~~TOP SECRET~~

MECHANIZATION IN SUPPORT

OF COMINT

PHASE III - FIRST EDITION

Appended document contains codeword material.

1 July 1955

COPY 8 OF 47 COPIES
PAGE ____ OF 72 PAGES

INTRODUCTION

Phase III of MECHANIZATION IN SUPPORT OF COMINT consists of a collection of suggestions for solution of some of the problems discussed in Phases I and II. Some problems have several suggested solutions. This should not be a deterrent to further analysis on these problems. In fact, it is hoped that readers of this report submit rebuttals and/or improvements to the suggested solutions to those problems of Phases I and II not adequately covered. The success of this study will strongly depend upon the number of individually suggested solutions from which an integrated solution can be drawn.

This report is only a first edition and contains suggestions submitted to the editors prior to 1 July 1955. Wherever known, the source of a suggestion is given. Future editions and supplements to this edition will be issued depending on the need for the inclusion of further suggestions, revisions, and integration. Readers are again invited to submit material for inclusion in future editions and supplements.

TABLE OF CONTENTS

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

INDEX

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

NOTE: Numbers refer to articles in PHASE III

This suggestion was made in a memorandum to Dr. Kullback by Mr. A. I. Dumey on 3 June 1955

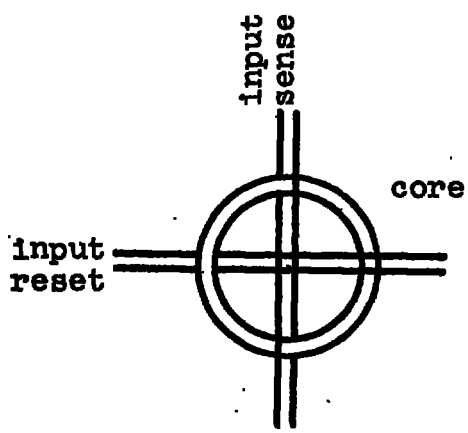
CHANGEABLE STATOR

In a paper written last December, I described a method of producing the development of a rotor by means of a core matrix and a set-reset procedure. Further work by R. Moulton of NSA-36 and S. Rubens of ERA subsumed this work, first by substituting the normal alphabet slide development for the developed rotor, and then by using a transistor array for the cores.

However, the wired rotor, under this arrangement becomes a stator, e.g., a plugboard, a terminal strip, an actual rotor, or the like.

There still remains the problem of rotor (stator) change, which would be accomplished by switching if the rotors are known.

Here is a method of producing stators at relatively high speed, on an arbitrary basis, one embodiment of which is shown.



Part of n^2 array of cores

There are two horizontal wires per core, one of which (the input) carries half current in either direction, the other in only one. There are two vertical wires, one of which is a setting wire, the other an output wire.

Originally, an n^2 array of such cores are all set (say) negative by pulsing all reset-input horizontal pairs.

The stator is then set up for use by setting successively each core corresponding to an input-output connection. Thus if $A_p = Q_c$ the A input horizontal line, and the Q vertical input line are pulsed, each with half current. n such choices constitutes the stator.

During use, any selected input causes the corresponding horizontal pair to be pulsed negative for reset, which attempts to reset the whole line. Since the matrix is a Latin square, only one core is actually reset, and the vertical sense line carries an output pulse to the slide matrix. As step two the input horizontal line, and the vertical input line activated by the associated chosen sense line, are pulsed positive, which puts the reset core into the ready state again.

The wiring shown is one of several possible. I will consider later the advantages or disadvantages of a three-core-per bit array for this purpose.

Realizing that the two step procedure is slower, I suggest that the transistor approach be studied to see whether it can be used here

also. This seems reasonable to the extent at least that a flip-flop embodiment of the device described seems possible.

As in the core device I wrote about in December, passage of a pulse through a cascade occurs sequentially, so that the motion must be programmed through delays.

This suggestion was made in a memorandum to

Mr. J. C. McPherson, Chairman NSASAB,

from Mr. W. L. Lawless, Jr. on 21 September 1954

THE MEDIUM SIZE EXPERIMENTAL JOB

There appears to be a need for an intermediate machine facility to provide better support to experimental analysis. Apparently, large experimental jobs are scheduled on available machines; small ones are often done by hand; intermediate sized jobs, unless very simple to plan and to get under way on machine equipment may not be done at all. This is especially true if the probability of worthwhile results on the project is not too great. Unfortunately it is in this intermediate area that many excellent solutions have occurred. This intermediate size analytic experiment is often the experiment that leads to an analytic solution rather than a brute force solution. Ideas and experiments in this area should be given the strongest machine support rather than the weakest.

I believe that the reason for the inadequate support in this area is, to some extent, due to shortages in machine personnel and facilities but is, to a far greater extent, due to the difficulty of planning, programming, and getting under way a complete job. The elapsed time to complete such a job is often substantial. Therefore unless the job is considered very important and is strongly supported there is a tendency not to attempt the job by machine. A

much smaller and perhaps less likely of success version of the job may be attempted by hand. Or perhaps, in some cases, the idea just isn't pursued.

This problem is not solved by getting more planning and programming personnel, or by setting aside a computer or two exclusively for this type job. The basic problem is, I believe, that it takes too long to program computers for the one time experimental job, and that, conversely, it takes too long to process many of the more complex experimental jobs on standard tabulating equipment. I suggest that the solution might be analytic machines which are aimed more directly at this intermediate experimental job.

What would be the general characteristic of machines aimed more directly at these jobs? Certainly one characteristic would be greatly simplified and much faster programming. Ease of machine set-up is important. Processing time must also be faster than possible with tabulating equipment on a typical complex, one-time job. On the other hand, these machines need not be competitive with computers or with very high speed analytic machines. In addition flexibility and reliability must be characteristics of this equipment.

In thinking about these characteristics it seemed interesting to note that most of them exist in the multiple machine tabulating installation. The major weakness in this system is the slow processing time. Thus if we had a machine system analagous to a tabulating system but with faster processing speeds, more capacity, and probably

a different processing medium; (e.g. magnetic tape instead of cards) yet still retaining the separate machine concept and the simple (probably plugboard) programming approach; we might have an excellent answer to the intermediate, analytic job.

I am doing some further thinking about this intermediate machine concept and will write up my thoughts on a possible system of machines in the near future.

This suggestion was made by Mr. A. I. Dumey

in a progress report to Dr. J. J. Eachus on 8 October 1954

RECOGNITION UNIT

Consider a configuration of magnetic cores of the "myriabit" memory type described by Rajchman. Such a memory locates a unique core in its plane corresponding to a 4-digit number, where the first two digits locate the x coordinate through a 10 x 10 translating square, and the second pair of digits do the same for the y coordinate.

If 10 such planes are used like a Whirlwind memory, each stands for a particular 5th digit of all 5 digit numbers, where the first four are located in the manner described in the preceding paragraph. Thus the output of such a core can be examined by the output storage, resulting in an overall saving in driving tubes and power.

Similarly, if three planes are assigned to each fifth digit, resulting in a memory of 10,000 thirty bit words, weights from ∅ to 7 can be assigned, etc.

Although this is a lot of hardware, it may be worthwhile to keep it in mind because:

a. The cost of this type of memory is going down steadily.

b. Such a memory is loadable from magnetic tapes or other high speed input.

c. The contents of the memory are easily changeable.

d. The problem of setting forth all differences of 100,000 groups in a memory is taken care of.

e. The system is quite fast.

f. However, for literal pentagraphs, the system seems as uneconomic as figuring out the weighted differences of 10 million groups among themselves. For literal tetragraphs, I think a feasible configuration may be worked out.

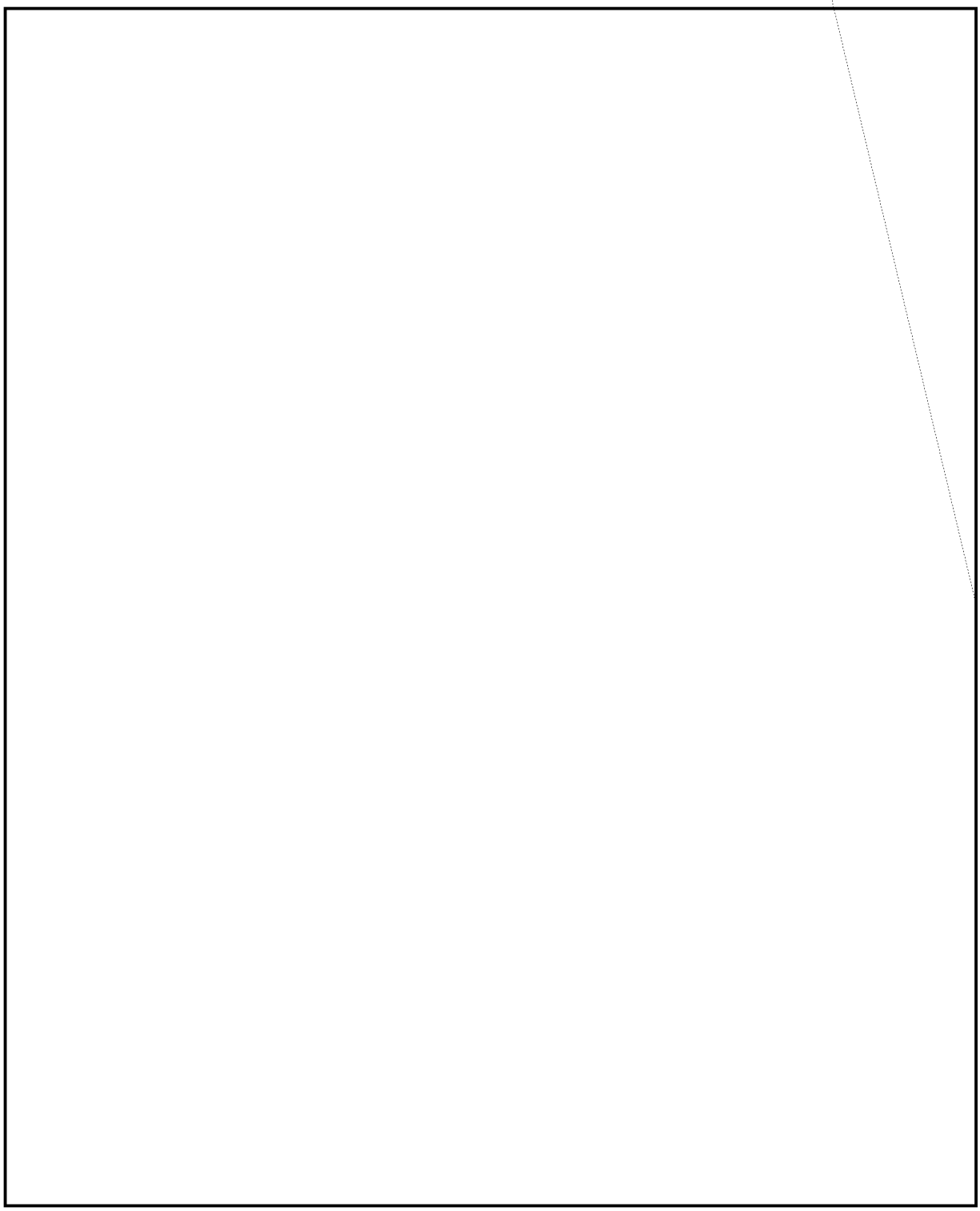
This proposal for a [redacted]

was prepared by Mr. R. L. Bowman on 16 December 1954

PROPOSAL FOR MURDOCK

This paper briefly outlines a proposal for an analytic machine

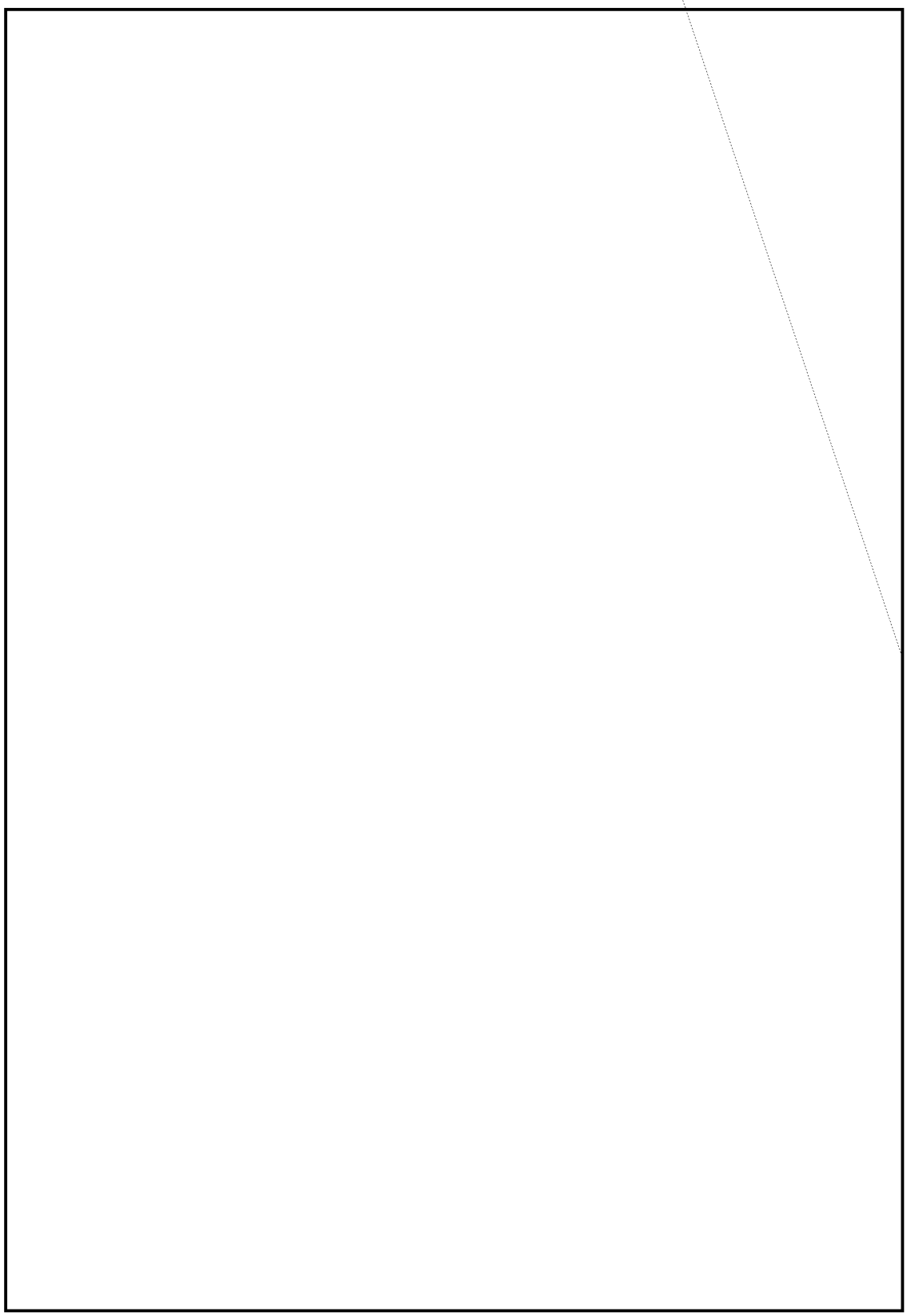
[redacted]

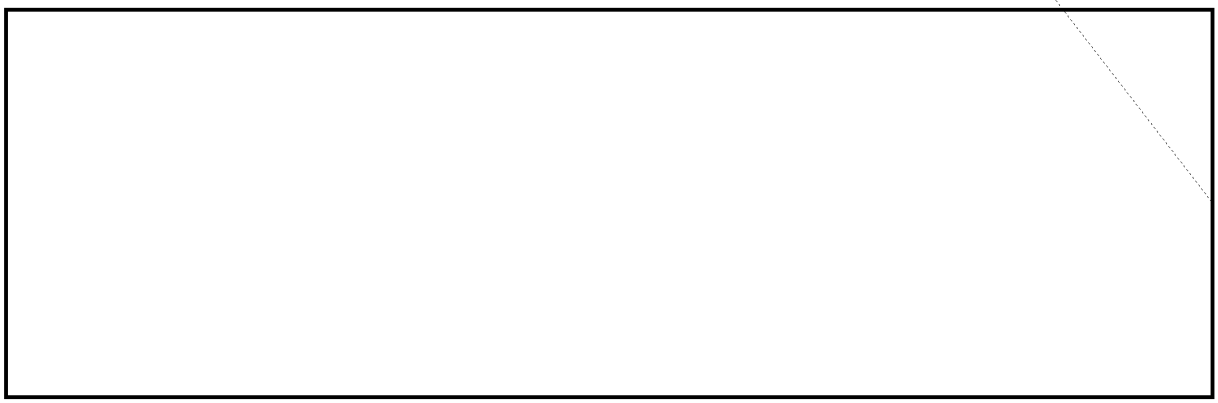


PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

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





WIRE 9

FIGURE 1.

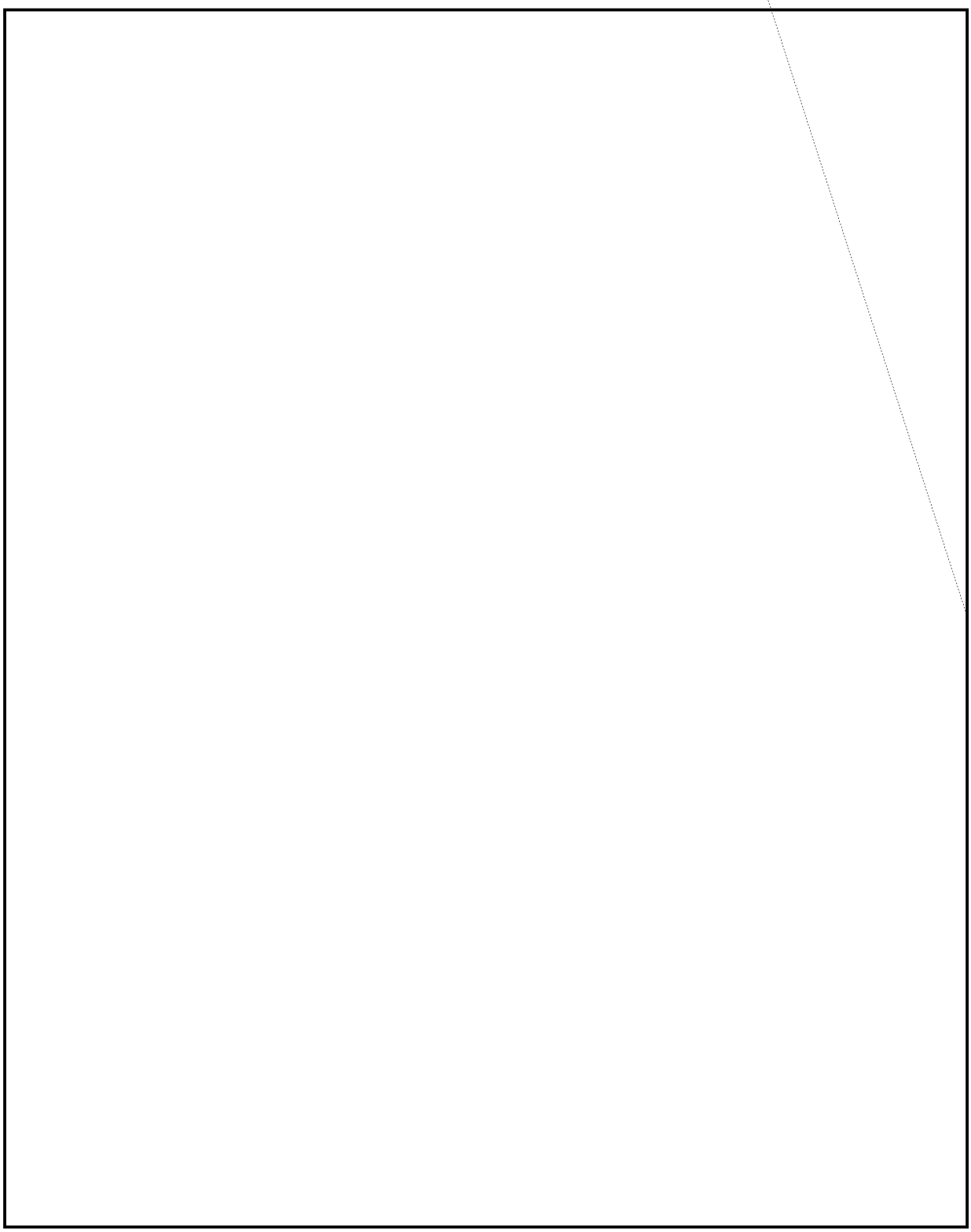
This proposal for a [redacted]

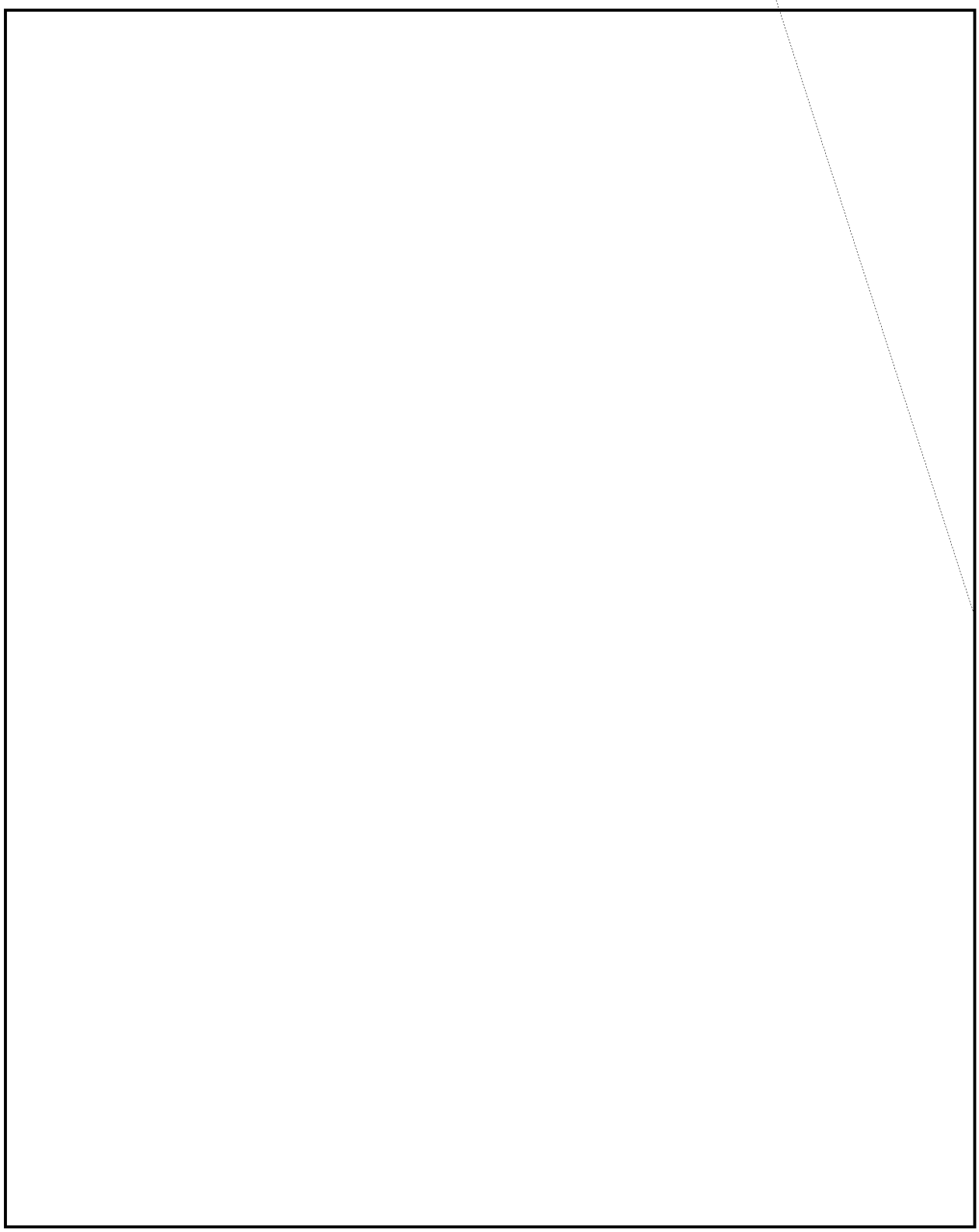
was prepared about February 1955 by Mr. D. L. Hogan, Mr. B. B. Desmond, and Miss M. J. Hobbs

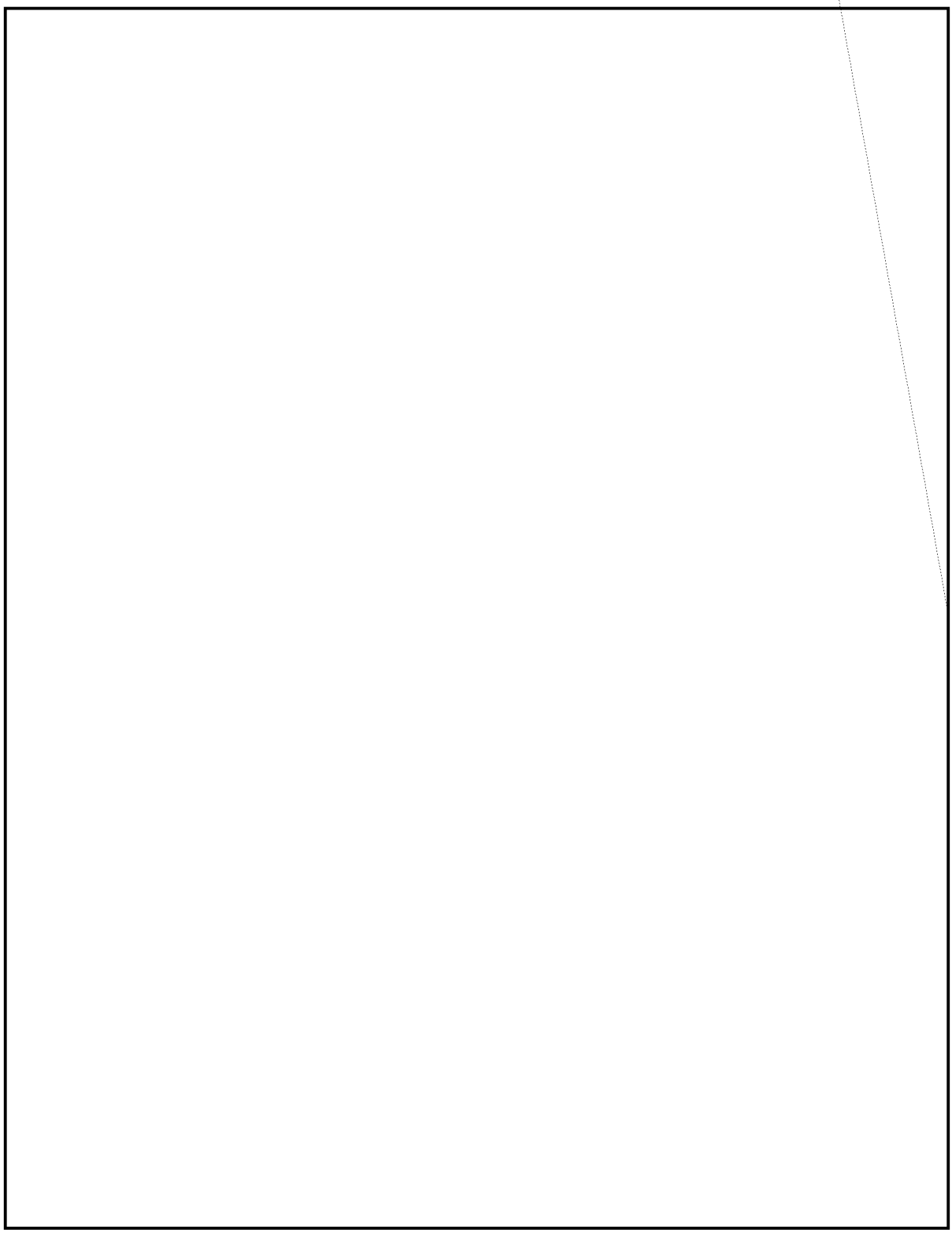
PROPOSAL No. 2 FOR MURDOCK

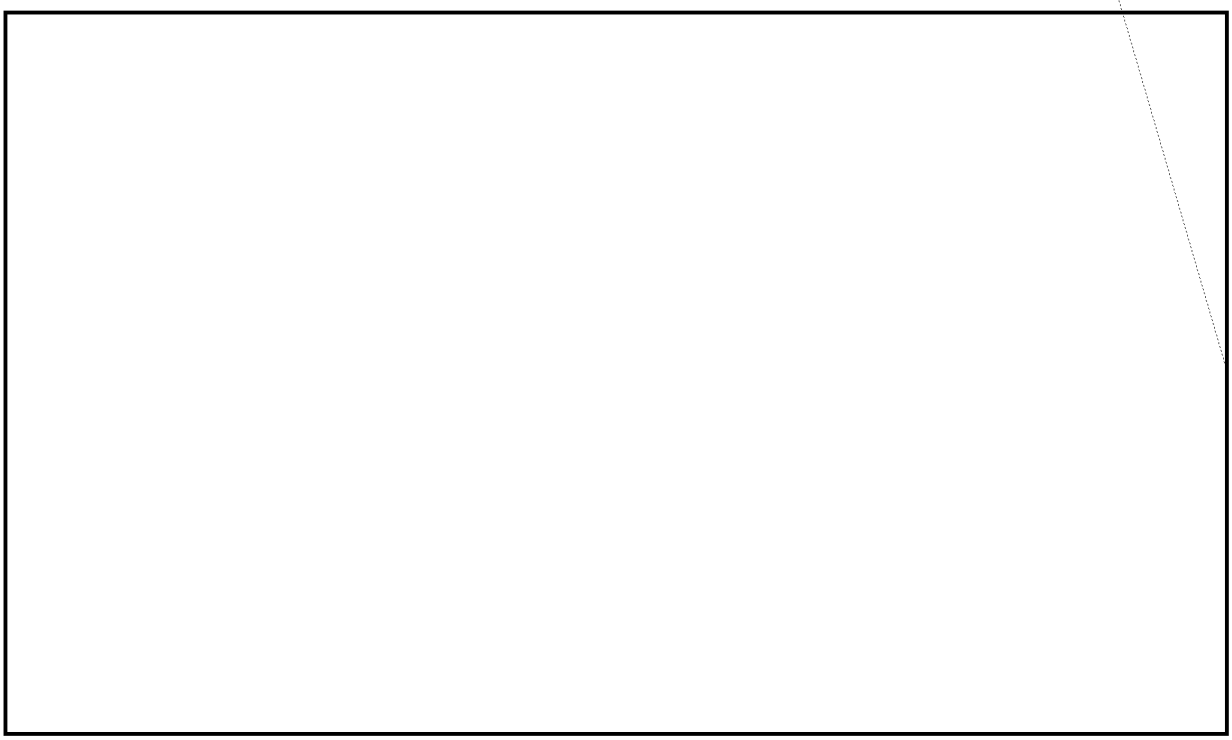
This proposal describes an [redacted]

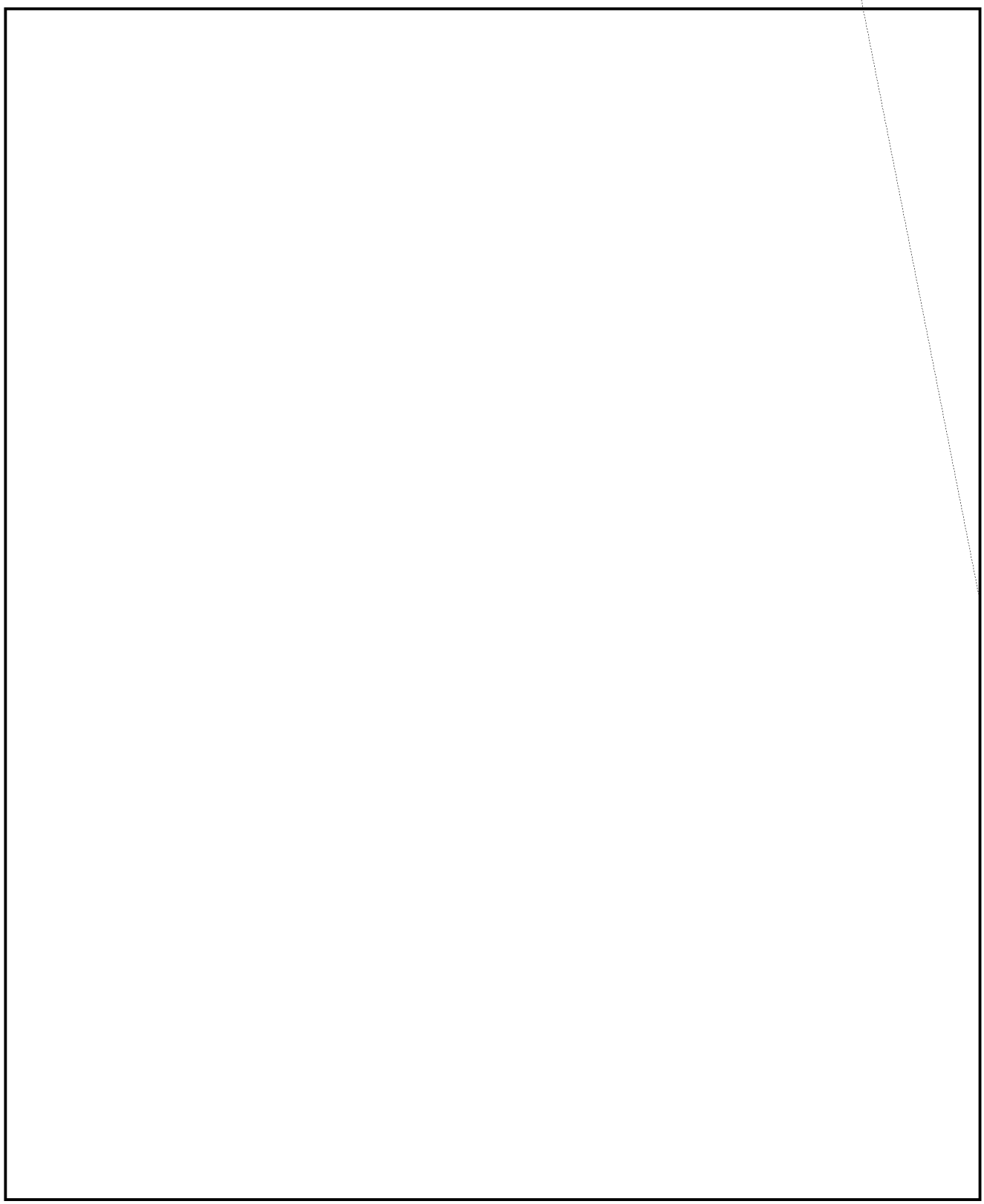
Briefly the logical procedure of the device is as follows: [redacted]

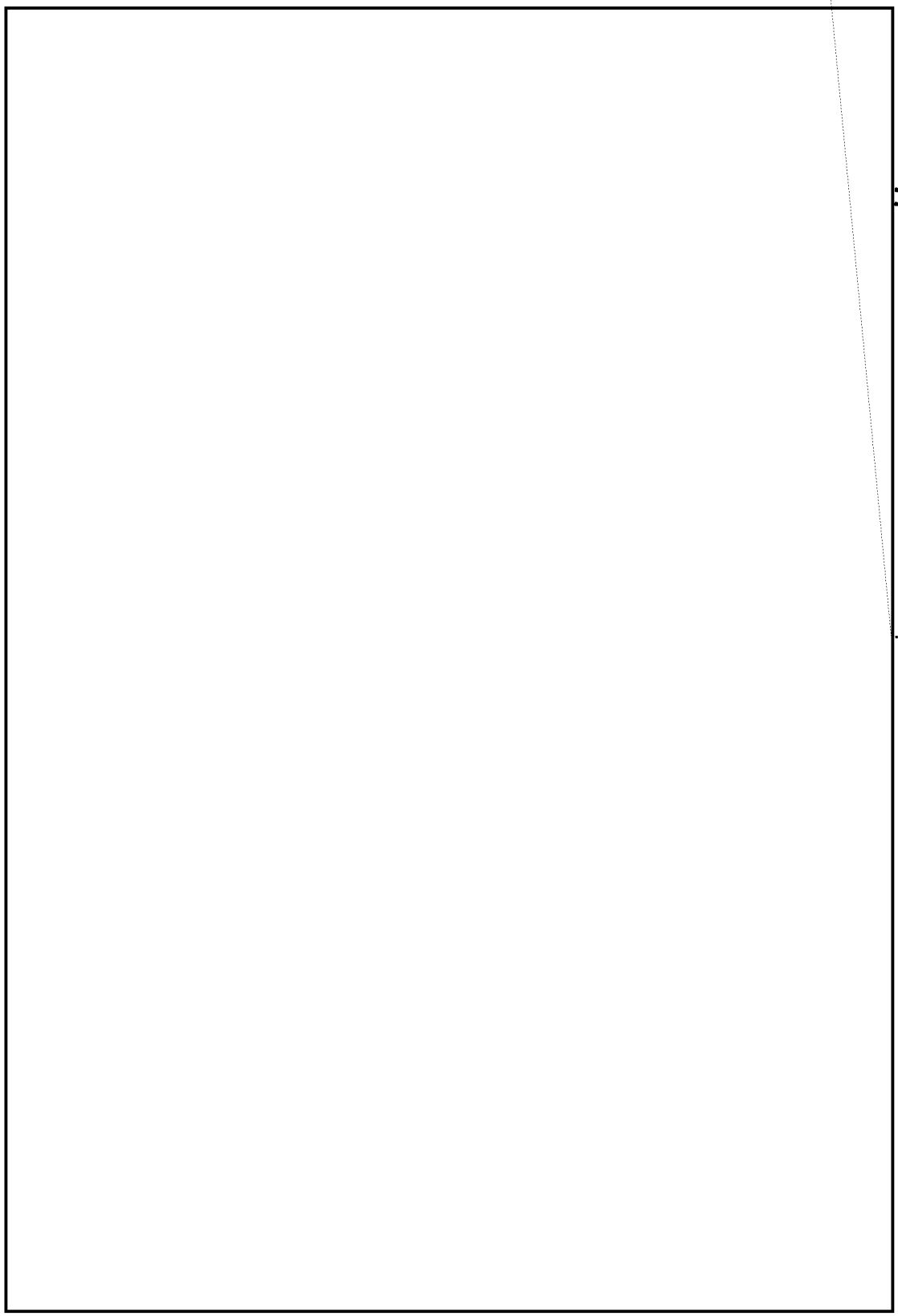




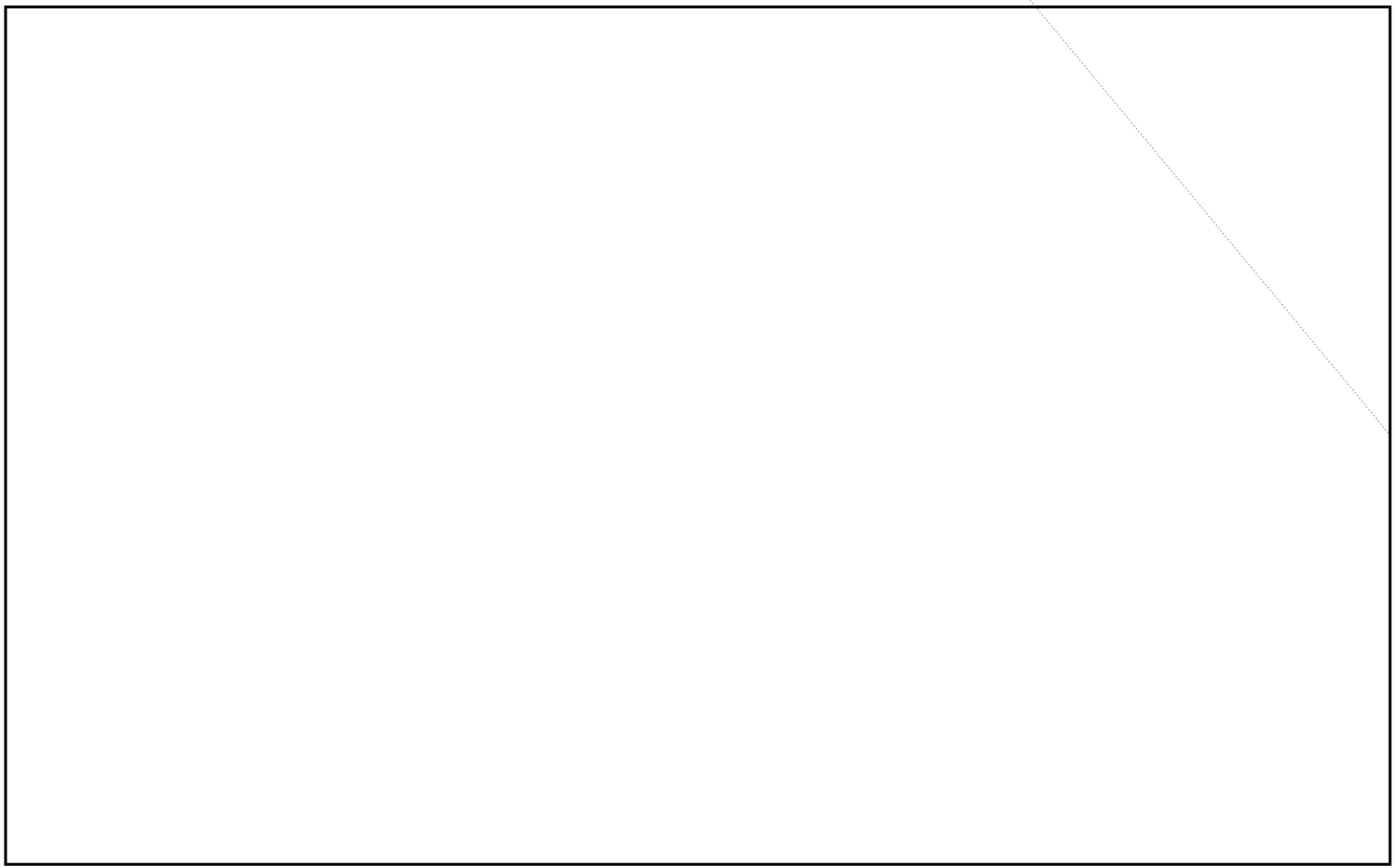








lect



This memorandum was prepared by the
Sub-Panel on General Purpose Analytic Equipment
of the NSASAB on 7 March 1955

1. The Sub-Panel on General Purpose Analytic Equipment has met twice for periods of several days at the Agency to review the development program of the Agency in this area and to try and formulate some comments and recommendations which may be helpful in extending our progress along these lines.

2. At the February meeting considerable emphasis was placed on the present state of the art and on the potentiality of achieving a very high speed arithmetic and logical unit in the milli-microsecond range. Dr. vonNeumann and others strongly urged an intensive research program in speed of components of this sort aimed at determining ultimate limits of the physical phenomena which are helpful to very high speed devices, such as the effective grain size and other physical limits. It was pointed out in particular while there are other groups in the government interested in this area that research of this type will not get itself automatically done and that the Agency appears to be the logical organization to initiate work in this area and that support might be secured from other sections of the Defense Department and the AEC if such a program were undertaken.

3. A general concept for a General Purpose Analytic Machine was set forth as a programmed-sequence-control machine incorporating

ancilliary units carrying out specific cryptologic operations or processes. In order to meet the wide variety of requirements in various types of work in the Agency it was felt that such a machine should have the capacity of modifying its instructions by a technique such as micro-programming which will permit the construction of new instructions which the machine can carry out after its completion and while it is in use. This would also permit the creating of complete instructions on what are essentially short high speed sub-routines which can be called into operation by a single instruction and applied repeatedly by a mechanism such as the 1103's repeat instruction.

4. A third requirement in the machine would be the development of some way of introducing a parallelism in the operation of various portions of the machine so that the quantity of work produced can approximate in some special cases that of special purpose analytic machines such as the comparators or the sled type machine.

5. It is felt that for this general area of machine operation a basically different logical organization from that of the customary electronic computer may be preferable. One point in particular in which there seems to be general agreement was that essentially all data processing and manipulation involves two streams of data and that the machine should be organized so that work can be effectively carried out on the basis from input through processing to output and the arithmetic unit be connected between the two streams and perhaps followed by a comparison device between the two streams. It is also

felt that because of the nature of the work the machine should be fundamentally based on character-at-a-time operation with variable word, message, and record length so that a single instruction can call for the complete processing of an area of data corresponding to any one of these classes.

6. One very important general requirement is that special attention be given to the simplicity of programming the machine so that more one-time jobs can be undertaken by the programmers and even by the analysts as they encounter situations where a machine run may be useful.

7. In view of the status of the digital computer art at the present time as indicated by machines in use, it appears quite reasonable to set up standards for magnetic tape input and output operations of 50,000 characters per second; for an internal electronic character handling rate of one million characters per second; and for magnetic drum reading of 250,000 characters per second. These basic character rates can all be modified by paralleling to secure more favorable ratios between the various classes of data storage.

8. In accordance with the discussions led by Dr. vonNeumann we should certainly use the fastest possible speed in the central analytic unit and work out the necessary mechanism for combining this high speed unit with the slower memories which are all that are available at the present time.

9. A discussion submitted at the last meeting with Mr. Snyder and Mr. Lathroum concerning the Farmer Project indicates that this program incorporates much of this thinking and is approaching a point where some definite design decisions can be made leading to the starting of a minimum system to which additional units can be added as developed. There is, however, a basic difference in that the Farmer system considers the individual analytic units as special machines which can be operated independently with separate input and output. The computer with its programmed sequence control is a vital but not essential one of the machines in the system. This in turn implies that the various machine units in the system have logical programming ability and that control would be passed from one machine to the next as it completed its work on some particular data. For instance, a minimum system might consist of input and output units, a modular arithmetic and a scoring unit, and this machine would be useful without the computer and its overall program control.

10. Because of a similarity between the Farmer Program and suggestions made by Panel Members in regard to the General Purpose Analytic Machine, it is strongly recommended that additional analytic and engineering effort be devoted to defining the elements of the Farmer System and to tablishing design standards for the system and review of possible logical organizations of the computer and of the auxiliary units such as comparators, the recognition units, rotor analogs, etc., and in particular, that the set of instruc-

tions particularly those which are peculiar to this work, be formulated for discussion and comparison with the most advanced digital computer machines.

It is well known that a wired rotor may be represented by a (1) a matrix, (2) a modular addition, a substitution, and a second modular addition. For a multiple path rotor operation, a cyclic shift of a set of lines is required instead of a modular addition. The following suggestion for a Cyclic Shifter was prepared in 30C by Mr. R. E. Winter on 8 June 1955.

A VARIABLE MODULUS CYCLIC SHIFTER

Given Y inputs and X outputs equal to $(2^{m+1}-p)$ where m+1 is equal to the number of binary levels, 2^{m+1} is the major modulus, and p is two's complement of the minor modulus $\leq 2^{m+1}$. X is to be a cyclic function of Y. Figure 1 is a cyclic shifter of a fixed modulus 2^{m+1} with $m = 4$. There are thirty-two input lines with subscripts denoting levels in the logical network. Thus, input 1_o represents the first line of the zero level; 2_o, second line of the zero level; etc. An output of a logical level is denoted by the algebraic sum of the level inputs when the binary level is active, i.e. line 2_o+2^o, when active, becomes the input to line 3_1 and line $2_o+\overline{2^o}$, when active, becomes the input to line 2_1, etc. Thus, any output is equal to the input line plus the sum of its binary shifting value modulus thirty-two. Using existing circuit techniques, i.e. diode-tube logic would require a 0.25 μs delay per level or 1.25 μs delay for the five level

cyclic shifter. The number of logical AND elements required would be three hundred twenty elements, or in general $(m+1)\ (2^{m+2})$ elements.

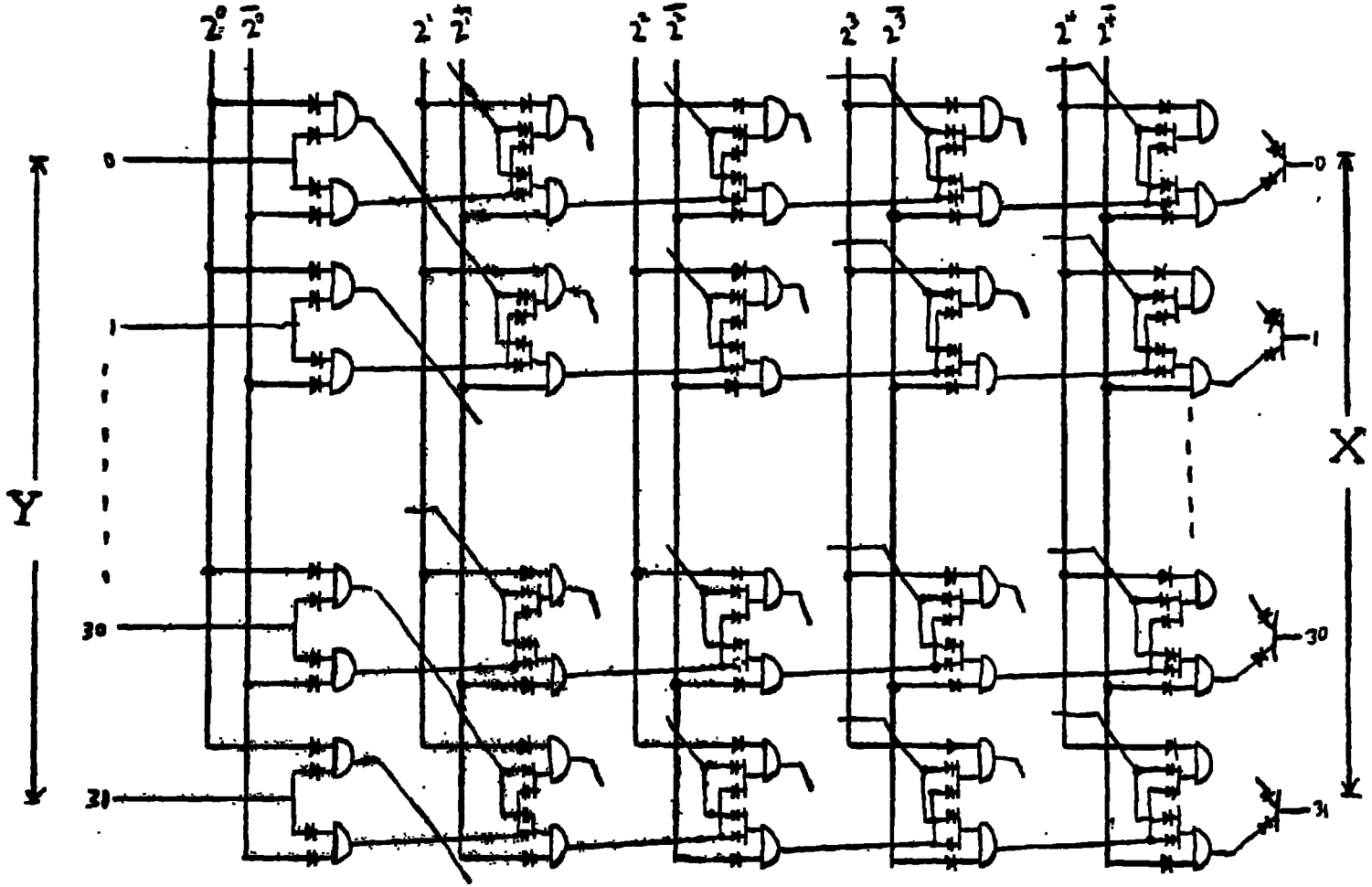
Figure 2 outlines a variable modulus cyclic shifter with major modulus 8, and minor modulus 5. i.e. m= 2, p = 3 with the following restrictions:

(a) A given minor modulus must be plugged.

(b) The binary shifting value must be limited to the minor modulus.

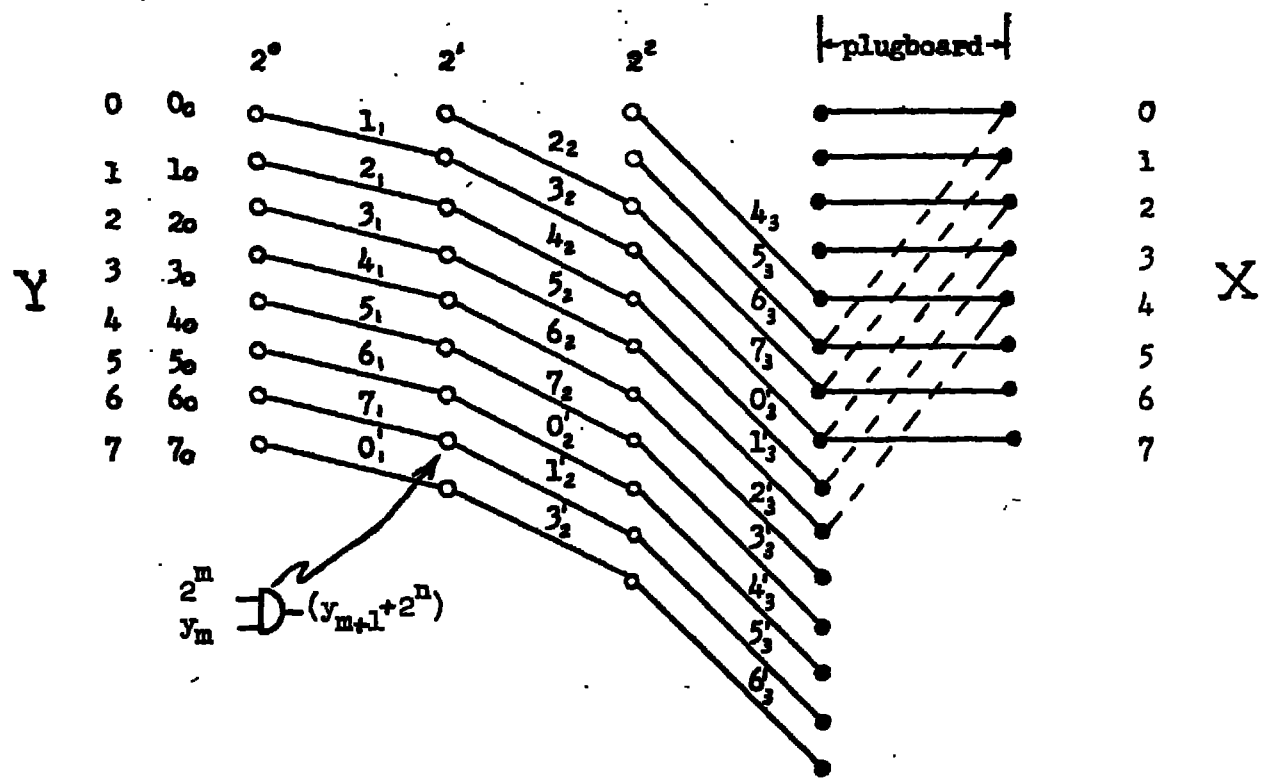
Additional logical circuitry needed for the variable modulus cyclic shifter is indicated by primed numbers, or in the case of Figure 2, twenty-two logical AND elements, or in general, the additional circuitry would be $2\sum_{q=0}^{m}(2^q-1)$. Thus, the circuitry to change Figure 1 to a variable modulus would be fifty-two additional logical AND elements.

	GENERAL MATRIX	VARIABLE MODULUS CYCLIC SHIFTER
m	$(2^{m+1})^2$	$(m+1)\ (2^{m+2}) + 2\sum_{q=0}^{m}(2^q-1)$
1	16	18
2	64	56
3	256	150
4	1,024	372
5	4,096	842
6	16,384	2,032
7	65,536	4,590



MODULUS = 32, M=4

FIGURE 1, FIXED MODULUS CYCLIC SHIFTER 5/20/55



Major Modulus=8, Minor Modulus=5; m-2, p-3

Figure 2, Variable Modulus Cyclic Shifter (shifted part only)

SECRET

A method for fast addition suitable for [redacted] "Bucket.Brigade" adders is proposed here. This suggestion was prepared in 30C by Mr. D. L. Hogan and Mr. R. E. Winter on 13 June 1955.

MAGNETIC CORE ADDER

If given an n digit binary number to which m digits are to be added, $m<n$. Addition of m and m of the n digits must have the characteristics of a full adder, i.e. being able to sum two digits and a carry, whereas the higher order (n-m) of the m digits have to propogate carries only. One solution of such a problem is a fixed magnetic core memory to perform the summing of the lower order m and n digits by use of a look-up table, and a rapid carry circuit for the higher order (n-m) digits.

An example with $m = 3$, $n = 9$ would consist of a magnetic core memory of sixe $8 \times 8 \times 4$. In general, the size of the core memory if its coordinates are X, Y and Z would be $X = Y = m^2$, $Z = m + 1$. One set of three binary inputs would be translated to one of eight columns; the other set translated to one of eight rows. The table is four deep to represent the sum of any two three digit binary numbers. The fourth digit of the sum will be used to propogate a carry for the higher order (n-m) digits (see Figure 1.).

For the higher order (n-m) digits a fast carry can be propogated in the following manner. The carry digit is supplied to all carry gates

of the (n-m) digits. Each carry gate is enabled by all preceding (n-m) digits in the "one" state. An active carry gate turns on the succeeding digit as shown in Figure 1. The first digit of the (n-m) group of digits to change state from 0 to 1 would reset all preceding digits of this group (this resetting is not shown in Figure 1).

It should be noted that the operation of such a device requires several steps. Suppose the sum is considered the output, then the following steps are required:

1. Clear the output, reset the fixed wired look-up table.
2. Transmit (a) column and row inputs to the magnetic core adder, (b) set the higher order (n-m) levels of the output if a preset number is desired.
3. (a) Sample the output of the magnetic core memory and set up the lower order m digits,
   (b) Propogate the higher order carries.
4. Transmit the output to its destination.

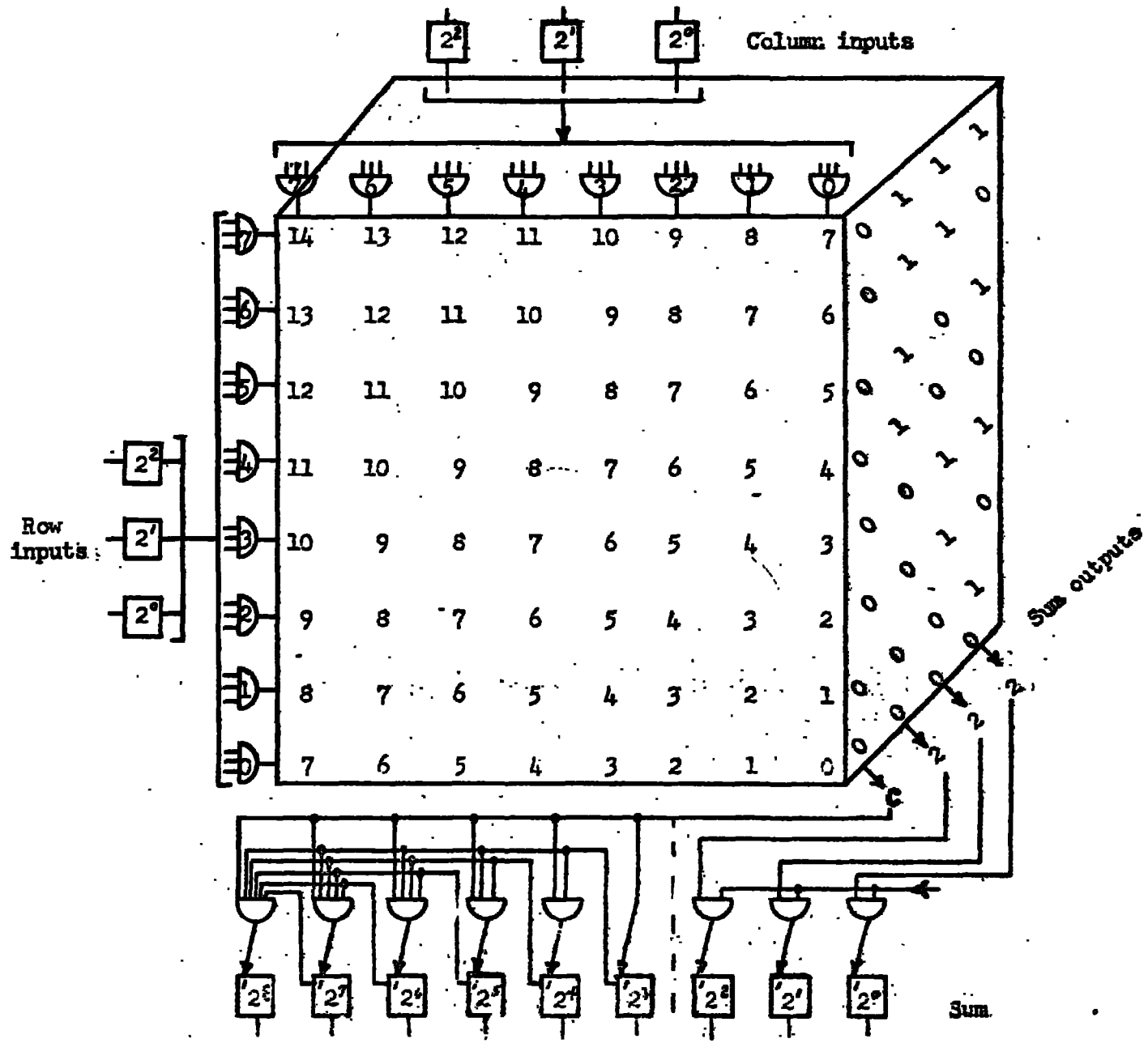


Figure 1.

CONFIDENTIAL

This suggestion was presented to 30C

by Mr. Dale Marston on 14 June 1955.

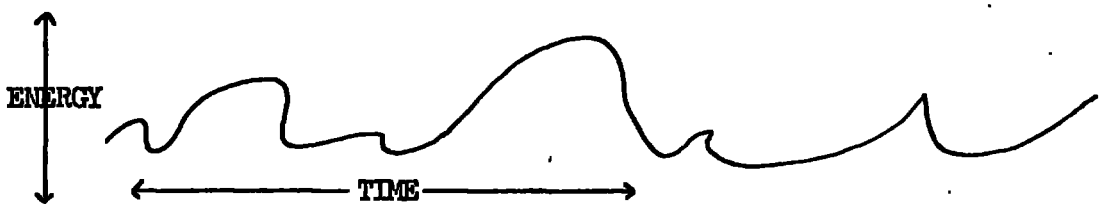
THOUGHTS ON DIGITAL RECORDING OF INTERCEPT

Let us assume that a recording is available of an intercepted signal which represents that signal in bit form. It is desired to proceed from this point to an accurate page copy of the information contained therein with certain other information that the cryptanalyst may desire.

The character of this tape is not completely specified at this time but might be defined as the energy contained in the signal during short but accurate periods of time. How short this time is or how many levels of energy must be denoted is not specified nor known.

However, if the definition is good enough to plot a curve representing the signal, it is from that point I wish to start.

Further let us assume that the signal is that of a single channel teletype, 400-OPM start stop operation. The duration of a character is $\frac{60}{400}$ sec or .150 sec. The signal is FSK,



At this stage of the game I don't even know exactly what the wave looks

like, but if I start backwards I can perhaps show what I am driving at.

The undulator tape I look at appears,

etc.

The magnetic tape from whence I get my undulator tape has a 2 or 3 kc tone representing when the original signal is marking or spacing.

At this point is where I want a binary representation instead of where we get the 2 and 3 kc tone.

This information on the magnetic tape would be fed into a computer, and a written program would take over and analyze the intelligence in the signal. I would proceed at this point to feed into the computer enough signal to represent perhaps ten characters. This would perhaps be 150 ms/char x 10 char x 1 energy char/ms. or 1500 characters. I would first try to determine the length of each baud in the teletype signal. This would be done by making a distribution of the distance between the changes from mark to space and space to mark. I would then attempt to determine the length of the character as a check. Of course, I already knew the approximate length, this is merely a check. Then I would proceed to match the optimum pattern of each character against the signal pattern and score the best match as successive blocks are fed into the computer. In the qutput I would carry along

some indication of poor matches. Further I would carry along a symbol representing the time between characters. I would tally any spurious signal characteristics which I might suspect in the signal. I would keep a running check of the timing of the teletype signal itself and keep a separate log of such information and make corrections in the analysis. I would look for certain information in the transmission such as setting up of the indicator and extract such information that the cryptanalyst needs for further analysis. I would assume that the analysis would be fairly lengthy on the computer. Special orders may be needed to handle the operations needed most often in the program. Even at the worst I think that a simple signal could be processed at 5-10 times the rate of intercept.

Although this method may be highly desirable for the simple type of signal, the real step forward lies in the more complex signal. I see tremendous possibilities in this approach such as:

Signal analysis

Demultiplexing

Dual Channel recording

Diversity reception

Radio Finger printing, etc.

I see in the future a computer coupled to the receiver not only doing the analysis but feeding back to the receiver and making necessary corrections to the tuning - even a completely automatic receiving position.

I see the possibility of handling signals which are now too poor to even bother copying. Of course, get the best signal possible if you can but if you can't -- be able to handle the poor signal.

I see further the automatic transmission of the data back to a central processing center in a form directly usable on computers for intelligence type processing.

I believe it can be done. I don't know all of the "hows" but by applying the ideas developed in the computer and telemetering business to intercept there appears to be worthwhile gains to be made.

This suggestion was made by Mr. Dale Marston on 13 June 1955. NOTE: RAMAC is a recent IBM disc memory development.

MAISIE OPERATION ON RAMAC

Although it is probably obvious to most that this device is usable for the code look-up requirement, it may be well to outline how it could be used.

The device contains 50,000 addressable 100 character blocks. An average of 500 millisec is required to read out or write into a block. The time varies from 100 to 600 ms. The present device has only one searching head, simple orders and a slow speed printer output. It was indicated that six searching heads could operate independently; also that several assemblies could be operated together.

The code group would simply serve as the address. In such a scheme 5-4 digit codes could be loaded at once and by dividing the 100 character block say into 25 character blocks 4 times as much could be handled. Likewise 5 digit codes could be handled by spliting the word in two blocks and using the first or last half according to the whether the code group is over 49,999 or not.

The majority of the codes are numeric but a four or five letter code could be handled by a double look-up. One way might be to break the group down into a trigraph and a digraph. Each trigraph would be associated with the digraphs that could follow it. Contained in the 100 character word would be the digraph and the address at which the meaning could be found. Other schemes could be used for 4 letter or lesser codes.

Additives or other encipherments could be removed by the standard order code.

The loading operation would probably be quite a lengthly operation but if several codes were loaded for use simultaneously, not much changing could be required. If the original code book was in order it is reasonable to assume that it could be loaded at the maximum rate 10 per second. Ten thousand groups would require about 1000 seconds or about 18 minutes. At the worst it would require about 1½ hours. Of course, present loading time is about 50 cards per minute.

One advantage of this device is that it could be operated directly from keyboard. Several keyboards could be operated simultaneously by using several searching heads or by a time sharing basis. Remote operation should not be difficult.

An improvement and also a simplification might be accomplished by reducing the word size to 50 characters instead of 100. This would reduce the buffers and arithmetic portion to 50 characters. This would give 100,000 addressable items. Fifty characters is more than adequate for a code meaning.

This suggestion was made by

Mr. Dale Marston on 13 June 1955

[redacted]

It seems to me that a basic improvement in [redacted] might be achieved by a type of testing with an attempt to expand a hit. Such a task of course, would depend on a mechanical expansion and would be based on language previously used in conjunction with the hit.

I would propose a secondary test based on this type of thing. There must be various ways of going about it but one way might be as follows:

[redacted]

and in any of these cases he may derive text that has not been used before but is nevertheless reasonable. There must, however, be some criterion for "reasonable". What is reasonable as compared to the fact that it has been used before? It depends somewhat on how much recovered plain text is available for study. The phrase "number _ _ _ _" obviously may be completed by any number from 0000 to 9999. However, by usage it may be known that it can only have a few limited values. At any rate it seems possible that we could specify that which has been used before and that which is reasonable to a certain extent.

Now the problem is how to go about doing this?

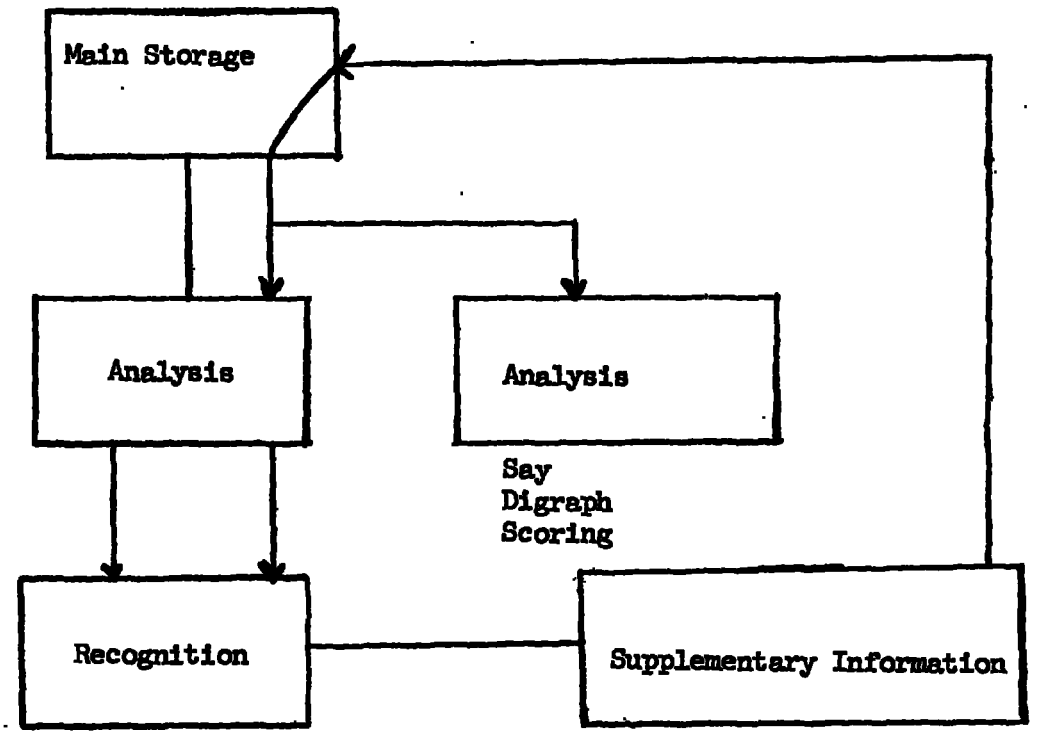
The catalogue of used plain text can be no larger than what we have recovered in most cases. That which is "reasonable" may be in the form of a collateral file, size unknown.

I would think that if in the recognition or crib test there could be associated those phrases which could be fed back into the testing operation the problem would be solved. This, however, requires a pretty large memory* It would not have to be used except when a hit was found but at that point it would have to put out the information at a reasonably fast rate.

The use of this supplementary information would require an evaluation by some other means than pentagraphs - say by digraph scoring. However, recognition of another pentagraph would start the process out again.

Considerable experimentation could be done on this hypothesis by investigating recovered systems. Indexes are available on a good deal of the plain text.

*This might be a use for the IBM Random Access Memory known as RAMAC.


Main Storage
Analysis
Analysis
Say
Digraph
Scoring
Recognition
Supplementary Information
4096
50 char-
acter
phrases.

This suggestion was made to R/D

by Mr. Dudley A. Buck in about March 1955

DECENTRALIZATION OF ANALYTIC EQUIPMENT TO FIELD STATIONS

It is proposed that analytic equipments such as ATLAS II be placed at or near intercept stations, and that such stations be staffed with programmers and maintenance personnel.

Points to be studied:

1. The traffic volume between field station and NSAW would be reduced. Intelligence digests and finished decryptions or translations would replace raw intercept. This would relieve communication centers of volume, but security level would be much higher. It is not clear, therefore, whether there would be more or less delay in the communication link between field station and NSAW.
2. The time delay between interception and analytic machinery would be reduced. By transferring analytic machinery to field stations, we are interested in cutting down the total time delay from interceptor to consumer -- not in merely shifting out present delays from Washington to some remote location.

   For example:

   If logging, editing, and punching takes two days at NSAW we have gained nothing by moving an ATLAS II into a field station if logging, editing, and punching still takes two days.

If the electrical transmission of information takes two days due to delays in information centers, we gain nothing by moving close to a field station if the delay is still two days. (The electrical signal, once on its way, accounts for about 100 milliseconds of the two-day delay.) Since waiting for favorable radio conditions is often part of the delay, however, closeness can shorten the delay time.

3. The quality of intercept would be improved by the close proximity of interceptors and analysts. Personal contact between analyst and interceptor may result in more devoted interception as the interceptor watches his copy being processed. This would be especially true of operational systems. On the other hand, if the entire volume is going into storage, perhaps it is best to store it in Washington, out of sight of the interceptor.

4. Maintenance would be difficult on remote machines unless maintenance personnel could be lured abroad.

5. Programmers might be difficult to obtain in remote locations.

   (a) They might also feel "out-of-touch" with the NSA-world and perhaps lose valuable council of "old-timer" cryptanalysts.

   (b) NSA-Europe, however, had many applicants from NSAW personnel.

   (c) Programs can be written and tried in Washington and sent out to the field.

6. Security would be adversely affected by location in the field of cryptanalysts, analytic machinery, and by the necessity for high-level communication back to NSAW.

7. The added cost of extra equipment, some of which might not be in full-time use, and the added cost of personnel transportation might be excessive.

8. Diversification in the event of war might be a valuable advantage. Another advantage might lie in the closeness of field stations to theatres of tactical operations in the event of war.

9. Communication between intercept stations would be increased if analysis is being done on information derived from several intercept stations. This would probably be raw traffic, and once again, we may move a bottleneck from one place to another.

It is therefore proposed that the following steps be taken.

1. Prepare time charts showing all delays in flow of information from interceptor to consumer for a number of operational systems in hopes that they will reveal where the bulk of time delay lies, and how much of this delay would be shortened.

2. Collect all available evidence on each of the above points by interviewing:

   (a) Intercept personnel.

   (b) Personnel returned from NSA Europe, or any other station where some field mechanization has been attempted.

   (c) Personnel in sections for which time charts have been prepared.

This suggestion was made to R/D

by Mr. Dudley A. Buck in about March 1955

MECHANIZATION OF INPUTS

Similarities between the Lincoln Air Defense System and the NSA information gathering system have led to a comparison of the two. NSA could develop an automatic input system which takes incoming raw traffic off of teletype lines and feeds it into a computer. The aim would be the shortening of delays in logging and sorting of incoming information for cryptanalysis. The possibility of doing automatic editing is not a necessary part of the system, but could most certainly be worked in ultimately. The system as outlined will distribute the information to the cognizant cryptanalytic sections, provide the section with a teletype-written log of incoming messages, distribute operator comments and chatter along with the messages, tie in with a room-full of referees who take care of situations that baffle the central computer, and who with the aid of character-display equipment can rapidly perform some automatic editing with the assistance of light-guns and a manual keyboard, and finally, the provision for assisting traffic analysis personnel with similar equipment whereby they may ask the computer (or a separate computer in communication with the central computer) for up to date information regarding the number of messages from a given transmitter within the last three hours, the number of these with exactly 110 groups, or between 105 and 115 groups, etc., obtaining answers to their questions within minutes instead of hours as in the present system.

A system similar to the present Lincoln input system could accomplish tie-in to the teletype lines economically. It is hoped that the present work on core and diode-amplifier components might include the teletype-line input problem as a toy problem toward which the researchers can direct their thinking. There are many ways to accomplish the basic job of bandwidth conversion, and the decision as to whether to use cores, diodes, transistors, or other devices is an interesting problem.

These suggestions were made to 30C
by Mr. S. S. Snyder, 3501 on 24 June 1955.

1. People in Support of Mechanization.

In the past five years, with demonstration of operational feasibility of the large automatic computer systems, there has been a tremendous change in the balance between people and machines. Perhaps the most notable difference is basically in the distribution of types of work that people perform. Much more time is spent by people interpreting machine-produced results, both because more results are available on jobs previously done on smaller scale, and because results are being generated from new jobs never before attempted.

The number of people engaged in development activities leading to new equipment, as well as the number of people assigned to operating equipment (including programming and maintenance) is far too small in view of the tremendous increase in output that has been made possible by the new developments. This shortage of planning personnel has contributed to the apparent aimlessness of the new developments, and as a result several classes of activities have been neglected or have been put off too long. Among these are research programming, high-speed circuitry studies, automatic reading and editing of intercept traffic, design of efficient desk aids to analysts, and engineering research on applications of transistors. Another effect has been that large equipment developments have been initiated with insufficient planning and little subsequent contract supervision.

Probably the greatest single contributing factor at the Agency, leading to this imbalance between people and machines, has been the ease of obtaining financial support for equipment procurement compared with the difficulty of recruiting, clearing, and training new personnel. The result has been that this Agency now has the largest digital computer installation in the world and probably, in proportion, one of the smallest staffs for its operation. And in view of the continuing need for even more large-scale developments, both general-purpose and special-purpose, our staff of research and development personnel is even weaker proportionately.

The following suggestions are offered as possible "extraordinary" steps that may help increase the strength of "people in support of mechanization":

(a) Establishment of a ratio of "people to equipment" for operational equipment. Similarly, both for development projects based on fulfilling PROD requests and for long-range R/D, some optimum basis should be determined for analytic and engineering personnel engaged in R/D activities. Maintenance of this ratio should be a responsibility of administrators at a level having authority to enforce it.

(b) Keeping in mind the possibility of changing emphasis in types and relative volume of work by analysts (for example, greater proportion of time spent handling or interpreting results produced by machine than was required before those machine jobs were available), consideration should be given periodically to transfer of personnel from PROD analytic activities to either PROD machine activities or R/D machine development.

The contributions to Agency cryptanalytic successes by machine developments justify support from PROD areas which have benefited, primarily because PROD is the best source of experienced cryptanalytic talent needed to improve machine design and operation activities.

(c) Establishment of personnel practices that encourage transfers of competent people into the field of equipment operation and planning. There must be recognition of the professional standing of people in this field, including encouragement of participation in activities of professional societies, undergraduate and graduate training, etc.

2. Local Mechanized Support.

The use of analytic equipment directly by analysts, or under their immediate control, has grown gradually but with little direction during the past few years. Development of decentralized machine aids has been slow because of difficulties from both analyst's and machine personnel's points of view. On the one hand, analysts have opposed location in their immediate vicinity of fairly large equipment which dissipates heat and noise, while maintenance of decentrally-located equipment has at times been inconvenient from maintenance engineers' point of view. Also, requests for small desk-top equipment have been slow in being fulfilled, partly due to difficulties in designing "silent", small-size, efficient equipment. At the same time, objections are raised from time to time by analysts because of administrative delays in processing machine work through regular Machine Division channels, or difficulty in getting help on what has been described as "one-time intermediate experimental jobs".

The following actions have been taken, more or less responsive to the needs and pressures mentioned. Several PROD divisions have their own machine rooms where various counting, deciphering and special-purpose equipment is operated. Projects are under way for construction of desk-top digital and alphabetic counting equipment (TERMITE, DIAC). An experimental installation is planned for remote-operated computer equipment to be shared by three or four PROD areas ("ROGUE"). Multi-purpose counting equipment is being designed (TOTALIZER) for performing selected monographic, digraphic, and various other special types of distributions and computations. Desk-size transistorized digital computer developments are under way which offer promise of eliminating heat and noise problems (SOLO).

It is suggested that the needs for local mechanized support be recognized by (1) establishing specific Machine Division group having responsibility for assisting PROD analyst machine areas, expediting machine jobs of intermediate size, and, by working closely with "area coordinators", proposing new ways of satisfying local needs as they arise, (2) increasing emphasis on automatic programming research, with particular attention to facilitating processing of new job requests within minimum administrative delay, and (3) encouraging Analytic Equipment Division researches in miniaturizing techniques which can be used later whenever large scale equipments are desired to be used locally.

This suggestion was submitted by

Mr. C. Laughlin, on 29 June 1955.

TIME EXPANDER FOR SPEECH

Purpose. The purpose of a time expander for speech is to do for the ear what the slow motion camera does for the eye. The tempo or rate of speech is slowed to allow the listener more time to reflect on the structural details of the sounds. This is accomplished by increasing the temporal redundancy and the result is improved interpretation of the meaning by the receiver, as compared with the intended meaning of the sender.

Thus, the effectiveness (success with which the meaning is conveyed) is improved when the semantic problem of language differences and transmission problem of distortion and noise is involved. By increasing the temporal redundancy to the listener, fewer errors should result since the listener has more time to reflect on the sounds and hence is better able to resolve problems in semantics and dialects. Employment of such a device in this Agency should increase the effectiveness and efficiency of linguists while reducing errors and wasted effort.

History. A wholly unsatisfactory device for reducing the tempo of speech was developed by the Kay Electric Company and is known as the Kay "Sona-Stretcher". A constant reduction of speaking rate of two to one was achieved by recording the speech at a given speed and playing it back at one-half the recorded speed through the "Sona-Stretcher". Playback at one-half the speed reduces every frequency component of the complex speech waves by one-half and the intelligence is all but destroyed.

The purpose of the "Sona-Stretcher" is to restore the frequency relations. This is accomplished by further distorting the speech by a non-linear electrical device which produces harmonics of the complex speech waves. It is then attempted to select the distortion components which are twice the frequency of the playback components.

The end result is very poor and is due in part to inherent deficiencies in the method and in part to engineering compromises in the device itself. First, the pitch is halved and cannot be removed; secondly, distortion components are passed because of compromises in the selective electric wave filters.

Prospective. Recent work at the University of Illinois appears to hold promise of being able to accomplish the reduction of tempo within certain limits in an entirely satisfactory manner. At present, the work is directed toward time or frequency compression and expansion with primary emphasis on the frequency dimension.

The value of this method in time expansion of speech has not been explored, but it obviously has many inherent advantages over the method used in the Kay "Sona-Stretcher". Sample recording made on an experimental model are indeed impressive and Dr. Cooper of Haskins Laboratories has expressed a favorable opinion of its possibilities and an interest in determining the general value of time expansion of speech.

A description of the method will not be given here since an excellent and thorough discussion may be found in the article "Method For Time or Frequency Compression-Expansion of Speech" by Grant Fairbanks, W. L. Everitt and R. P. Jaeger, Trans. IRE-PGA, AU 2. No. 1, 1954, p. 7-12.

This suggestion was submitted by

Mr. Ray D. Loyd, on 27 June 1955.

A UNIVERSAL AUDIO SPECTRUM SIGNAL GENERATOR

Purpose. To provide laboratory and field personnel with the means of generating a test signal with which to carry out research, development and maintenance of equipments.

Advantages.

a. To laboratory personnel: The means of generating many types of signals for research and development work is generally available in laboratories, but the time and effort expended in collection of required equipments and their setting up could be considerably reduced if one or more self-contained Universal Signal Generators were on hand. The Universal Signal Generator would also aid in the reduction of errors due to necessity of haywire hookups between isolated signal generating equipments now in use. Another advantage is in the reproduction of data taken at some previous time. In reproducing data it is a distinct advantage to use exactly the same signal generating equipment that was used to obtain the original data. The Universal Signal Generator is a self-contained unit and will be in one place. The isolated units of the present system will usually be in several places, and very often substitute units or systems must take their place.

b. To field personnel: The means of generating specific types of signals is seldom, if ever, available to field personnel. Failure of equipments in the field can often be traced to improper, or the lack of, maintenance of these equipments. Improper maintenance can in most cases be

traced to lack of proper test equipment or insufficient time in which to properly test the equipment. The former problem is being solved by making available the proper test equipment. The latter problem can be solved through the use of the Universal Signal Generator since it will supply the field personnel with a controllable overall check of his equipment. During period of short shutdowns there is not enough time to check equipments thoroughly by instruction book methods. The Universal Signal Generator provides a quick and efficient method of checking the condition of the equipment before it is returned to its task.

Conclusions. The circuits to be used in the design of the Universal Signal Generator are in most part already existing, both in commercial units and in our own laboratory notebooks. The final product will involve the correct assemblage of these units into one efficient, compact unit and the result will be the correct generation of controllable test signals. The foregoing idea may also be carried into the field of RF, but the specific requirements are unknown to me.

This suggestion was submitted by

Mr. John Sommer, on 27 June 1955.

SMALL GROUP DISCUSSIONS LED BY AN AUTHORITY ON TECHNICAL SUBJECTS

A large amount of basic circuit and component development is now being carried on separately in the various parts of the Agency without coordination. It is suggested that small panel discussions on technical subjects be held with an authority outside the Agency acting as the leader. In this manner all personnel closely associated with the subject would be better informed of the work, problems, and successes of others in the Agency. It is important that only those closely associated with the subject should be invited to attend these meetings. In this manner, while the groups would remain small and informal, a large amount of practical information could be disseminated. A number of speakers from the local IRE and other organizations would be flattered by the opportunity to lead such a discussion group.

This suggestion was submitted by

Mr. John Sommer, on 27 June 1955.

SUGGESTED READING LISTS

At present a large amount of worthwhile information is masked by the tremendous quantity of reading material being circulated throughout the Agency. At present there are some 23 magazines ranging in date from April 1954 to date, and innumerable lists of patents, progress reports, as well as brochures of new equipment being circulated in our branch. The work load of the personnel in this branch is far too heavy to spend the time to even casually browse through this reading material without purpose or intent.

It is suggested that:

a. A group of technical readers be established to review the articles covered in the abstracts that are listed in the I.R.E. and indicate the approach taken by the author. This list could have wide distribution throughout the Agency. Copies of the abstracts which this check list would accompany can be obtained separately from Wireless World. This list could also be reorganized into a yearly index of tremendous value.

b. This group of technical readers would also make note of articles of very direct connection to work being done by branches in the Agency, make copies of the article and send them directly to this branch. At present an article of importance may take as much as a year before arriving at the interested branch. In this manner, at least the more important developments are channeled directly to the consumer with minimum delay. An example of this delay has occurred in this office where earlier knowledge of a particular equipment could have saved many engineering and

technician hours. In this case, an article appeared in the April 1955 issue which dealt with a problem being pursued in this branch. This article has not yet arrived in the branch, and although a thorough search has been made, the magazine cannot be located. Through a personal subscription to this magazine, the article was located and called to the attention of the correct people.

This suggestion was submitted by

Mr. John Sommer, on 27 June 1955.

TUBE AGING BANK

During the early life of most vacuum tubes and neon bulbs, the characteristics change very rapidly, but after this initial change they settle down and can then usually be depended on to perform in a more stable manner. The tubes whose filaments will withstand the aging tests also have a much longer life expectancy. More information as to the benefits obtained by aging can be obtained from one of the tube manufacturers. Shake testing may be an expansion of this testing aging.

This application of a preliminary scanning technique to the recognition unit problem was made by Dr. J. J. Eachus on 27 June 1955.

RECOGNITION UNIT

A method is proposed here to substantially reduce the average time required for operation of a recognition unit of the DEMONETTE variety.

The DEMONETTE type of recognition unit involves the use of a sorted list of recognition groups. A group, X, to be a check against the list is compared with the middle group, M, of the list. If X is greater than M the first half of the list plus M is discarded. If X is less than M the second half of the list plus M is discarded. If X equals M the search ends. X is now compared with the middle group, M', of the retained list, and the process is continued. For a list containing 2^n-1 items at most n trials are needed to determine the presence or absence of a particular X.

Using presently developed techniques for ferrite core memories a read-rewrite time may be made in about 5 or 6 microseconds. For a 4095 word recognition list twelve lookups are required, or from 60 to 72 microseconds total. Non-destructive readout techniques (now in the research stage) appear to offer read times dependent upon selection time alone. If this is from 2 to 3 microseconds the time required for a 4095 word list would be from 24 to 36 microseconds.

This suggestion uses a preliminary scan to determine whether it is necessary to look in the recognition list and achieves a substantial gain

in speed.

Suppose the group length is 25 bits and the recognition list contains 2^{12} items out of the 2^{25} possible groups. Form a 16 bit function, F, of each group in the recognition list. At address F in a 2^{16} bit memory array, T, store a 1. There will be then, at most 2^{12} 1's in the array. Form F (X) and see if there is a 1 at that address in T. In the random case there will be $2^{12}/2^{16}$ or a 1/16 chance of finding a 1 there. If a similar but independent function F' (X) can be looked up in another memory T', then in the random case only once in 256 trials will a further evaluation be required. Assumptions have been made which are not precise. There will be less than 2^{12} unique F and F' values, on the other hand F and F' cannot be completely independent. A reasonable value might be 1 hit in 200 trials. This means that two 2^{16} bit memories plus one 2^{17} bit recognition list memory are required. If these memories utilize the slower ferrites the size, power, and cost can be greatly reduced.

Assuming a 15 microsecond cycle time, 199 groups require 15 microseconds each for test while one group requires 180 microseconds. The average test time will thus be about 16 microseconds.

This system is not suited to a synchronous machine, for the maximum look-up time is high. For an asynchronous machine this becomes unimportant.

This suggestion was submitted by

Mr. Thomas C. Blow, on 27 June 1955.

(Note: Mr. W. F. Friedman has made suggestions similar to this in the past.)

EXTRA-SENSORY PERCEPTION (ESP) RESEARCH

The use of ESP to glean cryptographic information is a possibility which should not be overlooked by NSA. At the present time many researchers throughout the world are investigating the possible power of the mind to sense facts by other than sensory perception. The Psychological Laboratory at Duke University has pioneered in this field for many years and published papers of Dr. Rhine at Duke are well known.

It would not be necessary for NSA to set up any research laboratory of its own, or to promote such research by any other group. However, NSA should establish a requirement to become fully apprised of progress in this field and the extent to which it might be used for cryptographic activity. Included in such a program of investigation would be the following:

a. Critical review of available literature and further research papers.

b. Field trips to observe experiments and experimental data of groups such as at Duke University when possible.

c. Consideration of U.S. subjects with high ESP powers for possible work with NSA if a need for their services should arise.

This suggestion was submitted by

Mr. Thomas C. Blow, on 27 June 1955.

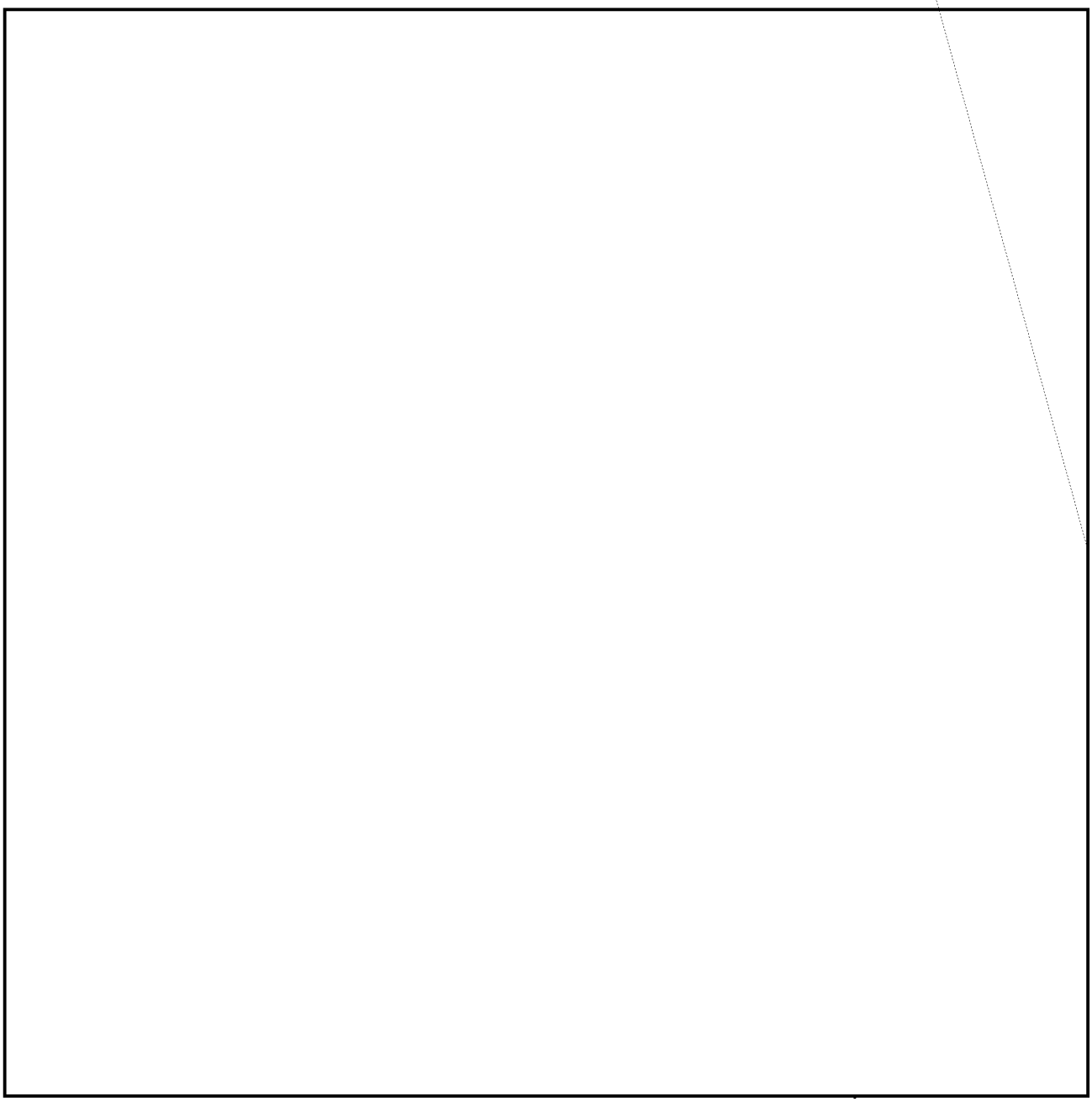
[redacted] CHARACTERISTICS OF TARGET SIGNALS

Without doubt it will be desired in wartime to [redacted] is well known, it may be that such methods will not best serve our purpose. It is, therefore, recommended that a study be made of the types of signals which would be most effective in [redacted] which NSA is interested in. Since the Radio Equipment Division of NSA has made a very close study of signals used for COMINT purposes, it is likely that this division would have many ideas for more efficient [redacted] than now exists.

This suggestion was made by

D. L. Hogan 30C with assistance

from Dr. W. A. Blankenship,34.



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