

a. Part Messages. Long messages are usually broken up into several parts for ease of handling or for reasons of cryptographic security. Indications of this may be transmitted in the preamble.

b. Message Type. Indicators may be included to designate the type of message, for example, service, air warning, personal, weather, practice, repeated message, etc.

c. Miscellaneous Items. Procedures may also be provided for the transmission of miscellaneous items such as, "Time of receipt requested," "Each group sent twice," "Message sent blind," "Text in five (5) digit groups," "Relay message."

29. Message Examples

The elements discussed in the preceding paragraphs appear in message preambles and postambles in fixed positions according to the

REF ID: A5384682

procedure prescribed. These procedures differ from country to country and also often from one branch of service to another and from one echelon to another. Examples taken from U. S. Army procedures follow:

a. AB9 V PT3 291155Z GR12
BT Text
BT 291155Z K
AB9—Receiving call and destination.
PT3—Transmitting call and origin.
291155Z—File date and time, repeated as postamble.
GR12—Group count.
BT—Break before and after text.
K—"Go ahead" sign sent after message.

b. 3XF B79 V FR8–O–P B79–T–RST–A–FR8
152312Z 3XF RST B79 GR 19
BT TEXT.
BT 152312Z K
3XF B79—Multiple call-up; receiving calls.
FR8—Transmitting call.
O–P—Operational priority. (Precedence designation.)
B79–T–RST—B79 to transmit message to RST.
A–RF8—Denotes origin.
152312Z—File date and time.
3XF RST B79—Action destinations.
GR 19—Group count.

c. A45 BR6 B STX P–A45 BR6–T–N–A45
A–79K 011046Z A45–W–F2P SLW BR6
GR 28
BT TEXT.
BT 011046Z K
A45 BR6—Multiple call-up; receiving calls.
STX—Transmitting call.
P–A45—Message is priority to A45 only; to others routine.
BR6–T–N–A45—BR6 is to relay to all destinations except A45.
A–79K—Originator of message.
011046Z—File date and time.
A45—Action destination.
W–F2P SLW BR6—Denotes information destinations.
GR 28—Group count.

Section V. TEXTUAL FEATURES

30. General

While textual features and cryptographic systems are chiefly the field of the cryptanalyst, the traffic analyst should also understand

REF ID:A58489

certain aspects, both for the purpose of assisting in his study of communication nets and in the accomplishment of his responsibility to the cryptanalyst. These aspects relate to the distribution, use, and identification of systems, and to the use of indicators.

31. Distribution of Systems

Many cryptographic systems are limited in distribution; this limitation constitutes a cryptonet. For example, a system may be distributed only to the corps headquarters of a theater. These corps then are a cryptonet. Or it may be given only to units along a line of communications. There may be several reasons for the delineation of these nets but the chief ones are security, the nature of the system involved, and the physical problems of distribution. Forward units, for instance, are generally furnished different systems than the rear echelons because first, they are more liable to capture; second, they cannot handle the more complex methods of encipherment; and third, their traffic does not require the same degree of security. Within the higher echelons, divisions are made to prevent the overuse of any one system and thus deny depth. Such divisions also arise from the major break-down in command which allows some latitude in the composition of codes and ciphers to individual services or units. Furthermore, special systems may be prepared for use in particular operations where a high degree of security is desired. The important point, however, for the traffic analyst is to think of cryptonets not in terms of locations, but in terms of order of battle units, and to recognize the exact relationship existing between a system and a unit or group of units. It should also be observed that the existence of cryptonets necessitates the re-encrypting of traffic which passes from one net to another.

32. Use of Systems

Many times cryptonets will exhibit another distinguishing feature. This feature concerns the use of the system. For example, a system may be used only for confidential material, or only for secret material; or it may carry only information about supply, or shipping, or personnel, or operations. Again, this distinction is of high traffic analysis value and provides, as well, assistance to the cryptanalyst.

33. Identification of Systems

Some external feature usually appears in the text of a message to designate the system used. Where only one system of a given external appearance (as 4-letter, 5-digit) is used between two correspondents, this is not necessary, but in most instances, this designation is required and it can be accomplished in two main ways. The first is

REF ID:A5384682

the use of the form of the message itself. For example, the last group of the message may contain a repeat of the group count or the indicators may be peculiar in their formation, or they may be placed in a unique position. Any distinction of this sort will serve. The second method is the addition of a discriminant to the message, generally as a part of the text, most often as the first group. This discriminant is usually composed in a distinctive manner, as five like letters, repeated digraphs, ascending or descending numbers. It may be enciphered. Where a discriminant is lacking, it is often the task of the traffic analyst to determine means of identifying systems and to isolate homogeneous traffic.

34. Use of Indicators

The difference between the discriminant and the indicator should be understood. The discriminant identifies the general system used, while the indicator provides the specific key for decipherment. These indicators are often in the clear and, if they display any peculiarities of use, they become a valuable traffic analysis weapon. The pages of a one-time pad, for example, may be applied in order and the page indicators will thus reflect the number of messages enciphered. The pad numbers themselves will also be of value since each pad will be limited as to its users.

35. Practice Traffic

When new nets are being established, or operators are being trained, practice traffic is often devised for exercise purposes. Sometimes special nets are set up to this end, and they carry nothing but practice material. On the other hand, certain schedules may be set aside on regular links.

36. Control Traffic

In order to mislead enemy traffic analysts, control traffic may be used. Such operations may range from the formation of dummy nets to the passing of dummy traffic over the usual links. Control traffic can be employed merely to hide an operation through maintaining a volume level on all nets, or it can be used deliberately to deceive by creating high volumes at points of slight military activity.

Section VI. COLLATERAL MATERIAL

37. General

Aside from the usual intercept material discussed in the preceding sections, there are many other sources of raw data which are of value to traffic analysis. They may be divided into two groups, the first

REF ID:A58489

directly related to intercept, the second more or less miscellaneous in nature. The first group includes direction finding. The second is concerned with the study of nets other than military, the use of decode material, intelligence reports, prisoner-of-war reports, and captured documents. With reference to this second group, it should be observed that traffic analysis, in both its analytic and applied phases, often involves the fusing of information and material of all types and from all sources toward the production of a complete communication picture. In this respect, traffic analysis touches to some degree upon almost every phase of intelligence, and to a great degree upon every phase of signal intelligence.

38. Direction Finding

a. Direction finding (D/F) is a method of locating radio stations through use of specially constructed receiving antennae. These antennae register the direction along which a radio signal is travelling as it passes on a great-circle path through the D/F location. When the direction of a radio signal is determined at more than one D/F site, the location of the transmitter may be plotted by noting the point at which the bearing lines intersect (fig. 23). A location determined in this manner is called a "fix."

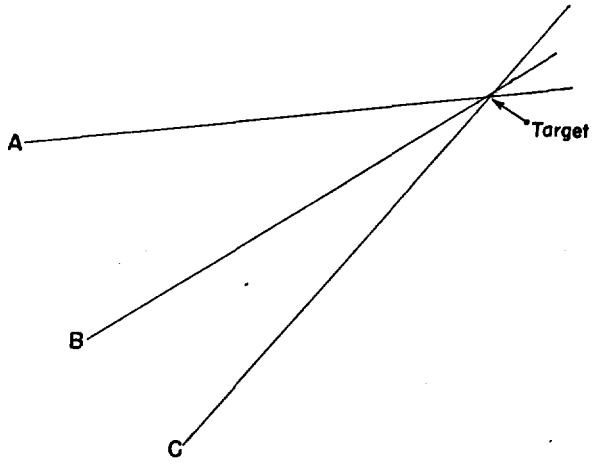


Figure 23

b. Usually, bearings will not yield a perfect fix, but will, depending on a number of factors, give a more or less restricted area. These factors include (1) the distance from the D/F station to the target, (2) the number of D/F stations involved in locating a target and the number of bearings taken, (3) the amount of the signal's deflection as encountered (for example, when the radio wave passes over mountains or shore lines), and (4) the quality of the D/F equipment.

RECD 10 : AD684682

Despite these and other limitations, D/F bearings seldom are misleading because the D/F operator is able to recognize whether or not a bearing is reliable and furnishes an evaluation of each bearing as it is forwarded to the plotting unit. The plotting unit also is in a position to make an accurate judgment on the reliability of a fix. An adequate arrangement for accurate direction finding requires a number of D/F stations (at least 3) located along a rather broad base (relative to the distance from the target) and so connected that they can all listen to the same signal and take their bearings simultaneously. It should be noted that D/F is particularly useful in low-echelon traffic analysis, but that over distances running into the thousands of miles it loses much of its effectiveness.

39. Information Derived from Cryptanalytic Results

Cryptanalytic solutions of traffic furnish, very often, the relationship between nets and order of battle. Since this is one of the ultimate goals of traffic analysis, detailed study of all solved messages, against the background of the nets, is a necessity. Study of solved messages should also be carried on for the purpose of relating internal information to external characteristics. This has an application to cryptanalysis for the identification of crib messages and to intelligence for the determination of the significance of traffic contacts and patterns. Message plain texts also yield a certain amount of signal information, as station locations and data concerning calls, frequencies, and schedules.

40. Intelligence Reports

Intelligence reports may vary from predigested order of battle lists to raw materials, such as captured documents or prisoner of war reports. Order of battle is the basis for the entire radio network and for the traffic passed over it. As such, an understanding of the order of battle is the necessary foundation for traffic analysis and its cryptanalytic and intelligence applications. The relationship is a circular one—intelligence added to traffic analysis yields additional intelligence. Aside from the broad phase of relating nets and battle order, this integration has specific applications in the analysis of traffic contacts and patterns and in the study of the uses of cryptographic systems and the transmission of routine messages.

REF ID:A58489

CHAPTER 3

RECONSTRUCTION OF THE RADIO NETWORK

Section I. INTRODUCTION

41. General

This chapter is concerned with the first objective of the traffic analyst, that of the reconstruction of the radio network. There are two phases to this objective, analysis of radio operations and net reconstruction.

42. Analysis of Radio Operations

This phase involves the identification and study of the elements discussed in the preceding chapter. It includes the identification of all components of the transmission, the analysis of their use, and the determination of their operating data.

43. Net Reconstruction

The nets are reconstructed coincidently with the study of radio operations. Each task helps the other; the distinction made here is only for academic purposes. In actual practice, attack must be carried out on all elements simultaneously, so far as possible, because analysis depends on the perception of relationships. Net reconstruction is concerned with the grouping of stations into nets, the determination of the links operating between those stations, and the identification of the stations with geographic locations, culminating in the production of the net diagram. The pertinent features of radio operations, such as calls, frequencies, and serial number blocks, may then be added to this diagram to complete the "pure" traffic analysis picture. The superimposition of the cryptonets and order of battle on the diagram is discussed in later chapters.

Section II. ANALYSIS OF RADIO OPERATIONS

44. Frequency Analysis

The main objectives of frequency study are (1) the determination of the system of use and (2) the solution of the system of allocation,

899152 O - 50 - 7

REF ID: A584682

including the method of original assignment, the pattern of rotation, and the reconstruction of the basic charts involved.

a. ANALYSIS OF THE SYSTEM OF USE. (1) The chief problem in the study of the system of use is the determination of accurate basic data. Once these data have been properly recorded the conclusion will usually be apparent. The basic data consist of who sends to whom and on what frequencies. To simplify study, a rough circuit diagram may be prepared. Two examples of these data and the conclusion to be drawn are given below.

(*a*) In the following example the net is a free star (fig. 24):

A to B on 5,000 KCS.
A to C on 5,000 KCS.
B to A on 5,000 KCS.
B to C on 5,000 KCS.
C to A on 5,000 KCS.
C to B on 5,000 KCS.

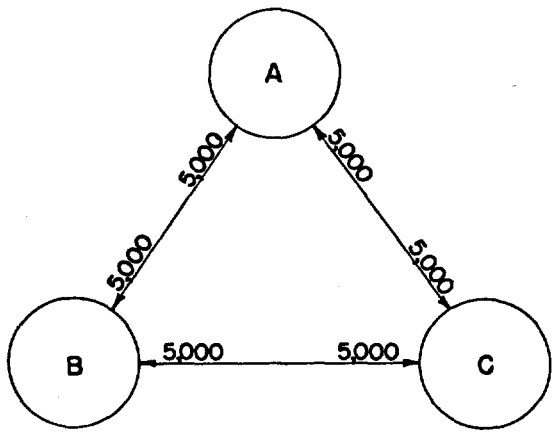


Figure 24. The net is a free star.

(*b*) In the following example the net uses the complex-sending system (fig. 25):

A to B on 5,000 KCS and 10,500 KCS.
A to C on 5,000 KCS and 10,500 KCS.
B to A on 4,000 KCS and 7,500 KCS.
B to C on 4,000 KCS and 7,500 KCS.
C to A on 3,000 KCS and 6,000 KCS.
C to B on 3,000 KCS and 6,000 KCS.

REF ID:A58489

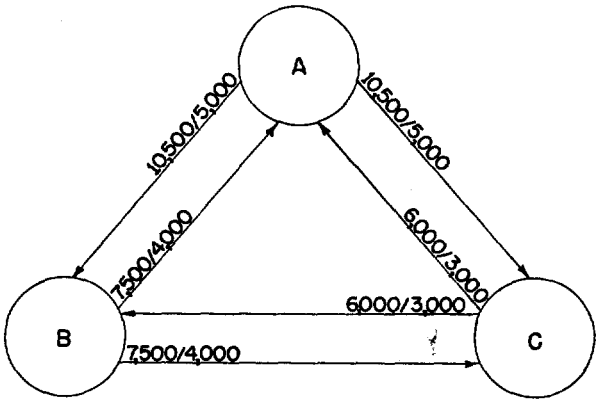


Figure 25. The net uses the complex-sending system.

(2) Arriving at accurate data, however, is often a fairly difficult task. It requires a detailed study of chatter for at least a week's period and usually somewhat longer, depending on the completeness of coverage during the period and the complications involved in the use of the frequencies. It is well to mention that, for the analysis of many features of radio operations, it is often desirable to have complete cover on a net for a limited period, such as a day, than to have spotty cover over a longer time. Generally, however, cover will be incomplete, that being one of the reasons why careful study of chatter is necessary before a decision is reached. A second difficulty arises where the enemy stations drift from the assigned channel. For example, a station allocated 4,650 kcs may vary all the way from 4,600 to 4,700 kcs. In the case of simplex and star working, much of this variation is intentional so that the one station can reply a little off the correspondent's frequency. A third problem is created by the assignment, as sometimes happens, of four or five or more wave lengths to a station. These wave lengths are not restricted to fixed times of day, but the station is at liberty to use whichever one can best be heard. It should be pointed out that there will often be exceptional uses of frequencies which cause the net to vary from its basic form of working. These exceptional uses should be carefully studied and explained, but they should not be considered as changing the net type.

(3) To illustrate some of these problems, assume that a cursory examination of a week's transmissions reveals the following:

A to B on 5,000 KCS, 11,600 KCS.
B to A on 5,000 KCS, 7,000 KCS, 11,590 KCS.
A to C on 5,000 KCS, 5,500 KCS, 11,625 KCS.
C to A on 5,010 KCS, 5,025 KCS, 6,995 KCS.

REF ID: A684682

B to C not heard.
C to B not heard.

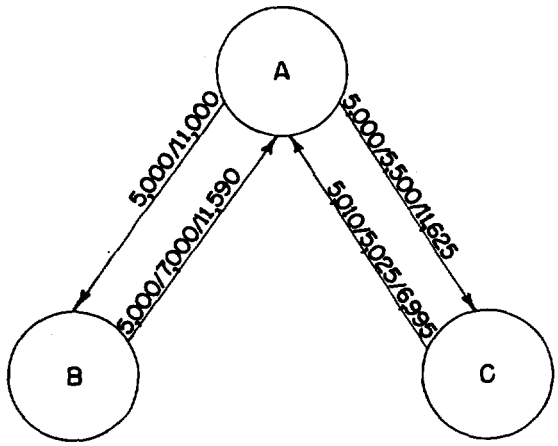


Figure 26.

The net, at first glance, appears to be a star (fig. 26) though there are several discrepancies to be explained. It may be assumed that C's 5,010 and 5,025 kcs are drifts of the base frequency 5,000 kcs, that A's 11,600 and 11,625 and B's 11,590 should all be 11,600 and that B's 7,000 and C's 6,995 are both 7,000. However, A uses 5,500 kcs to C, but neither B nor C have been heard on this frequency. This runs counter to the principle of the star. A check is made of the appearance of 5,500 kcs and it is found to have been used twice during the period under study, both times under the same circumstances. A came up on 5,000 kcs, C reported interference on this frequency, and A switched to 5,500 kcs. It is likely, then, that 5,500 kcs is an extra wave length assigned to the net for emergency purposes and that, in time, the other stations will also make use of it. In this instance the net is not working star since 5,500 kcs at A is corresponding with 5,010 kcs at C, but it is known that A did try to make contact under the established procedure first, so that this becomes the exceptional case and does not contradict the theory as to the star form. The 7,000 kcs at B and C also create a problem since A has never used this frequency. Again reference is made to the chatter logs where it is discovered that this frequency is used during the evening hours and has been heard once from B, twice from C. However, on all three occasions the A end of the circuit was not heard at all. It is possible that A was up on this approximate wave length but, because of some propagation or reception peculiarity, the intercept station was unable to hear it, or that the intercept station, for one reason or another, may only have been

REF ID:A58489

able to cover one end. Whatever the reason, imperfect coverage is apparent and, until A has been monitored on this schedule, nothing can be determined which would affect the star hypothesis. The net picture, as mentioned above, indicates that the star is controlled rather than free since B and C have not been observed in contact. Study of chatter, however, casts some doubt. At one point, A has asked B for a special schedule at 1500. B replies he cannot make it then since he has a schedule at that hour with C. On another occasion, A sends two messages to C for relay to B, A stating he has not been able to contact B. This chatter suggests that B and C work each other and that the net is a free, rather than a controlled, star. The evidence is slim since the schedules mentioned in the chat may only have been emergency ones, but it is sufficient to justify reserving decision and waiting for further developments.

b. SOLUTION OF THE SYSTEM OF ALLOCATION. Solution of systems of allocation requires at least several months of observation and, if some complex method of rotation is involved, may run into much longer periods. The problem is twofold: (1) the method of basic allocation and (2) the method of rotation, if present.

(1) It should be stated at the outset that usually a method of basic allocation will not be used except as it is tied into a system of rotation. Where frequencies are fixed, they have generally been assigned because they can be heard between two points and because there is no interference from other frequencies. This is particularly true on high-eschelon nets. It is always worthwhile, however, to check the frequencies of the various nets of a radio network for characteristics, if only to be sure. Some pattern may appear, for example, air-ground nets, wherever located, may be restricted to a definite set of frequencies, or divisional nets may be limited to a certain band. Anything in the way of a pattern, naturally, is possible. A tabulation of frequencies against net and the seeking of relationships in frequencies between related nets should serve to reveal most such patterns. Related nets may be so determined on the basis of function, such as air, shipping, line of communications, divisional artillery, by echelon, or by command.

(2) Whether a frequency system is fixed or changing, and if changing what the period of change is, can be discovered merely by observation. If a changing system is used, the first step in analysis is to determine some method of maintaining continuity so that if station A transmits on 4,300 kcs one day and 3,750 kcs the next day, there is some way of knowing that 4,300 and 3,750 are both the same station. Continuities may be established in two main ways:

(*a*) *Characteristics of radio operations.* Almost any item of radio operations may serve the purpose:

REF ID:A684682

1.

Calls. If frequencies change and calls do not, identification is a relatively simple matter.

2.

Schedules. Taken in conjunction with other data, schedules may provide a clue to continuities. They are likely to be characteristic for the stations of a net, but care must be exercised in the use of this technique and supporting evidence should always be present. Also of value is any mention of future schedules at the time of the sign off, for example, "QRX 0100" (next schedule at 0100). It is then possible to relate stations heard at 0100 on the following day back to the stations involved in the chatter.

3.

Serial numbers. If serial numbers do not begin over at the time of each frequency change, they may be utilized. In the case of message center serials, care must be exercised to avoid the use of relayed traffic. For example, in figure 27, A, on the 15th, may

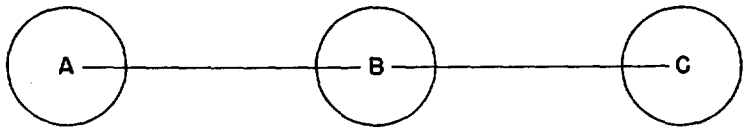


Figure 27.

send a series of messages over the A–B circuit with the message center serial range 1544–1573. On the 16th, the entire net changes frequency, and several messages are intercepted with the routing instructions A to C and the serials 1578–1581. It cannot be assumed that the new frequency heard on this transmission is at A since the traffic might have been passing on the B–C link. If some of the traffic, however, was routed A to B or else carried no routing indicating a local message, then the continuity might tentatively be established. Of far greater value in this respect are the radio station members, and, except in the case of the in-desk number where it is possible for several different circuits to be transmitting the same series, these ranges are reliable. Where serial ranges are fairly distinctive they may also be used in reverse. For example, station A may receive traffic in only a certain message center serial range from a correspondent. This may be caused by the fundamental assignment of the range to a definite service, for example, supply. Station A is at a quartermaster depot; consequently all the traffic to A from the correspondent will be in the one series.

REF ID:A58489

4.

Routings. Routing codes can also be of value when used by nets. It may be assumed that, as a general rule, a radio station will originate and receive more of its own traffic than it will handle on relay for other stations. For example, station A is at Gettysburg. If A changed frequency daily, it could probably still be spotted because of the large amount of Gettysburg correspondence transmitted and taken.

5.

Routines. Because of the requirements of military operations, it is necessary for units to make routine periodic reports. Very often these reports can be identified because of the stereotyped nature of the message externals. For example, a situation report, or a strength report, may be sent from station A to B, C, and D each day at approximately 2000. It would be a relatively easy matter to watch for this report to pass and to identify it purely by these external characteristics. Such routines furnish a trade-mark for the originating station and can be discovered and utilized without any knowledge of the text.

6.

Cryptographic systems. Cryptographic systems which are unique to certain correspondents can likewise be used as identifications. This also holds for some of the cryptographic features such as pad numbers of one-time pad systems. The 10th Division, for example, which sends through station A, is enciphering its traffic in pad number 1234. Usually, only one originator is permitted to encipher messages in a given pad because of its one-time nature. There may be one or several holders who can receive. Thus, until completely used, the pad will identify the originating station and, in some cases, also the recipient. Caution must again be exercised, however, with regard to relay messages and to the possi-

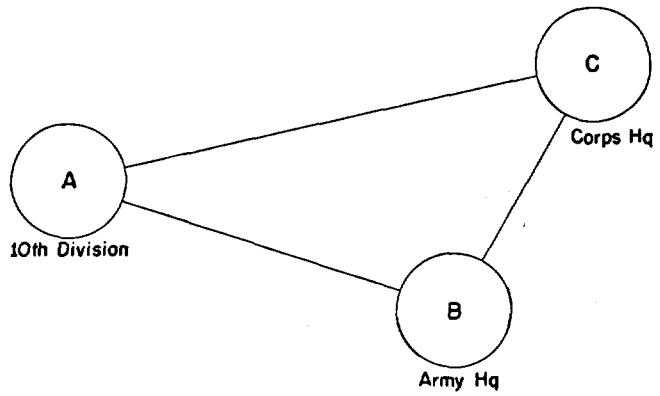


Figure 28.

REF ID:A5384682

bility of this traffic being transmitted over a different circuit of station A. If, for instance, the pad is used between the division and headquarters for some special purpose it could pass by several different paths (fig. 28). According to which route is available or readable, 10th Division's traffic may go directly to Corps or be relayed through Army.

7.

Services. Messages transmitted on one day may be serviced at some later date. If the date span bridges the frequency change, it may be possible to determine continuity.

8.

Chatter. Items of chatter often serve continuity purposes. Names of radio operators, for instance, may be observed in chatter, and, on recurring after a change, act as an identification.

9.

Procedural peculiarities. Some stations and operators develop unique habitual procedures which mark them. A station might, for example, regularly misspell a place name, or transpose the digits of a routing code number because of an error in the chart; an operator might send his call signs four times instead of the three used by others on the net, or send a separator between the hours and minutes of the file time though no one else does. Such peculiarities, which often arise from personal quirks, are usually rather difficult to discover because they involve painstaking attention to detail, but they are well worth the trouble. It is one of the phases to which the intercept operator, through his knowledge of the usual, can make an important contribution.

(*b*) *Use of direction finding.* This identification technique, described in paragraph 38, is a valuable means of providing continuities where efforts to use procedural characteristics have proved inconclusive. It is to be pointed out that, in general, procedural characteristics furnish a faster, less expensive, and more accurate method if they can be so utilized.

(3) Some of the techniques outlined above can stand by themselves, but it will always be found wise to apply several of them in combination so that one checks the other and reinforcing evidence is supplied. For example, the message center serials may indicate a continuity, and a routine message or the use of a restricted cryptographic system serves to confirm it. Incidentally, these methods of determining continuities are applicable to any sort of frequency change, whether periodic or irregular, and will also serve to tie together night and day frequencies and variant frequencies of the same station.

(4) When continuities have been established, the next task is the

REF ID:A58489

listing of the frequencies against the date breaks and the search for patterns of change or rotation. Once the general system has been solved, it will usually not be too difficult to keep abreast of changes. No attempt will be made in this manual to describe actual methods of solution further than to say that the problem, at this point, becomes one of cryptanalytic attack.

45. Call-sign Analysis

The main objectives of call-sign analysis correspond with those of frequency analysis, that is, (1) the determination of the system of use, and (2) the solution of the system of allocation.

a. Analysis of the System of Use. This analysis is conducted through a study of call signs as they are reported in the chatter. The period of call-up furnishes the most fruitful material, but all allusions to calls must be noted. A listing of the call-ups will generally provide sufficient information to identify the system.

(1) *Net using double-station call procedure* (fig. 29):

A calls B	DEF de ABC
B replies	ABC de DEF
A calls C	GHI de ABC
C replies	ABC de GHI
B calls C	GHI de DEF
C replies	DEF de GHI
B calls A	ABC de DEF
A replies	DEF de ABC
C calls A	ABC de GHI
A replies	GHI de ABC
C calls B	DEF de GHI
B replies	GHI de DEF

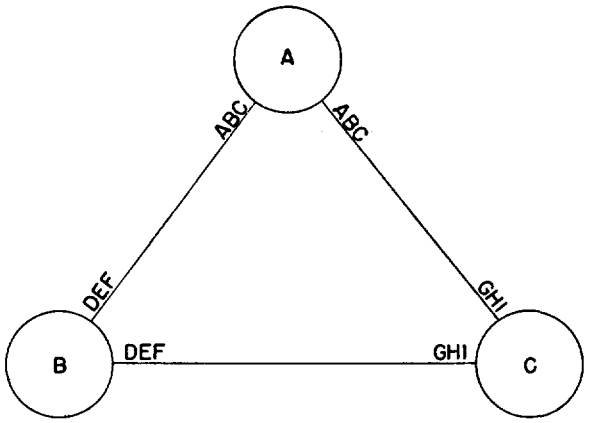


Figure 29.

REF ID:A58489

(2) *Net using link call system* (fig 30)

A calls B	ABC
B replies	ABC
A calls C	DEF
C replies	DEF
B calls C	GHI
C replies	GHI
B calls A	ABC
A replies	ABC
C calls A	DEF
A replies	DEF
C calls B	GHI
B replies	GHI

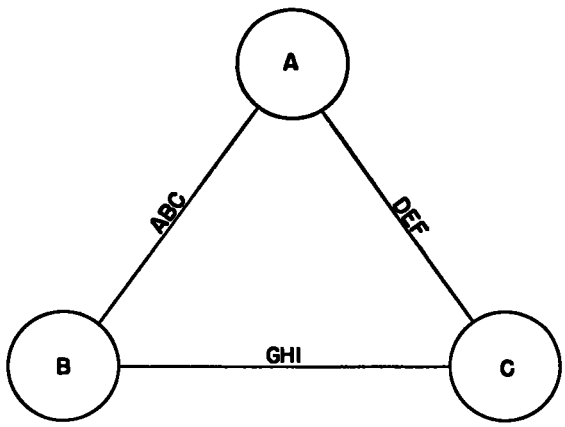


Figure 30

(3) *Net using single station call* (fig 31)

A calls B	DEF
B replies	DEF
A calls C	GHI
C replies	GHI
B calls C	GHI
C replies	GHI
B calls A	ABC
A replies	ABC
C calls A	ABC
A replies	ABC
C calls B	DEF
B replies	DEF

REF ID:A58489

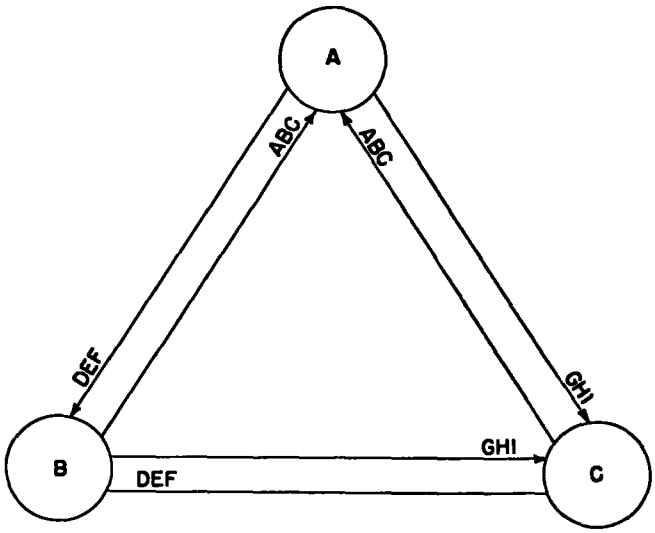


Figure 21

b SOLUTION OF THE SYSTEM OF ALLOCATION Like the study of frequency systems, the analysis of call sign systems may require anywhere from several months to several years Again like the frequency systems, the problem is twofold (1) the method of basic allocation and (2) the method of rotation, if present

(1) Calls must first be classified as to composition, for example, 3 digit, digit-letter-digit, etc, then these break-downs checked for pattern The allocation of calls may or may not be centralized. In the former instance, there will generally not be more than two or three systems to be solved, e g, Army and Air Force In the latter, however, depending upon the amount of decentralization, there may be a great many small systems Thus, in the initial analysis, calls should be listed by net, and the composition of the calls on each individual net observed If, for example, of all the nets under study, only two nets use 4 letter calls, it may be assumed, for the moment, that these nets employ a common call allocation After nets have been grouped by composition of calls, a search is made on each net for pattern For instance, the calls on three of the nets may carry "T" as a middle letter, indicating a possible grouping for study If a number of other nets also display similar characteristics, one using "R", another "V", etc, it is likely that all of the calls on these nets originate in the same general system The following lists of calls by net will serve to illustrate the general procedure

REF ID: A684682

Net I	*Net II*	*Net III*	*Net IV*
ABD	CDF	V7K	BCE
EFH	GHJ	V8J	KLN
FGI	LMO	X3M	OPR
JKM	MNP	Y4T	
		Y6S	

Net V	*Net VI*	*Net VII*	*NET VIII*
BAO	IJL	DEA	FQR
HIU	NOQ	HOA	JLT
KOE	PQS	JIE	SRM
MEA	STV		VTR
PAE			XOM
			XOA

(*a*) In the first quick grouping, the following division could be made:

Nets I, II, IV, V, VI, VII, VIII—3-letter.
Net III—letter-digit-letter.

(*b*) The first group then splits into three:
Nets V, VII—consonant-vowel-vowel.
Nets I, II, IV, VI—1st and 2d letters are in alphabetic order, 3d letter skips one from 2d.
Net VIII—apparently random.

(*c*) Thus, there are at least four systems of call distribution involved. On the other hand, studies of the calls on a number of nets may reveal no pattern at all. This is usually indicative of a large, general system in which control is highly centralized and the randomization carefully planned.

(2) Other features may also be employed to assist in the establishment of homogeneous call-sign systems for relationships between any of the elements of different nets that indicate possible relationships in other elements. For example, there may be some question as to whether or not the calls appearing on two separate nets can be grouped together. A cryptographic system, found nowhere else, is discovered on circuits of both nets. This suggests that there is some connection between the two nets and increases the possibility of a common call system. Procedural peculiarities of any type may likewise be used to associate nets. Order of battle, if known, furnishes another valuable method. All the nets of a given Army, for instance, will probably use the same call allocation. It may be that, in a highly centralized organization, a dichotomy can be established simply between Army and Air Force.

(3) Once the various systems have been segregated, it becomes possible to attack each separately. If a pattern exists within the call itself (as in Nets I, II, IV, and VI in (1) above), all possible

REF ID:A58489

calls can be listed and this used as a basis for the reconstruction of the allocation chart. If no pattern can be found, however, (as in Net VIII), it becomes infinitely more difficult to reconstruct these charts, and if the system is a large one it may be necessary to collect data over a period of years before a solution can be effected.

(4) Often these allocation charts serve as a base for the change or rotation of calls or for the choice of alternate calls at the same station. In analysis of the system of rotation, the first step is to determine the periodicity, which can usually be done simply by observation, and the second to establish continuities so that the calls related to each station or link and the order of their use are known. The techniques outlined in paragraph 44*b* (2) for the determination of continuities when frequencies change also apply to call signs with one exception (par. 44*b* (2) (*a*)*1*) and need not be further discussed here. In this one exception the reverse is true—if calls change and frequencies remain constant, the frequencies furnish the continuities to the calls. When continuities have been established, the calls may be listed in order for each station, and through the application of cryptanalytic techniques, the system attacked.

(5) In the practical aspects of call-sign system solution, it will be found that garbled and missed calls account for much of the difficulty in the initial stages of attack. Where there is a pattern to the call composition, garbles can be resolved with relative simplicity. In random composition, however, the problem is more complex and care must be taken to eliminate all spurious calls before beginning analysis. Garbles occur with some frequency in calls partly because the enemy makes an attempt to restrict their use, and partly because his operators become so familiar with them that they tend to send them in a quick, sloppy manner. In general, a call should be intercepted several times, preferably at different schedules, before it is accepted as genuine. Garbles can often be corrected by reference to the actual Morse equivalents. For example, if the call "AHV" has been established and the call "ASV" appears once on the same net, the Morse will indicate the possibility of error:

AHV .— ....—
ASV .— ... ...—

the difference being only a dot. Other link characteristics such as frequency, serial numbers, etc., will assist in confirming or disproving the identity of the two calls.

(6) Missed calls also present a problem to the analyst. They arise from imperfect coverage, and there is no remedy except to give more complete coverage and schedule information to the monitoring stations. Since calls are often sent only at the start of each schedule, this time is most important.

REF ID:A584489

(7) The following example, based on the call composition used in Nets I, II, IV, and VI in (1) above, will illustrate the general approach (since these calls have a definite pattern, all possible calls can be listed):

ABD
BCE
CDF
DEG
EFH
FGI
GHJ
HIK
IJL
JKM
KLN
LMO
MNP
NOQ
OPR
PQS
QRT
RSU
STV
TUW
UVX
VWY
WXZ
XYA
YZB
ZAC

(*a*) It is noted that calls change daily on the four nets involved; after the completion of one week, a tabulation by net and station can be made. (Garbled calls have been corrected.)

	1	2	3	4	5	6	7
Net I							
Station A	ABD	PQS	TUW	KLN	BCE	RSU	....
Station B	....	WXZ	BCE	EFH	HIK	....	UVX
Station C	MNP	JKM	MNP	WXZ	NOQ	XYA	CDF
Net II							
Station A	CDF	....	IJL	YZB	....	ABD	JKM
Station B	UVX	LMO	VWY	STV	JKM	GHJ	....
Station C	IJL	STV	OPR	ABD	DEG	MNP	WXZ

REF ID:A58489

Net IV

Station A	TUW	RSU	....	RSU	UVX	FGI	IJL
Station B	....	EFH	....	FGI	IJL	LMO	....
Station C	NOQ	KLN	....	XYA	OPR	YZB	VWY
Station D	HIK	XYA	....	LMO	CDF	STV	DEG

Net VI

Station A	....	ABD	DEG	MNP	PQS	BCE	....
Station B	VWY	....	PQS	TUW	....	HIK	....
Station C	DEG	YZB	JKM	GHJ	EFH	TUW	....

(*b*) Observation of the calls indicates that they are being rotated in a simple manner, and a check against the list of all possible calls shows that the difference of six between calls on the same net is fairly common. For example, on the 1st, MNP is 12 calls away from ABD; IJL is 6 away from CDF; NOQ is 6 away from HIK. It is also noted that the calls QRT and ZAC do not appear, probably to prevent confusion with Q and Z signals. This leaves 24 possible calls, and the periodicity of 6 suggests that the basic table is arranged as follows:

ABD	GHJ	MNP	TUW
BCE	HIK	NOQ	UVX
CDF	IJL	OPR	VWY
DEG	JKM	PQS	WXZ
EFH	KLN	RSU	XYA
FGI	LMO	STV	YZB

and that the calls are taken off across the chart and allotted to Net I, Net IV, Net II, and Net VI in that order. Within each net the calls are assigned to individual stations in what appears to be a random order.

46. Schedule Analysis

Schedule analysis is designed to discover what system is in use, whether the signalling is restricted or unrestricted and, if the former, what the time of each schedule is.

a. Analysis of the System. Analysis involves a tabulation of times of communication together with a study of chatter. Time is correlated with circuit and, if a definite pattern shows up several weeks running, it may be assumed that period signalling is in use. In the preparation of the data, record should be made of such chatter items as, "I have a schedule at 2200 with XYZ." Such information helps to fill in the gaps in cover. Also note must be taken of the very brief schedules where the stations have no traffic and merely call up, say, "I have no traffic," and sign off; or where a station is running over his schedule time and calls his regular correspondent

REF ID: A684682

to say, "I am busy," and then goes back to the first correspondent. If no pattern appears, however, it is then likely that either unrestricted signalling or priority signalling is in use. This can be determined by a check of the tabulation, since in priority signalling the control station will usually come up at regular schedule times. Chatter will also prove characteristic for this type of operating since the order of transmitting is fixed and usually only one message is sent at a time by each station. The type of unrestricted signaling can likewise be identified from chatter. Where arbitrary schedules are used, the stations will arrange for the next schedule at the time of sign-off. Incidentally, in period signaling, the stations also sometimes mention the time of their next schedule so care should be exercised not to confuse the two. The regular pattern of times over a long period will usually distinguish period signaling. In alert operating, no arrangements are made, all stations standing by for transmissions at any time.

b. Determination of Schedules. The tabulations made for the above purpose will also serve to determine the times of regular schedules. Each circuit may be plotted on cross-section paper with hours down the side and days across the top. This will give a month's picture at a glance (fig. 32). The letters in each square indicate

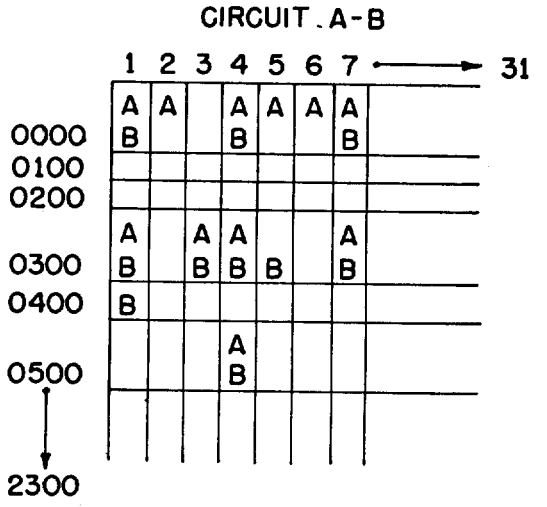


Figure 32.

the end of the circuit that was heard. On the 2d at 0000, for instance, only A was intercepted. Other items may be added to this tabulation if desired. These might include number of messages passed, indication as to which of the alternate frequencies was being used, and special notes from chatter relating to schedules. Two irregulari-

REF ID:A584489

ties will be noted in the pattern in figure 32. On the 1st at 0400 B ran over the regular 0300 schedule. Reference to chatter discloses that B asked A for additional time. On the 4th at 0500, A-B worked a special schedule. A check of chatter on other A circuits shows that A arranged for this schedule through a third station, which could contact both A and B, for the purpose of passing urgent traffic.

47. Procedure Analysis

Analysis of procedure is undertaken (1) to discover characteristics which will assist in identifications and continuities, and (2) to solve any encipherments employed.

a. Study of Characteristics. The normal characteristics of the procedure under study should first be established. This includes the call-up, exchange of readability, order of traffic, message externals, servicing methods, and sign off. In many communication systems, several normal procedures may be apparent, each representing a major division of nets. When this task has been completed, variations from the normal as applied to individual nets, groups, links, and stations must be identified. These variations may be of any sort. For example, one net may use break-in procedure for servicing, or may place the priority of the message in a different preamble position, or may tune up with a letter other than "V"; or a station may regularly place an NR before the link serial number while others do not, or fail to use an RQ before its request for services. These variations arise in several ways. They may be due to an oversight on the part of personnel, such as failing to change to a new method of procedure because of habit or because the station was not included in the distribution of the new instructions. Such situations will usually be corrected in time, or, if distribution is impossible, continue to serve as an important identifying feature. Or they may arise from the latitude permitted nets or stations in compiling their own rules. The only approach to this analysis is through the detailed study of chatter and the recording of the normal and the unusual.

b. Solution of Enciphered Procedures. The solution of enciphered procedures depends on the ability to determine the meaning of procedure signs and signals in context and, where a periodic change is involved, the equating of the same procedure in terms of different encipherments. For example, in the opening minutes of a schedule, procedures such as "Send V's," "How is my readability," "I cannot hear you," "Readability is poor," "Adjust your transmitter," etc., will be common. By study of the context over a period of time, it should be possible to identify the appropriate meaning.

RECD 100 : 2684682

48. Serial Number Analysis

The analysis of serial numbers is directed toward the determination of the type of number, the manner of assignment, the solution of any encipherments, and the identification of the series with units.

a. ANALYSIS OF TYPE. The type of the serial number, that is, indesk, message center, signal center, etc., is determined through a correlation of the numbers with other signal features. The numbers should be tabulated for a period of a week or more as necessary against call signs, file times, intercept times, cryptographic systems, routings, and similar items. The following discussion is not intended to be complete since there are so many possibilities involved in these manifold relationships, but it is hoped to give some general indications on how to think about them.

(1) Serials which run in order by cryptographic systems may be a code room number, a message center number, or a signal center number. It will rarely be a radio station number. The caution to be observed is that the cryptographic system may not be the basic factor and the serial the result, but rather the system, like the serial, may be the effect of something more basic. For example, a series is found which agrees with the cryptographic system and every message in that system is always in that series. It is noted, however, that the system is the only one held by the unit involved. Thus, both the system and the series are representative of the unit, and the number only accidentally follows the system.

(2) Serials which correlate with routings are also usually in the message/signal center phase. Sometimes several series which do not match with other features are observed originating at the same routing. These are often the expressions of several units operating through a single signal center. Such numbers may be put on at the unit message center or they may be added at the signal center, the latter maintaining several series, one for each of the units involved.

(3) Serials which run in order by file time may represent either the message/signal center or radio station stage. Usually, file times are put on at the radio station, but, since the traffic comes to the station direct from the message or signal center, its order is seldom disturbed, so that it could be numbered in one place and time-stamped in another and still demonstrate a relationship. In the case of radio station numbers, it will usually be found that several call signs, used at the same station, will run in a common series.

(4) Transmitter numbers will, as a rule, correlate with the sending call signs and the intercept time. Link serials will be evidenced by the further distinction of a separate series for each station called. Operator numbers are indicated by several series originating at one call, regardless of reply, unless the station works to only one correspondent.

REF ID:A58489

(5) It is just as important in the study of serials to have negative evidence as positive, so note should also be taken of what does not fit the series. If several routings fall in the same series, for instance, the number was not assigned at the message center if that is what the routing represents. Such a series is more likely to relate to the radio station which handles traffic for several different routings.

(6) Many times series will appear which bear a relationship to several items. It is then necessary to determine what is the basic consideration. For example, a tabulation of serial numbers reveals:

Serial	*Crypt. System*	*Routing*		*Call sign*		*File date and time*	*Intercept date and time*
		From	*To*	*From*	*To*		
326	A	A	B	PQR	XYZ	08 1040	08 1215
327	A	A	B	PQR	XYZ	.....	08 1217
328	B	A	C	PQR	XYZ	08 1040	08 1220
335	A	A	B	....	....	09 1230	09 1530
339	C	A	C	PQR	XYZ	09 1210	09 1532
340	A	A	B	PQR	XYZ	09 1235	09 1535
343	B	A	C	PQR	....	09 1300	09 1538
344	C	A	C	PQR	XYZ	09 1300	09 1600
345	C	A	C	PQR	XYZ	09 1250	09 1615
346	A	A	D	PQR	XYZ	09 1310	09 1619
362	C	A	C	PQR	XYZ	11 1240	11 1525
367	C	A	C	PQR	....	11 1500	11 1801
368	C	A	C	PQR	XYZ	.....	11 1820
429	B	A	C	PQR	XYZ	08 1100	08 1223
437	B	A	C	PQR	XYZ	09 1315	09 1623

Except for the last two numbers which are garbled, the serials correlate with origin, calls from and to, and intercept time. File time is slightly off in several places. Since intercept time fits so well, it may be assumed that this is a radio station number. Reference is now made to the circuit diagram and it is noted that PQR is on the edge of the net and that it is connected to it by the single circuit to XYZ. Thus the routing "A" is probably the only message center routing through PQR and, therefore, the relation between "A" and the serials is forced and not the true one. If it were the true one, it is likely that the intercept times would be somewhat out of order because of the routine of processing traffic and the passing of priority messages. But since there is only one link out of the station, the type of radio station number used cannot be defined. It may be an in-desk, a transmitter, or a link number. If the picture is expanded, however, to include an additional link with numbers, it will appear as follows:

REF ID: A584682

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
372	B	A	C	PQR	STN	08 0900	08 1025
733	A	A	B	PQR	STN	08 0910	08 1030
734	A	A	B	PQR	STN	08 0910	08 1033
759	B	A	C	PQR	STN	11 1535	11 1911
765	C	A	C	PQR	STN	11 1820	11 1914

The serial is a link number since the numbers run in a separate series for the PQR–STN channel.

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
603	B	A	C	PQR	MNO	171441	172010
604	A	A	C	PQR	MNO	171411	172013
605	B	A	C	PQR	MNO	171411	172016
606	B	A	C	PQR	MNO	171415	172021
610	B	B	D	GHI	STN	171430	171810
612	C	B	D	GHI	STN	171430	171812
612	C	B	D	CHI	STN	171430	171812
613	A	B	C	PQR	MNO	171440	172005
634	A	A	C	PQR	MNO	181120	181523
636	A	A	E	GHI	STN	181135	181803
639	A	A	D	GHI	STN	181150	181809
640	B	A	C	PQR	MNO	181155	181520
641	A	A	C	PQR	MNO	181155	181535

Note the correlation with file date and time and the interlocking of the call signs. This is an instance where file date and time are entered at the radio station.

(7) The following tabulation is that of a signal center number:

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
020	A	A	C	GHI	PQR	230910	231233
023	A	A	C	GHI	PQR	230910	231230
024	A	A	C	GHI	PQR	230925	231225
026	B	B	D	JKL	STN	230910	231413
029	C	B	D	JKL	STN	230915	231416
153	A	A	C	GHI	PQR	241120	241236
155	A	A	E	MNO	XYZ	241125	241228
156	D	A	E	MNO	XYZ	241130	241231
164	A	A	E	MNO	XYZ	241130	241238
166	B	B	D	JKL	STN	241145	241411
167	B	B	D	JKL	STN	241130	241402
170	C	B	D	JKL	STN	241145	241409
171	C	B	D	JKL	STN	241150	241421
172	D	A	C	GHI	PQR	241145	241250

REF ID:A58489

Both A and B route through the signal center where a common series is applied to the traffic of both. The possibility of this being an in-desk number is largely ruled out by the failure to correlate with file time.

b. Analysis of Assignment. Study of the manner of assignment of serial numbers is concerned with three phases: (1) composition of the numbers, (2) range of the series, and (3) over-all pattern of assignment.

(1) *Composition.* The numbers may consistently be two-digit, or three, or four, etc. They may incorporate such features as the date. Composition, if sufficiently distinctive, often furnishes a means of quick recognition.

(2) *Range.* The range of the series may be readily determined, or it may take several years. It can be established by observation of the reversion to the lowest number of the range, which will fix its limits in terms of either time or numbers, or both.

(3) *Over-all assignment.* Serial ranges of the same type of number should be checked for pattern of assignment against each other. In the case of message center numbers, for example, it may be found that each division of an army has been given separate blocks, 1–100, 101–200, 201–300, 301–400, etc. Similar patterns may appear with regard to signal center or radio station numbers. These patterns can be analyzed through a comparison of ranges representing groups which bear an order of battle or a net relationship to each other.

c. Solution of Encipherments. The solution of enciphered serial numbers is a matter of cryptanalytic approach. The initial break, however, can often be made by gathering a group of messages on which it is thought that the serials run in order. If, for instance, an in-desk number is involved, messages arranged by file time should assist in attacking the system. It also may be helpful to select the first message of the day, if possible, and use it as No. 1. It will serve as a base even though that may not be its actual number. If the numbers are thought to repeat daily a selection of this message each day may yield different encipherments of the same number. As a rule, these systems should not prove too difficult to solve unless the method is one of complete randomization.

d. Identification of Series. Once the type of series is known, the next step is to determine the actual unit behind each series. In the case of a message center number, for example, what message center is it? Or if there are three series of in-desk numbers out of the same station, what do each of these series represent? These identifications are established by "pure" traffic analysis plus the use of collateral material on the basis of the axiom that things equal to the same thing are equal to each other. For instance, a range of in-desk numbers appears only with codes A and B. Codes A and B are known to be

REF ID: A5384682

transportation systems. Therefore, the serial range represents the transportation unit at the signal center. Care must always be taken, in chaining data of this sort, that the basic assumptions are valid (in this case, that A and B are transportation codes) and that the things compared demonstrate an exact relationship (if A and B were also used on another range of numbers out of the same station, then it is unlikely that the first range represents transportation, but rather that it represents some other type of unit or else a specific transportation unit, these possibly being two at the station). Decode and order of battle material are invaluable in the study of these series. If some of the traffic related to a series can be read, solid evidence for conclusions is provided and often a definite unit can be identified. Order of battle will do much the same. For example, where only one air unit is carried at a given location and a series, tied to the air cryptographic systems, is observed out of that location, it may be assumed that the series represents the air unit.

49. Analysis of Priorities

The analysis of priorities is directed toward determining their order and the solution of any encipherments. The order is determined by comparing file times with intercept times. In general, the shorter the average time lapse, the higher the priority. However, time lapses should be compared within stations not between them since the size of the station and the volume of traffic handled will cause individual differences. Relayed traffic, of course, should not be included in the comparisons. The cryptanalysis of encipherments is naturally dependent on the system used, but it is of assistance to group messages according to expected priority, thus providing isologs.

50. Analysis of Routing Systems

The main objectives of routing system analysis are to discover the manner of use and to solve the routing codes.

a. Analysis of Use. When routings appear on traffic, it is first necessary to determine what they represent in terms of origin and destination. This is done by observation. If necessary a tabulation can be made against call signs which will readily reveal which routing is the originator and which the addressee. The difference where present between information and action addressees may be a little more difficult, but checks, for example against priorities, should assist. Further observation will indicate the manner of handling local and relay traffic and the nature of the routings in these instances. Any peculiar use of routings, as in the readdressing of traffic, can also be determined. Following these routings against the net diagram is often helpful.

REF ID:A584682

b. Solution of Routing Codes. The initial step in the solution of routing codes is to check the code groups for characteristics in composition and range. Once these patterns, if present, have been recovered, the next step is the specific identification of code and syllabary groups. Identifications are chiefly based on cribs from known systems to unknown, on net diagrams, on breaches of security, on decode and order of battle material, and on a number of variations of these. As identifications are produced, it may be possible to ascertain the structure of the code and syllabary, such as alphabetical, geographic, order of battle, etc., and this, in turn, assists in future recoveries. In order to suggest methods of attacking this problem, some of the possibilities are discussed below:

(1) *Tying the code group to a known radio station.* Where the station locations are known, several methods present themselves according to the use of the routing codes. The predominant originator out of a station may ordinarily be assumed to be located there. This also applies to the predominant destination, unless destinations are dropped on local traffic. But, because the identification is made with a location, this identification is a true one only if the routing numbers represent locations. If they represent units, then it is necessary to seek further, and the recovery of the location can only be considered tentative in lieu of something more exact. Along with the use of this technique, the lapse between file and intercept times should be averaged for each originator. Messages originating locally will show a shorter time lapse than those previously relayed. If destinations are habitually dropped on the last, or local, leg of a relay, they may be related to the receiving station. For instance, a message from A to C carries the routing "123–567" on the A–B link (fig. 33), but when B relays to C, it only carries "123", thus matching 567 with C.

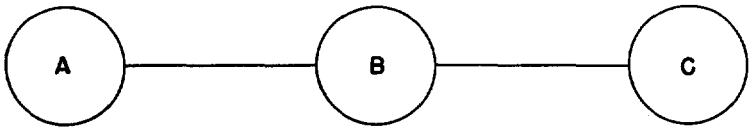


Figure 33.

When the same message is sent to several locations, the local copies may not carry routings while the relayed ones do, making possible the identification of the origin with the sending station. For example, in figure 34, A sends the same message to C and D. The message to C on the A–B channel is marked "123–567", that to D has no routings, thus identifying 123 with A.

(2) *Cribs.* The availability of cribs is chiefly based on the existence of several different routing systems. This may involve checking into networks other than military, such as Naval or domestic, for

REF ID: A684682

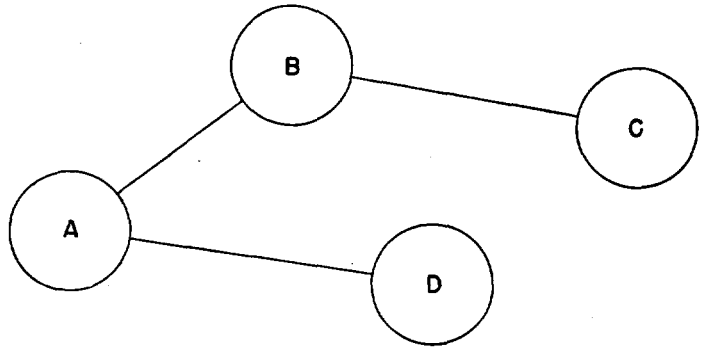


Figure 34.

such data. No possibility should be overlooked. Some of the crib techniques follow.

(*a*) *Relay crib.* If it is necessary for a message to pass over different nets with different routing systems, origins, and destinations can be correlated, and if one system is known, the other can be identified. For example, the message on Net I carries "123–567", on Net II "ABC–JKL", then 123 equals ABC and 567, JKL. One caution here relates to the destination. If this is a book message going to several addressees, there may be a direct correspondence between the originators, but not the destinations, since 567 may be one receiver and JKL another. Sometimes, this can be verified by checking the address and serial numbers.

(*b*) *Book message crib.* Where the same message goes to a number of destinations over different nets employing different routing codes, it is possible to crib originators. This often happens with large centers who work in several nets and may use several routing codes. It also occurs where traffic is relayed out of the net. Naturally, this would also yield a relay crib, but if the first transmission has been missed, the later relay can be used as a book message crib.

(*c*) *Serial number crib.* Serial numbers may be used to crib originators if the serial is a message or signal center number. For example, if a tabulation of serials reveals the following:

Serial	*Routing*	*File date and time*
53	123	092005
54	123	092005
55	123	092005
58	ABC	092005
59	123	092005
60	123	092015
65	ABC	092020
67	ABC	092020

then 123 may be cribbed with ABC.

REF ID:A684682

(*d*) *Error crib.* Where several routing systems are available to a station which works in a number of nets, it may occasionally happen that the wrong system is used. Such errors will generally be corrected yielding a crib between the two codes.

(*e*) *Address and signature cribs.* A unit or person addressed at one routing group in a known system will yield a crib against the same unit addressed at an unknown group. For instance, the 37th Division may be addressed at ABC, known to be Mannheim, on one message, and to 123 on another on the same day; 123 may then be identified with Mannheim. The possibility of unit movement, however, must be considered, and also that of detachments being addressed. The new recovery should be checked against the pattern, if present, of the routing system. In address systems where solution is only partial, but unenciphered code is available, the same address code groups may be used to crib the routing groups. Address code groups, for example, 1234, 5678, may appear with destination group ABC and also with 135. It is not necessary to know the value of 1234 5678 to crib ABC with 135. These same techniques are applicable to signatures and points of origin.

(3) *Operator chatter.* Operator chatter may give away the identity of a code group through the mention of a place name or a unit.

(4) *Address information.* Where addresses are separate from routing codes, use may be made of the address when readable. A unit, whose location is known from other order of battle sources, may be addressed at an unknown routing group thus identifying this group. Consideration must be given in such an instance to the possibility of the unit having moved. If there is some pattern to the composition of the code, the new value should be checked for fit. The recency of the date of the unit's identification and the trustworthiness of the source should also be noted.

(5) *Solved message information.* Solved messages may contain outright assignments of routing code values; more usual, however, is the traffic which permits correlation of internal originators, addressees, or subject matter with externals. All solved messages should be read for clues to routing code identities.

(6) *Miscellaneous sources.* These involve prisoner-of-war reports, captured documents, and similar materials.

(7) *Syllabary solution.* The syllabary to the routing code may be solved by using any of the above methods, but also available is the use of word patterns. If, for example, the routings consist of place names, a list may be constructed of all likely places which will show patterns of repeated or doubled letters, digraphs, etc., within each location, and this may be applied against similar patterns in the encipherments.

REF ID: A5384682

(8) *System change.* If the routing system changes, the continuity techniques discussed in paragraph 44 *b* (2) may be applied. For example, the continuation of a series of serial numbers may serve to identify a new routing designation with an old. Also of value are the contact patterns or associations in which a routing designation may be involved. If, for instance, routing number 123 sends traffic daily to three particular locations, and after the change of system, ABC is discovered following the same pattern, then 123 and ABC may be equated.

c. The above listing of methods of identification is only partial and specific application is dependent on the nature of the communication system under study and on the structure of the routing codes. Identifications, as made, should be evaluated and some sort of validity indicator attached to them as a guide to the reliability of the value. These validities are the result of personal judgment and the peculiarities of evidence and no rules can be laid down for their use on a general basis though in any specific problem definite standards can be set up. Where identifications are based on a crib, however, it should be remembered that the validity of the cribbed value can be no higher than that of the base value.

51. Analysis of Textual Features

The analysis of cryptographic features is concerned with the recognition, use, and distribution of systems, the use of indicators, and the identification of practice and dummy traffic.

a. Recognition. The recognition of cryptographic systems is the first step in their analysis either for traffic analysis or cryptanalytic purposes. Where a discriminant in the clear is present, this becomes a simple matter; encipherment somewhat complicates the problem. But, if there is no discriminant, it is necessary to make use of other features. In the attack, traffic should be sorted down by net and then studied for individual peculiarities. For instance, the following differences may appear as to the type of text:

Net	Type of text	No. of messages
I	4-letter	65
	4-digit	40
	3-digit	29
II	4-letter	48
	5-digit	73
	4-digit	51

Since the net usually represents an order of battle entity it also often represents a crypto-entity. Therefore, all 4-letter traffic passing on Net I (barring the discovery of any further distinction) may be assumed to belong and may be considered for the moment a hemo-

REF ID:A58489

geneous system in itself. Further study is then necessary on the relationships of the two possible systems. Some elemental difference as to form may be apparent which will distinguish them as separate systems, such as the presence of a digit indicator in one. On the other hand, no distinction may be noted and it will be up to the cryptanalyst to determine if the same or different systems are involved. Routings should also be checked in this respect, a relationship between routings (as to echelon, for example) evidencing the likelihood of the same system though passed on different nets. Other factors, beside type of text, are of course also valuable. These include priorities, characteristic serial number ranges, or features of the text such as the nature of the indicators.

c. Analysis of Use. Tabulations of the nets and routings of traffic will often indicate the use of a system. A system, for example, passing only over a water transport net may be identified tentatively as a water transport system, or one used only between intelligence units may be considered a special intelligence system. Caution should always be exercised in making such assumptions because of the ever present possibility that the transmitting of certain traffic over specific nets may result from communications necessity. Peculiarities as to priorities, serial number ranges, and miscellaneous preamble classifications may also assist.

d. Analysis of Distribution. Directly related to the study of use is the analysis of distribution which can be accomplished on the basis of the same tabulation. For instance, a given system may be identified as Air Force and, furthermore, it may be discovered that its distribution is limited to a certain type of Air unit. The tabulation may be as follows:

Net	*Routings*	*Volumes*	*Other characteristics*
I	A–B	354	All traffic uses 5-digit message center numbers.
	A–D	251	
	B–A	240	
	B–D	223	
	C–A	112	
II	A–E	232	5-digit message center numbers.
	A–F	227	
	E–F	116	
	F–E	34	
III	A–G	249	5-digit message center numbers.
	B–G	245	
	G–C	121	
	G–H	112	
	H–G	78	

REF ID: A5384682

Nets I, II, and III are known to be high-echelon Air Force administrative nets. The system under study appears only on these nets and a further check reveals that it composes the bulk of the traffic passed, indicating that it is probably the high-echelon administrative Air system. The 5-digit message center numbers are of interest because numbers of this size appear only on traffic of Air division or higher. Furthermore, most of the routings involved are known to be locations of Air divisions and higher headquarters. Thus, the limits of the distribution of the system are established and now the reasoning may be reversed: any routing appearing with this system may be assumed to be an Air division or above. One-time pads lend themselves to this type of analysis because of their highly restricted distribution. Tabulation of the pad numbers against other features will generally define the users, and since these pads are usually used in only one direction, fix the originator and the one or more recipients.

e. Analysis of Indicators. Where indicators appear in the clear they may be of traffic analysis value. Observation will reveal any peculiarities of the indicators and, if present, they can be correlated with other features.

f. Analysis of Practice Traffic. Practice traffic can often be identified through a study of the text. Messages may be made up at random which generally leads to a patterning and repetition of combinations of letters or digits. Also since there is usually no desire to disguise practice traffic, it may carry a designation in the heading. On the other hand, skillfully designed practice traffic, particularly if an effort is made to conceal it, may be undetectable except for security breaches in operator chatter.

g. Analysis of Control Traffic. Control traffic, if properly handled, may prove very difficult to identify. The usual means of analysis, such as operator chatter, distinctive serial number ranges, etc., are always open. For example, very fast receipting for traffic and few services may indicate that the operators know that the traffic is dummy and are not particularly concerned about it. On the other hand, in an efficient control operation, the operators will not know that they are dealing with dummy traffic and hence will furnish no clues. Another method open to the analyst, however, is the study of traffic volumes and proportions. A level traffic volume on a number of circuits may indicate an attempt to conceal the natural peaks and troughs of a military operation. Moreover, high volumes in areas which other intelligence sources reveal as inactive should be viewed with suspicion. Abnormal rises of certain types of priorities of traffic should be carefully checked for evidences of spuriousness. Control operations carefully planned will take into account the

REF ID:A584489

proper proportions between the various types, but, because of their complexity, breaches of security will often occur.

52. Miscellaneous Items

Every communication system has its own peculiarities in its procedure and traffic. No rules can be given for their analysis except to observe the manner of use and to seek out the relationships between them and other features. It is hoped that the foregoing discussion of certain specific components will not only serve to set the pattern for research on these miscellaneous items, but, more than that, will encourage the traffic analyst to use his ingenuity in the development of new techniques.

Section III. NET RECONSTRUCTION

53. Introduction

The reconstruction of the radio net proceeds simultaneously with the analysis of radio operations. (Furthermore, it is a continuing task since net formations and operating data are seldom static factors.) As noted before, it involves the grouping of stations into nets, the building of the net structure, and the identification of the stations with geographic locations and military units. The resulting net diagram may be drawn in either a schematic or geographic design, according to purpose, and signal features added. This involves, in effect, the reproduction of the radio communications section of the enemy "Signal Operation Instructions" (SOI). These instructions are the orders issued setting up the required signal nets for each military operation and include the assignment of frequencies, call signs, schedules, and miscellaneous data. For a more complete description of the "Signal Operation Instructions," and for United States Army examples of same, see chapter 4, FM 24–16.

54. Grouping of Stations

a. The initial step in analysis is to list all stations and their correspondents. This will yield a rudimentary grouping. For example, the study of a day's chatter reveals—

ABC works DEF
ABC works GHI
ABC works JKL
DEF works MNO
DEF works PQR
MNO works PQR
XYZ works STU
XYZ works ?

REF ID: A384682

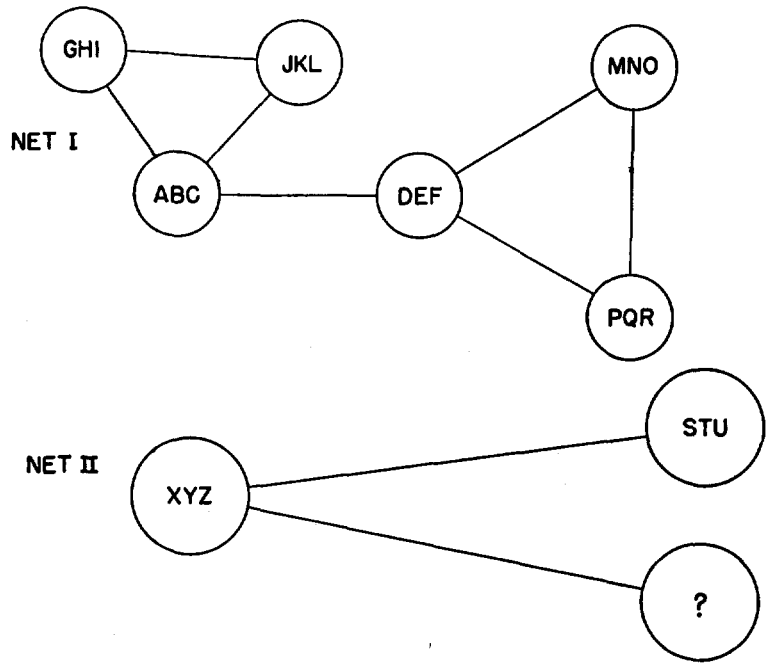


Figure 35.

Thus there are, for the moment, two separate groupings of stations with Net I apparently divided into two groups (fig. 35). It should be remembered that one day's intercept will rarely result in anything as complete as this, and that where daily changing calls are employed, the continuity techniques covered in paragraph 44 must be used. Missed calls present a similar problem. The next task is to study the characteristics of these stations as far as radio operation and procedure is concerned in order to refine the above groupings. It may be found, for example, on the one hand, that the ABC group and Net II exhibit such like characteristics that they appear to belong to the same net and that the connecting link between them has not yet been monitored; and, on the other hand, that the DEF group displays such different characteristics that it must be considered separate and that the DEF call must serve two groups (DEF–MNO–PQR and DEF–ABC).

b. The characteristics to be compared relate to all the features of radio operations:

(1) *Frequencies:*
(*a*) System of use.
(*b*) System of allocation.
(2) *Call signs:*
(*a*) System of use.
(*b*) System of allocation.

REF ID: A684682

(3) *Schedules:*
(4) *Procedure:*
(*a*) Call up.
(*b*) Order of traffic.

(c) Message externals (form and composition of preamble and postamble).

(*d*) Receipting.
(*e*) Corrections and services.
(*f*) Signing off.
(5) *Cryptographic systems.*

c. These items may be used as a check list. Stations, or circuits, do not have to agree in every particular to be grouped, but they should on the major features and, often, on the more characteristic of the minor. What constitutes this latter depends on the net itself. If, for example, strict instructions are issued by the net relative to the order of the preamble components, any deviation, however slight, may be taken as evidence of a separate net. On the other hand, if instructions are rather lax, deviations may not hold any significance. The traffic analyst seldom knows about the nature of the orders on operating procedure, but he can, through careful observance of the net, gain a general impression of how closely it is controlled and how well it is disciplined.

d. The following example illustrates the use of these techniques:

ABC works DEF
ABC works GHI
ABC works ?
XYZ works MNO
XYZ works PQR
STU works ?
? works ?

(1) *The diagrams* (see fig. 36).

(2) *The characteristics:*

(*a*) *Frequencies:*

Net I: Complex-sending Frequency Fixed.
Net II: Star Frequency Fixed.
Net III: Complex-sending Frequency Fixed.
Net IV: Complex-sending Frequency Fixed.

(*b*) *Call signs:*

Net I: Double-station Calls Monthly Changing.
Net II: Double-station Calls Monthly Changing.
Net III: Double-station Calls Daily Changing.
Net IV: Double-station Calls Monthly Changing.

REF ID:A584489

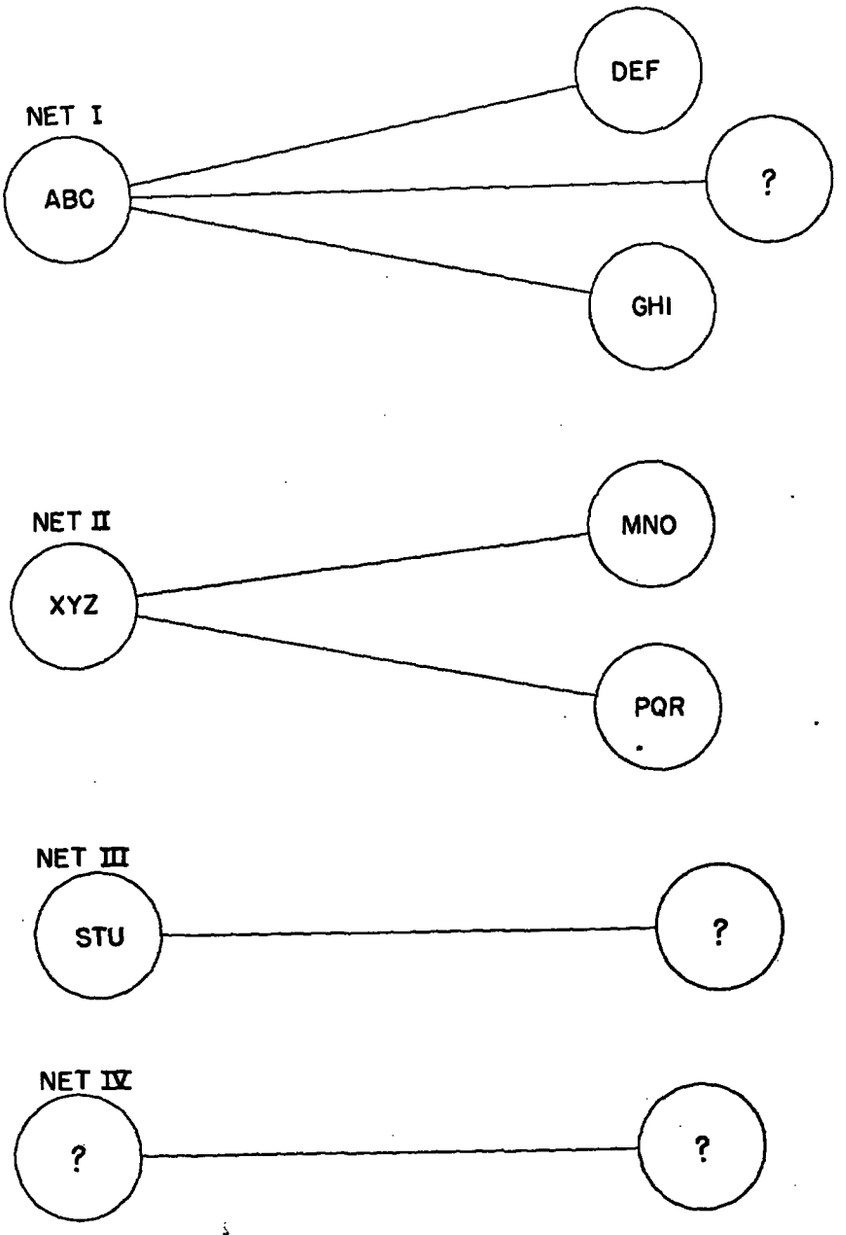


Figure 36.

REF ID:A58489

(*c*) *Schedules:*

Net I: Period.
Net II: Period.
Net III: Unrestricted.
Net IV: Period.

(*d*) *Procedure:*

All Nets: Q signals; International.

1. Call up:

All Nets: Usual.

2. Order of traffic:

All Nets: Precedence traffic first.

3. Message externals:

Net I:
Preamble: Circuit No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Net II:
Preamble: Circuit No.; Message Center No.; Group Count; File Date and Time; Routings.

Net III:
Preamble: In-desk No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Net IV:
Preamble: Circuit No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Separators: Same for all nets.

4. Receipting:

All Nets: Usual.

5. Corrections and services:

All Nets: Usual.

6. Signing off:

Net I: Usual.
Net II: Usual.
Net III: Makes next schedule.
Net IV: Usual.

(*e*) *Cryptographic systems:*

Net I: A, B, C, D.
Net II: A, E, F.
Net III: A, G, H, I, J.
Net IV: A, B, D.

e. It will be observed from the above that Nets I and IV have similar characteristics, and that II and III differ in certain important respects. Net II uses a net frequency. This alone would be insuffi-

REF ID: A634812

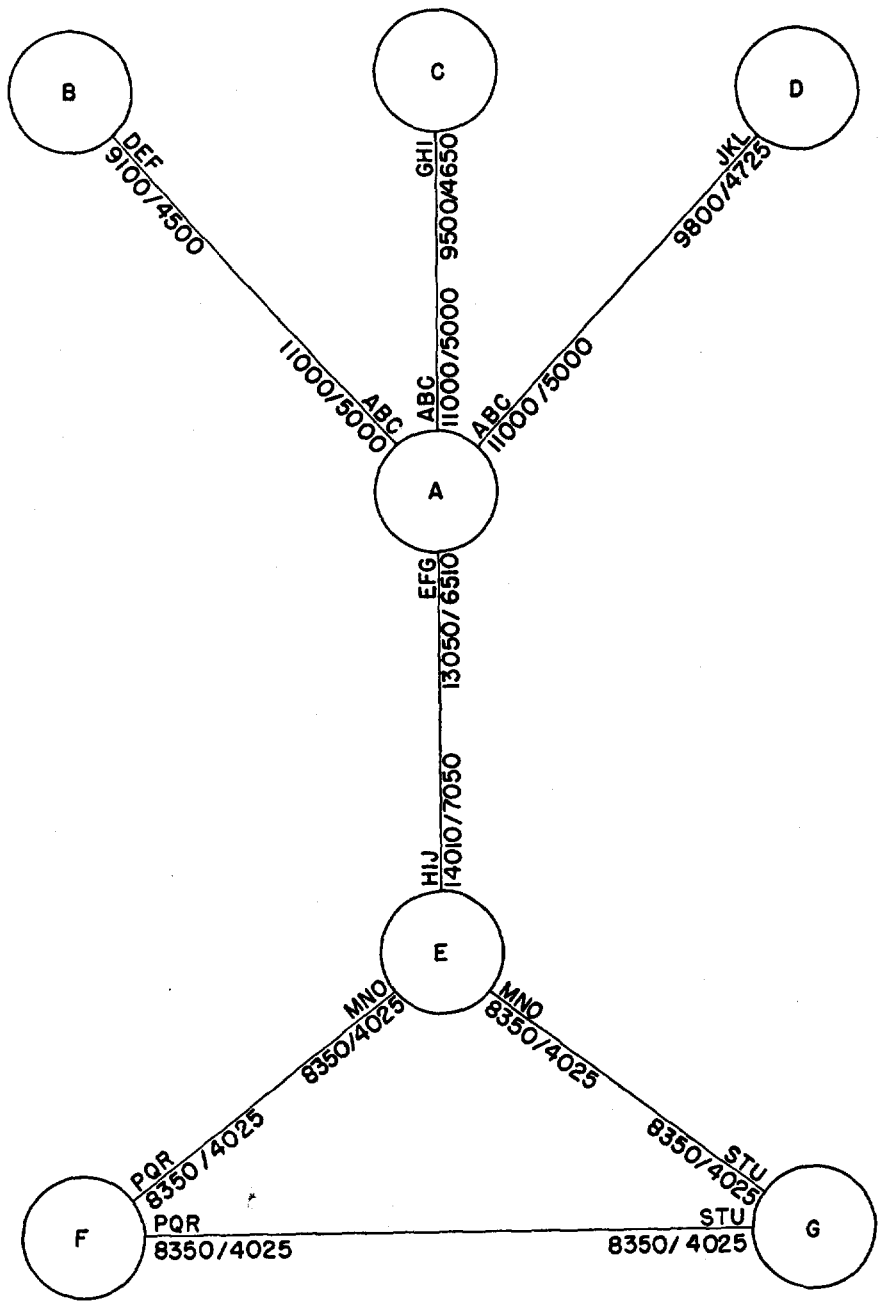


Figure 37.

REF ID: A58489

cient grounds for isolating it, but the position of the precedence in the preamble, and the use of different cryptographic systems furnishes enough additional evidence. Net III employs daily changing calls, usually adequate premise for setting a net apart. In this instance, added weight is given by the use of unrestricted signaling, the in-desk number, and the distinctive cryptographic systems.

55. Building the Net Structure

a. An elementary amount of net building is accomplished in the process of grouping the stations into nets. A number of additional techniques are now brought into play to complete the task. The crux of the problem involves the identification of different frequencies and calls with a station, in other words, that call ABC is at the same station as DEF, or that 11,000 kcs is at the same station as 9,050 kcs. When this has been done, the links and groups will fall into place and the net reconstruction be completed. It is difficult to set down definite methods to be pursued because much depends on the individual characteristics of the network. The following paragraphs discuss some of the principles involved and are suggestive of the general approach. Examples used are based on the diagram in figure 37.

b. Frequencies, Calls, Schedules. As a general rule, like calls or like frequencies may be assumed to be at the same station. Thus, in figure 37, the call ABC on frequencies 11000/5000 kcs was always considered the same regardless of station called. But caution should be exercised in arriving at this decision because it is always possible that no relationship may exist. A check of schedules is helpful. If ABC is heard working two different stations at the same time, it is likely that the two ABC's are separate stations. Other checks are traffic routings, cryptographic systems, etc.

c. Interlocking Serials. Where a radio station in-desk number is used, the serials out of different calls can be interlocked. When the serial is a message or signal center number, the interlocking technique may also be used, but account must be taken of the relay possibility. For instance, in figure 38 A and C are under analysis in an attempt to tie them together. Message center numbers on traffic out of ABC run:

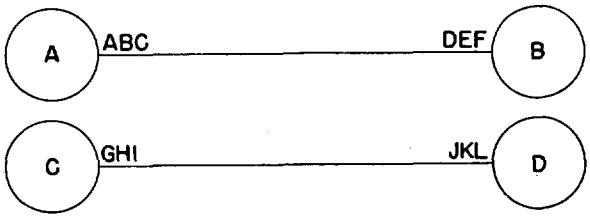


Figure 38.

RHCP 109 : AD684682

1578	1607
1579	1608
1585	1609
1586	1610
1587	1629
1588	1630
1589	1631
1603	1641
1605	1642
1606	1643

Message center numbers on traffic out of GHI run:

1581
1582
1583
1584

But, if the latter traffic shows evidence of being relayed and, if there are no other grounds for identification, a conclusion cannot be reached. On the other hand, if it is found that nonrelay traffic on this net carries no routings, but that relay traffic does, and that all the messages listed above under both ABC and GHI have no routings, it may be assumed that ABC and GHI are co-located. Other types of serials, such as link numbers, generally cannot be used for this purpose.

d. Traffic Routings. On the theory that the predominant originator out of a call or frequency and the predominant destination into a call or frequency represent the location of the call or frequency, a tabulation of traffic routings may be used for net-building. For example, tabulations of routings relative to ABC and GHI reveal:

Call	*Routing*	*Volume*
Out of ABC	1234	75
	2345	43
	3456	10
	4567	3
Into ABC	1234	58
	2345	12
	4567	1
Out of GHI	1234	158
	2345	79
Into GHI	1234	101
	2345	39

The similarities in routings suggest their co-location though further proof is necessary for positive identification.

(1) Also useful is the system of omitting routings on local traffic. Calls of the same station will demonstrate similar relay routing lists

REF ID:A584482

with the station's own routing rather low in the tabulation. Book messages can be used as explained in paragraph 50*b* (2) (*b*).

(2) A somewhat different use of routings is in the inferring of links which have not been heard. For example, the routing 1234–6789 is noted on a message from A to B. 1234 has been located at C, but no link from C to A has been observed. Nevertheless, there must be some connection either through another station or directly. It is difficult to determine which is the case; a check of file time against intercept time will sometimes serve to indicate whether, considering the precedence of the message and the usual time lapses on the net, how many prior relays are likely. A tentative diagram could be drawn as shown in figure 39.

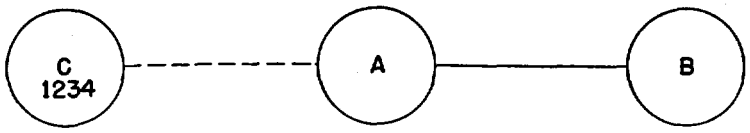


Figure 39.

e. Cryptographic Systems. On locally originated traffic, distinctive cryptographic systems, such as one-time pads, may be used to tie calls or frequencies together. As in the application of all message center features to radio stations, care must be taken to avoid relayed traffic.

f. Chatter. Items of chatter furnish important clues to net-building. In many instances, outright statements are made which relate one link to another. For example, ABC tells DEF, "At 1100 I have schedule with GHI." At 1100, JKL is heard calling GHI, indicating the identity of JKL and ABC. Mention of operators names or other local personalities also assist by the appearance of the same personality on different links.

g. Relayed Traffic. The study of relayed traffic presents one of the most important techniques in net-building. As messages pass from station to station, the net automatically reconstructs itself since it is only necessary to trace the messages' path to determine the structure. The chief caution to be observed is the possibility of having missed a relay, but this can generally be checked by differencing the intercept times. For example, a message is transmitted from ABC to DEF and an hour later from GHI to JKL. The diagram in figure 40 may then be drawn.

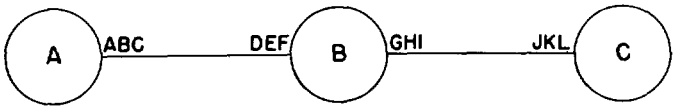


Figure 40.

REF ID:A684682

The possibility of the picture being as shown in figure 41, however,

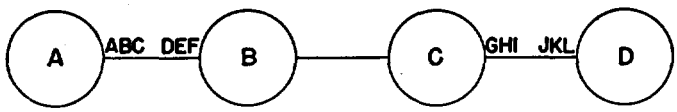


Figure 41.

does exist, but the short time lapse of one hour makes it unlikely that the extra relay took place. Of course, what constitutes a short time lapse is dependent on the habitual lapses and on the precedence of the messages under study.

h. Collateral Information. Direction-finding is an important technique and, when the radio system is highly secure, may furnish the chief method of net building. Decode material, captured documents, prisoner-of-war reports, when available, should also be used to the fullest extent.

56. Location of Stations

The geographic location of stations is the third step to be performed in the reconstruction of the radio system.

a. Identification with a Known Element. Identification with a known element is one of the chief means of locating the station. For instance, the tying-in of a station to an identified routing number will place the station. Similarly, calls, frequencies, serial ranges, and cryptographic systems which have been matched to locations may serve this purpose. The techniques involved can be derived from those discussed in this section and in section II. A validity should be attached to each station identification dependent on the weight of the identifying evidence.

b. Chatter. Chatter often furnishes identifications through operator carelessness. Clues to locations, such as mentions of weather, local conditions, and similar items, should be carefully appraised.

c. Direction-Finding. Direction-finding is here listed separately because of its importance in the locating of stations. Often it is the only means available. This is particularly true in low-echelon nets where movement is liable to be frequent and where message externals are held to a minimum. It may sometimes be necessary to utilize a knowledge of order of battle, geography, and military strategy in connection with direction-finding. Bearings will usually give a general area, larger or smaller according to the distance from the target and the accuracy of the bearings, but seldom will pin-point a location. However, inference as to the most likely location within narrow limits is permissible provided it is backed with sound reasoning.

d. Collateral Material. Order of battle information, decode

REF ID:A58489

material, captured documents, and similar items are often of great value in placing stations. For example, a division headquarters, whose radio station has been identified, moves to a new location. This new location is revealed by other sources. It may then be assumed that the headquarters radio station is also at this point.

57. Unit Identifications

a. The last step in the reconstruction of the radio system is the imposition of the order of battle. The order of battle underlies the entire net organization and each radio station must be identified with the units which it serves. In the high echelons, the nets are usually composed of large fixed installations which serve a number of units in the vicinity. Generally, however, there will be one major unit which the station represents. In the lower echelons, on the other hand, there will be a close correlation between unit and station. This is partially the result of the customary policy of manning large installations with an independent signal organization, while in the lower echelons the signal sections operate as an integral part of the unit.

b. The techniques of matching units with stations are only outlined below since it is felt that the preceding discussion sets the pattern of reasoning.

(1) *Identification with a known element.* This involves such items as call sign or frequency patterns which may be distinctive for certain commands or echelons, serial number ranges, routing systems, cryptographic systems, and procedural characteristics.

(2) *Chatter.*

(3) *Order of battle.* Beside the usual method of identifying a unit with a location and a location with a station, it is sometimes possible to force identification. For example, the order of battle information given in figure 42 is known, and a net is reconstructed as illustrated in figure 43.

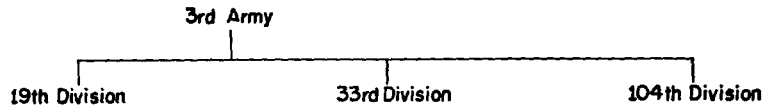


Figure 42.

It becomes apparent that station D is probably the 104th Division. In many cases, the echelon of command can be determined from the structure of the network and this may later lead to the identification with specific units. For example, the network shown in figure 44 is built.

REF ID: A384682

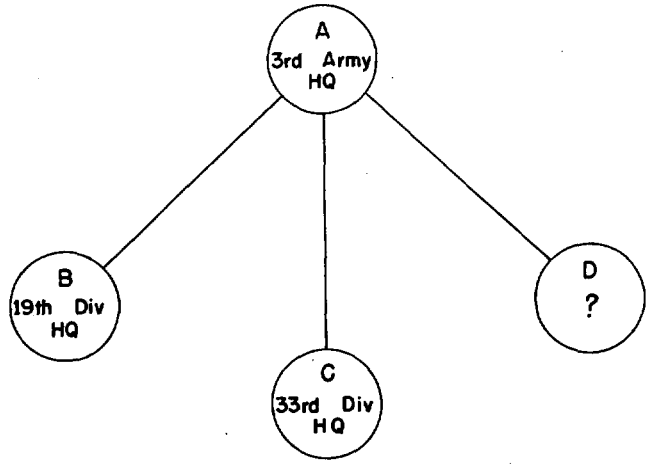


Figure 43.

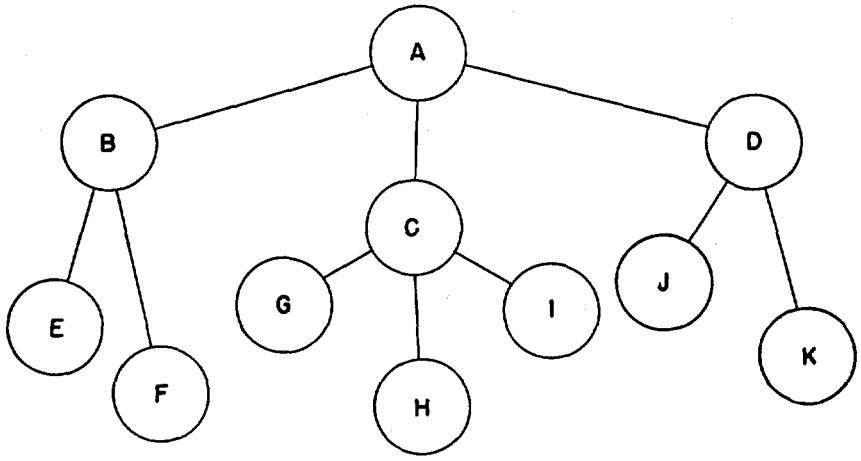


Figure 44.

It will be observed that A is probably the top headquarters, that B, C, and D are lower equivalent units, and that their out-stations are still further down the line. If anything is known of the order of battle in this area, it may be possible to match it with the net diagram.

(4) *Collateral material.*

58. Dummy Nets

Dummy nets and stations may be set up for the same purpose as that served by control traffic. Often when a headquarters is moved, a radio station is left operating at the former location to conceal the redeployment. Similarly, when it is desired to misdirect the

REF ID:A58489

enemy's attention, entire spurious nets may be employed to create the appearance of activity in an inactive area. The detection of such nets and stations may be difficult to accomplish and is largely dependent on the ability to uncover breaches of security resulting from careless chatter or ineptitude.

59. The Integrated Diagram

The immediate objective of the reconstruction of the nets is the production of the integrated network diagram which will serve as a

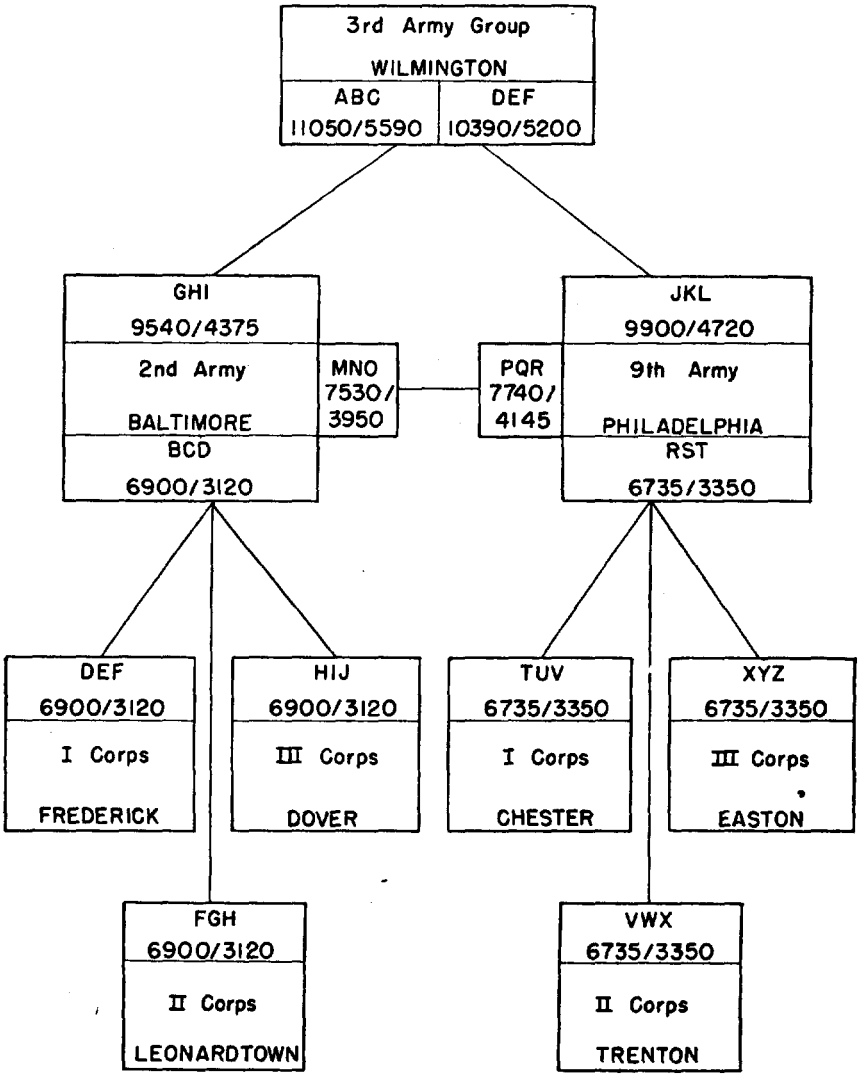


Figure 45.

REF ID: A5384682

backdrop for future study of the nets and for the production of intelligence and cryptanalytic aids. Because of the limitations of space and the complexities of some of the data, however, it is often not possible to include all the information necessary to a complete network picture in diagrammatic form. Therefore, certain basic diagrams may be produced either in schematic or geographic arrangement, and the omitted data supplied in accompanying charts. An example of such a basic diagram is given in figure 45. It will be noted that it contains order of battle units, locations, frequencies, and call signs, and is drawn schematically. Other data, which could be appended in chart form, might include range of serial numbers at each location or on each link, cryptographic systems used, and routings which appear or are identified with units or locations.

Section IV. METHODOLOGY OF ANALYSIS

60. Introduction

The preceding sections of this chapter dealt with the techniques of traffic analysis in regard to the study of radio operations and the reconstruction of the nets. In order to perform this analysis and achieve these ends, the proper machinery for processing raw material must be employed. This section is concerned with this machinery, and includes the processing of the chatter logs and the maintenance of appropriate files. The methods and forms outlined are only suggestive of the possibilities and changes should be made as necessary to meet individual situations.

61. Intercept Operator's Log

a. The raw material of traffic analysis is the chatter log. This is a complete record of the transmission as it is copied by the intercept operator and includes both traffic and chatter. An example of a portion of such a log follows (procedure is Q signals and international):

ABC	(2765 kcs) VVVVVVVVVV	
	DEF DEF DEF de ABC ABC ABC VVV QSV K	2133Z
DEF	(3152 kcs) VVVVVVVVVV	
	VVVVVVVVVVV ABC ABC ABC de DEF DEF	
	DEF VVVVV K	2135Z
ABC	V's QSA ? QSA ? K	2138Z
DEF	QSA4 QSA4 QSA? K	2139Z
ABC	QSA4 QTC 2 OP	
	QTC2 OP K	2140Z
DEF	QRV QRV K	2141Z

REF ID:A58489

ABC	QTC QTC	
	NR695 OP GR14 121541 BT	
	1904 2391 6025 8034 1709	
	6123 8051 6843 2967 1035	
	4114 EEEEEEEEE 4104 5281 7399	2144Z
DEF	3? 3?	
ABC	7399 1211 BT QSL? QSL? K	2145Z
DEF	R	2145Z
ABC	AS5 AS5 K	2146Z
DEF	OK OK OK	
	SAW TOM IN TOWN LAST NITE	2148Z
ABC	WHERE WAS HE GNG?	2149Z
DEF	31 Div They lost 2 ops in raid	2151Z
ABC	TOO BD AS AS	2151Z
ABC	QTC QTC QRV? K	2155Z
DEF	QRV QRV QRV K	2156Z

b. The important items of this chatter log must be extracted and recorded. The usual method to accomplish this is the use of the intercept operator's log on which is entered the significant features of the transmission as they occur. A sample log based on the above chatter is shown in figure 46.

c. The log is the basic analysis recording. Once it has been completed it should not be necessary, except in rare instances, to go back to the chatter logs. Consequently, considerable care should go into its preparation. It should contain all the data required for analysis and for the compilation of files.

62. Files

The contents of files are largely determined by the particular problem. It will generally be found advantageous, however, to maintain files based on the following:

a. Frequency. A master-frequency file containing a record of all frequencies, the time and date when first heard, associated frequencies, location, calls if reasonably fixed, net, etc.

b. Call Signs. A master call-sign file containing a record of all calls, date when first heard, associated calls, location, frequencies, net, etc. The information on the card here or in the frequency file may be kept to a minimum if one is adequately cross-indexed to the other.

c. Serial Numbers. Where practicable, files should be maintained on the various serial number ranges together with related features.

d. Routing System. A file of routing code groups with proofs of identifications.

e. Cryptographic Systems. A file of all cryptographic systems, how they can be identified, by whom used, for what purpose, and net.

REF ID: A584682

Date_____

GMT	Freq.	C/S	No.	Serial	Origin	Dest.	Remarks
2133	3152	ABC					V's DEF de ABC
2135	2765	DEF					V's ABC de DEF
2138		ABC					QSA?
2139		DEF					QSA4
2140		ABC					QSA4
2144		ABC	695				OP GR14 121541 1904 . . . . 7399 1211
2148		DEF					SAW TOM IN TOWN LAST NITE
2149		ABC					WHERE WAS HE GNG?
2151		DEF					31 DIV. THEY LOST 2 OPs IN RAID

Figure 46. Sample intercept operator's log.

In the case of distinctive features, such as one-time pads, files should also be maintained for each pad together with other pertinent data.

f. PROCEDURE. A file on the meanings of noninternational procedure signs and signals.

g. PERSONALITIES. All personalities appearing in traffic or chatter together with the connection in which they were mentioned. Personalities derived from other sources can be added to this file but they should be so marked.

h. ORDER OF BATTLE. All order of battle identifications originating with traffic analysis plus that available from other sources.

i. NET, GROUP, AND LINK. A running record should be kept on each net or, where necessary, group or link which will act as a history and also include the basic data for station identifications as to location and order of battle.

REF ID:A58489

j. COLLATERAL MATERIALS. Appropriate files should be maintained for all collateral materials. In the case of direction-finding, information must be organized to suit the particular problem. Files, as required, should also be maintained on solved messages, captured documents, and similar items.

REF ID: A5384682

CHAPTER 4

APPLICATIONS OF TRAFFIC ANALYSIS

Section I. INTERCEPT OPERATIONS

63. Introduction

Traffic analysis plays an important role in the direction of intercept. It furnishes the basic information necessary to the intercept station for the performance of its mission; its requirements are coordinated with those of intelligence and cryptanalysis for the purpose of prescribing cover and fixing priorities; and it checks certain phases of station performance. Depending on the nature of the organization, traffic analysis may also be responsible for the specific determination of missions for the intercept stations.

64. Intercept Information

a. The elementary function of traffic analysis in intercept control is the providing of basic net data to the stations. This includes chiefly frequencies, calls, schedules, and station locations. Other information may be added as required. A sample listing follows:

Locations	*Frequencies*	*Call signs*	*Schedules*
Hoboken Zanesville	10500/5030 11350/6125	ABC DEF	0100; 0300; 0500; 0700; 1700; 2100
Hoboken Overton	10500/5030 16400/7625	ABC GHI	even hours
Overton Zanesville	16400/7625 11350/6125	GHI DEF	0900; 1100; 1300; 1900; 2300
Star Lake Ticonderoga	8430/4175 8600/4235	MNO PQR	0700; 0900; 1800; 2200;
Star Lake Buffalo	8430/4175 7550/3965	MNO STU	0400; 0600; 1900

b. Technical reports may also be furnished to the intercept station. Certain items are fundamental. For instance, in the case of a changing-call system, the elements of the system are necessary for con-

REF ID:A58489

tinuity in cover; the same is true of frequency systems, procedure signs and signals, etc. In the determination of the type of materials to be forwarded, a balance must be struck between the requirements of security and those of intercept. All information is of use to the station, but some is more essential. Thus, it should be the policy to furnish everything that is available, consonant with security. Even much data which appear irrelevant may be of value if only to indicate to the intercept station the importance placed upon its product.

65. Types of Coverage

If it were possible to cover all desired nets or links twenty-four hours a day, there would be few problems to intercept control. Because of limited facilities and operators, however, such is not the case, and it becomes necessary to draw a number of fine distinctions with regard to types of cover and the order of priorities. Thus, cover may be divided into several types according to the purpose it serves.

a. FULL TIME. This is the highest of all intercept priorities (except in special instances) and consists of complete daily monitoring of each assigned net or link on all known schedules. The number of missions included in the full time classification should be sufficiently small to permit the monitoring station to cover all of them with ease so that, unless something entirely unforeseen intervenes, intercept is assured. Full time cover should never tax the maximum facilities and personnel of the station except under unusual circumstances, since positions should be reversed for other types of cover. These positions may, of course, be switched to full time if absolutely necessary.

b. SAMPLING. Nets or links which cannot be covered on full time may be put on sampling. The net is checked at regular intervals, the intercept station listening to several missions each day and rotating them until all have been monitored when the list repeats. This method yields some traffic on a variety of nets and enables the traffic analyst to keep abreast of current developments.

c. SEARCH. This mission consists of a search through a frequency band or bands for new transmitters and for changes of wave lengths. In the early stages of traffic analysis, this mission is of first importance since it serves to outline what is on the air.

d. PRELIMINARY CHECK. New frequencies discovered on search must be followed up to ascertain their genuineness and desirability. To accomplish this, they are placed on preliminary check, actually an extension of the search mission. If proved valuable, these links are then transferred to either full time or sampling.

e. SPECIAL CHECK. Special check is the complete cover of a net or link for a limited period of time. The check may serve a variety of

RECD 10 : AD684682

purposes such as whether the link is still active, or what its schedules are, or whether it can be heard at the monitoring station.

66. Factors in Assignment

The main considerations in the assignment of missions to specific intercept stations are:

a. The ability of the station to hear at the times desired.

b. The availability of positions and personnel for coverage at the station.

c. The most economic use of the station's time. This involves the problem of the common transmitter which makes it desirable to assign an entire net, where possible, to one station. For example, in the net shown in figure 47 both the A–B and A–C link should be assigned

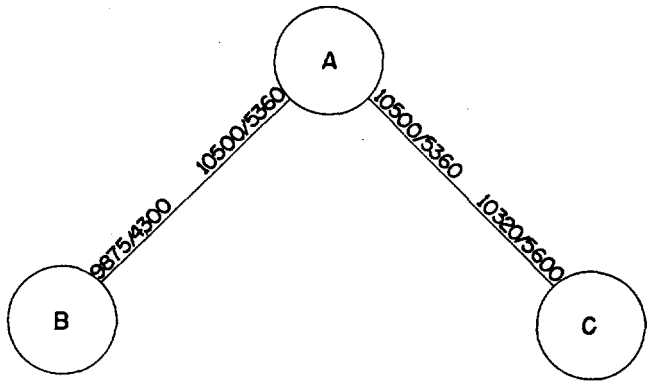


Figure 47.

to the same station, for by covering A throughout the day the activities of the net can be followed. On the other hand, if the intercept unit can hear A and B, but not C, it would become necessary to split the assignment. A second consideration in following this procedure is that the common transmitter arrangements tend to spread out until they include more links than can be handled at a single station. For example, C works another station on 10320/5600, B does likewise on 9875/4300, etc. Thus, a compromise assignment must often be devised.

d. The communication facilities between the station and the central analysis agency. In many instances, it is of prime importance that traffic arrive at a central point for analysis within the shortest possible time. For this reason assignments are sometimes made to the station which, though unable to provide the best cover, can forward the traffic the fastest.

REF ID: A584682

67. Factors in Priorities

The determination of priorities rests on the threefold requirements of intelligence, cryptanalysis, and traffic analysis. The traffic analysis needs are:

a. INTELLIGENCE. Traffic analysis, on its own, contributes to the intelligence picture and consequently is interested in seeing to it that the nets which yield the major portion of traffic analysis intelligence are adequately covered.

b. ANALYSIS OF RADIO OPERATIONS. In the study of certain elements of radio operations, intensive cover may be found valuable for limited periods of time, for example, the defining of schedules on a given net. Special check may be used to this end.

c. NET RECONSTRUCTION. Traffic analysis must maintain an up-to-date picture of all radio nets for the benefit of intercept control personnel regardless of the needs of intelligence and cryptanalysis (because those needs may change from time to time), and information must be available to permit the immediate assumption of coverage. In the reconstruction of nets of little current significance, or where the significance is unknown, special check is useful. Where nets have already been reconstructed and it is merely desired to watch them for changes, sampling cover is satisfactory.

68. Interpretation of Requirements

Besides making its own demands on intercept, traffic analysis frequently interprets the requirements of intelligence and cryptanalysis in terms of links and nets. For example, intelligence expresses interest in a given area; traffic analysis knows what links or nets to monitor in order to blanket the area. Or cryptanalysis wants more traffic in a given system, a certain routine message, or a type of isolog; traffic analysis knows what nets or links carry large portions of this traffic.

69. Station Performance

a. In order to insure proper performance by the intercept station and to check on the fitness of the assignment, coverage results are continually evaluated.

b. If a serial number, relative to the sending station, is available, it may be analyzed for missed traffic. Forms can be devised for the simple maintenance of this data which, in turn, can be obtained from the intercept operator's log. Other features, such as message center serials, may also be employed to check for missed traffic though care must be exercised in making use of them. Incidentally, there is a tendency to place emphasis on the volume of traffic copied at a station as a gauge of its efficiency. This attitude is to be discouraged since

REF ID: A384682

it is often necessary to monitor nets or links which yield little traffic, but do carry cryptographic systems of great cryptanalytic or intelligence value, or possess useful traffic analysis features.

Section II. APPLICATIONS TO CRYPTANALYSIS

70. Introduction

a. The relationship between traffic analysis and cryptanalysis is not easily defined. Often an arbitrary line must be drawn between them when it is desired to keep the functions separate, but it will be found necessary, whatever the distinctions made, for the cryptanalyst to be grounded in traffic analysis and the traffic analyst in cryptanalysis. This arises from the basic concept of traffic analysis and cryptanalysis as closely related processes with traffic analysis furnishing the frame of reference within which cryptanalysis is performed. The material supplied by traffic analysis falls into four main categories:

(1) General background information.
(2) Crib messages.
(3) Isologs.
(4) Chatter.

b. It should be borne in mind by the traffic analyst that the requirements of the cryptanalyst vary according to the stage of solution. At times, for example, an isolog may be of great value, at other times it may be of no use at all, and at still others it may be of potential use pending the development of the problem. Therefore the traffic analyst should gear his production in this field to the needs of cryptanalysis.

71. General Background Information

Traffic analysis furnishes a large amount of routine information relative to communication features which assist the cryptanalyst. Some of the main items are—

a. Routings. The knowledge of the origin and destination of traffic is fundamental.

b. Identification of Systems. Traffic analysis contributes to the identification of cryptographic systems where discriminants do not form an obvious guide and assists in the sorting of traffic into homogeneous groups.

c. Use of Systems. Through discovering the use of systems, and any peculiarities relative to it, traffic analysis aids the cryptanalytic processes. Specific applications, of course, depend on the nature of the system and the externals available.

72. The Crib Message

a. DEFINITION. When it is possible to assume portions of the underlying plain text through the recognition of external characteristics, a message may be termed a crib message. Crib messages may be divided into two main groups.

(1) Messages which display a direct external-internal relationship, as the correlation of an internal signature with the external originator.

(2) Messages which are proforma reports. These arise out of the command function which necessitates the rendering of reports both up and down channel. They are usually formalized to insure completeness and thus present several portions of predictable plain text. Reports are of two types: those periodically filed which are called routines, and those which are forwarded as the situation requires.

b. IDENTIFICATION OF CRIB MESSAGES. (1) *Use of originator or destination.* If traffic contains internal addresses or signatures, they may be assumed by a knowledge of order of battle in relation to the message routings. Thus, messages originating at Dallas, known to be the location of the 14th Division, may contain the "14th Division", its commanding officer, or one of its subordinate units in the signature position. The possibility of several units at a location should not be overlooked.

(2) *Use of serial number range.* The serial number range may be tied to an internal originator, and the signature on all traffic in the series may be predicted.

(3) *Use of other features.* In the study of internal originators and addresses, other features, such as cryptographic system, relationships between preamble originators and destinations, etc., should be correlated with the above. For example, a specific originator may be defined by a combination of routing origin, serial range, and cryptographic system.

(4) *Use of external patterns.* In the case of report messages, these can often be distinguished by the characteristics of the traffic which chiefly include—

(*a*) *Destinations.* Because the report is regularly rendered to specific people, the destinations will furnish one peculiarity of the message. If order of battle is known, the relationship between the originator and the destinations may be explained and it may even be found possible to identify the nature of the report. When the routine pattern has been established, the order of battle must be watched for changes which will result in alterations of the pattern.

Note. Crib messages bear a very direct relationship to the military situation and the order of battle since they are, particularly in the report type, instrument of the command process. Thus, a detailed knowledge of enemy dispositions and movements is essential to the study of crib traffic.

REF ID: A3846B2

(*b*) *Cryptographic system.* Reports usually pass in the same system. But, where a change does take place and it can be recognized, the crib may assist in a solution of the new system.

(*c*) *Serial number range.* Because the same unit generally originates the same report, characteristic serial number ranges may be of value.

(*d*) *File date and time.* Reports which are routine in nature often exhibit a periodicity in the file date and time. For example, a ten-day report will be filed every tenth day, or a daily report as of 1700 will usually carry a file time after 1700 of that day.

(*e*) *Message length.* Because of the stereotyped nature of a report, the group count may show some consistency. In many cases, however, the length will be determined by the amount of information to be filled in, so while the message length acts as a guide, lack of regularity in this respect does not rule out the possibility of a genuine crib message existing.

(5) *Use of solved messages.* The reading of messages often produces crib traffic not previously suspected. This traffic should be studied and its characteristics noted to aid in future solution. Furthermore, it may be assumed that, if one unit originates a report, the same report is required of all other similar units. A check with order of battle will reveal the location of these other units and the specific traffic can be studied. For instance, a report may be observed from an oil depot to headquarters. This suggests that other oil depots also originate a similar report. These depots are then located and their traffic examined for the proper external characteristics as indicated on the decode.

73. The Isolog

a. DEFINITION. An isolog exists where the underlying plain text is encrypted in two different systems. There are many types of isologs depending on the nature of the cryptographic system, and it is hardly possible in this text to explore all the likely variations. Isologs arise from the cryptonets which, in turn, bear a close relationship to the order of battle. They are caused in three main ways:

(1) *The relay isolog.* When a message is relayed from one cryptonet to another, an isolog is likely. In figure 48, a message passed from A to C is reenciphered at B who holds both systems I and II. This type of isolog is usually formed by traffic passing up and down channels where reencipherment is necessary into simpler and simpler systems, the more forward the unit.

(2) *The book-message isolog.* Messages which are to be sent to a number of recipients in different cryptonets must be enciphered in different systems. In figure 48, for instance, if B wants to send the same message to A and C, the appropriate system is used for each.

REF ID:A58489

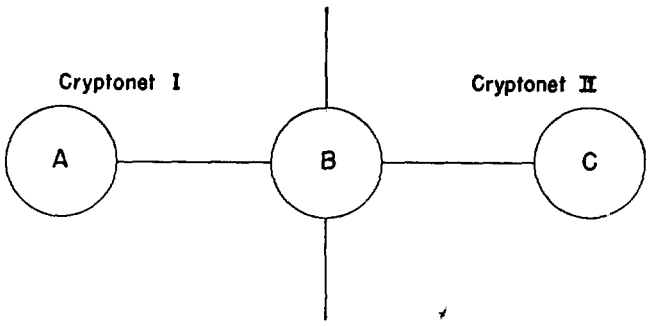


Figure 48.

(3) *Cryptographic error.* At times the code clerk will encipher a message in the wrong system. This will be refused by the receiver and the originator will reencipher in the correct system, yielding an isolog.

b. Identification of Isologs. (1) *Mechanical approach.* Isologs may be found by sorting traffic by originator and then looking for similar group counts and file dates and times. Where the two systems involved are not radically different in makeup, group counts should be close. Likewise, file dates and times, under most circumstances, will be similar.

(2) *Use of cryptonets.* A knowledge of cryptonets often simplifies the search for isologs. Certain locations, because they are in several nets, will be predisposed to the transmitting of this material. For instance, in the group of cryptonets shown in figure 49, the logical

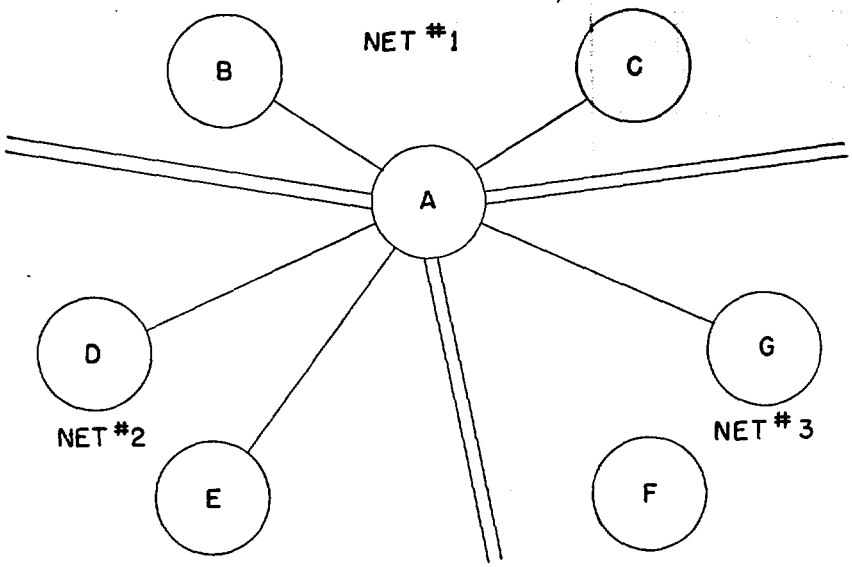


Figure 49.

REF ID:A5384682

traffic to study for isologs would be messages received and transmitted by station A. Order of battle changes should be carefully followed for the cryptonets are formed by units, not radio stations, and the movement of a unit often means that a new location must be taken into account.

(3) *Use of refused traffic.* When messages are originally sent in the wrong system they will be refused or serviced, sometimes in the clear. This is a signal to watch for a retransmission of the traffic in its correct version. For this reason alone, it is important for the traffic analyst to be thoroughly familiar with procedure and the methods of servicing both encrypted and plain traffic.

74. Chatter

The study of chatter occasionally produces information of cryptanalytic value. Some of this material may be simply a discussion in the clear of cryptographic features by the radio operators. In other instances, the derivation of information may require some analysis.

Section III. APPLICATIONS TO INTELLIGENCE

75. Introduction

a. It is one of the chief objectives of traffic analysis to produce direct intelligence. Seldom will this be "pure" traffic analysis intelligence, but rather it will represent the fusing of traffic analysis data with material from other sources. In some cases, traffic analysis will furnish the initial indication; in others it will act as confirming evidence. The ability of traffic analysis to contribute to order of battle is based on the necessity for communication between military units and the fact that these communications are expressive of the enemy's dispositions and intentions.

b. The problem breaks down into three parts—

(1) Determination of order of battle relationships.
(2) Determination of movement.
(3) Identification of units.

76. Determination of Order of Battle Relationships

a. NET STRUCTURE. The net structure is one of the chief keys to the study of order of battle relationships. Methods of utilizing this element are covered in paragraph 57.

b. CONTACT RELATIONSHIPS. (1) *Traffic associations.* A study of the traffic contacts of any one point gives some indication of the nature and the echelon of the unit since every message passed implies a relationship between the sender and the recipient. In order to use

REF ID:A58489

this technique, some of the factors must be identified and the general principles of the enemy order of battle known. For example, if the following set of contacts are recorded over a period of time, and B, C, and D are all air transport units, it is likely that A is also—

Location A

To B	43 messages
To C	29 messages
To D	12 messages
From B	38 messages
From C	15 messages
From D	3 messages

Of course, other factors must be considered and these may alter the conclusion. In some orders of battle, for instance, certain of the air transport units may come under the command of an Army unit and A may represent this Hq. Thus, hasty interpretations relative to traffic associations cannot be made, and the use of all available collateral material is necessary. It may be noted, for example, that certain types of traffic associations are characteristic of units at divisional level. These associations may involve heavy traffic with Army Hq., somewhat lighter traffic with Army group, and a little traffic with characteristic points in the homeland. Similar patterns of other locations may indicate the presence of a division. There are so many variations to this type of analysis, and it is so dependent on the order of battle concerned, that it is not possible to develop the problem completely here, but the analyst's ingenuity should suggest the many applications.

(2) *Book messages.* Book messages are of particular interest because it is likely that some relationship exists between the various recipients which causes them to receive the same message. Some inferences can be made if something is known of any of the elements, such as the originator, a few of the recipients, or the use of the cryptographic system. A message, for example, passes from A to B, C, and D. A is an Army Hq., and B and C have been identified as divisional locations. Then it is probable that D is the third division of the Army. On the other hand, if the cryptographic system involved is one used by water transport units, it may be that D is included as a water transport unit which is handling the movement of some men for the two divisions.

c. Cryptographic Systems. If a cryptographic system is associated with a certain type of unit or with a definite unit and its subordinates, it will serve as an identification. For example, a system may be employed only by headquarters of Army or higher. Thus, every location sending in this system is probably Army or higher. Receiving in a system cannot be regarded as good evidence unless

REF ID:A58489

it happens in some volume, because of the possibility of a sender's error. To send in a system it must definitely be held, but receiving in it only implies that it is held. Systems restricted to Air Force, or supply, etc., may similarly be used to infer the nature of the unit at the location under study.

d. PATTERN OF SIGNAL FEATURES. These patterns may be of any type and concern almost any signal item. Three-letter calls, for instance, may only be assigned to Air Force units, or the manner of assignment may reflect the echelon of command. The same holds true for routing codes. Serial numbers which are 5-digit may be used by higher units, while 4-digit are reserved for division or below. Here again the possibilities must be developed to fit the individual case.

e. VOLUME OF TRAFFIC. The volume of traffic originated and received by any one point is indicative of its importance. Consideration, however, must be given to coverage facilities and assignments so that the traffic counts are not unduly weighted.

f. CHATTER. Security breaches involving units or clues to units occur occasionally, and chatter should be carefully scanned for them.

77. Determination of Movement

a. CHANGES IN NET STRUCTURE. It is apparent that most changes in net structure result from a more fundamental change in order of battle. Items to be noted include:

(1) Appearance of new stations on the net which often indicates the addition of a new unit.

(2) Disappearance of old stations which may mean the deactivation or move of an old unit.

(3) Moves of radio stations which usually denote the redeployment of the using unit. In moves of this sort, there is often a period of several days, between the closing of the old station and the opening of the new, when the unit will be off the air.

b. CHANGES IN CONTACT RELATIONSHIPS. (1) *Traffic Associations.* Any change in the traffic associations of a location should be carefully examined as it may indicate a resubordination or the move of a unit. For example, Army HQ at A regularly sends traffic to a division HQ at B. This contact later changes, A to C, indicating the move of Army HQ to C or else the division to a different Army if A continues to show the characteristics of an Army Hq.

(2) *Book messages.* Changes in the pattern of recipients of book messages indicate underlying order of battle changes. This is particularly applicable in the case of routine traffic where a distinguishable message passes regularly to several locations. If, for instance, a routine situation report sent daily from A to B, C, and D, changes to B, C, and E, it may be assumed that the unit at D has shifted to E.

c. CHANGES IN TRAFFIC VOLUMES. Changes in the traffic volumes

REF ID:A58489

handled at a point indicate some sort of activity though other techniques must be employed to determine the nature of the activity. In order to watch for changes, a standard of traffic volume into and out of each location is established as normal. Any rises or drops suggest changes in the situation. For example, a location handling an average of three or four messages per day suddenly jumps to 50. It is apparent that units are moving in the vicinity, that preparations are under way for a move, or that it has assumed a more important role. And the possibility that it may be caused by the use of control traffic for the purpose of deceiving the analyst should not be overlooked. As a corollary to this, changes in the volumes of precedence traffic, or in the usual file times, may also be of significance.

d. Moves of Serial Ranges. A message or signal center serial range, which is sufficiently distinctive, may be used as an indication of unit moves. For instance, an Army located at A is employing message center serials running 563–581 on the 10th. On the 12th, messages with serials 585–593 are observed originating at B, suggesting the Army's move to B.

e. Moves of Cryptographic Systems. Similar to the move of serial ranges, the move of a characteristic cryptographic system often signifies an order of battle change. A one-time pad, for instance, held only by a certain division and appearing on messages out of location A, suddenly is noted out of location B.

78. Identification of Units

The initial identification of units usually does not result from traffic analysis. Rather traffic analysis furnishes the means for following a unit about, once it has been identified. But, through the study of net, contact, and cryptographic associations (and the use of other signals features when applicable) it is often possible to define the nature and the echelon of a unit at a given location, and in some cases to name it. Chatter, also, may furnish the specific designations of units through breaches of security.

79. Conclusion

The traffic analysis techniques discussed in this manual require considerable study. It is difficult to cover a subject of this type, where so many individual bits and pieces must be fitted together, in text form since, in order to convey effectively the concept of traffic analysis, no one part should be presented before the other but rather the whole presented at once. For this reason, the text should be read and re-read. It is further to be noted that this manual is chiefly a theoretical text, that the field is still expanding, and that it is the task of the individual analyst to devise the applications best suited to his specific problems.

REF ID:A58489

APPENDIX

REFERENCES

FM 7–24	Communication in the Infantry Division.
FM 11–22	Signal Operations in the Corps and Army.
FM 17–70	Signal Communications for Armored Units.
FM 24–6	Radio Operators Manual, Army Ground Forces.
FM 24–10	Combined Radiotelegraph (W/T) Procedure.
FM 24–16	Signal Orders, Records and Reports.
FM 24–17	Signal Center and Message Center Procedure.
FM 24–18	Radio Communication.
TM 1–465	Air-Ground Communication.
TM 11–454	The Radio Operator.
TM 11–455	Radio Fundamentals.
TM 11–462	Signal Corps Reference Data.
TM 11–484	Elementary Military Cryptography.
TM 11–485	Advanced Military Cryptography.
JANAP 122	Joint Communication Instructions—Part II—Security.
JANAP 127	Joint Communication Instructions—Part VII—Joint Tape Relay Procedures.
JANAP 143	Communication Security.

U. S. GOVERNMENT PRINTING OFFICE : 0—1950