~~TOP SECRET~~

NATIONAL SECURITY AGENCY

MECHANIZATION IN SUPPORT OF COMINT PHASE II

WARNING

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

TOP SECRET CONTROL NUMBER 5300678
COPY 5 OF 53 COPIES
PAGE ______ OF ______ PAGES

~~TOP SECRET~~

3

MECHANIZATION IN SUPPORT OF COMINT

PHASE II

Editors

H. F. De Francesco	R/D
D. L. Hogan	R/D

Report Committee

W. A. Blankinship	R/D
H. F. De Francesco	R/D
D. L. Hogan	R/D
R. A. Leibler	R/D
A. J. Levenson	PROD

Directed by

A. B. Clark	R/D
J. J. Eachus	R/D

PREFACE

This report contains the results of the second phase of the study "Mechanization in Support of COMINT". It is a somewhat detailed statement of what is being done at the present time, and attempts to point out the weaknesses of that effort. Phase Three will comprise suggestions as to what can be done to eliminate these weaknesses. Readers of this document are invited to contribute suggestions for inclusion therein. The fourth and final phase will be a considered selection of these proposals, intended to form an integrated Research and Development program.

Chapter A was written by H. F. De Francesco and reviewed by O. R. Kirby. Chapter B was written by A. H. Housman and E. Fergusson. Mr. O. R. Kirby also reviewed this chapter. W. A. Blankinship wrote the chapter on Traffic Analysis; it was refereed by H. L. Conley. The chapter on Weather was written by H. F. De Francesco and reviewed by A. W. Kellond and L. Schlauch. D. L. Hogan and H. F. De Francesco compiled the chapter on Plain Language which was checked by P. A. O'Sullivan. The chapter on Machine Ciphers was prepared under the general supervision of A. J. Levenson. The section on Hagelin was written by J. E. Bates, Selector Machines by T. A. Evans and M. H. Budenback, Sturgeon by G. F. Stahly, Introduction and Section on Enigma by A. J. Levenson.

The chapter on Hand Systems was written by R. A. Leibler. The final chapter was written by H. F. De Francesco and D. L. Hogan. It was edited by M. M. Mathews and A. B. Clark.

In addition, L. W. Tordella, H. H. Campaigne, A. B. Clark and J. J. Eachus read through selected chapters of this report and gave many valuable suggestions as to form and content.

Many others, whose names are not listed, have freely contributed both time and talent to the fact finding tasks and editing chores. To these people we are especially indebted.

TABLE OF CONTENTS

TABLE OF CCNTENTS (cont'd)

PL 86-36/50 USC 3605
EO 3.3(h)(2)

TABLE OF CONTENTS (cont'd)

TABLE OF CONTENTS (cont'd)

D WEATHER

E PLAIN LANGUAGE

PL 86-36/50 USC 3605
EO 3.3(h)(2)

TABLE OF CONTENTS (cont'd)

PL 86-36/50 USC 3605
EO 3.3(h)(2)

F MACHINE SYSTEMS

TABLE OF CONTENTS (cont'd)

TABLE OF CONTENTS (cont'd)

EO 3.3(h)(2)
PL 86-36/50 USC 3605

TABLE OF CONTENTS (cont'd)

G HAND SYSTEMS

TABLE OF CONTENTS (cont'd)

TABLE OF CONTENTS (cont'd)

A TRAFFIC COLLECTION ACTIVITY-I

I. INTRODUCTION

The starting point of NSA's COMINT activity is the collection of target countrys' communications Most communicators employ radio transmission; others employ messengers, etc. In what follows we shall discuss only the intercept of foreign radio communications and the problems associated with this operation. If the communications are not transmitted electrically, we usually are not able to intercept them.

In order to cover the communication links used by Russia, Poland, Communist China, and all other target nations of very high or low priority, we require a worldwide setup of intercept stations. Presently the United States has about 120 sources from which traffic is obtained. These sources range from intercept stations containing 100 or more positions (a position is a receiver and its associated equipment) to very small detachments which operate one or two receivers. Some intercept stations are located in very unusual spots around the world.

II. PROBLEMS OF COLLECTION

1. One of the problems of collection is to locate and intercept transmissions sent over temporary or newly established communication links. The program under which this problem is studied is called the General Search Program. Another problem is searching for and

identifying new and unusual types of transmissions. For this problem we utilize Technical Search facilities. We differentiate between there problems because there is a difference in our approach to them. New and unusual types of transmissions such as scatter and noise communications, are presently receiving little attention. The search for standard high frequency communications falls under the general search program which is PROD's responsibility. The search for new and unusual types of transmissions is part of the Technical Search program which is R/D's responsibility and which will be discussed in the next chapter. When we can intercept new and unusual signals, we usually try to set up an operational intercept program to collect worthwhile material.

We also have the problem of developing new equipment, new techniques, and new methods for intercept. We will touch on this problem and give a few examples in what follows, but as a matter of information we must point out that target nations sometimes surprise us with new and different signals about which we have little or no previous knowledge.

2. In order to have an effective intercept program, we must situate and assign our intercept facilities properly and supply them with the best equipment available. These axiomatic requirements are quite difficult to meet. For instance, we never seem to have enough intercept operators, stations, and equipment to cover all the targets on the air at any given time. We have to set up priorities of coverage whereby the most important targets are covered first.

We then cover as many of the less important targets as we can. The assignment of intercept stations to specific targets during specific periods of time is called "intercept control.

With reference to the problems of cryptanalysis and traffic analysis we find that the collection effort of the United States leaves much to be desired in terms of accuracy, quality of coverage, and the extension of the total amount of coverage.

There are some definite reasons why this happens and why we are not able to achieve the ultimate in intercept coverage. These reasons will now be discussed.

First of all we have definite limitations on the location of intercept sites. We would like to intercept all of the low-level communications emanating from the Moscow area. Unfortunately, we are not able to go to Russian territory and set up an intercept station to intercept this traffic. Nor are we able to operate a VHF voice intercept installation from an air field or from aircraft in the vicinity of Moscow. For all practical purposes we cannot locate in any part of Russia or within the satellite countries. Our only recourse is to pick locations as close to the target as possible and as much "in line" to the signal direction as possible. In most cases we intercept traffic under non-ideal conditions.

3. Next there are budgetary limitations which prevent us from having equipment and personnel sufficient in number and quality. The NSASAB conducted a study on the potential of COMINT to supply early

warning of an impending enemy attack. This board recognized the importance of having high quality intercept operators, analysts, etc. These are the people on whom we must rely to obtain the material from which COMINT is derived. Most of our operators are military personnel many of whom serve for a temporary period and then return to civilian life. The permanent military people also remain with us in the COMINT activity for a limited period of time and are then rotated. We will point out what is being done on this problem in the sequel.

4. We also have some administrative problems. These center on the lack of authority we have over field commanders, construction organizations, and others who have a say in the actual construction of intercept sites and equipment. We must work through a chain of command. During this procedure there is a great deal of time lost. Moreover, our requirements may not conform with the requirements of the services. As a result there is much time lost from the inception to the completion of required intercept facilities, wherever modifications, new sites, and equipments are necessary. When it is required that a specific communications link be intercepted, we would like to get there with the equipment and men as soon as possible. At present we are not able to modify existing sites or put up new sites within any short period of time.

5. Another problem is that of acquiring the technological "know how" to find, identify, and intercept new communication systems as they

EO 3.3(h)(2)
PL 86-36/50 USC 3605

come on the air, This means that we must employ, or retain under contract, the best talent in the communications field so that we might keep ahead of target countries and be prepared to cope with any communications system they may employ in the immediate future. In the past we were faced with the intercept of manual morse and hand-speed morse transmissions in the medium frequency band. Next we had the problem of radio-teletype. The result was that most of our effort was placed on intercept by means of standard radio receivers and teletype equipment. Presently the shift has been to higher frequency transmissions, the ranges being not only the 5 to 30 megacycle range but also the low to ultra-high frequency range. Here we require more modern types of intercept equipment. Recently, the Russians have employed a [redacted] multiplex transmission system. This is a [redacted] multiplex system with which the Russians can transmit on [redacted]. In addition they can [redacted] within a short period of time. A complicating cryptanalytic feature is that all channels are [redacted] while the transmission is on the air.

As a point of interest, Russia has very good North - South communication links. We are off to one side trying to pick up this type of transmission, and the results are not very heartening. We are having difficulties intercepting this material and then trying to produce usable page copy from it. Adding to the lack of directivity the fact that we are trying to intercept transmissions having a [redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

of about [redacted] one can readily see that we really need the best technological approach to this intercept problem in terms of equipment, personnel, and operating procedures.

Presently we are dealing with three different intercept operations, setups, and procedures. Each Armed Service has its own equipment, modes of operation, and setup procedures. Also, differences exist within each service; e.g., ASA stations intercepting hand-speed morse employ different equipment, setup procedures, and modes of operations. These differences must be minimized.

III. PRESENT AND FUTURE EFFORT

In the preceding paragraphs we have listed some of the major problems which face us. Now we shall discuss what we are doing to improve the present situation and what we intend to do in the future.

1. First of all we are starting a standardization program for intercept operation. This does not mean that we intend to make every intercept station look like every other intercept station. What we propose to do is to design every station so as to obtain maximum efficiency and effectiveness in the intercept activity and in the handling of raw material within that station. Within the Armed Services we wish to have uniformity among positions performing essentially the same functions. We do not specify that every service will employ a Collins HF receiver and use that receiver to the exclusion of all others. We

could have two or three standard types of receivers within the service to perform the same intercept mission, provided that these receivers have equivalent characteristics.

To accomplish the standardization needed we suggest a procedure as follows. First, we establish the types of transmissions with which we have to contend. These may be manual morse, voice and high-frequency transmissions, ultra-high frequency, voice and microwave type transmissions, teletype of various sorts, facsimile, or others. Then we must determine the type of equipment necessary to intercept these signals. Then we must specify how the equipment should be operated. In particular some questions to be answered are the following. How should the receiver be tuned? What recorders may be connected to the different type receivers? What is the best procedure for recording the intercept?

2. After we categorize the types of transmissions and the types of equipment best suited to intercept the transmissions, we then have to supply operational procedures and information to the intercept station. We must determine the number of people required to do a specific job, at a given intercept position at a given time.

Our attempt is to emphasize correct operation and production of accurate copy of desired targets rather than interception of large volumes of material. For instance, there may be a frequency range over which a target nation transmits extremely valuable information but does so infrequently. Here it might pay to guard this frequency range even though we obtain only several messages a month. Because of the value of the product, it might require two attendants to the position to obtain high quality intercept. Normally these two attendants might operate four positions. The results that come off the four positions might not be worth much, but too often the tendency in the field is to assign the two attendants to the four positions rather than to the one position. This is the tendency we are trying to overcome and it is one of the administrative problems facing us. We propose to prepare minimum standards for all of our major intercept operations. These standards will give the minimum requirements for satisfactory intercept in terms of equipment, personnel, and operating procedures. Stations will not operate below the minimum standards and most should operate above the standards.

3. We are also trying to keep ourselves fully informed on modifications to existing intercept sites and on the plans for new intercept sites. We intend to look at all plans for construction and modifications before they take place. We have some examples of intercept installations which were improperly modified or designed. In at least one station, for example, several antennas were actually cut off the transmission lines without affecting the operation of the station. In order to avoid these errors we need to review proposed plans to ascertain that the stations will meet the minimum requirements necessary for satisfactory operation. Moreover, we would like the stations to be flexible enough to cope with changing requirements on directivity, frequency

ge, etc., without being overequipped and overstaffed.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

4. The best way of illustrating the requirements placed on us is to discuss a few types of transmissions we have to intercept. About [redacted], the Russians started to employ [redacted] transmission which they had never used before. This increased the number of types of Russian transmissions we must be capable of intercepting. The Russians also employ [redacted] and others. We can usually intercept the single channel [redacted] transmissions using standard equipment. However, the requirements of [redacted] dictated that more information on the transmission had to be obtained. This required that something had to be added to the standard equipment. As an example we consider two Russian stations, A and B operating full duplex and employing start-stop teletype. Such a situation may be considered as equivalent to two send positions each employing an enciphering device and a teletype. Except for the frequencies used, the positions A and B are essentially identical. What we would like to obtain now is the time relationships in the messages passing between A and B. We definitely wish to pick up and record the time delays between the stops and restarts which occur during transmission. A may send to B for a length of time and then stop for one reason or another. During this pause, B might stop sending to A. Using standard start-stop equipment, we have no way of knowing when A or B is not sending. One requirement on intercept of this signal is that we record both sides of the duplex link

EO 3.3(h)(2)
PL 86-36/50 USC 3605

simultaneously. If the recording is equally good on both sides of the communications channel, and if time relationships are known, then a side by side character analysis will point out where "busts" occur. When this problem first arose we had no means of using on-line page printers in the field to give us exact time relationships for both channels of communications.

We now obtain time relationships by means of a tape recorder. What we use are dual-track magnetic tape recorders. This equipment simultaneously records the activity on both links of the channel and makes analysis much simpler.

5. A great deal of our efforts in this particular intercept problem is directed toward obtaining accurate copy. In some instances we employ the Central Processing System wherein the intercepted signal is analyzed and copied (usually from magnetic tape recordings) under controlled laboratory-like conditions. Originally this system was devised to satisfy the side by side presentation requirement on the copy of duplex signal. We employ a similar technique on Russian [redacted] Multiplex. This procedure is particularly useful where we are not able to set up demultiplexing equipment in the field and keep it properly maintained. Instead we record the multiplex signal on magnetic tape and then process it by means of the Central Processing System.

We have found that Central Processing is not adequate to meet mass production requirements. We cannot, for example, afford to

PL 86-36/50 USC 3605
EO 3.3(h)(2)

duplicate hour by hour in our central processing the time spent at stations in recording [redacted] transmissions. We are, therefore, embarking on an on-line printing program in the field, using model 28 teletype printers to produce page print directly from the intercepted signals. For simplex and [redacted] intercept, these printers are modified in such a way that they will produce page prints which retain the time relationship between channels and within each channel. This program will in time reduce the amount of central processing required at this headquarters.

We are trying to produce standardization procedures to back up operations in the field. These procedures should avoid some of the glaring errors that occur in the operation of field stations. We would like to find out if there is something wrong in a good percentage of stations, and if some stations are not carrying the load their equipment is capable of carrying.

6. A large variety of equipment is necessary to intercept any one type of transmission. For instance, we may be intercepting a double frequency shift transmission one side of which is a 6-channel multiplex system, the other side being a simple signal. To intercept this we require an antenna array to pick up the signal, a cable to lead the signal into a receiver, the receiver itself, a double frequency shift demodulator, demultiplexing equipment, printers and/or recorders and the various test and maintenance equipment. Not only does all

this equipment have to be kept in good repair, but it must be properly operated as stated before. One of our biggest problems is to keep competent people on the job at intercept sites. In order to alleviate the shortage of trained operators, we are setting up the Civilian Intercept Operator program. We have been authorized 100 civilian billets as a trial test. These are NSA billets which will be assigned to Army stations. We believe that by means of such a program we can develop and keep professional intercept operators.

To take care of some of the complicated technical problems of intercept, we have set up the Technical Search Mission. Possibly in time we may be able to handle ultra-high frequency microwave intercept and find answers to some of the other plaguing problems. We are enjoying a little success in some of these problems but much remains to be done. R/D is considering many of these problems as well as the problems discussed in the preceding paragraphs. The next chapter will contain some technical details concerning the equipment discussed here and gives some specific recommendations on how this equipment might be improved.

B TRAFFIC COLLECTION ACTIVITY-II

I. INTRODUCTION

1. The Traffic Collection Activity of NSA is defined, for the purposes of this paper, to be the collection of raw traffic in the field and the subsequent forwarding of this traffic to concentrating centers both overseas and in the U.S. The problem includes the reduction of the traffic to a form suitable for Traffic Analysis and Cryptanalysis, said reduction being effected at the intercept stations and/or the concentrating centers. The Traffic Collection Operation is described in Section II of this chapter.

2. Section III of this Chapter attempts to present a quantitative picture of the effectiveness of the Traffic Collection Activity. This evaluation is performed first on a technical basis on those elements of the intercept system which are common to each of the three basic intercept positions now being manned by NSA. For example, antennas, transmission lines, and multicouplers, are evaluated first as they are generally common to Morse, Radio Printer, and Radio Telephone intercept positions. This evaluation is performed in the light of developments which are technically feasible within the present state of the art. It is followed by an operational evaluation of each of three basic intercept systems. The latter is essentially an evaluation of the Traffic Collection effort on the basis of operational factors and measures the administrative effectiveness of the organization in terms of adequacy of personnel, of facilities [granting

technical adequacy of system components] and of coordinated planning in the collection of what is needed in a form in which it can be used efficiently. In the broadest sense, this is a partial evaluation of the overall effectiveness of the management of the COMINT effort First, criteria of effectiveness and definitions of the scale of measurement will be given. Second, although the scale of measurement is admittedly coarse, the effectiveness of collection will be measured in a number of key intercept categories, and attempts will be made roughly to assess the relative impact of the various effectiveness gradations on the overall effectiveness of the COMINT collection effort. Last, an example will be given to serve as a rough measure of the loss to NSA in material which must be discarded, or only partially exploited, because of the inability to handle the mass of certain types of material in the form in which it is now collected. Throughout, when fruitful inferences may be drawn, particular problems will be examined in relation to functional categories [ICR, etc.] or other significant factors.

3. The evaluation of the collection effort is performed with regard to the intercept of conventional communications signals below 30 mc, leaving the evaluation of non-conventional signals and communications signals over 30 mc to Chapter G.

4. Section IV of this chapter contains comments and recommendations.

II. GENERAI DESCRIPTION OF THE TRAFFIC COLLECTION OPERATION

1. The three types of intercept, which comprise almost all of the current traffic collection effort of NSA and the supporting cryptologic agencies, with the approximate percentage of the total collection effort which they represent are as follows: Morse Intercept (69 percent), Radio I rinter Intercept (23 percent), and Radio Telephone Intercept (8 percent), a fractional percentage of the total traffic collection effort is devoted to "special signals" e.g. facsimile and microwave signals. Some traffic is obtained by [redacted] means which are not within the cognizance of NSA and will not be discussed here.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

2. Before mentioning features of the collection process that may benefit from improved equipment or from mechanization of present manual processes, it is instructive to review the quantity and the nature of the traffic received.

Traffic is obtained in many forms. The most common form is hard copy [one to-six copies of each item]. There is some manuscript single copy material and an increasing amount of magnetic tape recordings. Undulator tape and clean punched or chadless teletype tape, microfilm and photostats are also received in large quantities. There is also a small amount of high precision disc recordings and other miscellaneous media.

3. While accurate quantitative measurements are not obtainable, a few figures will illustrate the magnitude of collection activities. More than two and one quarter million morse messages are received each month as page prints. Over two million non-morse messages are received, not counting intercept that is not distinguishable as message units. More than two thousand magnetic tape recordings of non-morse signals and nine thousand pounds of perforated tape that cannot be divided easily into message units are received. From non-U.S. sources; come about three hundred thousand messages each month. These are on microfilm, photostats, perforated tapes and other media.

4. The United States currently uses approximately 2115 intercept positions [operator and associated equipment] of various types. They are located mainly in military installations and in all parts of the world. Other sources are at best only partially under United States control and, in the main, are not subject to technical improvement as a result of our efforts.

5. The bulk of the raw material is received at NSA Headquarters by courier. There are about 37 tons of such material delivered each month. In addition, nearly 30 million groups a month are forwarded by teletype. They are largely duplication ot mail shipment and represent priority material for which bulk shipment constitutes a back up. Upon receipt, raw material is

routed according to whether it requires further processing to prepare page copy or merely sorting and distribution to analytical sections.

a. Generally speaking, magnetic tapes and punch tapes are processed at NSA Headquarters to produce page copy. In these operations, conventional communications equipment is used. Sometimes preliminary scanning of intercept logs or of text printed on the tapes is performed to minimize the amount of material to be listed. In all cases listing is at automatic or manual typewriter speeds [maximum 100 wpm].

b. Printed material is visually scanned and manually sorted and distributed by messenger to using organizations where additional classification and handling are frequently necessary prior to analytical processing. At least three copies of hard copy are normally required, one for exchange purpose, while others are used for Traffic Analysis and Cryptanalysis.

III. EVALUATION OF EFFECTIVENESS OF CURRENT OPERATIONS

1. Technical Evaluation of Elements Comprising Intercept Systems

a. Antennas

The majority of antennas employed in the medium frequency and high frequency bands at permanent and semi-permanent stations are full rhombics and non-resonant half-rhombics. An attempt is made to lay the antenna fields out along semi-circular arcs normal to the direction of target coverage; for diversity reception, 2 or more rosettes of rhombics are installed. Each individual antenna has a nominal power gain of approximately 12 to 16 db and provides frequency coverage over about a two to one frequency range. Standard antenna kits are available to the services for installation at intercept sites; thorough technical data is available describing the operating characteristics of these antennas. For example, a standard manual is available to all intercept stations describing different sizes of rhombics, with details on the suitability of each antenna in terms of target range, the db response as a function of frequency and from 4 to 22 mc, and the db response for vertical incident wave angles from 0 to 50 degrees.

For low frequency and medium frequency coverage, long wire (Beverage) antennas are installed, if physical conditions permit.

For mobile operations, a standard military antenna kit is available which does little more than provide a mass of wire to string out, wherever physical conditions permit, to try and capture as much energy as possible from the electro-magnetic field.

It is recognized, on purely technical grounds, that antennas superior to those antennas now being employed are available. For example, by modifying the terminating resistor on a full rhombic, the backward response of the antenna can be modified to the extent of knocking out the response in any specified backward direction. This could prove advantageous in reducing interference in some cases, but this technique is not known to have been employed at field stations. Similarly, the possibility of employing resonant antennas, in particular the commercially employed Vee-antennas in stacked arrays, on certain fixed frequency targets, has not been exploited.

A rather thorough study of the effectiveness of the antennas employed in the COMINT collection effort has recently been completed by the NSA TMB*. This study revealed that although the currently employed antenna systems may not be up to the level of modern developments, and recommended that R/D undertake a critical evaluation of the problem, by far the major problem was in effectively utilizing the facilities which are available. It was found that NSA, in making intercept assignments to a particular intercept station often did not use the available information on antenna facilities at that station. It was also found that the technical groups in the services, charged with designing antenna fields in fulfillment of NSA assigned missions often did not know enough about the intended mission assignments to properly design the antenna field. In one case, involving mission assignments to the Navy, it was found that the engineering personnel at the Bureau of Ships charged with the antenna design were not

*TMB - The Technical Management Board is composed of representatives from the Office of Comptroller, P/P, COM, R/D, C/SEC, and PROD in NSA and from the three Cryptologic agencies, ASA, NSG, and AFSS. This Board has been charged with the mission of developing good management practices and techniques in the operational and technical areas under the direction of the DIRECTOR, NSA.

adequately cleared to enable a proper description of the problem to be presented.

Steps are being taken to improve this situation yet much remains to be done. NSA (PROD) is making concerted effort to improve communications between the group assigning missions and the groups in the field attempting to fulfill these missions. In addition NSA (PROD) recently completed and distributed a publication "Antenna Handbook for Field Stations" NSA (R/D) has prepared a technical description of a study to be undertaken by an outside group, under contract, to perform a critical evaluation of the adequacy of currently employed antenna fields in terms of optimum performance, minimum size, etc.

b. Coupling Transformers

The effectiveness of currently employed coupling transformers between antennas and transmission line was also studied recently by the NSA Technical Management Board. The substance of this study was that existing coupling transformers did not adequately cover the frequency spectrum. It was found that coupling transformers for operation with Beverage antennas in the range 75 kc to 300 kc were satisfactory, but there were no coupling transformers for operating in the range 15 kc to 75 kc. Furthermore, it was found there were no transformers operating in the range 300 kc to 2 mc; finally, it was determined that the range of existing high frequency transformer (4-20 mc), used in profusion in the field, should be extended to cover the range 2-30 mc.

The following steps are being taken to remedy this situation: (1) a coupling transformer design has been found which appea rs to cover the range 15 kc to 75 kc; this transformer is being evaluated in R/D, (2) joint service military characteristics for a coupling transformer operating over the range 300 kc to 2 mc are being prepared by the Intercept Technical Committee of RADAC*, and (3) the Bureau of Ships, which was found to be developing an improved coupling transformer, has been asked to incorporate the joint cryptologic service agencies' requirements over the range 2 to 30 mc.

c. Transmission Lines

The effectiveness of currently employed transmission lines is another recent NSA Technical Management Board study. This study revealed that many stations were using open wire transmission lines with lengths ranging up to 3200 feet. Although the cost to install such a line is less than the cost of shielded co-axial cable, maintenance is a much more serious problem. It was reported in some cases that the open wire line was so long and in such disrepair that the rhombic antenna at the terminating end of the line could be shorted and the received signal strength in the operations building undisturbed.

Such situations as this were actually well known before the members of the Technical Management Board undertook their

*RADAC - The Research and Development Advisory Council advises the Director NSA on the programming, budgeting and implementing of R/D programs and the coordination of R/D requirements of the departments and agencies engaged in the National COMINT and COMSEC effort. This council is composed of the three Deputy Directors (R/D, PROD, and C/SEC), P/P, LOG, COMP, and S/ASST.

study. NSA (PROD) had attempted to remedy this particular situation by letters to the services recommending the use of co-axial line. The services in turn had acknowledged the advantages of co-axial line and had begun to take corrective steps, in certain cases. They in turn, however, ran into time delays in their own supporting groups due to such factors as the requirement to program for the funds to procure the co-axial cable in the succeeding fiscal year. Once the material was obtained and shipped to the intercept stations, additional delays were encountered in waiting for the engineering and construction groups to make the necessary installation. It is worth noting that such delays as this have been a major contributing factor to the fact that there has never been more than one case of a major antenna field change as a result of an NSA request.

In March 1954, NSA (PROD) made another attempt to improve the situation by issuing an NSA Regulation establishing a set of minimum standards for all intercept stations. For example, in the case of transmission lines, over the range 2-30 mc, shielded co-axial cable was made mandatory at all permanent and semi-permanent field stations. A maximum line attenuation of 6 db was permitted, thus limiting the length of the transmission line.

Unfortunately there has been little improvement as a result of this NSA Regulation. The reason for this lies chiefly in the fact that the services have considered these regulations to be in the form of recommendations and advice only and therefore not binding upon them. The services do not consider these regulations as authorative, basic guidance for the planning of intercept installations and for the determination of the adequacy of these installations, even though the regulations were issued as such.

NSA (PROD) has recognized the situation and is now preparing a paper for DIRNSA on this subject. This paper is being prepared in the form of a letter to the services, to be issued by DIRNSA, in which he declares his intent to use his authority under NSCID No. 9 as the responsible agent for all U.S. COMINT resources. NSA (PROD) is planning to ask the director to use this authority (a) to specify the standard which must be met for acceptable COMINT intercept operation and (b) to evaluate intercept facilities to insure that standards are being adhered to.

Should the suggestions offered to DIRNSA be acceptable, it is believed that great strides will have been made toward solving a major administrative problem.

d. Multicouplers

An evaluation of the effectiveness of radio frequency multicouplers has recently been completed by the Intercept Technical Committee of RADAC. It was determined that currently employed multicouplers fell considerably short of that which is technically available within the present state of the art. It was determined that the frequency coverage was inadequate, particularly below approximately 3 mc; the noise figures were on the average of 15 db, while 8-10 db is considered easily feasible; the generation of spurious responses due to intermodulation characteristics was found to be quite poor, it being estimated that these responses could generally be reduced by as much as 30 db.

The Intercept Technical Committee of RADAC is in the process of completing a set of joint military characteristics describing a multicoupler which is believed to reasonably well fulfill current and anticipated requirements. These military characteristics will serve as the basis for an R/D contract to develop this multicoupler. Past experience with the normal contract development-production schedule in NSA on an item as simple as this multicoupler indicates that 5 years will elapse from the time the military characteristics are agreed upon until the time production equipments will be in operation in the field in quantity. However, it is possible to reduce this period by 30 percent to 50 percent. To do so would require (a) streamlining the procedures associated with letting an R/D contract and (b) overlapping the development, service-test and production phases. This would naturally entail a certain element of risk, but by sharpening the organization, this risk could be minimized.

e. Receiving Equipment

A general study of the adequacy of radio receivers being used in intercept operations has just been completed by the NSA Technical Management Board. The substance of this study was that although certain VLF/LF and MF/HF receivers in use are obsolete and unsatisfactory for COMINT operations, there are other receivers covering the same frequency range which are available to the services and are generally satisfactory. A few small problems with regard to these latter equipments, such as the VLF receiver bandwidths being too narrow for optimum voice intelligibility and one of the h-f receivers not being as stable, by modern standards, as it could be were brought out. However, there are two new receivers about to become available in quantity to the services; one receiver, the R389, covers the range 15 kc to 500 kc and the other receiver, the R390, covers the range 500 kc to 30 mc. These receivers are expected to rectify the problems noted by the Technical Management Board study group and be satisfactory for normal intercept operations. It should be noted that the noise figures of these receivers is expected to vary from about 3 to 8 db across the frequency spectrum, which by modern design and production techniques is considered to be quite good. The dial stability, readability and overall receiver frequency stability of the receivers is truly outstanding. Although these receivers have yet to be employed extensively by the intercept services and it is always possible that unforeseen "bugs", especially of a maintenance nature may develop, high hopes are held for these equipments to satisfy the majority of the receiver intercept requirements over the range 15 kc to 30 mc.

As the result of a recent SIPB*study, it was determined that increased emphasis should be placed on the VLF portion of the spectrum in particular in the band from 3 to 15 kc. Although there are no military receivers covering this range, NSA (R/D) has developed an experimental model of such a receiver. A limited number of these equipments are being crash produced to fulfill these recently developed requirements. There are a number of technical deficiencies in this particular receiver and it is planned to contract for the development of an improved model during calender year 1955.

The services use a variety of diversity receiving systems, some designs dating back to over 20 years ago. The latest equipment to become available in quantity is the AN/FRR-28, a dual space diversity receiving system which gives satisfactory performance. However, it is reported that there have been numerous component failures, and although the causes have been minor in nature, a maintenance problem has resulted, nonetheless. A new dual diversity receiver is under development, the AN/FRR-23, which is yet to be technically and operationally evaluated.

*SIPB - The Special Intercept Problems Board is composed of representatives from PROD, P/P, R/D in NSA and from ASA, NSG, AFSS, and CIA. This Board is charged with the mission of studying special intercept problems and advising the Director of the conclusions and recommendations reached. Subsequent to his approval, the Board is responsible for coordinating actions with NSA and other cognizant governmental agencies implementing the recommendations.

NSA (R/D) has developed a dual diversity antenna switch which switches between antennas, but utilizes only one receiver. A thcoretical evaluation of this equipment shows it to be slightly inferior to a normal dual receiver diversity system. However, due to the simplicity of setting it in operation, it has been found in field research stations evaluations to be generally equal to or slightly better than more complicated diversity systems. Eight of these diversity switches are being fabricated for service tests by the cryptologic service agencies.

Recent investigations made in the field of diversity reception have shown that the existing diversity switching or combining units fail to take full advantage of all that diversity reception offers. One design of a dual diversity system shows an advantage of 3 db over the best of the more conventional systems. This 3 db advantage is not a constant with signal levels, however, and in fact decreases for signal levels greater or less than an optimum value. Just what this new approach would mean in statistical terms in reducing garble rates of intercepted traffic is now the subject of an NSA R/D contract with a local concern.

f. Recording Equipment

An evaluation of the adequacy of COMINT recording equipment has been the subject of an intensive study by the Intercept Technical Committee of RADAC over the past year. This study has recently been completed and reveals that the services have used a wide variety of commercial and military recording equipments to fulfill voice and signal intercept functions. These units have not given satisfactory service, primarily due to their high maintenance requirements, fragility, and physical size. In addition, no single unit was found to provide the requisite auxiliary functions needed in these services, and the variety of equipments in use has presented a standarization problem. On a recent trip by a member of the Intercept Facilities Division in NSA (PROD), it was found that at any one time almost 50 percent of the normally employed recording equipments were in the maintenance shops for repair.

An NSA R/D contract is about to be let for the development of a rugged low maintenance magnetic tape recorder-reproducer requiring minimum panel space and suitable for recording and transcribing voice signals in any language. The specifications for this equipment are based on a joint set of military characteristics prepared by NSA and the three cryptologic service agencies. Another set of joint military characteristics is under preparation calling for the development of a militarized magnetic tape recorder-reproducer capable of recording and reproducing facsimile and complex signals. Based on the development and production schedules of the past, the program will require 4 to 5 years for production models of both the Voice Recorder and the Signal Recorder to be in the field in quantity performing in fulfillment of the COMINT mission.

Looking ahead, it is apparent that some means for increasing the "packing factor" of information on tape would be of major benefit to the operation of the agency, not only from an economical viewpoint, but more important to reduce the bulk of material which must be handled. At the present time, NSA R/D is soliciting the interest of major commercial concerns interested in this problem. One concern has already put forth a reasonable technical proposal for increasing the packing factor by an order of magnitude. It must be emphasized that this work is a long range effort of a very basic, experimental nature. Based on past performance for research, development, and production, success would probably not be felt significantly in field operations in less than 8 years. By following streamlined procedures, in particular, by significantly overlapping research, development and service testing phases, this time may be cut by one-quarter to one-half.

g. Demultiplex Equipment

(1) Frequency Division Equipment

The vast majority of the frequency division multiplex signals being intercepted are known as "DFS" or "double frequency shift" signals. This type of signal is nothing more than a single carrier frequency, sharply shifted from one to another of four possible discrete frequencies. Each of these four discrete frequencies corresponds to one of the four possible states which can exist between two single channel "mark-space" signals operating independently. For example, take two ordinary single channel teletype transmissions, each comprised of sequences of marks (M) and spaces (S). If we let one teletype signal be represented by M_1 or S_1 and the other teletype signal represented by M_2 or S_2, then at any instant of time, four possible states exist, i.e. M_1 M_2, S_1 S_2, M_1 S_2, or S_1 M_2. Each of these states is then represented by one of the four discrete carrier frequencies mentioned originally.

There are two equipments utilized to demodulate this signal, one equipment operating from the intermediate-frequency (i-f) of a receiver, and the other equipment operating from the audio (a-f) output of a receiver (the beat frequency oscillator of the receiver being on). There are many more audio equipments than i-f equipments, and audio equipments possess an audio diversity switching system, prior to demodulation of the signal. Generally speaking, both equipments are satisfactory; however, very close scrutiny is being given the audio equipment, as it is being used to demodulate the Russian [redacted] Multiplex [redacted] Signal. This signal is one of the major technical problems which the Agency faces. NSA R/D has a contract for the evaluation of this equipment as a part of the whole [redacted] Multiplex intercept system evaluation.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

Recently, requirements have arisen to intercept certain single-side band signals containing multitone transmissions. To date commercial and/or military equipments have been found which after relatively minor modifications, have proved satisfactory in handling the cases which have arisen. However, this situation could be improved since some of the equipments pressed into service were "border-line" in the sense that extremely high maintenance standards must be met to keep quality of the intercepted traffic up to par. This technical problem is now being studied.

(2). Time Division Equipment

PL 86-36/50 USC 3605
EO 3.3(h)(2)

There are quite a variety of time division demultiplexing equipments in the field. There are "universal" demultiplexers, both electronic and electromechanical, capable of handling from 2 to 9 channels of time division multiplex traffic e.g. Model CXOF Universal Electronic Demultiplexer, and there are special purpose demultiplexers, both electronic and electromechanical, intended to specialize on a particular multiplex signal, e.g. Model AFSAV D-24 Two Channel Time Division Demultiplex Equipment. Generally speaking, the majority of these equipments have performed quite well. From time to time modifications to improve performance have been made. As an example, the "clock driving and synchronizing portion" of the Model CXOF Universal Electronic Demultiplexer is now being redesigned by NSA R/D to simplify the maintenance procedure. Recently, with regard to the Russian [redacted] Multiplex system, it was necessary to provide a modification to the Model CXOF demultiplexer to enable it to synchronize with this new signal. An equipment capable of taking a shorter band length is also required. At the present time, a special equipment to operate on the [redacted] Multiplex signal is under development. This is necessary because of the general limitations of the CXOF equipment for the GTP intercept problem. The main advantages of this new equipment over the Model CXOF will result from the fact that it is simpler equipment, tailored for only one signal, and hence the read out, a punched tape operated at high speeds, will be much more efficiently achieved. All this adds up to a smaller device which should be easier to maintain.

At a relatively low priority, projects are being undertaken in NSA R/D to reduce the size and complexity of demultiplex equipment by the use of transistors, bi-stable magnetic elements, and specially developed tubes for counting purposes.

h. Single Side Band

The single side band intercept problem has come belatedly to NSA. It is now the subject of a study by the Special Intercept Problems Board. It appears that the agency can fulfill its basic requirements with a recently developed militarized signal-side-band receiver, Model AN/FRR-41 to become available to the services in the near future. Until this militarized equipment actually does become available in the desired quantities, commercial equipments, electrically equivalent to the military equipment, can be put into service. Additional requirements, over and above those which the AN/FRR-41 fulfills, are expected to develop as a result of the Special Intercept Problems Board study. These requirements will likely be filled by the development of an improved equipment under the auspices of NSA.

i. Morse Operator Analysis (MOA)

Morse Operator Analysis (MOA) is a process of identifying manual key (morse code) operators by the characteristics of their hand-set transmissions, viz by their "fist" The process of operator identification has been studied for many years, and although several different analysis systems afforded a limited degree of success in World War II, the use of MOA techniques during peace time was not justified until the recently developed AFSAV D31 Morse Operator Analysis equipment became available. Heretofore, the task of measuring individual character elements on an ink tape recording and undertaking the process of averaging, computing, etc., was simply too laborious to interest those who would potentially benefit from this operation.

In May 1951, development of the AFSAV D31 Morse Operator Analyzer equipment was initiated in order to mechanize the particular analysis method which was widely employed at the end of World War II. This equipment photographically recorded the time distribution of dots, dashes and spaces on a Polaroid-Land Camera and similarly recorded the individual character formations on a 35mm. moving film. In the first model of this equipment, the data from the polaroid film recording was punched onto McBee Keysort Cards for mechanical selection of possible matches. Six of these equipments were fabricated, of which three were delivered to the cryptologic services for service testing, two were provided to CIA, and one was retained in NSA R/D for further evaluation.

Installation of these equipments in the field resulted in a renewed interest in Morse Operator Analysis by the services. However, use of the AFSAV D31 in large scale identifications of operators under service conditions indicated certain limitations inherent in the analysis system. When many operators had to be considered, the similarity between operators became increasingly apparant. Investigations of other classification systems by NSA (R/D) revealed the same basic limitations.. It was found that a "best-fit" method of card comparison, substituted for the McBee Keysort, increased the effectiveness of the AFSAV D31 by a factor of about seven under laboratory tests. As a result, an equipment, termed the AFSAV D69 Card Comparator was developed to operate in conjunction with the AFSAV D31 to enable mechanization of the improved analysis procedure.

At the present time, the AFSAV D31 equipments are in a service test status and the fabrication of AFSAV D69 Card Comparators to go with this equipment is nearly completed. Concurrently, NSA (R/D) is in the process of contracting for the services of a competent research group to study, evaluate, and develop improved methods and equipment for identifying manual key operators. It is recognized that an investigation of improved MOA techniques is basically a problem in the statistics of small samples, and it is intended that the study of the collection of data and reduction of data for MOA analysis be directed toward the use of machine techniques.

Whether any additional AFSAV D31/AFSAV D69 MOA equipments will be built, will be determined on the result of the service tests now underway. The study contract will not be completed in less than a year and the development and evaluating of improved MOA techniques in the field will very likely require an additional 2 years. If such work is carried out successfully, and Production equipments are required, an additional 2 years should be allowed for construction and distribution to the field; thus, it will be at least 5 years before any significant COMINT utilization will likely be made of MOA techniques. As pointed out before, by streamlining procedures, this time could be reduced by one to two years.

j. Radio Finger Printing (RFP)

Radio Finger Printing(RFP) is a process of identifying transmitting equipment by the inadvertant amplitude and frequency modulation characteristics usually present on any given transmitted carrier frequency. Basically, the operation consists of photographically recording, on a moving strip film, two traces which describe the amplitude and frequency deviations from the norm of the intercept signal.

From an analyst's standpoint, the problem of classification and cataloguing RFP data is difficult. Unfortunately, RFF analysis is more of an art than a science. The analysis operation is largely subjective and based on the individual classifier's interpretation of the evidence available to him. The currently used range of RFP characteristics is large, and their potential identifying value, whether used individually or in combination, varies within wide limits. For th's reason, RFP identification reports must be considered as graded statements of possibility or probability, the validities of which depends upon the number and nature of the characteristics involved and the amount of distortion (noise, multipath, interference, etc.) present in the individual records considered.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

In spite of the subjectiveness of the analysis procedure, it has been possible to build up a large library of catalogued quantitative data; this catalogue was employed on the [redacted] On this problem, RFP served in a relatively minor though valuable position as an aid in positively confirming Direction Finder and Traffic Analysis reports; howe·er, only six RFP equipments, out of a total of some 45 produced, were suitably located and available on a world wide basic to attack this problem; hence the net contribution from RFP was very small.

The equipment in use today represents a modernized version, circa 1950, of the original RFP equipment developed in 1940. A study has recently been completed on the efficiency of operation of the equipment now in the field. This study was based on a critical examination of 180 monthly equipment failure reports from 14 different stations, coupled with interviews of approximately fifty people who had served at outlying stations within the past 20 months. The study indicated that the equipment was reasonably well designed and was capable of performing much better than failure reports seemed to indicate. The equipments have been out of operation for maintenance a disproportinate percentage of the time, primarily due to poor training of the maintenance men assigned. Cases are recorded where technicians have required thirty-five hours to ascertain that a cathode ray tube was not functioning properly; on other cases, as long as five hours have been required to find that a rectifier tube was burned out. The nature of these failures has largely been such that redesign of the circuitry is not indicated.

In spite of the operationally developmental position of RFP, technical work has been undertaken in NSA (R/D) to improve the existing equipment. This work has taken two forms: (1) experimental work on a system to employ reusable magnetic tape in place of the one-time use of photographic film or paper, and (2) development of a system to remove some of the subjectiveness from the analysis procedure in classifying RFP data. On this later point, an RFP correlator has been developed which is fundamentally a simple digital

EO 3.3(h)(2)
PL 86-36/50 USC 3605

computer to average RFP data. [redacted]

k. Direction Finding (D/F)

The majority of the direction finding operations occur in the high frequency (2-30mc) range, where the bulk of the COMINT collection effort is applied. The equipments employed are pre- and early World War II designs which have begun to outlive their usefulness. They are obsolete, and maintenance is a problem. In addition, they are not capable of coping with the kind of targets which may be anticipated in a future war. This situation became clearly apparent in 1950 and possible courses of action were studied. The Director, NSA, delegated the problem of high frequency direction finder (HFDF) research and development to the Navy, to be accomplished on behalf of all the cryptologic service agencies.

The problem, as undertaken by the Navy has been stated as follows: "To meet anticipated operational requirements, it is required that the HFDF networks be able to determine the location of a distant radio transmitting source within a few miles, when its emissions consist of short and extremely short signals. It must do so as rapidly as practical. As a first step, it must be able to cope with signals which last just a few seconds. Ultimately, it must be able to cope with signals which last only a fraction of a second."

The Navy analyzed this problem and concluded that a fully adequate solution is difficult, expensive, and quite some time away. Accordingly, an interim solution was adopted, based on the use of potentially available equipments, and already developed techniques. The interim approach involves modification of present equipment, and procurement of new HFDF network control and target acquization equipment.

As a result of the Navy program, a new HFDF and network control equipment has been developed which incorporates all of the advances known to date. It is more sensitive, more accurate, and it is able to cope with signals of about 15 to 20 second duration. It is the best equipment which can be supplied now. Effective operation of this new HFDF to achieve its ultimate capabilities requires provision of ancillary equipment. These HFDF stations will be linked with semi-automatic secure teletype circuits to attain rapid operation, in response to the directions of the network control station. The most advanced type of conventional radio teletype equipment available has been selected.

The new type HFDF equipment and the associated control apparatus is now in production for the Navy and is expected to be delivered during the calendar year 1955. The Navy will receive sufficient quantities of this new equipment to replace all of the existing, outmoded HFDF equipment now installed both within and without the Continental USA. By mid-1956, all of this new equipment should be installed and operating. In the meantime, the Navy R/D program is continuing in the direction of increasing the sensitivity, accuracy and speed of operation of this new net by developing improved search receivers and channel watching equipment. These improved equipments are expected to reach the Navy field stations by 1957.

Unfortunately, the Army and Air Force cryptologic groups have lagged considerably behind the Navy in improving their D/F nets. These two services are still using the outmoded HFDF equipment which the Navy is now replacing and they have not ordered replacements. They are thus about 15 years behind the Navy, although there appears to be no reason why they can not relatively quickly close the gap.

Outside of the high frequency band (2-30mc), comparatively little work has been done since the end of World War II. NSA (R/D) is currently making a survey of all reported military and commercial research and development efforts in the direction finder field throughout the entire radio frequency spectrum. This task is not being carried on at a very high priority, although the part time services of a local consulting firm are under contract to accomplish the job. At the present time, a report on the modern state of direction finding is due in NSA (R/D) by June 1955. This report is intended to serve as the basis on which decisions can be reached on the research and development tasks which should be undertaken in support of the COMINT operation. As pointed out above, such research and development programs normally lead to fruition as field equipments many years after they commence; in the high frequency direction finding case, it is evident that great strides can be made by two of the three cryptologic groups based on the research and development work recently accomplished by the Navy.

1. Automatic Morse Translating Equipment

It has long been recognized that automatic high speed morse, which is now taken on an undulator inked tape recorder and visually read, could be reduced to hard copy without a morse code operator. Devices have been built in the past for recording the high speed transmissions on a magnetic tape recorder, then reproducing the signal at low speeds for either aural translation by an operator or machine translation by a relatively slow speed electric typewriter. Such devices were unacceptable in intercept operations not only because the equipments were large and cumbersome and required a slow speed reproduction of the traffic, but because an operator could more quickly and easily accomplish the job by visually scanning the undulator tape.

In the past few years, however, a device has been built in NSA which permits on-line processing of high speed automatic morse transmission. It is possible to punch paper tape on-line at speeds as high as 350 to 400 words per minute (wpm) and convert to hard copy on electromatic typewriters. Although the electromatic typewriter is limited to speeds of about 100 wpm, the flow of traffic to the typewriter often comes in spurts, averaging arouhd 100 wpm or less. Four of these new equipments have recently been completed and are about to be employed in service tests by the cryptologic services. It is anticipated that these equipments will be used primarily on those high speed automatic morse circuits where the percentage of legitimate traffic is high; on those circuits where most of the traffic is "trash" which can be quickly spotted by an operator scanning an inked tape recording, the manual method is expected to predominate. The extent to which the automatic morse translator can mechanize this intercept operation is one of the basic reasons for the service test of this equipment.

A study is being made in R/D of the applicability of the automatic morse translator to hand sent morse transmissions. Although the automatic equipment is capable of following average changes in speed of an automatic morse transmission, it is not adept at following a poorly sent hand-keyed transmission. This study is devoted to determining whether "classes" of hand sent transmissions possibly cannot be handled by different settings of the machine under close operator supervision. It has been argued that even if one morse intercept operator were required to constantly supervise 2 or more machines, this would proportionately cut down on the number of required morse intercept operators. The training of morse code intercept operators is a major COMINT problem, particularly to the Army Security Agency this could be of material benefit. Prospects for accomplishing much in R/D in the near future along the line of a simple machine for in the field translation of crudely sent hand-keyed morse transmissions are quite low.

m. [redacted] Positions

EO 3.3(h)(
PL 86-36/5

The intercept of [redacted] signals presents the most difficult of the traffic collection problems. Fundamentally, the reason is that the cryptanalyst must have the highest quality traffic with which to work. Although there are a number of distinctive [redacted] type signals, ranging from single channel synchronous teletype to the complex [redacted] multiplex, it is primarily with regard to the [redacted] multiplex signal that the greatest intercept problem has existed. The philosophy behind the intercept of this signal has been to make a recording in the field as close to the front-end of the receiving system as possible, thus demodulating the signal the least amount possible before recording. The record so made is then shipped to a central processing installation at NSA Headquarters for full demodulation and print-out of the hard copy. This procedure has been adopted because it is believed that the demodulating equipment will be under better control in a central processing installation than at a field station; furthermore, the cryptanalyst has available for his close inspection, if desired, the incompletely demodulated signal. It has been argued that if interference is present, this procedure may enable the cryptanalyst and the central processing team to work together in a much closer manner than would be feasible at a field station. Also central processing is the best interim procedure until demux equipment suitable for field use is developed. It will also be necessary to maintain a central processing facility to cope with future requirements.

The result of this philosophy has posed a very difficult technical problem to R/D, for the recording/reproducing operation on the partially undemodulated signal must now introduce less distortion than full demodulation in the field would produce. After considerable experience with this intercept problem, it now appears that control processing on [redacted] multiplex traffic is feasible provided maintenance standards on the equipment in the field are raised considerably beyond what would be normally required on a more conventional system. The standards are so high, in fact, that it has been proposed that special [redacted] Multiplex Maintenance teams be assigned overseas to provide maintenance on a routine basis. This proposal is now under study in the Agency. It is believed that the present system, when properly maintained and operated, is capable of producing traffic with garble rates of less than 1 percent on good signals.

EO 3.3(h)(2)
PL 86-36/50

NSA (R/D) has developed and is continuing work on a

EO 3.3(h)(2)
PL 86-36/50 USC 3605

large number of operating aids in connection with this problem. These include special tuning indicators to aid the operator in the field in tuning in the intercepted signal and holding it in tune. A garble rate indicator has been developed which measures the quality of the synchronizing channel in the multiplex signal in order to gauge the quality of the [redacted] traffic. A page copy print-out of the [redacted] traffic is desired by the cryptanalyst on a rather elaborate format, and a device to produce the material is under development and about to be delivered to the Central Processing group. A contractor is performing a thorough technical evaluation on the present system and proposing improvements.

There are a large number of miscellaneous items being worked on in R/D to improve the sensitivity, stability, and efficiency of this operation. However, operating under the present philosophy of central processing, it is believed that it will be at least 5 years before the extremely high standards for field maintenance can be lowered by the introduction of a superior system to the field. The philosophy of central processing itself, on the scale now employed and envisaged deserves close re-examination.

n. Intercept Sites

The selection of intercept sites is a difficult problem in which logistic/administrative factors must be considered in addition to the basic technical considerations. Needless to say, the selection

EO 3.3(h)(2)
PL 86-36/50 USC 36

of any given site usually represents a compromise between many opposing factors; once a site is selected, the assignment of missions also often represent a compromise between that which is technically desired and that which is administratively feasible. For example, the assignment of a complex intercept mission, such as against the Russian [redacted] Multiplex signal, may be made to a station poorly located in terms of the target signal, yet well staffed with a relatively strong operational group and possessing the necessary physical space to accept a large and complex intercept equipment.

The appropriate elements in NSA (PROD) keep a running account on the times that intercept of a given signal is obtained at a given intercept site. This account is graphically portrayed by plotting the day of the month on the abscissa of a chart and the hours of the day on the ordinate. The period of intercept then shows as a vertical bar, broken if the intercept was interrupted, for each day of the month. Compiling a large mass of these data provides the mission assigners with a considerable appreciation for the capability of intercepting given target areas from given intercept sites over a period of time.

It is very difficult to assess quantitatively the effectiveness of the present method of site selection and mission assignment. One receives the impression that those people engaged in this operation usually strike a reasonable balance between technical factors and administrative factors in making mission assignments. It is only in isolated cases that the operation obviously breaks down; then one is led to suspect that the system could be improved. A recent example is afforded by the assignment of a Russian [redacted] Multiplex Mission to an intercept station 90 degrees off the beam of the transmitted signal; in another similar case, the intercept station was 180 degrees off the beam. In some cases, such a poor technical assignment may be warranted on administrative grounds, and technically acceptable provided the intercepted copy is still usable. However, when dealing with special cases, such as [redacted] traffic, where the quality of traffic must be very high, then the evidence points to possibly improving the system.

PL 86-36/50 USC
EO 3.3(h)(2)

2. a. The operational evaluation definitions follows:

Excellent - Substantially garble free traffic, the kind analysts need to work most effectively against new crypto, call sign, address systems and so on.

Good - Fully exploitable against known systems, and permitting analysts to work at reduced effectiveness against new systems.

Fair - Can be used if system is completely exploitable but is useless in attacking new systems.

Poor - Generally not usable.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

Traffic will be called:

> "Nearly all" excellent, good to excellent, etc. if 90 percent or more falls in those categories,
>
> "Mostly" excellent, etc. if 80 percent to 90 percent falls in those categories.

Approximate figures will be given in other cases.

[redacted]

For Radioprinter, the criterion is [redacted] specifically the [redacted] station. Intercept reaching NSA is nearly all excellent. Although this excellence is partly due to a rigid field station screening program, the missing serials in traffic reaching NSA do not indicate an excessive discard percentage, and undoubtedly the screening helps catch troubles before they cause serious intercept loss. In any case, [redacted] provides a suitable criterion of excellence. However, the suitability of [redacted] as a criterion must be tempered by the following considerations.

1. [redacted] has a very limited cover assignment and only hears approximately 6 RCA links.

2. It is also a research station for T Department.

3. Their manning standards are considerably higher than NSA standards..

4. It is a unique unit, the only one of its kind based on geographical considerations, [redacted] organization, etc.

EO 3.3(h)(2)
PL 86-36/50 USC 3

There is no criterion available for radiotelephone.

What can be accomplished by the U.S. services is illustrated by the fact that about three stations, operated by two services are head and shoulders above the other U.S. service operated stations.

The factor(s) for cited shortcomings will be cited thus:

"Chiefly Responsible" - Correction of this factor would raise output quality more than halfway to "nearly all excellent"

"Largely Responsible" - Correction of both the Chiefly and the Largely (if any) responsible factors would certainly improve quality to "nearly all (90 percent) good to excellent".

"Partly Responsible" - Correction of these and the above would generally bring "nearly all (90 percent) excellent" results.

"Slightly Responsible" - Correction of these would generally serve to increase the degree of excellence.

Factors will be listed in decreasing order of importance, and evidence will be cited for each.

b. Morse

Sixty-nine percent of the currently manned U.S. intercept positions are assigned to Morse, both Manual and Automatic. Most of these positions are Manual, and most of the Manual positions are on Military Tactical* (Army, Navy, Air) assignments; in fact a single

*For the purposes of this paper, the various communications intercepted for NSA have been divided into 6 functional categories:

1. International Commercial Radio (ICR) - Message traffic is handled by common carriers.

2. National Commercial Radio (NCR) - Internal message traffic is carried by common carriers or some state owned monopoly.

3. Government Communications Services - (GCS) - Message traffic is handled by internal nets opeated by such government agencies as Border Guards, Secret Police and the like.

4. Military Tactical (MT) - "Low level" traffic is handled to and from tactical military units; Army, Navy and Air Force are included in this category. Exploitation of this traffic yields "order of Battle" information, and its intercept is generally considered a Close Support function.

5. Military Strategic (MS) - Potentially "High Level" traffic is carried on circuits connecting higher headquarters.

6. Support Communications (SC) - Broadcast and point-to-point communications, such as weather nets and broadcasts, and navigational aids and services are handled by various agencies, usually governmental.

problem - [redacted] - accounting for nearly half the Manual Morse take, represents more than one quarter of the total intercept groupage entering NSA from all sources on all problems (excepting [redacted] plain text). Most of the high speed Automatic Morse is on International Commercial radio (ICR) and [redacted] [redacted] although great quantities of ICR are intercepted, only a small percentage, mostly [redacted] cipher, is transcribed and sent to NSA: full coverage may be ordered on [redacted] circuits. (NOTE: Low speed automatic morse, such as [redacted] nets, are intercepted the same as manual morse.)

PL 86-36/50 US
EO 3.3(h)(2)

(1) Manual Morse

Under normal conditions, and depending on service, assignment and station, Manual Morse intercept runs from nearly all good to excellent to as low as 70 percent good to excellent. The 1

[redacted]

breaking into the new system to one half the above figure, i.e., if previous take had been 70 percent good to excellent, only 35 percent was now usable; this drop was caused by operators copying the wrong cases as well as other factors arising from a changed situation. However, appreciable recovery was noted in the first month after the change. When a situation changes the percentage cut tends to be deeper with the weaker stations, hence, in a crisis, the value of a station may be substantially lower than the normal condition figures would seem to indicate. Factors involved in station and/or service shortcomings include:

(a) Chiefly Responsible - Operators

Evidenced by:

1. Changes in efficiency when major personnel rotations occur.
2. Drop in efficiency in new situations in which technical factors remain unchanged.

(b) Partly Responsible - Particular Problem Assigned

Evidenced by:

1. Experience shows certain problems to be more difficult than others because of poorer available sites and other factors.

(c) Partly Responsible - Plant Facilities, intercept Assignments and other administrative factors.

Evidenced by:

1. Such items as 12 mcs. rhombic antennas assigned

to 3 and 4 mcs. problems; failure to lay out antenna fields according to problems; failure of NSA to give adequate information before station construction and similar factors.

(d) Slightly Responsible - Technical inadequacy of available equipment and Techniques.

Evidenced by: 1. As described in Technical Evaluation Section Above.

It will be noted that the major factors susceptible of improvement are administrative in nature, and in regard to each of these the cognizant PROD element is now actively pursuing remedial measures.

PL 86-36/50 USC
EO 3.3(h)(2)

(2) Automatic (High Speed) Morse

Automatic Morse intercept is generally satisfactory, running nearly all excellent on International Commercial Radio (ICR) and only a little poorer (largely because of signal quality) on [redacted] radio. Automatic Morse is generally transmitted at speeds as high as circuit conditions permit (up to 250 words per minute). Since high speed Automatic Morse generally appears on main line circuits, good operating practices are the rule and favor the interceptor, who also profits from the fact that good copy can be readily distinguished from bad, even when enciphered. The receiving and recording equipment used is standard, and easily and quickly adjustable, and the operation of a position is relatively simple to learn; hence, the stringent need for skilled operators, so apparent in the Manual Morse problem, does not exist here. There are no special quality improvement measures required in this problem. However, manpower requirement may eventually be eased by the NSA (R/D) developed Morse translator (AFSAV D48) now undergoing service test. Otherwise, Automatic Morse intercept will naturally profit from the improved Plant Facilities which should follow current PROD efforts; slight improvements may be expected to accrue from such technical improvements as those described in the Technical Evaluation Section above.

c. Radioprinter

Although only 23 percent (483) of the U.S. intercept positions are currently assigned to Radioprinters, clear text and enciphered on both single channel and multiplexes, approximately 2,285,000 messages are intercepted per month. Most of this take is Russian and, since about 80 percent of the circuit time intercepted is plain text, it will be seen tha [redacted]. represents NSA's largest single traffic source; however, the volume alone does not justify conclusions as to the relative value of this

PL 86-36/50 USC 3605
EO 3.3(h)(2)

EO 3.3(h)(2)
PL 86-36/50 USC 3

traffic compared with other traffic on a group by group basis. Most of this plain text is [redacted] and it should be noted that more and more of these links are going to [redacted] single channel and 2 channel Baudot multiplex account for significant groupages, while other government communication services contribute some single channel; military and government communication service messages are generally enciphered, with more military [redacted] appearing. Both single channel and multiplexed radioprinter are now common on [redacted] and are covered the same as [redacted] Automatic Morse, with about the same degree of success.

(1) <u>Russian Service Radioprinter</u> [redacted]

<u>Most of this traffic is</u> [redacted] Under normal conditions, only about two thirds of the take is good to excellent. This relatively poor showing stems largely from the fact that our operators are not equal to the greater demands made by the interception of military traffic as against [redacted] in part, unfamiliarity with the language, sloppy transmissions (variable teleprinter speeds, frequency shifts, etc.), high percentage

* There are many literal enciphering systems which are used to prepare messages for transmission by any means; the term [redacted] generally refers to a particular enciphering system used with automatic printing equipments.

of enciphered traffic and frequently poor signals are contributing causes. The intercept of [redacted] is even more demanding, but an evaluation of the intercept belongs elsewhere in this paper. (See Chapter VII) Factors involved in these shortcomings include:

(a) Chiefly responsible - Personnel - Operators and Maintenance Men.

Evidenced by:

1. Changes in efficiency when major personnel rotations occur.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

2. Drop in efficiency in new situations in which changes in technical factors should not produce such striking effects - example: appearance of [redacted] using unorthodox shifts and printer speeds;

(b) Largely Responsible - Plant Facilities and other administrative factors.

Evidenced by:

1. Such items as lack of suitable diversity antennas; failure of NSA to give adequate information before station construction and similar factors.

(b^1) Another factor largely responsible for poor traffic if the lack of a suitable variable frequency shift converter.

(c) Slightly Responsible - Technical Inadequacy of available equipment and techniques.

Evidenced by: 1. As described in Technical Evaluation Section above.

It will be noted that major factors susceptible of improvement are administrative in nature, and in regard to each of these the cognizant PROD element is now actively pursuing remedial measures. The NSA (PROD) on line Model 28 program will certainly be a definite and in the production of more accurate intercept. With a direct page copy, the operator will be able to monitor his link more easily and will know when his traffic is garbled and can take the proper steps to re-tune, etc. With the on-line program we also achieve standardization with the three services. Training for the Model 28 maintenance is available at Teletype Corporation and will also be included in the services' training program, thereby producing more qualified maintenance personnel.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

(2) [redacted] ntercept is

PL 86-36/50 USC 3
EO 3.3(h)(2)

mostly good to excellent; an evaluation of the intercept of the [redacted] Single Channel and [redacted] Multiplex [redacted] may be found in Chapter VII, while the research and development aspects of the [redacted] Multiplex are covered in the Technical Evaluation Section above. Some of the plain text is on single channel radio-printers, but the great bulk of the main line traffic is carried on Baudot time division multiplex systems, carrying as many as nine 30 word per minute channels on a single multiplex. However, the Baudot system is obsolescent, and its rapid disappearance is foreseen. The relatively good quality of this plain text intercept is due to the operator's ability to evaluate his results by looking at the output text, to the relatively high and consistent standards of Civil operation (as compared to the military) and similar factors. It must also be borne in mind that higher garble rates are permissible in plain text traffic. Factors involved in existing shortcomings include:

(a) Chiefly Responsible - Personnel - Operators
Maintenance Men

Evidence by: 1. Previous evaluations of unusable traffic.

(b) Largely Responsible - Plant Facilities and other Administrative factors

Evidenced By: 1. Lack of suitable diversity antennas; failure of NSA to give adequate information before station construction and similar factors.

It will be noted that the major factors susceptible of improvement are administrative in nature, and in regard to each of these the cognizant PROD element is now actively pursuing remedial measures.

d. Radiotelephone

About 8 percent of the currently manned U.S. intercept positions is assigned to radiotelephone, chiefly Military Tactical. Evaluated on an overall basis, this radiotelephone intercept is mostly good to excellent, and would be nearly all good to excellent if it were not for technical handicaps suffered by the operator-linguists. Provided the operator properly adjusts his receiver and recorder, nearly all the intercept is good to excellent; unfortunately however, that traffic which is garbled in transcription, in spite of having been properly received and recorded, is often garbled because of unusual words or non-routine comments which would have special intelligence value and, therefore, the overall results - intelligence wise - fall somewhat below what would seem to be indicated by the "mostly good to excellent" evaluation. Factors involved in these shortcomings are:

(1) Chiefly Responsible - Operators.

Evidenced by: a. Equipment maladjustments and linguistic failures.

(2) Largely Responsible - Inadequate Recorders

Evidenced by: a. Lack of convenience items required for efficient transcription of voice intercept.

(3) Partly Responsible - Particular problem assigned.

Evidenced by: a. Experience shows certain problems to be more difficult than other because of language, poorer available sites and other factors.

(4) Partly Responsible - Plant Facilities and other administrative factors.

Evidenced by: a. Such items as inadequate antennas and transmission lines: failure of NSA to give adequate information before station construction and similar factors.

(5) Slightly Responsible - Technical inadequacy of available equipment and techniques, excepting recorders.

Evidenced by: a. As described in Technical Evaluation Section above.

It will be noted that, while two major factors are administrative in nature, inadequate recording equipment is an important factor. Cognizant PROD elements are now actively pursuing measures to alleviate the administrative factors, while current programs to improve recorders are discussed in the Technical Evaluation Section above.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

e. <u>Qualifying Statement</u>

In assaying the overall U.S. intercept performance in terms of the above Operational Evaluation, two points must be kept in view

(1) The criteria used - as [redacted] generally equal or better these standards, but so do various other intercept services (some from nations with installations technically inferior to those of the U.S.) as evidenced by traffic obtained through special sources. Even allowing that special sources usually bring in traffic these other groups are peculiarly located or adapted to intercept, one must weight heavily the fact that four to five years - in one case, ten years - combined

training and experience is required before a man may become an operator in these intercept services.

(2) The evaluations given have referred entirely to the quality of the intercept in the form it is transcribed at the intercept position, without regard to the ultimate suitability of that form. Thus, in the vitally important [redacted] problem, currently accounting for more than a quarter of NSA's total take (excluding [redacted] plain text), only 40 percent is given Basic Processing and the remainder is ignored on a geographical area basis; as the groupage rises, this figure will decline. The reason is that, so long as present techniques are the best available, this Agency cannot - and does not plan to try - to process all Manual Morse because the typewritten copy made by intercept operators is fundamentally not adapted to methods which permit full exploitation with reasonable economy of personnel.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

IV. COMMENTS AND RECOMMENDATIONS

1. The analysis of our traffic collection operation indicates that much can be done toward improving the effort. The area in which must improvement can be made is considered to be chiefly administrative, i.e. (1) inadequate training of operator and maintenance personnel by the cryptologic services, and (2) lack of definitive authority to enforce standardization programs on equipment, plant layout, etc. The importance of the personnel problem

has been well recognized in the Agency and positive corrective actions are being considered and undertaken. NSA (PROD) has recently sponsored 100 civilian intercept billets in the Army Security Agency under a pilot program which is intended to develop a corps of permanent, highly skilled personnel for field operations. The problem of lack of definitive authority to enforce standardization programs is also recognized. Efforts are being made with NSA (PROD) to build up a group which will establish minimum standards for acceptable COMINT intercept operations and insure adherency to these standards by conducting evaluations of intercept facilities.

While considerable improvement of the traffic collection activity could be achieved by proper administration of field facilities along the lines indicated, there is also much that could be done by way of implementing an NSA program to devise better, simpler and durable equipment for field use.

2. Research and development on more advanced intercept techniques will naturally aid in the Traffic Collection operation. The contracted research-development-production schedule, as it is currently being followed, requires approximately 5 years for full realization in the field. This period of time is considered to be too long, but there is much that could be done to cut this by 30 percent to 50 percent by streamlining current procedures. Research, development and production, when undertaken locally within NSA, is

realized in the field in a fraction of the time which the contract program requires, as is to be expected. However, there is room for improving this operation as well, particulary by speeding up the process for component procurement.

It is to be noted that the area for which the most significant improvement in performance may be expected from R/D is less in connection with the pure intercept of traffic itself than it is with the reduction of this traffic to a form more suitable for traffic analysis and cryptanalysis. This point is elaborated upon later in this report.

3. It is believed that a closer tie between NSA (R/D) and NSA (PROD) would aid in establishing an R/D program which would be more closely tailored to the current and anticipated needs of the Agency. In the past, this connection has been attempted primarily by bringing NSA (PROD) personnel into NSA (R/D) on various committees and panels engaged in planning operations. It is believed that an advantage would be gained by having some of the senior NSA (R/D) personnel engaged in planning R/D operations, spend more time gaining a "first hand" appreciation for the problems in PROD.

C TRAFFIC ANALYSIS

I. INTRODUCTION

Traffic analysis is defined as the study of radio communication by all means short of cryptanalysis of message text (either deciphering or decoding) so as to produce unique intelligence, to assist cryptanalysis, to direct intercept, and to influence our own communication security practices. However, the intelligence derived from message texts can have such a strong influence on the interpretation of T/A data that the functions of T/A and C/A are not entirely divorced in NSA. Thus the office charged with T/A responsibility is also charged with exploiting all easily readable cryptographic systems, and is designated the Office of Exploitation. For this reason we shall discuss T/A from the point of view of the Office of Exploitation rather than per se.

II. DESCRIPTION OF T/A DATA

The principal data contributing to the end product of traffic analysis are contents of Bona Fide Messages, practice traffic, call signs, message headings, message routing, and transmitter identification and location. All these items are interrelated, each contributing to the other as well as to the end product. We shall attempt here to indicate briefly the manner in which they contribute intelligence:

1. Call Signs. Call Signs indicate lines of communication, which in turn indicate organizational structure. In general the more complicated a call sign system is, the more productive it is of intelligence once it is broken. The complicated system must be more highly integrated in order to be intelligible. This greater unity usually reflects more completely the organizational structure of the activity employing the system.

2. Message Heading. The format of the message heading tends to identify the country and service sending the message. In some cases it can even identify the originator and his geographical location. In addition, the method of serializing messages can give indications as to routing, traffic volumes, etc.

3. Operator Chatter. Chatter contributes miscellaneous bits of information about equipment, operating schedules, personalities, local conditions, message routing, message content, encryption of call signs, etc. Chatter may also serve to link or associate encrypted messages, thereby yielding valuable clues to the cryptanalyst.

4. Practice Traffic. Since a given set of practice messages is usually assigned to a small set of users, identification of a practice message tends to identify the transmitting station. In the case of an unknown call sign system, practice traffic can be a valuable tool in maintaining call sign continuity. A study of the methods by which practice traffic is generated frequently gives clues as to the method of

encipherment of bona fide messages. Practice traffic recognition is also very essential in order that Practice Messages may be culled out from bona fide traffic when other indications are either unknown or missing.

5. Bona Fide Messages. (plain text and decryptions) These provide direct intelligence on any and all subjects in a rather obvious manner.

III. DESCRIPTION OF T/A PROCESSES

1. Analysis of foreign communications actually begins at the point of intercept. The Morse intercept operator or the R/T transcriber produces in the form of page copy has best interpretation of what he hears on the air. In addition he includes certain parenthetic notes on the hard copy which show such information as frequency on which the transmission was heard, readability, time, case number, and any other comments which he feels may be of assistance in later analysis. In the case of other types of transmissions, the intercept operator cannot contribute these latter comments, and due to lack of knowledge of the language, can seldom make any statements as to readability. (This is a serious problem as our radioprinter intercept is notoriously poor. It is believed that in many cases improper tuning is responsible for this and that a greater familiarity with the language would provide the operator with criteria by which better copy could be produced.)

2. In the cases for which page copy is produced at the intercept station (manual morse and some R/T) an elementary semi-processing of the traffic takes place at the intercept station. The extent of this semi-processing depends upon the local "take" and upon the number and calibre of available personnel. Except in the case of Naval traffic this semi-processing consists primarily of extraction and sorting of significant portions of the transmissions. The result of this semi-processing is called a TECSUM and consists of a digest of all meaningful information intercept by the operators.

The TECSUMS are forwarded by electrical means to NSA and to the theatre processing headquarters where they form a basis for COMINT reports which are supplied to theatre and other interested consumers. In NSA the TECSUMS are combined and further processed in a more complete manner yielding less timely but more comprehensive intelligence. In this respect considerable progress has, in some instances, been made toward mechanization, since the TECSUMS are received on perforated tape which lends itself to immediate machine processing (subject only to the correction of transmission error).

3. After the semi-processing at the intercept site, the raw traffic is forwarded physically to NSA (Washington) for more complete processing. Prior to extraction of intelligence, the traffic must be put into intelligible and analyzable form. This

involves transcription, identification, editing, sorting and logging the traffic.

4. Transcription. Since there are at present no machines for sorting or analyzing raw traffic, it must all be transcribed in the form of page copy so that it can be scrutinized visually and processed manually. This is true of all forms of intercept except hand sent morse and low-speed automatic morse which are taken down originally in page copy. The processes involved are as follows:

a. Radioprinter intercept may arrive in the form of punched tape, undulator tape, magnetic tape, or occasionally page copy. In any event it is transcribed -- manually, in the case of undulator tape -- into page copy.

b. Radiotelephone intercept is recorded on magnetic tape and is transcribed manually onto page copy by skilled linguists. A large part of this is done at the intercept site or at some field processing center. It would be desirable to be able to scan radiotelephone intercept automatically to detect the presence of key words. To accomplish this an analysis of spoken language with respect to phoneme construction and representation will be necessary.

c. All other transmissions (except some facsimile) are recorded on discs or magnetic tape and forwarded to NSA for research.

5. Identification. In most cases the tranbmissions are already identified by the intercept operator through a foreknowledge of call signs and frequency schedules, i.e. because the operator knew what he was seeking to intercept. Identification consists of assigning a "case number" to the transmission. A case number is a sequence of four letters and five digits. The four letters identify the transmission as to country, service, and type (morse, R/T, etc.). The five digits identify the net and individual link. About 20 percent of the traffic arriving at NSA is unidentified or incorrectly identified. In identifying traffic, all the techniques of traffic analysis are brought to bear on the problem, since the traffic is worthless unless the originator can be identified to some extent. On some circuits, e.g. many radioprinters, the problem of identification is paramount, since calls are seldom, if ever, used and little intelligence is passed on the circuit. (These circuits are, however, a potential source of intelligence as they are maintained in a standby state to carry overloads from other circuits.) In the case of hostilities or a breakdown of landline facilities, these circuits are capable of handling a great deal of traffic.

6. Editing and sorting. These are the most time-consuming and tedious operations in the agency. In some divisions of NSA-90 as much as 85 percent of the personnel and time is devoted to these operations. In order for intelligence to be extracted from copy, it must be presented to the analyst in some logical order. The particular

order will depend on the type of intelligence to be extracted. In general the operations proceed more or less as follows: First, the traffic must be sorted by case number and arranged in chronological order. At this point the chatter can be analyzed, call signs logged, and messages decrypted or extracted for subsequent analysis. At the same time the intercept operator's parenthetic notes are taken into account and appropriate changes made. Also the traffic must be "deduped". This involves searching through all the messages transmitted, and combining duplicate messages, i.e., comparing and resolving discrepancies. The "deduping" is not confined to an individual link. A search across all related links must also be made. This, in addition to giving a "best" copy of the message, gives information as to message routing, the importance of which we have previously noted.

After the messages have been deduped, and classified as to practice or bona fide, they must be classified according to cryptographic system and transcribed (perhaps in decrypted form). If the messages are easily decrypted, then the consequent intelligence must be logged in such a manner that it can be evaluated properly and later included in an intelligence report. Some of these messages are individually of no intelligence value. The intelligence to be derived would be of a statistical nature arising from the evaluation of a large number of such messages. An outstanding example of this is the Russian [redacted] [redacted] system in which several million messages per month are

EO 3.3(h)(2)
PL 86-36/50 USC 3605

passed. An individual message is merely [redacted] However, the totality of messages, when properly evaluated, gives a vivid picture of the Russian [redacted] system (both organizational and geographical), [redacted] concentration, etc.

If the messages are not easily decrypted or are encrypted by an unknown system, they are passed, together with identifications along to the cognizant cryptanalysts. There they undergo further transcriptions and sorting in various (and frequently not predetermined) forms. This is discussed in detail in another chapter.

7. Analysis. References have already been made in the preceding paragraphs to the actual processes of traffic analysis Although it is believed that the bulk of what is now called analysis is in fact paper shuffling (i.e. getting the data into the proper order and form) which could be mechanized, there still remains the problem of evaluation, which must ultimately be done by a person. Phases of traffic analysis which cannot be profitably done by machine are the following:

a. Decision. The analyst must continually survey and resurvey his raw data, in order to determine what intelligence can be extracted and which facets of the data contain this intelligence. This is a very important aspect of both C/A and T/A. Old sources of intelligence are constantly disappearing and new sources crop up. The analyst must be continually on the alert for new sources. He must then decide how the intelligence is to be extracted, or in what form the data must be presented in order to facilitate extraction. He must also estimate the amount of work involved and decide whether or not the latent information is of sufficient value to warrant the expenditure of that effort.

b. Evaluation. The analyst must analyze the intelligence produced by the above processes, decide whether or not it is of significance, draw conclusions (preferably probability statements) from it, and possibly decide what further processing is called for. Finally, he must compile the intelligence in as complete, yet concise, a report as possible for delivery to the consumers.

8. Filing and Storage. In order to properly evaluate data, the analyst must have access to the past history of a situation. This entails storage and indexing of all significant data as it occurs. The data to be stored consists of raw traffic and information extracted from traffic or other collateral sources. The former is primarily a storage problem, as the need to consult old raw traffic is relatively infrequent, and when called for, the identity and location of the traffic is usually known. Projects FREEZER and DEFROST are expected to handle this problem adequately by microfilming all traffic and providing a machine for quickly producing photostatic copies of any selected portion.

The problem of filing information is somewhat different. An item of information, to be fully exploitable, must be filed under a number of different categories, and in such a manner that is physically easy to locate and read. Due to the bulk and variety of information, this has become practically impossible with conventional methods of filing. Additional filing space is no longer available, so that only a carefully selected portion of new information can be filed, and this at the expense of old but potentially valuable information which must be burned.

Although the problem of space will be solved (at least temporarily) by the move to Ft. Meade,. the paramount problem of access will still remain. Files are of little use unless they are extensively cross-indexed or can be scanned easily and quickly. Cross-indexing is in general unsatisfactory with the types of problems encountered here because of multiplied bulk and because it is impossible to predict all the indices by which it may be desired to enter the file in the future. At present many potentially productive avenues of research are constantly being blocked by the work factor involved in collecting the data from bulky and inadequately catalogued files.

IV. MAGNITUDE

1. Table A gives a breakdown of the estimated 350 million (5-character) groups which must be processed monthly by NSA-90 during 1958. (The overall present figures are about 10 percent less.) These figures represent about 80 percent of the total traffic processed by NSA, although somewhat less than 80 percent of the total analytic effort.

2. Table B shows the extent to which we are able to exploit our present take of traffic. In this table "Basis Processing" means sorting, scanning, and extracting elementary T/A information. "Advanced Processing" means decryption of known systems and more detailed traffic analysis. It does not imply complete exploitation. It would be quite optimistic to assume that 25 percent of inherent intelligence has been extracted even from that traffic which has undergone "advanced processing".

3. After advanced processing there is still a great deal of intelligence which could be recovered by cross-reference, collation, and proper statistical and mathematical treatment of the results. These are not fully exploited for two reasons. First, all available personnel are swallowed up in the task of basic processing, which must necessarily be done first and always. Secondly, although most of the advanced analysis could be done by machine, the data to be analyzed must first be put into a form adaptable to machine treatment. This is impossible with our present (or any reasonable future) complement of key punch operators.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

V. COMMENTS AND RECOMMENDATIONS

1. From fifty to seventy five percent of the basic traffic processing now being done manually on specific problems, such as Soviet [redacted] [redacted] could be done much more quickly and efficiently by machines. The biggest problem is that of data handling. However, a

machine cannot handle data intelligently unless the data is in a form which the machine can interpret. There already exist means for mechanically changing coded data (in the form of magnetic tape, punched tape, punched card, etc.) into page copy. But there is as yet little hope of developing a practical method of changing page copy into coded form. Furthermore, there is no likelihood that the manpower will ever be sufficient to accomplish this process manually to the extent that is desirable. Add to this the fact that intercept is transcribed from two to five times during processing, and it becomes evident that the only solution is that the intercept be taken down originally in coded form. This is mechanically easy to accomplish, but it will require considerable research into the requirements of the analysts to determine what form to use, how to include parenthetic notes, how to edit it, etc. It will also require the development of some extremely flexible type of data editing equipment in order to take maximum advantage of the operators' parenthetic comments.

2. Another advantage in taking down intercept in coded form will be realized in that it will then be adaptable to immediate superencipherment and forwarding by electrical means. Although it appears unlikely that we will ever have the facilities for forwarding all intercept electrically, there should always be means available for electrically forwarding any given portion on a priority basis, in case that portion

should become productive of critical and perishable intelligence.

3. There is also a need for a more adequate method of filing COMINT and collateral intelligence (as discussed under Filing and Storage). A system somewhat as follows seems to be indicated:

a. A file containing punched cards (or the magnetic equivalent of punched card). Each "card" would contain an item of intelligence and a code symbol indicating the format in which the intelligence is entered. For example it may contain, with respect to an enemy activity, the basic station trinome, military unit number, location, subordination, types of transmission, type of operation in which engaged, date, location (in the raw traffic storage files) of the source of this information, special remarks, etc. Other types of information cards might be case activity summaries, personality files, traffic resumes, cargo information, etc.

b. A means for electrically scanning the file at high speed in search of any specified logical combination of the bits of data (for example, to search for all evidence of submarine activity in the Japan Sea between 1340 and 2400 on 12, 14, or 17 April 1951 or 26 Jan 1957).

c. A means of reproducing the items selected either on a screen or in the form of page copy.

d. A means for revising or erasing information already entered into the files, as well as a means for entering new information. The File should be capable of being consulted locally by the individual seeking the information. Probably the tasks of entering, revising and erasing data should be left to specialized personnel.

The basic components for a device of this type already exist. The IBM 702 could probably handle a year's volume of information. However, a device with a much greater memory capacity and more specialized set of instructions would be more economical and efficient.

4. Other than the equipments just discussed, there seems to be little use for special purpose equipment in the office of exploitation. In general the problem is one of sorting, collating and summarization. After these processes have been accomplished, there will also be problems of a mathematical nature and some problems of decryption. However, each such problem by itself would be relatively small and of indefinite duration. It seems advisable to plan to treat these problems on general purpose computers until such time as their magnitude and duration indicate otherwise. At any rate, there would be no point in building special purpose equipment until we are prepared to feed data to it.

The "small" problems referred to above are by no means unimportant. They include such problems as summarization of results, DF fixing, plotting locations of radar stations, and many others. Of late, much attention has been devoted by members of 90, 82, and 34 to the mechanization of these problems on existing computers and IBM equipment. This support should be continued, as the "small" mechanizable problems are numerous, and new ones are constantly being created.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

ESTIMATED GROUPAGE
FISCAL YEAR 1958

	High Grade Messages	Low Grade Messages	Practice Messages	Plain Text	Chatter	Total	Groups to be Fwd. Electrically each month
[redacted]	1,075,640	951,240	4,847,140	2,096,620	20,889,270	29,958,910	5,228,600
[redacted]	12,672,500	1,104,520	206,000	1,002,120	2,411,590	17,396,730	2,800,000
[redacted]	831,750	2,063,520	None	482,040	2,280,090	5,657,400	1,106,700
[redacted]	7,717,240	2,439,430	5,440,050	1,135,410	2,697,890	19,430,020	14,430,900
[redacted]	306,360	301,440	1,143,570	955,470	3,771,600	6,478,440	4,641,150
[redacted]	702,270	47,050	40,200	None	359,800	1,030,520	241,000
[redacted]	735,270	372,120	5,268,680	73,150	39,014,030	45,463,250	5,625,600
[redacted]	67,350	7,453,400	490,790	5,624,820	15,413,900	29,049,260	4,002,600
[redacted]	712,420	51,074,120	3,936,230	None	38,484,980	94,207,750	22,867,200
[redacted]	8,350,940	121,140	None	84,000	5,571,010	14,127,190	2,857,880
[redacted]	31,846,450	11,295,290	5,247,930	2,070,400	38,609,150	89,069,290	13,654,800

TOP SECRET EIDER

Table B

PERCENTAGE OF TRAFFIC PROCESSED

	Percentage of Traffic on which Basic Processing has been completed	Percentage of Traffic which has undergone Advanced Processing
[redacted]	85%	45%
[redacted]	85%	80%
[redacted]	100%	85%
[redacted]	~~95%~~	60%
[redacted]	100%	40%
[redacted]	85%	50%
[redacted]	85%	50%
[redacted]	40%	30%
[redacted]	85%	70%
[redacted]	90%	30%
[redacted]	95%	85%
[redacted]	90%	15%
[redacted]	70%	42%

D WEATHER

EO 3.3(h)(2)
PL 86-36/50 USC 3605

1. INTRODUCTION

The Weather Division (NSA-95) and the weather field stations are primarily concerned with extracting special weather intelligence from [redacted] communications. Interest exists in European Satellites' weather intelligence, but [redacted] presently has responsibility for this area.

Weather intelligence, to be of use to the consumer, must reach the consumer within six hours of the initial weather observation. The time involved in transmitting or delivering the intercepted weather traffic to NSA is far greater than six hours. Hence, if useful intelligence is to be extracted from weather traffic, the traffic must be exploited in the field or the traffic must arrive at NSA within an hour of intercept. At present field units process and exploit the weather traffic wherever possible.

The Weather Division at NSA concerns itself with the training of personnel for NSA field station duty, advises on the operation and functions of the field stations, and performs the cryptanalytic research and traffic analysis necessary to maintain and constantly improve intercept and analysis of weather traffic. Weather intelligence reports are compiled in the Weather Division.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

II. INTEREST IN WEATHER

Our main interest in [redacted] weather intelligence is due to the value of this weather intelligence in helping to predict or substantiate [redacted] offensive action against their enemies. If a full scale offensive action were to be carried out by [redacted] weather conditions would have to be suitable for the scheduled activity. Also, if a full scale offensive were to be launched against [redacted] weather conditions over the attack area would have to be completely known at least twenty four hours in advance. The development of nuclear weapons puts an unusual value on all weather intelligence.

Our secondary interest in the [redacted] weather stems from its value in predicting weather conditions in parts of the world other than [redacted]

III. WEATHER TRAFFIC FLOW

[redacted]

In the [redacted], weather observations are made at observation posts and are transmitted as weather reports to collection stations which serve as assembly and retransmission points.

The weather reports of the services do not flow in established patterns as do reports on the hydromet nets. There is a heavy exchange of weather reports on an "as needed" basis.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

IV. INTERCEPT POINTS AND VOLUMES

[redacted]

V. CRYPTANALYSIS

[redacted] These systems are fully discussed in the chapter titled "Hand Systems" and hence will not be discussed here. The mechanization of the solution of these systems affords problems which differ little from some problems discussed in the chapter titled "Hand Systems." The amounts and type of mechanization required by the Weather Division will also be included there.

VI. TRAFFIC ANALYSIS

The traffic analysis functions of the Weather Division do not differ essentially from the functions performed in the Traffic Analysis Divisions. A discussion on the mechanization of these functions has been fully discussed in the Traffic Analysis Chapter and will not be included here.

VII. RECOMMENDATIONS

1. Recommendations on the mechanization in support of performing T/A and C/A functions are included in the chapters on T/A and Hand Systems respectively. The specific requirements of the Weather Division should be carefully studied in subsequent phases of this project.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

2. If the exploitation of [redacted] weather traffic is to be accomplished at the NSA, then the recommendations set down in the chapter on T/A on processing traffic at field stations and forwarding the traffic electrically to NSA also hold. In that speed is of prime importance in the exploitation of weather traffic, special requirements may have to be satisfied here.

3. Efforts should be made to intercept weather traffic at the observation outpost level. Obtaining the traffic at this level will aid considerable in compromising the crypto-systems employed during later transmissions.

E PLAIN LANGUAGE

I. INTRODUCTION

Analysis of plain language traffic accounts for a substantial share of the intelligence obtained on the economic and military status of the countries forming the communist bloc. This information is not as easily obtained from the plain language messages as one might suspect. In most cases considerable processing and analysis is required to recover and recognize items of importance. In many cases relevant items are referred to by number, drawing, or contract, and not by name.

II. SOURCES

PL 86-36/50 USC 3605
EO 3.3(h)(2)

There are many types and sources of plain language traffic: [redacted] in that these are representative of the type of processing and analysis required; moreover, they constitute an important source of information on the economic and military potential of [redacted].

III. [redacted] COMMUNICATIONS

1. General. [redacted] communications are communications

passed on nonmilitary links. primarily those of the [redacted] [redacted] The traffic contains both official and private correspondence. Thc official part consists of communications between [redacted] Virtually all the traffic of this sort obtained by NSA is through the efforts of our intercept stations. Almost all the transmissions utilize Radioprinter and Automatic Morse. There are some facsimile and voice transmissions. The total intercept averages 1,000,000 non-voice messages a month and approximately 1000 voice magnetic tape recordings.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

2. Non-Voice. The non-voice intercept is forwarded to NSA Washington where it is put through a preliminary scanning process which eliminates about 80 percent of the traffic intercepted. The scanners, by process of noting key words, classify the remaining 20 percent according to subject matter. The retained traffic is page printed, serialized, and microfilmed and then further studied with respect to criteria determined by current intelligence interests. The high priority material is further analyzed and the intelligence value extracted. Non-priority material is stored for possible future use.

3. Voice. The voice tapes are forwarded unprocessed to the appropriate area in the Agency where they are audited by linguists

PL 86-36/50 USC 3
EO 3.3(h)(2)

for intelligence content. Only selected portions are transcribed and sent to the analyst.

4. Intelligence. The foregoing processes of scanning, categorizing and subsequent analysis of voice and non-voice plain language intercept culminate in a substantial amount of intelligence concerning the [redacted]

IV. INTERNATIONAL COMMERCIAL RADIO

1. General. International Commercial Radio is a communications medium by which the commercial and governmental organizations of the [redacted] (and other nations as well) communicate with each other. There are some national nets, controlled by the [redacted] services, which carry international commercial communications. Russian, Chinese Communist and Satellite traffic on the monitored ICR links received in NSA averages 100,000 messages a month. The national nets yield another 20,000 messages a month. This represents only 5 percent of the ICR traffic intercepted. Not all traffic on the ICR links is in plain language. From 20 to 50 thousand commercial code messages per month are also received. The code systems employed are mainly those which are commercially available. Some of the code systems are privately constructed. It is estimated that almost all of these systems could be read if need be. However, at present effort is restricted to reading only select commercial code messages. Few intercept stations are assigned to intercept ICR

traffic exclusively. Other stations intercept ICR plain language but discard it when they recognize it as such.

2. Intercept Control. The intercept stations assigned to the intercept of ICR scan and select traffic according to a predetermined scan guide. The selected traffic is forwarded to NSA where it is scanned according to the countries involved in the communication or by the originator of the message and sorted accordingly. The traffic is then scanned for intelligence content. This scanning results in the retention of about half the traffic originally processed.

3. Intelligence. All the [redacted] and ICR messages which survive the preliminary elimination processes are studied by competent analysts. Several thousand messages a month are translated and published individually. The contents of many thousands more are published in reports, tabulations, compilations, and summaries. All messages of potential value are filed, several hundred thousand per month being retained.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

V. AREAS FOR MECHANIZATION

An area in which machines can give support is in the early sorting and selection stages where relatively simple but decisive operations are performed on vast quantities of traffic. Several equipments which will assist in the mechanization of scanning and page printing operations and which will completely mechanize the page printing operation of [redacted] radioprinter traffic are under development (these are Project

NELLY and Project BUDDY). The BUDDY device will scan chadless tape and page print messages selected by message endings. The NELLY device will be an experimental model of a scanning device which will incorporate the functions of BUDDY as well as select messages by category for page printing. A modification of a Model 28 teletype machine will make possible on-line processing of radio-printer traffic and the automatic production of page print copy. Another current development is an electronic transcriber which will operate on-line in the recording of automatic Morse transmissions and produce hard copy. Since automatic Morse is now recorded on undulator tape, the amount of tape that can be scanned is definitely limited. This electronic transcriber should result in a considerable increase in the amount of automatic Morse traffic which can be processed. Automatic translation from undulator tape has proven a problem due to variability in the inking of the tape. This is a problem on which more effort should be placed.

Scanning, categorizing, decoding, and printing of commercial code messages could be mechanized with slight variations on the NELLY approach. Other operations which might be performed mechanically include (1) Automatic language translation, (2) Automatic editing, mass data processing of messages, and automatic filing and file recovery, as discussed under Traffic Analysis. A potentially mechanizable field requiring additional analytic research is that of phoneme analysis for the automatic detection of "hot" words in voice recordings together with improved equipment to perform this function.

F MACHINE SYSTEMS

1. INTRODUCTION

1. Crypto-systems can be divided into two categories depending on how the encipherment is performed, by hand or by machine. Hand systems are treated separately, and for purposes of this report machine systems are defined as those in which the key used is produced as encipherment takes place; the key is generated on the spot. In some usages previously prepared key is combined with plain text electrically or mechanically. These are not regarded as machine systems since they consist of mechanizing a hand process. If it were determined that such key had been produced by means of a cipher machine, study of the key and the machine would of course be regarded as a machine problem.

Cipher machines have many advantages particularly for middle and high echelon military use. They are rapid and usually provide printed copy; their use avoids many of the complicated problems of distribution raised by key pads and key tapes. Their speed of encipherment permits the handling of large volumes of traffic; teletype systems can be operated at tape reader speed and so can handle messages several thousand characters long. Machines requiring no outside power source are very good for field use. These factors make cipher machines particularly adaptable for military use so that it is extremely likely that we will be working against cipher machines for some time.

2. Two principal categories of cipher machines are those that use (1) rotors (wired rotors) or (2) pin wheels to produce key. A rotor is a wheel with two faces, called input and output faces, each with n contacts or studs and a set of n wires making electrical connections between the faces. The number of interconnecting wires is usually equal to the number of letters in the alphabet of the language for which it is being used. Twenty-six is the most common number for western countries and thirty for Russia. With recent developments such as re-entry (where a circuit may pass through the rotors more than once) this number can vary. The classical machine uses a series of rotors set between two plates, one of whose points are connected to the keyboard and the other to the printer. These are referred to as the input and output endplates respectively. At a particular position or setting of the rotors a key is depressed, this excites a point of the endplate; the current goes through the rotors to the output endplate and thence to the printer. The resultant letter constitutes the encipherment of the letter on the depressed key at the indicated setting of the rotors. At this setting each letter on the keyboard will be associated with a unique output letter. This association of all the letters makes up the enciphering alphabet at a particular position of the rotors. This alphabet persists as long as none of the rotors alters its position. However, if one or more of the rotors move, a new enciphering alphabet is set up. The encipherment of each letter will then show

only an apparently random relation to its previous encipherment if randomly wired rotors are employed.

A rotor machine then consists of a series of rotors set between a pair of endplates and a determinable means of rotating them (called the rule of motion) in such a way that a long series of apparently unrelated non-repeating enciphering alphabets is produced. Some machines have the property that enciphering alphabets are reciprocal: (i.e. if A is enciphered by N then N will be enciphered by A) and no letter can be enciphered by itself. A rotor machine called the ENIGMA, widely used by the German Armed Forces during the last war had this feature. The ENIGMA also had a set of jacks which permitted a daily rearrangement of the order in which the keyboard was connected to the endplate. The addition of these jacks provided more security than the addition of a rotor whose position must remain fixed for many encipherments.

3. a. An example of the other type of cipher machine which uses pin wheels as opposed to rotors to produce key is the Hagelin model C-38. A pin wheel is a circular disc with pins set in the perimeter that can take either of two positions. The basic principle of operation consists of sliding two alphabets, one in normal order and the other reversed, against each other in such a way that successive juxtapositions of the alphabets depend on the internal structure of the machine. Here each juxtaposition produces one of twenty-six related alphabets since there are only twenty-six possible juxtapositions of twenty-six letter alphabets. Security is inherent in the highly

irregular sequence in which the various juxtapositions are used. The sequence of juxtapositions or offsets is the key which is a function of the activity of the pins and a set of lugs each of which provides for a single displacement of the alphabet. Again a particular setting of the wheels is associated with a given displatement. In order to get a long series of such displacements the wheels are made to move. In the C-38 all the wheels move a single step between encipherments. To guarantee a long period before the series of offsets repeats the wheels are made relatively prime. The C-38 has six wheels which range in length from 17 to 26 giving it a cycle length of about one hundred million.

3. b. Another type of pin wheel cipher machine is one which generates key for the encipherment of the baudot code. The Baudot code is the binary code employed to represent the characters of the 32 character alphabet of a teletype machine. The function of the pin wheels is to produce five binary streams, each stream may be represented as a series of dots and crosses or marks and spaces. Encipherment consists of adding these streams level by level to the plain text. The rule for addition is usually dot plus dot and cross plus cross sum to dot, and dot plus cross or cross plus dot sum to cross. Certain machines have a further encipherment at this stage which involves permuting the levels of this sum. Again it is clear that the wheels must be made to move since a particular letter of key will always be associated with a given setting of the

wheels. Also there must be a way of insuring a long period before the sequence of key letters starts to repeat.

4. There are cipher machines which produce key through the use of telephone selectors, others use commutators. There is a wide variety of methods of moving the elements of the machine, but the machines mentioned above are the basic types.

5. The cryptanalysis of these machines is extremely complex and mechanization of the methods of cryptanalysis requires a large quantity of high speed electronic equipment. An outline of these methods will be given to show why such equipment is necessary. We shall often speak of the "solution" of a cipher machine. This will have two meanings. The first meaning applies to the term "machine solution" whereby we shall mean that enough information is known about the machine to allow us to simulate the machine's deciphering (and hence enciphering) process. For example, the ENIGMA machine is solved when all rotors, their motion notches, their wirings, and the rule of motion are obtained. This information alone is not sufficient to ensure continuous reading of the device. Again, the capture of a cipher machine and all its components constitutes a solution of the machine. The second meaning applies to the term "daily solution" whereby we shall mean that all the parameters of the device are known for the crypto-period. For example, the parameters of the ENIGMA machine which change "daily" are the wiring of the reflector and stecker, the rotors

employed, their order and their initial settings. Thus to obtain a "machine solution" of the ENIGMA knowing the nature of the machine, we would have to recover the number of rotors that are employed and the wiring of each. Supposing there are eight available rotors to be used three at a time, this would mean that we would have to try (26!) wirings for each rotor to recover the correct wiring. The number of trials necessary to recover all rotors would approximate 10^{80}. This number exceeds the number of atoms in the universe and obviously transcends the speed and capacity of electronic equipment which may become available in the foreseeable future.

5. a. The cryptanalytic exploitation of the ENIGMA is a good example of the use of high speed machinery. The ENIGMA machine was used on almost all communication links of the German military establishment. The wiring of the rotors was completely known because machines were captured; even so there remained many unknown elements in the encipherment of a message. First, the choice of rotors used and their order (In the Army an ordered sequence of three was selected from a set of 5 . This can be done in 60 ways.); second, the setting of the rings which governed the motion of the wheels (this can be done in 17,576 ways); third, the setting of the exterior jacks (150,738,274,937,250 possibilities); finally, the setting of the rotors at the beginning of the encipherment (17,576 possibilities). This totals to approximately 10^{24} possibilities.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

5. b. [redacted] Without having any particular way to make the correct guesses, exhaustive trials of all rotor orders, ring settings and initial settings would be required. This would amount to 10 billion man hours of work — clearly out of the question. However, it was possible to build a special machine, called a Bombe, consisting of sixteen analogues of the Enigma machine and a great deal of electronic sensing equipment which reduced the time to test a single assumption of wheel order, ring-setting, and initial setting to one millisecond. Furthermore, it was possible to handle ring settings in rather large blocks. The effect was to reduce the time for a complete set of exhaustive trials of a matched plain and cipher to a few hours of Bombe-time. Of course, there were many possibilities for error; a garbled character in the assumed plain text stereotype used as a crib (or a minor variation from one day to the next) would invalidate the entire run.

5. c. When one message was read on a particular circuit on a certain day, then the rest of the messages on the circuit that day were easier to read because the rotor-order; ring-setting, and jack-plugging would remain the same for the entire day.

5. d. More than 200 bombes were kept busy 24 hours a day breaking out traffic enciphered on the ENIGMA. The bombes generally required 10 minutes per wheel order or about 10 hours in the worst possible case. Various weaknesses of German usage frequently reduced this considerably.

6. We see that while machine or daily solution by exhaustive trial (or brute force) is not feasible with the highest speed equipment available today, solution by hand methods is also not feasible. What is done is to reduce the number of trials to the point where solution can be achieved by high speed electronic devices. The bombe is an example of a machine designed specifically for the ENIGMA problem. With the advent of computers we have available a weapon for more general attack on cryptanalytic problems. By means of such devices it is possible to solve the ENIGMA statistically without the use of cribs. This, however, requires a fairly long message, but it is an example of how more powerful equipment has made possible new methods of attack.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

derived from the reading of a depth — the encipherment of two or more different messages at the same set-up of the machine. The [redacted] This is an example of how modern equipment has made possible attacks considered out of the question a short time ago. More detail of the solution [redacted] machines will be given in the discussion of Hagelin and Sturgeon problems.

7. b. The entering wedge to the solution and exploitation of cipher machines in most cases is a result of either the unauthorized acquisition of the rotor wirings and other details or the detection and breaking out of bust messages which result through machine failure or operation misuse. The first centering wedge is self-explanatory and involves capture, theft, or defection. The second covers all unintentional mis-use of the machine. [redacted]

EO 3.3(h)(2)
PL 86-36/50 USC

[redacted]

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

II. THE HAGELIN PROBLEM

1. The Hagelin machine, type C-38, is a cryptographic device which involves reciprocal (in the sense that no encipher - decipher switch is needed) substitution and uses reversed standard alphabets slid against each other according to a long mechanically developed key. Slight variations exist but these variations do not effect this discussion. The initial offset, called slide, of the two alphabets is variable. The parameters involved in the manufacture of the key are (1) a set of 27 bars with two lugs on each bar, (2) a set of six pin wheels of lengths 26, 25, 23, 21, 19, 17 . Each bar has eight possible resting places for the lugs on it — one for engagement by each wheel, and two neutral positions. The amount of "kick" (distance and alphabets are slid for a given encipherment) is controlled by the activity (or inactivity) of the pins on the wheels, and the number of lugs set in the paths of the active wheels. The presence of an active pin on a given wheel causes a kick of one for each bar having a lug resting in the path of that wheel. In the case where both lugs on one bar are resting in the paths of wheels, activity of either or both wheels will cause that bar to contribute only one to the total kick. These wheels are said to be "overlapped" by the number of bars they have in common. The wheel motion is regular — each wheel stepping one position before each encipherment.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

2. Properly used the Hagelin machine can be very secure; [redacted]

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3
EO 3.3(h)(2)

[redacted]

[redacted]

PL 86-36/50 USC
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

5. It can readily be seen that it is not feasible to apply all of the above outlined methods by hand.

[redacted]

PL 86-36/50 USC
EO 3.3(h)(2)

[redacted]

5. b. Several programs are available on digital computers to carry out both placement and statistical solution attacks.

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

6. Even with these extensive aids to solution and placement, certain difficulties arise which are not yet completely under control.

[redacted]

[redacted]

7. Current Traffic and Readability

USER	VOLUME MSG/MO	SUCCESS
[redacted]	250	Good
[redacted]	300	Fairly Good
[redacted]	60	Good
[redacted]	900	Poor, can read depths
[redacted]	5	Poor, can read depths
[redacted]	10	None
[redacted]	130	None
[redacted]	100	Excellent
[redacted]	50	Excellent

PL 86-36/50 USC 3605
EO 3.3(h)(2)

*See page 78

USER	VOLUME MSG/MO	SUCCESS
[redacted]	50	Fairly Good
	200	Excellent
	550	Partial (insufficient and poor intercept)
	1000	Partial (low priority)

EO 3.3(h)(2)
PL 86-36/50 USC 3605

III. THE MODIFIED B-211

1. Usage. This machine is a [redacted] modification of the 1928 commercial Hagelin Model B-211. [redacted]

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

2. Description. The modified B-211 is a wired-wheel cipher device. Input is via a standard typewriter keyboard; output may be a gummed tape or into an electric typewriter. The basic cryptographic elements of the machine are (excluding motor, print mechanism, gears, etc.)

(1) Input and output fractionating devices (squares)

(2) Four sets of pluggings (steckers)

(3) Six wired cipher wheels (numbered I, II, III, IV, V, VI)

(4) Four motion wheels (numbered VII, VIII, IX, X)

Only the fractionating squares, the steckers, and the cipher wheels are involved in the actual encipherment of a letter, the function of the motion wheels being solely to impart a non-regular movement to the cipher wheels during encipherment.

2. a. The fractionating devices can each be visualized as a 5x5 square with the letters A-Z (excluding W) written into the square in random order (the same order in each square). The function of the input square is to resolve a letter into two components (row and column),

each of which is enciphered separately and then recombined in the output square to produce a cipher letter.

In encipherment (or decipherment) electrical pulses originating in the input fractionating square and ending in the output square actually pass through the pluggings and cipher wheels. The cipher wheels and steckers simply provide a path or circuit for the original pulses.

2. b. The cipher wheels are of two types: wheels I, II, III, and IV are rotors, Wheels V and VI are equivalent to a half rotor with a set of slip rings providing input and a rotor face for an output. Each rotor has 15 settings or positions. Wheel settings are divided into three families of five each with family wired to family

Resting against the faces of the rotors are endplates, each of which have five contacts which are spaced opposite every third contact of the 15 rotor contacts. Thus a path through any of the five input points of an endplate travels through the rotor, coming out at one of the five output points of the other endplate. Moving the wheel varies the paths.

The half rotors have ten settings (in two groups, even and odd). On one face of the wheel are ten contacts, which ride against an endplate with five contacts, while on the other side of the wheel is a shaft with five slip rings. Each slip ring is wired to two of the points on the face, one in each family. Five brushes provide the input to the half rotor.

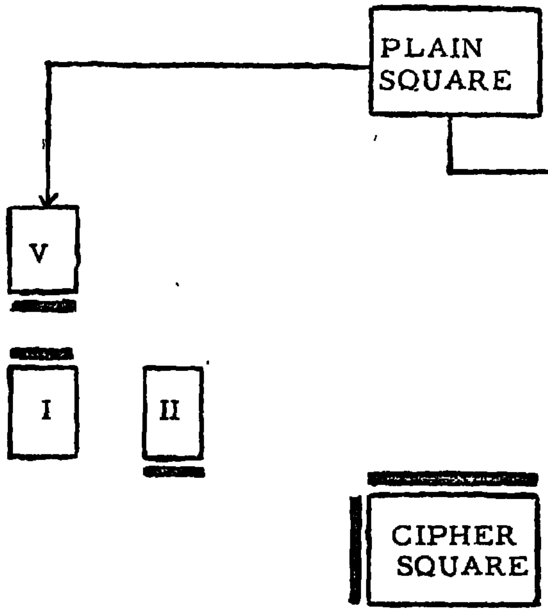
The five brushes of each of the two half rotors are wired directly to the five rows and five columns of the input fractionating square respectively, so that encipherment proceeds from the fractionating square to the V and VI half rotors.

2. c. The four variable steckers (plugging) in the machine permit further variation in circuitry. Two of the steckers connect the output points of rotors V and VI with the input points of rotors I and IV . Here we can have V plugged to I (with VI plugged to IV) <u>or</u> V plugged to IV (with VI plugged to I). The latter plugging in general, presents a more difficult problem of cryptanalysis. This plugging is referred to as "cross-plugging."

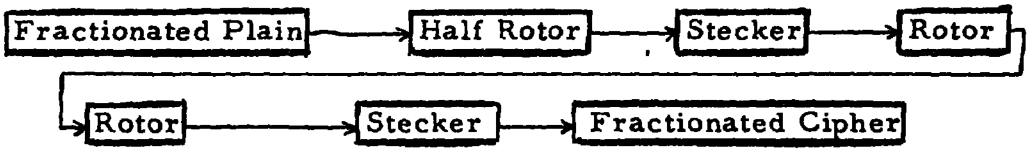
The output points of rotor I are connected permanently to the input points of rotor II. The same is true of rotors IV and III . The output points of rotors II and III are plugged into rows and columns of the output fractionating square. A variation in "direction" of plugging is also possible here, so that II may be plugged into rows, with III plugged into columns, or vice versa.

Each stecker has 120(5!) variations, there being five elements to plug.

2. d. A block diagram of the rotor and stecker layout for the machine is given below. Here the fractionating squares are referred to as plain and cipher squares. Steckers are not shown but the heavy lines indicate where the plugging is located.



Note that with any variation of plugging the order of encipherment of either plain component is



For encipherment or decipherment by hand the wiring of the rotors can be expressed as related alphabets, and the process of tracing a path through the wheels becomes one of successively applying alphabets to the plain components.

2. e. The four motion pin wheels have 23, 21, 19, 17 settings respectively. Each wheel has a movable pin in its rim at each setting (axis of the pin is perpendicular to the face of the wheel) which may be set in an "active" or "inactive" position. Movement of the rotors is controlled by the action of the pins of the motion wheels. The 23 and

21 pin wheels control movement of rotors V and II, both V and II stepping if an active pin comes up in either or both of the pin wheels Wheels IV and VI are similarly controlled by the 19 and 17 pin wheels. These four rotors are called "fast" rotors, they step about 75% of the time. Rotors I and III are called "slow" rotors, since they step only when II and IV step from H to I respectively (about 5% of the time). The combined cycle of the 23 and 21 pin wheels is 483, after which rotors V and II undergo exactly the same sequence of motion. Similarly the cycle of the 19 and 17 wheels is 323.

3. Machine Methods. A number of machines and machine methods have been developed for application to this problem. These include:

3. a. FROG, an electronic crib dragger which is an operational version of an earlier experimental electronic crib dragger (which was used operationally for over two years). FROG has been used operationally since April, 1954 and occupies approximately 70 cu. ft.

The purpose of this machine is to "drag" a 20 letter crib through a message in an attempt to find settings, steckers, and motion which convert the given plain into cipher. Only messages for which the plugging is from rotor VI to IV ("straight" plugging) are acceptable, and only those rotors involved in the encipherment of a single column component are considered (wheels VI-IV-III).

The straight plugging requirement is the only limit to the generality of this machine. If a message is straight plugged (and with the current indicator system about 40% of the traffic is straight plugged), and the crib is not garbled, then the machine will place it.

Since FROG became operational all breaks into new cryptographic periods have been made with the machine. FROG is used about 100 hours per month.

3. b. Computer Programs are used for message placements when indicator groups are partially known. About 40 hours per month of data preparation time and 40 hours per month of computer time are used.

3. c. Analogs. There are three of these relay-type machines, which duplicate the cryptography of the B-211. Cipher is typed into the machine via an input keyboard; plain text is simultaneously typed out by an electric typewriter.

Wiring of the cipher wheels, steckers (plugging), and motion wheel pin patterns are all contained on plugboards, allowing complete flexibility of the machine. These machines are primarily used to decipher traffic, but their extreme flexibility makes them also very valuable in certain cryptanalytic methods.

3. d. Handtesters. These are simple devices, in effect, analogues of the B-211 without motion wheels. By manipulation of switches (steckers are plugged beforehand) a letter can be deciphered through any given cipher wheel settings.

There are three of these devices. Their primary use is in the recovery of motion when cipher wheel starting points and steckers are known.

PL 86-36/50 USC
EO 3.3(h)(2)

4. Standard B-211. The commercial B-211, which lacks the [redacted]

IV. STURGEON

1. Description. STURGEON is the cover name for a German invented teletype [redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

3. Machine Methods. A number of computer programs are available to perform various processes for STURGEON. [redacted]

PL 86-36/50 USC
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

V. JAPANESE MACHINE SYSTEMS

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

1. b. <u>Purple</u>. The Purple machine was originally built as an encipher-decipher device. Depression of a key from a typewriter keyboard caused a current to flow through a stecker, telephone

PL 86-36/50 USC 3605
EO 3.3(h)(2)

selectors, and back through the stecker where finally a key from an electromatic typewriter automatically printed the end product. Current from a set of six letters passed through a single six-input telephone selector while current from the other set of 20 letters passed through a bank of three 20-input selectors. All selectors had 25 levels. Various motion patterns were used but in any event the machine cycled at 15,625 letters. (Note that a monoalphabetic substitution on the plain-text would result without wheel motion.) Motion patterns and stecker were changed periodically.

Some pages of early books of key were generated by typing one of five 500-long sequences for the link system or two 1250-long sequences for an early version of the circular system into a non-stepping Purple machine, thus essentially only applying a monoalphabetic substitution to the sequence.

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

3. Exploitable Weaknesses.

[redacted]

PL 86-36/50 U
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

These results are later sorted by IBM equipment into a more convenient order for hand examination.

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

VI. ENIGMA

The ENIGMA machine substantially as it was used by the German Army during the war has been resurrected by the East German Police. They pass about six hundred messages per month. Four stored bombes have been put back into service to cope with this problem. It is handled precisely as described in the introduction. The bombe is provided with a short stretch of matched plain and cipher. By making all assumptions of plugging, wheel order and settings these elements of the key are recovered. This problem is also being used for experimental purposes to test new equipment designed to work on rotor machines.

VII. RU[redacted]

VIII. ALBATROSS.

Note: These sections are bound separately.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

IX. FUTURE MACHINES.

1. Basic descriptions of the work done on a number of active cipher machine problems have been given. Some of these devices have been around for a long time and we must anticipate the day when they will be supplanted. Others are fairly recent and as yet unsolved. This is particularly true of those in which we have the greatest interest. Both of these facts are of tremendous importance in any discussion of future equipment. In both cases we must expect more complicated devices designed expressly to overcome weaknesses that have become matters of quite common knowledge. This means electronic equipment of greater flexibility and extremely high speeds. [redacted]

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

[redacted]

It is clear that the solution of a cipher machine involves the need for considerably more complicated high speed equipment. With each advance in the design of the device a much greater advance in the analytic equipment is required. For example, the outside motion control of the ENIGMA is a relatively minor change, but the redesigning of the bombe that is needed to cope with this is extremely difficult. It is therefore necessary to keep abreast of all developments in the computer field if we hope to cope with the cryptanalysis of cipher machines.

X. COMMENTS AND RECOMMENDATIONS.

Two dominant characteristics of cipher-machine problems are the small but definite number of parameters which have to be recovered to effect a solution and the tremendous number of trials necessary to recover these parameters. In the recovery of these parameters (wheel order, initial wheel setting, etc.), analytic equipment must make use of available information such as cribs, busts, etc., and run through logical or statistical tests at very high speed. At the same time, the analytic equipment must be able to utilize an analyst designed decision process discriminating enough to limit probable answers to a manageable number while being sophisticated enough not to miss the right answer. The problem solution procedure has two phases: entry and exploitation. Both phases require that equipments operate at the highest speeds currently attainable. The entry phase requires flexible general-purpose equipment that can be set up quickly to carry out any process that the analysts hit upon, i.e., the machine must be easily programmed and readily available to the analyst. Too often suggested processes are not carried out because of the difficulty and time involved in programming the process and the non-availability of the appropriate equipment. The exploitation of any specific cipher machine usually is attempted and studied on general-purpose equipment. After success has been attained, existing special purpose machines are usually modified or new machines are designed to handle the problem whenever such machines are more efficient than the general purpose machine. In both phases computers are in most cases inadequate; they have the versatility but not the speed. Analytic equipments that have the speed need further increases in versatility.

In both these fields new and sophisticated approaches have been proposed that present equipments are unable to handle. For the most part these approaches are characterized by requiring a combination of high-speed analytic equipment, large-volume data handling, and complex control and decision facilities. The importance of such attacks will increase as more extremely complex cryptographic systems come into widespread usage.

The types of equipment required to best perform the mechanization of cryptanalytic procedures are listed as follows.

1. General computing equipment of substantially higher speeds than presently available (Atlas II, IBM-701, etc.).

2. Data processing equipment of larger capacity and higher speeds than presently available (IBM-702).

3. General utility devices of greater capacities in storage and recognition units and more flexibility particularly with regard to sequencing of data. (DEMON'S, SLED)

4. Elimination of bottlenecks at points such as editing and key punching.

G HAND SYSTEMS

I. INTRODUCTION.

1. A great deal of intercepted traffic is of the so-called hand system type. This label covers a wide variety of systems but primarily describes those in which the encoding process involves a large amount of hand labor by the cipher clerk. Included are: monome-dinome substitution, multinomic substitution employing a rectangle, transposition, multinomic code, literal code, and combinations of these. A monome—dinome substitution is one wherein literal or numeric text is enciphered by means of a rectangle containing the alphabet and digits. The rectangle is bordered by numerals. A text element is enciphered by selecting as cipher the border elements of the enciphering rectangle which locate the text element. Some rectangle elements are located by a single digit (monome), others by two digits (dinome). A multinomic substitution employing a rectangle is one wherein plain text is enciphered in essentially the same manner described above. Each text element is enciphered into a set of two or more digits, the number of digits being determined by the border of the enciphering rectangle. A transposition system is one wherein cipher text is obtained from plain text by reordering the plain text elements. As an example, plain text can be entered into a rectangle in the natural writing order (filling in row by row). If the plain text is then reordered by removing its elements from the rectangle

PL 86-36/50 USC 3605
EO 3.3(h)(2)

in a columnar fashion, the resulting text is a transposition of the original text. A multinomic code is a code wherein words and phrases of the plain text are given multinomic equivalents and are listed in a code book in numerical or alphabetic order. A multinomic code book may be thought of as a dictionary in which every word or phrase likely to occur in text is given a numeric equivalent (numeric meaning), and vice versa. A literal code is a code wherein words and phrases of the plain text are encoded by means of a set of letters according to a prescribed code book.

2. Hand systems are often further complicated by the application of key which is usually either one-time-used, several-time-used, exploitable-phychological-random or exploitable-machine-non-random.

[redacted]

PL 86-36/50 U
EO 3.3(h)(2)

[redacted]

II. DIAGNOSTIC OPERATIONS.

1. Where messages appear which are neither plain text nor in some readily readable enciphering system, we must, in the absence of outside information, analyze the text of the message in order to determine the cryptosystem involved.

2. The analysis of the messages can often be carried out by hand for small systems [redacted] but for some of the large systems described in the preceding section mechanization is required. Preliminary to an analysis of the text it must be edited, de-duped, and put on suitable medium such as IBM cards, perforated tape, etc. These three steps are at present outstanding bottlenecks in this and later stages of exploitation. For example, of the 10,000 hours per month of machine time [redacted]

3. The first step in the analysis is to attempt to identify the cryptosystem. Searches are performed to find exploitable intrinsic characteristics of plain language and its encipherments. Examples are the widely varying frequencies at which the individual letters occur in literal text and the cohesion of plain language as exhibited

by the rough frequency distribution of pairs of letters (digraphs), triples of letters (trigraphs), etc.

4. In Hand Systems where the enciphering process does not involve key (as examples, monome-dinome substitution, codes, etc.), diagnosis is often not too difficult. Hand analysis, standard IBM techniques and programs on general purpose computers (IBM's 701, Remington Rand's 1103) usually suffice.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

III. <u>EXPLOITATION (Systems with no superencipherment by key)</u>

1. When a Hand System has been identified it is necessary to determine the parameters of the system so that messages can be decrypted. [redacted]

[redacted] In this area there is a need for desk aids which will lighten the clerical tasks performed by the analyst and help increase his output.

IV. EXPLOITATION

[redacted]

PL 86-36/50 USC
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

V. EXPLOITATION

[redacted]

PL 86-36/50 USC 36
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

VI. COMMENTS AND RECOMMENDATIONS.

1. As stated in II. 2, editing, de-duping and hand punching and printing of traffic are major problems in the preparation of text preliminary to analysis. To speed up these processes it is recommended that more effort be placed on the mechanization of the editing and de-duping functions. Hand punching and printing pose more difficult problems in that they are human operations which cannot be speeded up by

EO 3.3(h)(2)
PL 86-36/50 USC 3605

an significant factor. However, the amount of hand punching required at NSA can be reduced by having traffic transmitted to NSA in a form suitable for machine handling and human analysis.

2. Not stated in III. 2 is the problem of reading encoded messages when received as such or when any superencipherment has been stripped from code messages. When a major portion of the code book has been recovered, the problem reduces the looking up meanings. Code reading is being performed on MAISIE, a special purpose decoder. The MAISIE's are not handling this function adequately. A large amount of decoding must be performed on IBM due to MAISIE time not being available. It is recommended that effort be placed on making the MAISIE's more reliable and more flexible. It is further recommended that the MAISIE's or their successors be designed to handle larger size code books.

3. As stated in IV. 2 the processes involved in preliminary processing [redacted] are indeed a bottleneck in exploitation. However, these functions could adequately be performed on general data processing equipment such as the IBM-702 or on an equipment especially designed to handle these and other functions (Farmer-Nomad study).

4. As stated in V. 2 both general purpose computers and special purpose machines are employed in the principal processing of systems using exploitable key. General purpose computers are flexible enough to adequately perform many phases of this processing. However, computer time is at a premium and a definite need exists for more general

PL 86-36/50 USC 3605
EO 3.3(h)(2)

purpose devices. The SLEDS and DEMONS are also in great demand. Man jobs are inefficiently performed on other pieces of equipment due to the non-availability of DEMON or SLED time. SLED is quite difficult to program and could be made more flexible. The DEMONS should be improved by a programmable and more flexible device which is widely applicable to the mechanization of Agency problems.

[redacted]

There is a definite need for equipment and personnel to make such runs when the information at hand warrants them.

H OTHER SIGNALS

PL 86-36/50 USC 3605
EO 3.3(h)(2)

I. CRYPTOGRAPHIC RADIATION

1. Electrostatic and electromagnetic fields are associated with the operation of electrical and electro-mechanical devices. The radiation is caused by changes in currents, sparking during switching, etc. In particular, unwanted radiation is usually associated with the operation of electrical cryptographic devices. This is due to the nature of operation of these devices, e.g., the making and breaking of circuits in the device. Experience has indicated that our own cryptographic devices may radiate information which may compromise either the plain text or the machine. Every effort is being made to minimize unwanted radiation in our cryptographic devices.

[redacted]

[redacted]

II. NOISE COMMUNICATION

1. A noise communication signal may be loosely defined as a signal that, when received on a typical amplitude modulation of frequency modulation receiver of standard design, has an output having characteristics simulating those which would be produced by an input (over a restricted bandwidth) of "white" noise. In other words, provided the received energy from the noise signal is greater than the background noise of the receiver due to atmospheric noise and tube noise, an observer would suspect that he is listening to a pure noise generator being fed into the receiver. Noise communication is attractive to communicators because it possesses both concealment [redacted] Noise communication systems generally use some reproducable form of "noise-like" signal as a carrier which is modulatea uy the intelligence signal. To a properly designed noise communications receiver and decoding mechanism, the output sounds like a good signal reasonably free from noise. However, the signal as picked up by an ordinary receiver would sound like ordinary noise. In

a single practical system known to be given serious consideration, no attempt is made to conceal the signal from an ordinary receiver. The reason for this is that the advantages claimed by the designers are not concealment, but rather, [redacted] features.

2. Several groups are studying and developing noise communication systems. Most of these groups are not supported by or directly associated with NSA. However, R/D is trying to keep abreast with the findings of these groups. NSA 314 is giving minor support to the MIT study. A modest research and development program directed toward intercept problems is being carried out both locally and under contract. [redacted] It is anticipated that this particular phase of the study will be completed by late summer 1955.

[redacted]

PL 86-36/50 USC 3
EO 3.3(h)(2)

[redacted]

IV. CIPHONY, CIFAX AND SPEECH PRIVACY

1. Introduction.

1. a. Since communications are conveniently and rapidly carried out by means of telephony, it is natural for communicators who require secret communications to consider enciphering telephone conversations. The field involving making telephone communications secure is called ciphony (ciphered telephony). Examples of the need for enciphered telephone conversation are the requirements of the aircraft pilots and high-ranking government officials who desire to make secure their conversations and transmit them directly to specific locations or persons without delay or human intervention. Small beginnings of use of such systems occurred in World War II. NSA has developed several ciphony systems and some of these are now under trial. Quite wide application of ciphony seems probable in the not distant future.

1. b. With the advent of facsimile transmissions, there came the need for making such transmissions secure. For example, a general (in the field) may wish to obtain by facsimile transmission from headquarters a copy of a weather map showing the weather conditions existing over the area under his command. A copy of such a map would be invaluable to the enemy. To avoid the occurrence of compromises, systems were developed which enciphered facsimile transmissions. This field of secret communications is called cifax (ciphered facsimile).

1. c. Speech privacy is the term used to denote speech systems which afford their users only limited security. Speech privacy systems may employ either digital or non-digital methods of representing the original speech signal. For illustrative purposes and for simplicity we shall restrict the discussion on speech privacy to non-digital speech security systems.

EO 3.3(h)(2)
PL 86-36/50 USC 3

2. Ciphony and Cifax

2. a. Little attention has as yet been given to the problems of deriving COMINT from ciphony or cifax transmissions. [redacted]

2. b. To produce a ciphony or cifax signal the original continuous waveform or graphic material, respectively, is digitalized and then enciphered before transmission. Three methods of digitalization are currently in use: Delta-modulation (Delta-mod), Pulse Code Modulation (PCM), and Vocoder followed by PCM.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

[redacted]

3. Non-digital Speech Security.

3. a. In non-digital speech security systems the speech signal is generally filtered through a set of band pass filters which divide the frequency spectrum of the signal into a set of adjacent frequency bands. The output of each band is a waveform whose frequency content is limited by the band pass filter. To these outputs are added or subtracted signals of constant frequency. The frequencies of the additive or subtractive signals are so chosen that the resultant frequency bands exhaust the frequency bands of the original signals. Some of the frequency bands may be inverted during this process. The signals are then mixed to form a new signal which is transmitted as enciphered speech.

[redacted]

PL 86-36/50 USC 3
EO 3.3(h)(2)

[redacted]

Analysis of this type of system can be performed by comparison of the signal waveforms with known segments of voice waveforms. It is believed that from this type of analysis various kinds of split band systems with or without transposition and/or inversion of bands may be reconstructed. After such reconstruction, the intercepted signals become readily readable.

Some consideration is being given to the desirability of developing a flexible (with regard to number and size of bands, transposition of bands, and inversion of bands), non-digital speech security intercept equipment.

V. FACSIMILE INTERCEPT

At the present time, the Agency is engaged in a relatively small facsimile intercept operation, there being only approximately 10 facsimile intercept positions in operation. The systems currently being intercepted are not encrypted. Much of the intercepted traffic is recorded in the field on magnetic tape and forwarded to NSA Headquarters for central processing, although a small amount is recorded on facsimile equipment in the field.

The problem is not very difficult, but some mechanization can be effected to improve efficiency. At the moment, reproduction from the magnetic tape recordings at the Central Processing installation is subjected to distortion due to tape stretch and reproduction on a machine which, although of the same type as the recorder in the field, is slightly different due to normal engineering tolerances permitted in production. As a result, an operator must scan the facsimile picture as it is being reproduced and attempt to compensate for the distortion by manual adjustments. R/D has recently developed a device for recording a reference tone on the magnetic tape in the field, and then automatically using this tone upon reproduction to compensate for the normal distortion. This equipment greatly reduces the burden on the operators and is expected to result in a marked improvement in the quality of the copy.

The equipment can also be used in the field to supply a synchronizing tone for on-line processing. Fortunately, a limited number of reference synchronizing frequencies have been found to suffice for all known Russian Facsimile transmissions, and the exploitation of this feature should facilitate high quality on-line processing in the field. This improved equipment is now being fabricated for service test by the services. It is anticipated that "crash production" of a limited number of these equipments will enable the currently employed facsimile positions to be converted by the end of the calendar year, while future facsimile positions should be equipped with equipments obtained through normal production channels.

VI. VERY HIGH FREQUENCY INTERCEPT (VHF)

The VHF/UHF problem has been broken into Categories I and II; the VHF problem as here discussed is essentially Category I, which is defined as follows:

"CATEGORY I comprises problems which may generally be solved, at least in part, by the application of well-known techniques and currently available equipment types. Roughly speaking, Category I communications are of wide-spread types, often low-powered, tactical, omni-directional and of a state of sophistication common among communicators of the major nations. At present, Category I communications are predominantly MCW and unenciphered speech, with possible future speech privacy, ciphony and other more sophisticated systems as the growth of the art permits. Typical Category I communication services include air-air, air-ground, tank-tank, ship-ship, ship-shore and low echelon ground-ground."

Operationally, the VHF Category I problem is very important, with a strong and increasing AFSS effort and certain near-future expansion of small Army and Navy near-VHF and VHF activities. At the present time, this problem is under study by the Special Intercept Problems Board.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

At this writing, the equipment picture in the near-VHF (20-30 mcs) and the VHF (30-300 mcs) is sad, with most service successes due to field initiative in doctoring available receivers and preparing special antennas. However, an improved, militarized receiver, the R-220 (also known as the AN/URR-29 when equipped with antennas of no particular COMINT use) is scheduled to come off the line in limited quantities before the end of calendar 1955. While this receiver, which covers the range from 20 to 250 mcs, may fall considerably short of the ideal, its great superiority to older receivers in the field and the fact that it is under quantity procurement by all three of the service cryptologic agencies should soon bring a considerable strengthening of the Category I intercept effort. In the 100-150 mcs. range, of prime importance to the Air Force and also of great Navy significance, a commercial receiver the Clarke 167J1 is applicable. This receiver, which has been the backbone of the AFSS effort for the last three years, will probably have even greater future usefulness. Antenna-wise, local initiative has been the major source of improvement. Although

[redacted]

At present, R/D is continuously monitoring all military and commercial receiver and antenna developments which are applicable to this problem. Plans are under way to exploit the "hot" Clarke in an effort to provide maximum receiver sensitivity for special Category I problems. The "hot" Clarke is a standard Clarke 167J1 with an NRL developed low-noise preamplifier and any one of several appropriate bandwidth reduction systems.

Recently R/D has been authorized to establish two experimental field research and development positions on the VHF intercept problem, one in the far East and the other in Europe. These units are expected to be activated before September 1955, and should enable experimental equipments and techniques to be evaluated and developed under actual field conditions.

Future R/D plans call for service testing of "hot" Clarke receivers, and the development of panoramic receivers and adapters for use in the 100 to 150 mcs. range, where an operational requirement has already been expressed by AFSS. The study of antennas, such as the vertical rhombic developed by the Bureau of Standards, and the retention of commercial antenna consultants will aid in eventually bringing to the field antennas with maximum directivity. It is also intended to study rotators and towers to assure the field of antenna systems of maximum operational utility. It is intended to strengthen R/D Field Support through several activities;

(a) Continued and expanded field trips.

(b) Establishment of a task type contract to provide a ready source of development equipment for the R/D Field Positions.

(c) Establishment of a local experimental mobile van which will be used as a proving ground for equipment and techniques. To assure maximum understanding of propagation phenomena, contacts have been made with NEL and CRPL of BuStandards, to determine what assistance they can provide for prediction in the VHF range; two outstanding CRPL men are now being cleared for COMINT so they can be brought into the entire problem.

VII. ULTRA HIGH FREQUENCY INTERCEPT (UHF)

The VHF/UHF problem has been broken into Categories I and II; the UHF problem, as here discussed, is essentially Category II, which is defined as follows:

"CATEGORY II comprises special systems, often highly directive with complicated multiplexing and high traffic densities used in relay type systems on a point-to-point basis; "High Level" traffic may appear in appreciable quantities on these systems. Category II represents technical and operational problems of a higher order of difficulty than those in Category I and, therefore, may require

PL 86-36/50 US
EO 3.3(h)(2)

research and development, special equipment and personnel for each new problem."

[redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

As in the case of VHF intercept, it is intended to strengthen the R/D Field Support through several activities:

(a) Continued and expanded field trips. Further, a contract is being negotiated for a total of 6 field technical representatives. Although the impetus for this "Tech Rep" program has come from the Category II, program, these people will be used for other purposes, notably VHF Category I, as the occasion arises.

(b) Establishment of a task type contract (to be shared with VHF) to provide a ready source of development equipment for the R/D field positions.

(c) Establishment of a local van (to be shared with VHF) which will be used as a proving ground for equipment and techniques.

To assure maximum understanding of propagation phenomena, contacts have been made with NEL, and CRPL, of BuStandards, to determine what assistance they can provide for prediction in the UHF range; two outstanding CRPL men are now being cleared for COMINT so they can be brought into the entire problem.

VIII. COMMENTS AND RECOMMENDATIONS

1. The amount of R/D effort currently being placed on each of the problems associated with the generation or intercept of "other signals" is implied in the section discussing the signal. The problems are sufficiently diverse and important to recommend continuation of

PL 86-36/50 USC 3
EO 3.3(h)(2)

the current R/D effort being placed on them.

[redacted]

3. The problem of detecting radiated plain text signals in the cipher signal is in some respects similar to the problem of detecting a signal in the presence of noise. Communication theorists are doing considerable work on the general signal detection problem. Only a limited amount of work is being done in the Agency. It is recommended that the Agency increase its present efforts in this problem.

4. The analysis of non-digital speech security systems currently requires equipment capable of splitting and mixing frequency bands. At present very little R/D effort is being placed on the development of new techniques and equipments. It is recommended that more effort be placed on the problem.

5. The problems of decrypting sophisticated ciphony and cifax systems have, as yet, received preliminary consideration only. It is recommended that a plan be drawn up and approval sought, for a powerful attack on these problems.