~~TOP SECRET FROTH~~

TO: Chairman, Analytic Equipment Technical Committee

15 Nov 54

FROM: S. S. Snyder, R/D 3501

SUBJ: Report of Special Study Group on FARMER-NOMAD

1. Transmitted herewith is the Report of Special Study Group on FARMER-NOMAD, as directed by motion approved by Analytic Equipment Technical Committee at its June 1954 meeting.

2. The findings of this report represent the opinion of the undersigned representing PROD 064, PROD 82 and R/D 35. Mr. E. P. Neuberg, representing R/D 34, participated in the conferences, but started on a leave of absence shortly thereafter; it was decided that it would not be feasible for a replacement from R/D 34 to participate in drafting the report.

3. The undersigned join in expressing appreciation for the spirit of wholehearted co-operation among personnel of the various PROD and COMSEC segments interviewed. Particularly helpful, also, were those technical "area men" from PROD 821 who steered us to the right people, and helped keep the conferences on a sound technical base by their intimate knowledge of the current situations in their particular areas.

Samuel S Snyder
SAMUEL S. SNYDER, R/D 35, Chairman

Leo W. Lathroum
LEO W. LATHROUM, R/D 35

George Hurley, Jr
GEORGE HURLEY, Jr., PROD 064

Joseph Blum
JOSEPH BLUM, PROD 82

Ivan R. King
IVAN R. KING, PROD 82

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

ANALYTIC EQUIPMENT TECHNICAL COMMITTEE

Report of

Special Study Group on

Analytic Requirements for

FARMER - NOMAD

Nov 1954

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

CONTENTS

~~TOP SECRET FROTH~~

1. INTRODUCTION

1.1 Pursuant to a motion passed at the June 1954 meeting of the Analytic Equipment Technical Committee, the FARMER-NOMAD Study Group was set up for the purpose of making suitable preliminary studies of Agency COMINT needs for large-scale analytic equipment and preparing recommendations leading to design studies. This group has interpreted this directive as follows:

1.1.1 Sufficient inquiries would be made to establish broad categories of machine needs, with detailed analysis of problem requirements to be left for subsequent functional design studies.

1.1.2 Engineering characteristics of proposed system(s), if mentioned at all, would be discussed only from the point of view of operational features, particularly in the light of past experience.

1.1.3 Problems of collection of traffic would not be directly considered.

1.1.4 Any particularly interesting observations affecting other classes of equipment would be noted and made a part of this report.

2. SUMMARY of MACHINE SUPPORT

2.1 Seventeen conferences have been held with technical personnel representing various segments of PROD and COMSEC, with the cooperation and technical guidance of cognizant PROD-821 personnel. In several cases, visits to operating areas contributed to a better appreciation by Group members. A few analytic areas were omitted from the survey, either because advance knowledge plus advice of PROD-821 indicated no applicability of large-scale analytic equipment, or because recent studies by various members supplied sufficient data for present purposes. The information gathered through the series of conferences is discussed below, under five headings:

a. Decryption

b. Analytic Aids

c. Data Handling

d. Additive Problems

e. Cipher Machines

2.2 Decryption. The problem of deciphering and decoding usually occurs in connection with current and exploitable systems. The optimum procedure is determined by factors of timeliness, the volume of work, and the facilities available for data preparation. Existing equipment is adequate for these needs, though future developments may indicate the desirability of including such processing in FARMER. Any increase

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

in demands for decryption, such as processing commercial codes, could presumably be handled by an expansion of the volume of equipment of the present type.

2.2.1 Cipher-machine Decryption. The main requirement here is that the machine be capable of analoguing the cryptologic processes of the different cipher machines. Speed must be sufficient to handle the anticipated volume without hurting the timeliness of the output. At present, these requirements are being met by using electrical analogs with typewriter and paper-tape input. Should the volume increase, the digital computers will probably be adequate; however, enormous volumes could result in a bottleneck in data preparation and in printed output.

2.2.2 Decodes. Decoding is handled on standard IBM equipment. When the MAISIE equipments are fully operational, it is hoped that all decoding will be done on MAISIE. In some problems [redacted] it would be desirable to have decoding facilities built into the FARMER equipment. In some Traffic Analysis and weather problems, decryption and decoding are both required. Here the big problem is data preparation and output. The large volumes may require magnetic-tape input and fast printer output. In some cases, automatic editing will be a necessity before decryption and decoding can proceed.

2.2.3 Minor hand systems. In these systems the volume is usually small; decryption or decoding is done by hand concurrent with the required analytic work. When the volume suddenly becomes quite large, the digital computer is generally able to fulfill the need. Occasionally the economics of the situation indicates the need for a special-purpose device.

2.3 Analytic Aids.

2.3.1 Indexes, [redacted], listings. The preparation of these types of analytic aid, when moderate in size, will continue to be the specialty of punched-card equipment for some time, much as has been the custom in past years. Recent high-speed commercial developments indicate that magnetic tapes, controlled by large electronic data-processing equipment, may take over a large portion of the task when volumes and requisite speeds dictate. However, the inclusion in one system of facilities for manipulation of data to form a printed index, together with the anticipated tremendous analytic potential of other FARMER units, is bound to increase the possibilities for new and interesting analytic applications. The machine processes necessary to make indexes practically and efficiently, include ability to sort rapidly and with flexibility as to field of data, and ability to collate and select. For proper balance, attention should again be given to data-preparation requirements and to provision of facilities that will produce printed copy rapidly.

2.3.2 Other catalogs. There are included in this category such jobs as making catalogs of cipher alphabets for cipher-machines, and making catalogs of cipher-machine settings [redacted] In such problems the input data is small and large amounts of information must be generated and printed out. Present equipment is more than adequate for handling the jobs described above.

2.3.3 Mathematical jobs. In this category are included the following types of problems:

a. Construction of mathematical and statistical tables.

b. Linear calculations such as matrix inversion, evaluation of determinants, solution of systems of simultaneous linear equations, eigenvector and eigenvalue determination.

c. Direction-finding problems.

d. Analysis of noise modulation systems.

These problems are best serviced by high speed computers specifically designed for mathematical problems. Such machines are commercially available, and the Agency has several. These problems constitute a small fraction of the over-all work load on the computers. It is therefore felt that this area is adequately covered by existing facilities.

2.3.4 Diagnostic programs. Progress has recently been made in diagnosing unknown systems by applying a battery of statistical tests to a sample of the traffic. The demands of the analysts are increasing for more extensive tests on larger volumes of material.

2.3.5 Research jobs. Some analysts have found it convenient to use computer programs to try out new analytic techniques before committing them to a full production program. These jobs, like many other one-time jobs from which they differ little, seem to be handled well by present computer facilities.

2.4 Data Handling. Although not identified with any particular class of cryptographic systems, the mere rearrangement or classification of large volumes of data is itself the basis for uncovering relationships not possible to detect in raw, unordered material. Although it is frequently necessary to combine complex processing with rearrangement, in this discussion of data-handling mention is made only of those areas or uses where this analytic method is comparatively free of other complicating processes. Data-handling in combination with more complex processes is discussed in later sections.

2.4.1 Traffic Analysis and Related Problems. Probably the greatest bulk of data received on a continuing basis is handled by groups assigned to traffic analysis, flight service, and air defense. The machine processing is predominantly of one type: the preparation, for study by the analysts, of listings of pertinent data sorted according to each of a number of information items. Theoretical studies are under way to test the practicality of automatic machine techniques for derivation of intelligence from data, to partially eliminate the preparation of printed listings in the future. Meanwhile, receipts number millions of messages per month, and current processing facilities are handling only a small fraction. The need is both to procure and process still greater volumes, further emphasizing the importance of editing, punching, sorting,and listing. Furthermore, the essence of success in this field is timeliness. Daily interpretations should be the goal. Successful timely treatment of this great bulk of material requires solution of the parallel problems of transmission, editing, and punching. Increase in facilities for transmitting data to Agency collection headquarters from the field, including some degree of format control, will be a necessary preliminary step to successful use of automatic-cditing techniques. Recent recognition of the importance of developing techniques for automatic editing is encouraging; the urgency of this cannot be overemphasized.

2.4.2 Plain Language. Some 2,000,000 messages per month, available on punched chadless tape with overprinting, are scanned for important subject matter by searching for the presence of expressions and addresses in varied order and lengths from selected lists. Experience indicates that only approximately 20% of the messages contain intelligence which warrants preparation of hard copy for further inspection. A machine process to perform this function must include facilities for storage of key words and phrases and for making some decision upon recognition of one or more such expressions in a stream of plain-language material. Under present practice, the decision is followed by production of a printed message together with a category identification. Special-purpose equipment has been designed for this requirement and should be available within a year. It is unlikely that FARMER would be utilized for this particular application, but techniques are required that will most likely be available in FARMER.

2.4.3 Practice Traffic. A large and annoying problem is the examination of large volumes of messages to separate operational or pertinent traffic from practice or non-pertinent traffic by some predetermined criterion. In some cases, practice traffic represents a large percentage of total traffic and must be separated for the sake of homogeneity. In addition, it is of analytic value to study on a continuing basis cryptographic systems and procedures used in practice traffic. The basis for performing traffic separation is not always the same, but the machine techniques are related to those required in automatic editing and in plain-traffic scanning. Both require ability to perform test decryptions.

2.4.4 <u>File Maintenance</u>. The increase in breadth of the Agency's intelligence-gathering activities through the years has led to the accumulation of an enormous amount of collateral information. This wealth of miscellaneous factual data has become an indispensable source of reference material for the analysts, but its usefulness is often measured by its completeness and availability to the analyst. The sorting, filing, and collation required to maintain files numbering many millions of items deserves serious consideration for treatment both by automatic file-maintenance equipment and also by some process that provides more direct accessibility of particular items for the analyst.

2.5 <u>Additive Problems</u>. Machine applicability is treated below under three headings:

a. [redacted]

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

b. Exploitation

c. Reading

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

"Additive" here is meant also to include certain substitution systems involving the combination of key and plain.

[redacted]

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

~~TOP SECRET FROTH~~

[redacted]

~~TOP SECRET FROTH~~

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

[redacted]

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

~~TOP SECRET FROTH~~

[redacted]

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

[redacted]

~~TOP SECRET FROTH~~

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

[redacted]

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

[redacted]

2.6 Cipher Machines. Cipher-machine problems are a major present and future concern of PROD, both in cryptanalytic effort expended and in potential value of intelligence derived. Machine attacks on these problems have two outstanding characteristics: (1) the large number of trials required, and (2) the great variety and individuality of problems. The second characteristic follows naturally from the first; for many cipher-machine problems would be impossibly long if they did not direct their attacks at the individual points of weakness, which are different for every different cipher device. Despite the great variety of problems, it is possible to make some general statements, at the risk, of course, of making some statements that apply very questionnably to some individual cases. The attack on a particular cipher device generally falls into three phases:

a. Basic recovery of the structure of the machine, wirings, etc.

b. Recovery of machine elements that remain constant for some period of time, such as pin patterns, notch positions, pluggings, etc.

c. Setting of individual messages.

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

[redacted]

2.6.2 Recovery of a machine set-up generally proceeds by more straightforward processes but still requires long, complicated repetitive trials on small segments of text.

2.6.3 When solution of the indicator system fails, setting of individual messages can be the most laborious phase of all, since every message must be processed individually. The tremendous number of possible settings makes essential the use of a statistic sharp enough to avoid overwhelming the analyst with random answers.

2.6.4 Machine attacks on cipher-machine problems repeatedly involve certain basic types of manipulative processes. The most fundamental of these is decryption, partial or complete, a process whose exact nature will of course depend on the device attacked. Typical processes include decryption through a rotor maze or generation and application of a key stream. Another basic type of process needed is the generation of settings in a device that may step according to complicated rules. Finally, the results of each trial must be scored according to some criteria, which may be complicated.

2.6.5 Certain cryptanalytic machine attacks would benefit from the availability of equipment that can generate, store, and make reference to large catalogs in an integrated operation. More important, certain attacks on cipher machines have been proposed based on [redacted] The outstanding requirements are to store and manipulate huge volumes of data. The provision of such facilities should make possible unique and valuable analytic attacks.

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

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

2.6.6 More specifically, we are called upon to deal with two broad types of cipher machine and with a number of unique machines. The first broad type is the wired-rotor machine, used by both the United States and some foreign governments. Some aspects of this problem are receiving considerable attention on computers, on SIED, and on other special-purpose equipments as well as on comparators and standard IBM. A big problem remains. Any general-purpose equipment that meets these problems would likely also be able to handle any requirements from COMSEC.

2.6.6.1 The second broad type is the teletype scrambler, typified by [redacted] Analysis of these machines requires operations on long streams of bits. The cycle of the machine can be very long, so that attacks must proceed at very high speed [redacted]

However, the preparation of data for [redacted]

2.6.6.2 The Hagelin ~~C-28~~ C-38 is well covered at present by computer programs and special-purpose machines. Any CX-52 traffic that appears will tax our present facilities severely. It will require more complicated, faster programs; and most of the present special-purpose equipment will not be applicable.

2.6.6.3 The simple B-211 is a small problem, adequately handled. The modified B-211 problem relies heavily on FROG, with some assistance from computer programs. When the indicator system is unreadable, we have a serious volume problem of message setting.

2.6.6.4 The [redacted] machines currently are used as generators of additive key and do not demand much machine attention as a cipher-machine problem per se. If plain text were enciphered through the machine, this problem, which from the analytic machine point of view is now an additive problem, would become a cipher-machine problem.

2.6.6.5 The recent appearance of Gretener traffic poses some serious and unusual problems. The cryptography of the machine is so distinctive that it may strain the versatility of even a general-purpose analytic unit. Information inside the machine appears not as characters but as many simultaneous streams of bits. Furthermore, the large number of possible settings and permutations of components may make message setting laborious. The 14-baud nature of the cipher also complicates the intercept problem.

3. MAJOR NEEDS

3.1 Listed below are the major analytic needs not adequately fulfilled by present equipment. These needs are summarized at this point without any implication that they are all to be satisfied by FARMER equipment.

a. Preparation of data.

Many analytic projects are fast approaching a volume which can be handled only if automatic editing and automatic de-duping become available.

b. Sorting, Indexing and Listing.

When no complicating requirement is present, additional speed for large volumes of material is chief factor. Equipments now on order are expected to satisfy needs, except possibly for high-speed printing.

c. Treatment of output data from small-scale machines.

There exists a repeated requirement for immediate sorting-listing-indexing of tape output data.

d. File Maintenance.

Massive; probably deserving of a set of its own magnetic tape equipments.

e. Scanning.

Massive; allied in concept to de-duping and automatic editing approaches; special recognition and printing requirements.

f. Separation of Practice Traffic.

Massive; partly a scanning technique using predetermined recognition characteristics; partly a statistical testing.

g. Diagnostic Analysis.

Preparation of a series of analytic and statistical testings limited in scope only by the analytic machinery available.

h. Matching.

Cipher-cipher - an enormous task, even when delimited, demanding high speeds and ability to handle tremendous volumes of data; coincidence rate and/or recognition provide the testing criteria.

Cipher-key - smaller volume than cipher-cipher; but requiring more flexible scoring.

Key-key - volume still smaller, but matching may also be to detect (1) isomorphism and (2) imperfect coincidence.

i. [redacted]

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

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

[redacted]

m. Cipher-Machine Attacks.

Analoguing - Decryption, partial or complete, is needed at higher speed than is now available.

Control - High speeds must be applied to more complicated control and decision procedures than are now available in flexible high-speed equipment.

Scoring - The number of tests is frequently so tremendous that only the ability to use a highly discriminating statistic can keep the number of random answers within practicable proportions.

Secondary testing - Even in the best of circumstances, the number of random answers may be so large as to require that secondary testing be a major portion of the total effort.

Generating, sorting, cataloguing - Ability to sort large volumes of generated data in an integrated operation is needed for certain attacks.

4. DISCUSSION

4.1 Analytic Advantages. The proposed FARMER system of equipment would provide two important advances in analytic power: (1) a simultaneous increase in speed and flexibility of equipment and (2) the ability to interconnect blocks of equipment that ordinarily would belong to separate machines. In evaluating the ability of the proposed project to satisfy the needs of PROD, attention should be paid to both these characteristics.

4.1.1 The proposed system of equipment would provide several other advantages: (1) compatibility of input-output media for a large class of equipment, (2) uniformity of design and maintenance, (3) possibility of putting a part of the total system into operation while other parts are still being designed and constructed, and (4) ability to incorporate into the system units to satisfy as yet unpredictable analytic needs.

4.2 Since editing and straightforward data handling can be carried out on less powerful equipment than FARMER, the principal need for FARMER is in the two fields of additive and cipher-machine problems. Although there are few problems in PROD that would not profit from the availability of more powerful analytic equipment, it is these two classes of problems that suffer most from the inadequacies of present equipment.

4.3 Speed with flexibility is the key to the machine attack on cipher-machine problems, at present and in the future. Not only are there recognized approaches which on present-day equipment are impossibly time-consuming; but there is already indication that cipher machines will become more complicated in future years, so that even presently acceptable techniques will take too long to carry through. Moreover, even for the problems that are presently vulnerable, an increase in the speed of analytic equipment would often lead to quicker solutions by safer but heretofore too time-consuming methods, eliminating the delays caused by reliance on quick but unsuccessful programs.

4.4 The increase in speed of processing will bring with it some serious statistical problems as the number of trials increases. The consequent increase in the number of random answers will greatly increase the importance of secondary testing, whether by hand or by machine. For hand testing, the difference between success and failure in a particular project may depend on cutting down the number of random answers by arranging the machine scoring equipment to use the sharpest statistical criteria possible. Flexibility of the scoring unit is therefore of great importance. This argument applies to additive systems as well as to cipher machines.

4.5 If secondary testing is, by choice or necessity, to be done by machine, the intermediate results must be fed into another machine, either directly or through an input-output medium. Such a medium must be able to read and write information at high speed. In many cases the rate of production of intermediate answers will exceed the maximum rate of operation of available input-output media, so that it becomes desirable to connect one machine directly to another. The problem of relative speeds here suggests an assembly consisting of a high-speed analytic unit feeding intermediate answers, through suitable interlocks, to a computer-type device. As cipher machines appear with more and more possible settings, more and more emphasis will have to be put on primary testing that does not isolate a unique answer but merely reduces the number of possibilities by a moderate factor.

4.6 For the most part the attack on cipher machines uses special-purpose devices where available and relies on general-purpose computers for the remaining problems. Where the volume of standardized work has justified their construction, the special-purpose machines have handled their job well. Their success emphasizes, by contrast, the frequent inadequacy of general-purpose computers for these problems. The success of certain computer programs should not be allowed to obscure the fact that general-purpose computers are too slow for a great many machine-cipher problems. Special-purpose devices are already available which satisfy the requirements of speed; but the need in the future is for general-purpose machines -- or machine components -- which will handle the problems as they come up without the delay or expense involved in constructing a special device for each problem.

4.7 Analytic Equipment Design Philosophy.

4.7.1 "Direct" vs "Stored-Program". The processes involved in analytic problems are presently carried out by two basically different machine approaches. In the "direct" approach, exemplified by SLED I, components are assembled, through plugboard connections, in such a way as to carry out the desired functions in a direct manner. In the "stored-program" approach, used by the digital computers, the machine refers to its storage for instructions, which initiate successive simple operations whose total effect is to carry out the desired operation. The stored-program approach has the advantage of permitting a single machine to handle a large variety of problems, at the expense of a loss of speed; the direct approach has a large advantage of speed at the expense of a lack of flexibility for any given assembly of equipment. For many jobs requirements of speed clearly demand that the basic operations be carried out by direct equipment under the immediate control of other direct equipment. The operations that are required less frequently may, according to convenience, be carried out either by direct or by stored-program equipment. The amount of equipment required for direct control increases in proportion to the complexity of the program, while stored-program control requires nearly the same amount of equipment for all jobs. It may therefore be most convenient to carry out simple programs completely with direct equipment but to use a combination of direct and stored-program equipment for complicated programs.

4.7.2 Combined Equipment. The combination of direct and stored-program equipment into a single assembly is a major analytic advantage that FARMER equipment will offer. Another type of combination that is strongly needed is that of flexible analytic equipment with large-volume

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

high-speed data-handling facilities. [redacted]

4.7.3 Increased Analytic Potential. To a large extent, the thinking of both cryptanalysts and machine technicians is conditioned by the capabilities and utilization of present equipment. The availability of FARMER equipment, with great analytic power and flexible combination of facilities, may be expected to broaden analytic horizons. By its very nature, this advantage is impossible to evaluate at the present time; but it should by no means be underrated.

5. RECOMMENDATIONS

5.1 This committee feels that PROD has four major unsatisfied machine needs:

a. Automatic editing and data preparation.

b. Large-volume, high-speed sorting, indexing, and listing.

c. Large-volume, high-speed data-handling, combined with complicated analytic processes.

d. High-speed analytic processes on cipher-machine problems, combined with sophisticated control and decision procedures.

5.2 Favorable action on the FARMER task is recommended, with FARMER equipment to be aimed at satisfying needs 5(c) and 5(d) above, which cannot be satisfied by any other existing or planned general-purpose equipment. Such equipment will incidentally be able to satisfy need 5(b), but commercial data-handling equipment is likely to satisfy this need to a large extent before FARMER equipment is available.

5.3 It is recommended that the existing NOMAD Task be abolished. This committee considers that the Agency has great need both for large-volume high-speed data handling equipment and for high-speed computing equipment, but that these facilities should not be restricted to the specific assembly thought of as NOMAD. They should, separately or together, be available as integral parts of the FARMER system.

5.4 Vigorous action is recommended to produce a solution to the editing problem. The overwhelming burden of data preparation repeatedly dominated our discussions of PROD needs. It is potentially the largest machine need for which no satisfactory solution has been devised.

5.5 A Disposition Form from R/D 353 to R/D 35, dated 5 April 54, a copy of which is attached, sets forth proposed features of the FARMER system.

5.5.1 This committee approves of the proposals in general and of the following points in particular:

a. Compatibility and uniformity.

b. An increase in speed, as far as practicable.

c. Break-up into separate units that can be freely interconnected.

d. Multiple copies of those units that are required more frequently.

e. Ability to put early units into operation before other FARMER units are completed.

f. Ability to add new unit types as their need appears.

5.5.2 Stored-program techniques should be available, with enough general-purpose features to insure versatility and adaptability to variations in problem needs. Where considerations of speed make it desirable, we favor direct assembly of components for control functions, in combination with over-all control by a stored program of sequentially-executed instructions.

5.5.3 As indicated in 5.3 above, this committee recommends that high-speed, large-volume data-handling facilities be made a part of FARMER equipment.

5.5.4 This committee has reservations on the subject of using a central switching system rather than direct interconnection of FARMER units. Further study of this question is recommended.

5.6 The planning involved in the FARMER project falls into three stages: (1) study of cryptanalytic needs and the ability of the proposed equipment to satisfy them, (2) formulation of a list of FARMER units, with characteristics of each and a proposed mode of use and interconnection, and (3) logical and engineering design of units. This committee now considers the first stage to be completed and recommends that work on the second stage begin immediately.

SECRET

~~SECRET~~

~~SECRET~~

DISPOSITION FORM

SUBJ: Proposal for FARMER

TO: 35
3501

FROM: 353

5 April 1954
R. L. Bowman/mmp/530

1. The purpose of this paper is to outline a proposal for a long range development program covering a period of three to five years beginning early in fiscal year 1955. It would involve the coordinated efforts of several segments of R/D 35 and some of PROD 82. FARMER is the suggested cover name.

2. The objective in this program is to develop a compatible system of analytic equipment embodying a variety of cryptanalytic functions. The character rate is aimed at somewhere in the range of 150,000 per second to 3,000,000 per second. The procurement of SLED II is not included in, this proposal but items now being considered for SLED III do fall within the scope of this proposed program. In achieving this objective, prime consideration must be given to overall programming compatibility and flexibility, overall operational utility, and engineering practicability.

3. The characteristics of FARMER are influenced by a number of factors.

(a) A general purpose cryptanalytic device must be capable of performing all sorts of cryptanalytic processes.

(b) Due to the constant increase in number and complexity of problems the trend has been to build bigger and bigger analytic machines which in turn produces bigger and bigger engineering and maintenance problems.

(c) Continual advances in the cryptographic art imply that for effective cryptanalysis larger numbers of trials must be made which in turn reflect higher electronic speeds in analytic machinery.

4. The initial conception of FARMER embodies the idea of dividing a large machine into several small ones. This facilitates engineering and maintenance problems and provides better programming flexibility and overall operational utility. The heart of the system would be the control system which is envisioned as a sort of a grand central station. It has switching facilities for directing the flow of data from any unit to any other unit. It is sequenced controlled which permits computer type programming and may contain a nominal amount of memory. This feature is very desirable when successive steps of a problem are contingent upon the results of earlier steps. Other units of the system are tailored to specific analytic processes and might well be identified by their functions such as: arithmetic unit, group IC unit, group recognition unit, wired rotor unit, matrix unit, input unit, memory unit, output unit, frequency distribution unit, etc.

5. One might envision FARMER as consisting of one, two, or three control units surrounded by a collection of analytic units which for any particular problem may be connected in an appropriate manner either by physical cable connections or automatic switching. When not used in one problem the excess units are available for another problem in conjunction with another control unit.

SECRET

~~SECRET~~

SUBJ: Proposal for FARMER

TO: 35 FROM: 353 5 April 1954
R. L. Bowman/mmp/530

6. To develop this system for efficient use much study will be needed to determine the appropriate characteristics and quantities of the various units. In addition, standards for character coding, checking, programming philosophy, inter-unit pulse characteristics, and pulse rates must be established.

7. It is recommended that this or a similar program be initiated. It is further recommended that it be implemented in R/D 35 for the following reasons:

(a) Past experience has shown that it is unwise to hand a program of this nature and magnitude to a single contractor. It gets out of hand and virtually impossible to supervise. On the other hand portions or phases of it can be contracted in such a manner that adequate supervision can be achieved. Also normally more prospective contractors are interested in items which do not tie up all their plant facilities.

(b) It is impossible to lay out or prescribe a complete set of characteristics for such a system of analytical functions when it is desired to extend the state of the art of analytic equipment. Therefore the results of exploitation and development will dictate to some extent the number and character of functions suitable for incorporation into a compatible equipment system.

(c) By keeping the control and supervision of the entire program within R/D 35 there is better opportunity for 3501 and 351 to fulfill their responsibilities regarding the formulation of analytic characteristics and system functions.

(d) There is a lot of room for learning on the part of R/D 35 engineers in this program.

(e) By the beginning of fiscal year 1955 a number of tasks including FROG, COUNTESS, VIVIAN, JENNY, and MILLIE will be disposed of. This will permit several engineers to be available to embark on the proposed FARMER program.

/S/ RAY L. BOWMAN
Chief, Analytic Machines Branch

Inclosure to Report of Study Group on FARMER-NOMAD