

ROUTING			
TO:	NAME AND ADDRESS	DATE	INITIALS
1			
2			
3			
4			

<input type="checkbox"/>	ACTION	<input type="checkbox"/>	DIRECT REPLY	<input type="checkbox"/>	PREPARE REPLY
<input type="checkbox"/>	APPROVAL				
<input type="checkbox"/>	COMMENT				
<input type="checkbox"/>	CONCURRENCE				
REMARKS:					
FROM: NAME					

~~Top Secret~~  
(Security Classification)

CONTROL NO. \_\_\_\_\_

The Bissell Report of 18 Feb, 1965

*Report #52*

Handle Via

Channels

Access to this document will be restricted to those approved for the following specific activities:

---



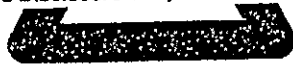
---

**Warning Notice**

Sensitive Intelligence Sources and Methods Involved

**NATIONAL SECURITY INFORMATION**

Unauthorized Disclosure Subject to Criminal Sanctions



~~Top Secret~~  
(Security Classification)  
E2 IMPDET

*Relativ  
10.000*

*b.3*

~~TOP SECRET~~

[Redacted]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

18 February 1965

REVIEW OF SELECTED NSA CRYPTANALYTIC EFFORTS

SUMMARY - 1508

1. Present cryptanalytic efforts against the [Redacted] high-grade systems constitute for the most part an investment that must be justified by the expectation of a future yield of intelligence. The primary concern of this report is with the prospects for success in this effort. The report and its annex contain information on the current and projected costs of these cryptanalytic programs but is necessarily inconclusive about the value of the intelligence that may in due time be produced. Although the scope of the inquiry was limited to the [Redacted] high-grade ciphers, some attention is given to the allocation of resources as between these and other cryptologic activities.

2. The NSA's experience during the seven years since the Baker Report was written does not invalidate the proposition therein stated that technology is tending in the long run to shift the balance of advantage from

[Large Redacted Area]

FILE COPY - RETURN TO EXECUTIVE REGISTRY

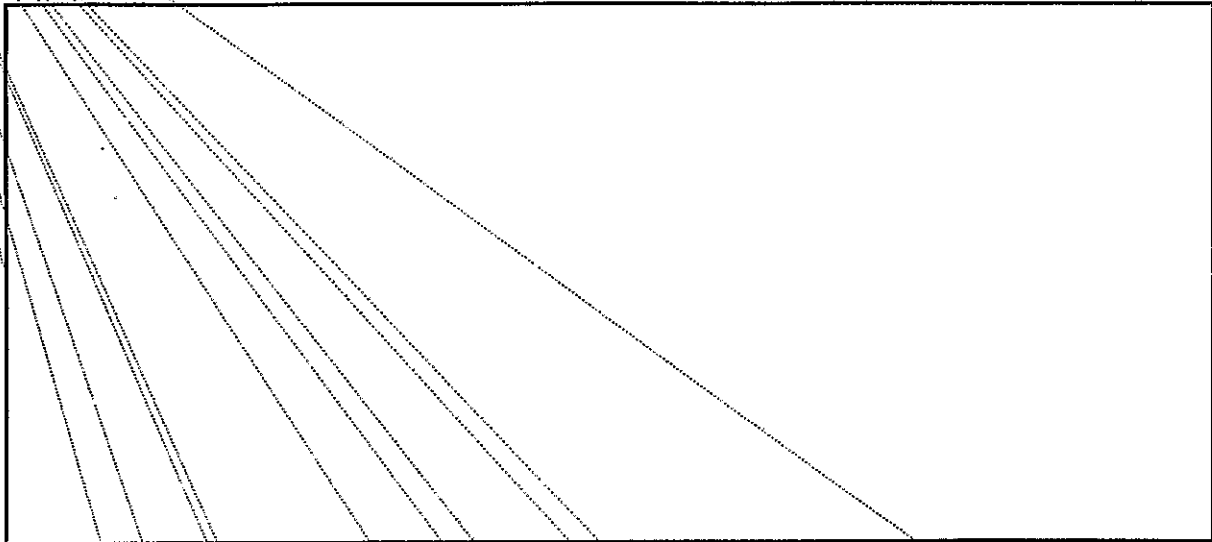
SC-01287-65  
Cy 15 of 15 Cys

~~TOP SECRET~~

[Redacted]

(b) (1) [redacted]  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

~~TOP SECRET~~ [redacted]



3. Of a group of some [redacted] top-level cryptanalysts (excluding those not currently working in cryptanalysis) about [redacted] are assigned to the [redacted] high-grade ciphers as against [redacted] to all other targets. Of a slightly less senior group about [redacted] are working on the [redacted] high-grade systems. In terms of personnel of all grades, the cryptanalytic effort as a whole is employing some [redacted] in the current fiscal year of which [redacted] are assignable to these [redacted] targets. In dollar terms, the cost of the whole effort is [redacted] of which [redacted] is estimated to be allocable to the effort here under consideration.

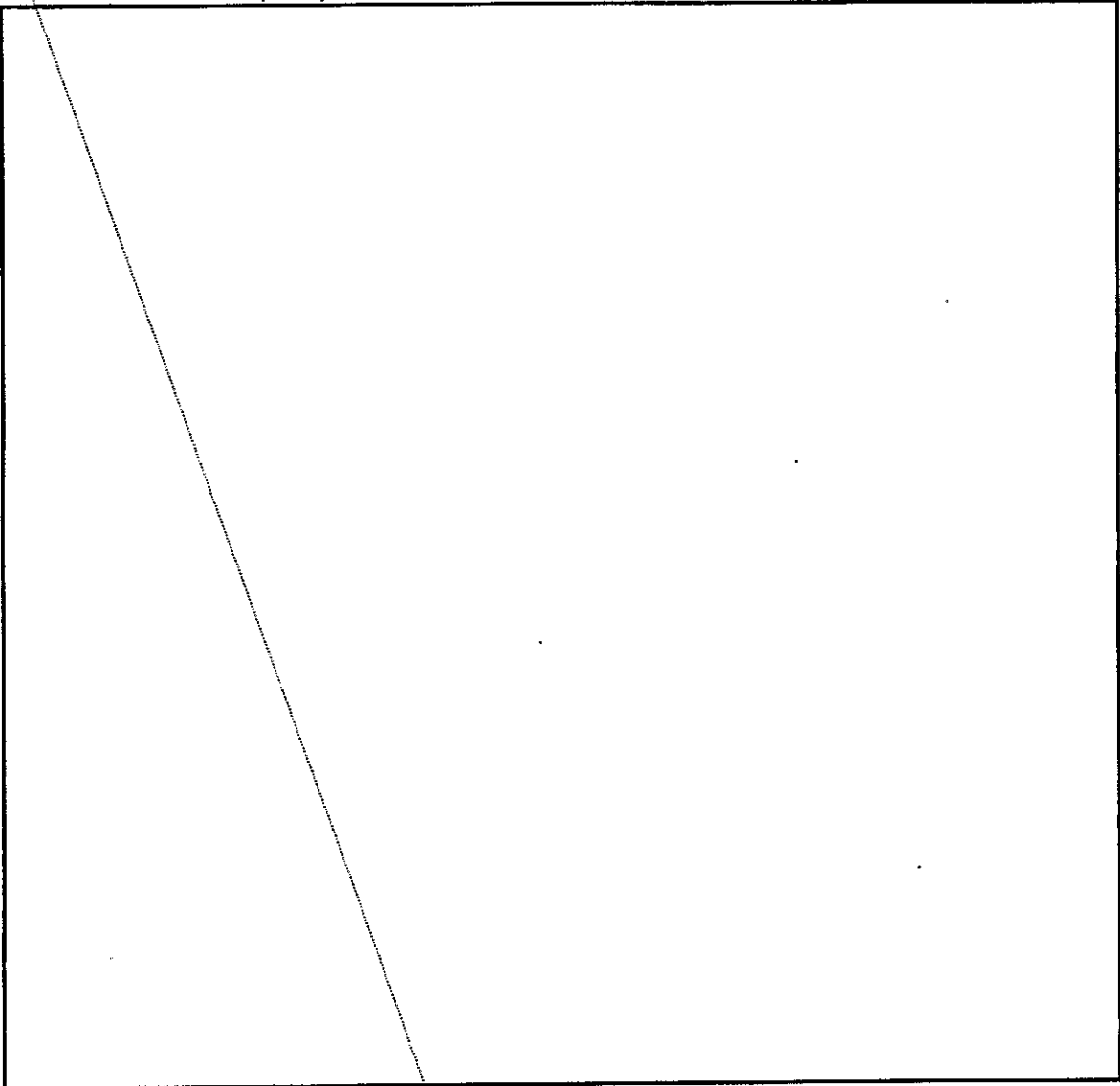
4. The principal conclusions of the report are judgments concerning the status and likelihood of success of the attacks on each of the major [redacted] high-grade systems (or sets of systems). These judgments, which attempt to embody the opinions expressed by a range of well-informed

~~TOP SECRET~~ [redacted]

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

~~TOP SECRET~~ [redacted]

individuals within and outside the cryptanalytic community as synthesized by the reporter, may be summarized as follows:



5. Even taking as given the above estimate of the probabilities of success against the high-grade [redacted] systems, it is impossible to

~~TOP SECRET~~ [redacted]

~~TOP SECRET~~ [REDACTED]

- (b) (1)
- (b) (3)-50 USC 403
- (b) (3)-18 USC 798
- (b) (3)-P.L. 86-36

evaluate the intelligence that may be obtained and thereby to judge whether the scale of the effort is appropriate. In part this is because the placing of a dollar value on a specified flow of intelligence is essentially arbitrary (just as is the assignment of a dollar value to "national security"). It should be possible to make cost effectiveness comparisons between different intelligence activities but this would require at least that the "effectiveness" (utility) of one flow of intelligence be quantitatively comparable with that of another. Such cardinal, comparative evaluation has seldom been performed in the intelligence community, because relative values may change frequently, because different users of intelligence would make differing evaluation, and because the comparisons might be regarded as invidious. What should be feasible with respect to the efforts here under consideration is a simple qualitative evaluation which would pay particular attention to the fragmentary character of the intelligence that may be derived from exploitation of [REDACTED] high-grade systems, and to the time lags that are to be expected between the transmission of traffic and its decipherment. Such an evaluation could not be undertaken as a part of this inquiry, however, and would have to involve a number of agencies in the intelligence community.

6. For both practical and intellectual reasons, the judgment about the appropriateness of the effort against the high-grade [REDACTED] systems requires consideration not only of dollar costs and potential benefits

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36

~~TOP SECRET~~ [redacted]

(b) (3) -P.L. 86-36

(somehow evaluated) but also of alternative possible uses of the cryptologic resources against other targets. It is clear that some part of both the funds and the senior professional personnel employed in [redacted] would contribute greatly to other cryptologic activities. Resources could be shifted to less difficult cryptanalytic problems already known and identified as such (such as [redacted] systems) or to developmental activities, essentially exploratory investigations of newly encountered systems and the state of cryptographic practice in various countries. Theoretically, it should be possible by accepting a somewhat more pessimistic outlook of the exploitation of the high-grade [redacted] systems to buy either a larger, more timely, or more predictable flow of COMINT of all sources taken together (with a small portion being [redacted] or more flexible and extensive developmental investigations. The choices among these options may require the weighing of a smaller, more uncertain flow of more vital intelligence against a larger, more predictable flow of less vital intelligence, or the weighing of capital formation in the form of advances in the state of the art of cryptology against larger near-term output. Although this report can embody no judgment as to how the choices should be made (since the investigation was limited to one set of programs) it is suggested (a) that the allocation of resources should not be dominated by a single priority established some eight years ago, and (b) that the procedure

LIMITED DISTRIBUTION

~~TOP SECRET~~ [redacted]

~~TOP SECRET~~

within the community for making these decisions might be susceptible of improvement (see paragraph 7. b. below).

7. The report concludes with three recommendations. The first of these (and in lesser degree the other two) extend in scope beyond the terms of reference of the inquiry and the area actually studied; to this extent, they are not supportable by the evidence that was gathered.

a. There should be no reduction in the over-all cryptologic effort of the United States. Even if, as predicted in the Baker Report, the yield of decrypted traffic from high-grade systems must be expected to show a slow decline trend over the long-run, this can be a very slow process and there is a fair likelihood that in the next few years the yield (in terms of both quantity and quality) will increase significantly. At the same time, there is in progress a steady increase in the total volume of encrypted traffic in the new nations, much of which should be subject to exploitation. If any of the assets (people, continuity of coverage, technology) currently employed in cryptology were dissipated, their re-assembly or reconstitution would require very long lead times indeed. The recruitment and training of additional top-level analysts should be pushed vigorously.

~~TOP SECRET~~ [redacted]

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

b. The desirability of some reallocation of cryptologic resources as between the attack on [redacted] high-grade systems and other cryptanalytic problems should receive consideration. A procedure that might be useful in any such consideration would be the definition by the cryptologic community of several different options, the estimation of what it would be reasonable to expect from each in the form of a flow of future intelligence, and the presentation of such estimates from time to time to appropriate members of the intelligence community. The purpose would be to inform the consumers about capabilities and technical opportunities in a form of preference for one option as against another. Such reconsideration of the allocation of resources should be infrequent because it is wasteful to shift resources around in response to short-term changes in requirements and to try to produce results in a hurry.

c. Consideration might well be given to a systematic evaluation on behalf of the intelligence community of the intelligence currently being produced through the exploitation of [redacted] and of that which might be produced through the successful exploitation of [redacted]. Even though such evaluation would have to be purely qualitative, it would give a firmer basis for judgments concerning both the scale

~~TOP SECRET~~ [redacted]



~~TOP SECRET~~

of the whole cryptologic effort and the allocation of cryptanalytic resources than now exist.

d. It must be made explicit that neither of the two preceding recommendations is intended to imply that there should be changes in organization, especially in the form of any additional committee structure, or that the authority of the NSA top management should be diluted.

~~TOP SECRET~~

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

A cipher machine makes use of an enciphering box which converts plain-text letters to enciphered letters. The cipher box may be operated by a typewriter keyboard and print out the cipher text, or it may be operated by a teletypewriter tape and produce electric signals which are transmitted directly. The plain text is converted to cipher text by a complicated maze of electrical circuits which are rearranged in some fairly regular manner after each text letter has been enciphered. A similar equipment decipheres by running the enciphered text through the ciphering box backwards. Cipher machines, since they operate at typewriter speeds or faster, can accommodate much larger volumes of traffic than

Enciphering or deciphering a message requires first the cipher machine itself together with any auxiliary parts to be used with it, and second the key to be used with the individual message. This key usually consists of the selection of certain auxiliary components, the plugging of certain wires on a plugboard, the setting of certain dials, etc. In practice, certain parts of the key, usually those requiring the greatest physical effort to change, are the same for all messages on a particular day on a particular circuit, and only relatively minor changes are made in the key from message to message.

While the number of components in the key is relatively small, rarely over a dozen, the total number of different keys is found by multiplying the number of possibilities for each component and the resulting numbers may be of a size much too vast to be dismissed as merely astronomical.

#### Experience with Earlier Machines

The cryptanalysis of a machine system falls naturally into two stages. First, there is the recovery of the machine itself; that

Only in Final Shell

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

is, the determination of exactly how the machine works and the wiring of all circuits in the machine and any of its auxiliary components. Second, there is the determination of the individual key for each message. Because of the practice mentioned above, this usually breaks into two parts, determination of the daily key and subsequently the message keys. Understanding of the basic process is perhaps best obtained from the following sketch of the attack on the Enigma which was the principal middle-level cipher machine used by all the German military services during the recent war. Success in reading this system was almost total and may well have had a decisive influence on the war against the U-boats and the air war over Britain.

The machine itself was a modification of a commercially available machine. Through covert action on the part of the Poles just before the war began, the basic design of the machine and the wheel wirings were known. The key was made up of four parts: the stecker which consisted of a number of wires to be plugged, the wheel order, the ring setting, and the window setting. The stecker wires could be plugged in some [redacted] different ways. The wheel orders offered [redacted] possibilities, the ring setting, [redacted] and the window setting, about [redacted]. The total number of possible keys is the product of all these numbers, that is about [redacted]

This number is more or less typical of the situation presented by any cipher machine. The principal thing it teaches is that large numbers, in themselves, offer no guarantee of security.

German communications procedure changed the first three parts of the key daily; only the window setting varied from messages to message on the same day on the same circuit. This meant that

(b) (1)

(b) (3)-50 USC 403

(b) (3)-18 USC 798

(b) (3)-P.L. 86-36

(b) (3)-50 USC 403

(b) (3)-18 USC 798

(b) (3)-P.L. 86-36

we had to solve the really difficult problem of finding a whole key only once per day per circuit; after one message was out the rest could be read much more easily. One technique for the latter task was simply to decipher the message using every possible window setting and select the one which made sense. Since there were only about a half-million possibilities this proved to be relatively easy with high-speed electronic mechanical equipment.

A similar try-all-the-possibilities attack on the daily key is completely impossible, since even at the highest electronic speeds we can rationally imagine it would take centuries of machine time to make the trials.

The daily break-in was accomplished by an ingenious combination of exhaustive trials and guessing. First, one had to guess the plain text underlying a short stretch of cipher. If the ring setting was favorable at this point in the cipher then it had no effect on the recovery of the other three elements, the stecker, wheel order, and window setting. An electrical circuit was devised which could test in one step all possible Steckers for each combination of window setting and wheel order. The required number of these trials was then about [redacted] (for the window setting) times [redacted] (for the wheel order) or some [redacted]. A large number of special machines (called Bombes) were built which could make these trials in a few milliseconds each and an exhaustive run could then be made using about 100 hours of machine time. About [redacted] was expended on these machines which represented a major diversion of our electronic skills during the war.

Once the routine breaking of the traffic started a number of favorable facts were observed. The daily key lists were apparently

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

made up in a non-random manner and this materially reduced the amount of machine time required for a break-in; diligent study of the texts of deciphered messages improved our ability to make the all-important preliminary guess of the plain text underlying the cipher; certain operators were found who habitually violated the German communication rules in a way which simplified our task; etc. The over-all effect of these "dividends" was that we were able to keep current on most of the traffic from 1942 until the end of the war, in spite of the fact that the Germans introduced a number of additional complications into their usage as the war progressed.

These possibilities as discussed primarily for the German Enigma had been brilliantly made use of in other cases, as when masters of the cryptanalytic art, such as William Friedman, solved Japanese machines and early models of the Hagelin machine, which used a letter-for-letter addition of a generated sequence of characters to the plain-text characters.

Unhappily, the actual readability of a message depends not only on the amount of key used, but on both the [redacted] and [redacted] of the enciphering machine and also upon the intelligence and care with which it is used. [redacted]

[redacted] Pre-  
sumably, either the messages enciphered are too brief to allow decipherment, or separate keys are used for portions of longer messages.

[redacted]

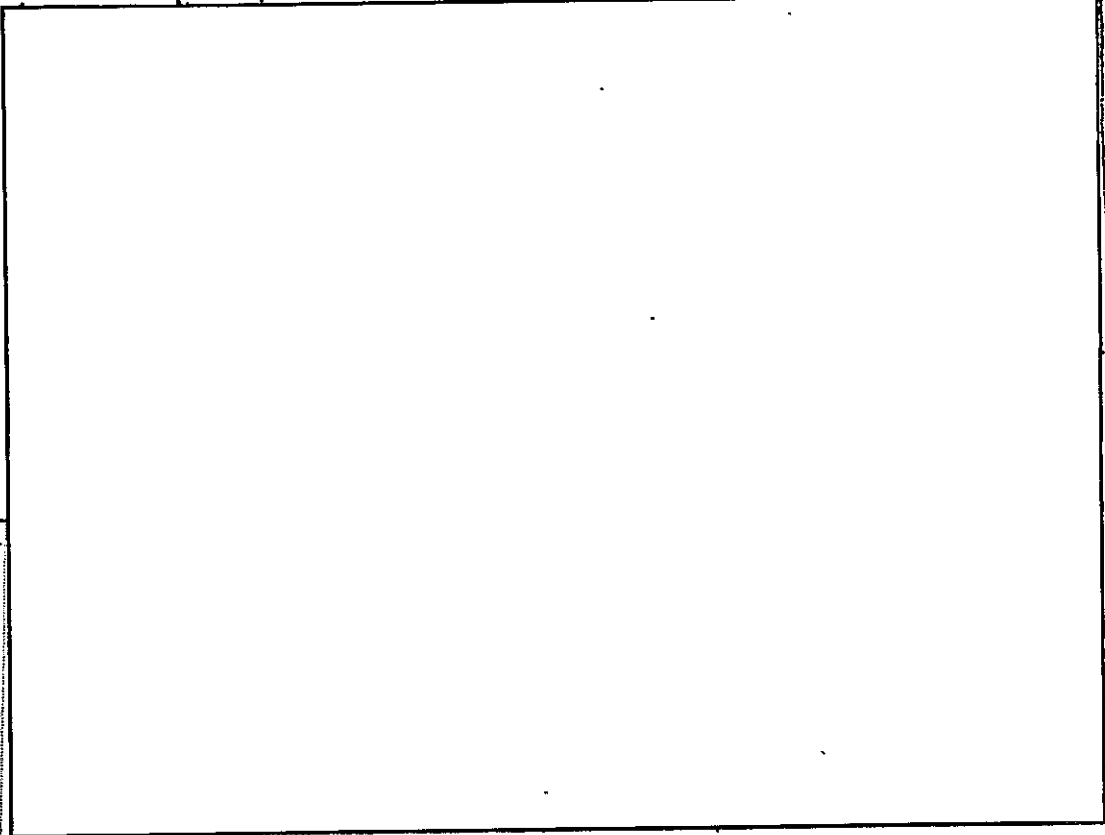
(b) (1) [REDACTED]  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

In fact, while a deeper understanding of cryptology and cryptanalysis tells us that machine-enciphered messages are in some sense theoretically readable, its chief practical results have been to provide machines which are now practically unreadable and also to show that the output of such machines cannot be deciphered by any straightforward effort of any physically possible magnitude. In particular, [REDACTED]

Indeed, in the case of the most complex modern machines, the only analytic sources of knowledge of the construction of a machine has been enciphered when the machine was misused or maladjusted. A message enciphered improperly, or while the machine is malfunctioning, is called a [REDACTED] and the word [REDACTED] is used generally in referring to the misuse or malfunction of a cipher machine or, more generally, a system. The Central position of [REDACTED] in the whole COMINT effort is brought out later in the report, and also in Appendix I.

Returning to the Enigma experiences, it is certainly true that the Germans could have modified their communications rules in such a way as to have ruined our exploitation techniques. The fact remains, however, that they did not. It is not easy to make a change in a major communication network even in peace time, and it is clearly much harder in war time. The changes they did make seemed to be largely directed toward the prevention of [REDACTED] and while they slowed us down we weren't stopped. [REDACTED]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36



(b) (1) - -  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36



(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~

18 February 1965

REVIEW OF SELECTED NSA CRYPTANALYTIC EFFORTS

1. Scope

Present cryptanalytic efforts against [redacted] high-grade cryptography serve two purposes which need to be distinguished in any commentary on or evaluation of this activity. They produce a flow of intelligence from the fragmentary reading of one of [redacted] which constitutes a current return from the activity. To the extent, however, of probably [redacted] of the resources expended, they constitute an investment that must be justified by the expectation of benefits it will yield in the future. Therefore, a judgment about the proper scale of the activity logically requires an estimate of the magnitude and timing of the benefits it will ultimately yield, and some means of placing a dollar value on both current and anticipated future benefits for comparison with the costs that are presently being incurred.

Our ability to exploit one [redacted] today in fragmentary fashion is of course the result of efforts made over a considerable period of years. Accordingly, most of the costs of the flow of intelligence currently produced have long since been paid; they are sunk costs; the outlays that must now be made month-by-month to maintain this production are modest. There is little doubt, therefore, that if this part of the total effort against [redacted] high-grade

LIMITED DISTRIBUTION

SC-01287-65  
Cy 15 of 15 Cys

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~ [REDACTED]

systems were separated out for consideration, no one would question the wisdom of continuing it. Most of the difficult decisions that have to be made about the use of resources in this area concern the scale on which it is appropriate to make risky long-term investments and the choice of investments to be made. Hence the focus of this report is "on those analytic areas where the effort in terms of intercept, analysis, and expenditure is extensive and the cryptanalytic success not immediately apparent or possessed of high probability of achievement."

For the most part, this report will be concerned with the primary judgment that must be made about any risky investment, that is with the required estimate of the timing and magnitude of the benefits it is realistically likely to yield. What is the probability that some degree of success will be obtained in the attack on [REDACTED] high-grade systems; what degree of success; when? Since "success" in this endeavor is measured in terms of a flow of intelligence, the logical second step in the evaluation should be to place a dollar value on the predicted output. Unfortunately, however, no one has ever found a way to quantify the value of a prospective flow of intelligence in money terms, for reasons discussed below. Thus a tidy result in the form of a comparison between what the effort is worth in dollars and what it costs in dollars is precluded. The best that can be hoped for is a qualitative evaluation of the possible future output but even this could not be attempted within the limits of time and scope that circumscribe this report.

TOP SECRET [REDACTED]

~~TOP SECRET~~ [REDACTED]

To confine attention to the costs and benefits of the investments actually being made would, however, yield a conclusion too narrow to be of great value, even if a comparison could be carried through. As a practical matter, no one would seriously consider completely terminating the activities here under consideration. The question really at issue is whether they should be moderately reduced or expanded. Many of the resources involved, including people and their skills, equipment and other facilities, and institutional arrangements, are highly specialized and, if freed in part from their current assignments, would find by far their most valuable employment in other cryptologic activities of the U.S. Government. Thus, a diversion of resources from the massive current investment in the attack on the [REDACTED] high-grade ciphers could be used to expand these activities rather than to reduce the total cryptologic effort and budget. Accordingly, some attention is given in this report to the alternative uses for these specialized resources within the NSA, even though the other cryptanalytic activities fall formally outside the terms of reference of this inquiry.

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

- 3 -

~~TOP SECRET~~ [REDACTED]  
LIMITED DISTRIBUTION

~~TOP SECRET~~ [REDACTED]

2. Limitations of the Evaluation

The difficulties encountered in attempting to assess the value of as yet unsuccessful cryptanalytic activities are reasonably obvious but it is worth commenting on them if only to suggest the function and the limits of usefulness of a report such as this one. The central judgment that must underlie such an evaluation concerns the degree of optimism that is appropriate with respect to the ultimate success of the cryptanalysts in any group of tasks. What is the likelihood that they will complete their diagnosis of a machine or an electronic system? Assuming they will be successful in this primary operation, what are the chances that they will be able to recover the machine or the logic of the cryptographic system? And assuming success in this second phase of the attack, how much of the traffic transmitted in the system in question will be exploitable? Nor can these questions be asked without reference to the time dimension; with respect to each of the three phases it is necessary to inquire not only what is likely to be accomplished but how soon.

It is repeatedly emphasized that cryptanalysis of high-grade systems is essentially the art of exploiting the mistakes of the other side, mistakes in the design of machines (and other systems), in cryptographic practices, and in daily operation. Obviously, therefore, any estimate of cryptanalytic accomplishments is inherently highly uncertain. There is absolutely no way mathematically to calculate, for instance, the probability that diagnosis of

~~TOP SECRET~~ [REDACTED]

- (b) (1)
- (b) (3)-50 USC 403
- (b) (3)-18 USC 798
- (b) (3)-P.L. 86-36

~~TOP SECRET~~ [REDACTED]

the [REDACTED] will be completed and the machine recovered within, say, two years. The cryptanalysts working on this problem by now know some of the characteristics of the machine, they have had experience of the frequency of [REDACTED] and they have lived through the history of attacks on other cryptographic systems. They can develop a feeling of moderate optimism or pessimism but they cannot quote an objectively determined probability of success and their qualitative judgments are inevitably in part subjective.

Paradoxically, these circumstances may help to explain the limited role of an outsider in the evaluation of cryptanalytic activities with which he has no organizational connection and in which he has no professional competence. (It should be said at this point that to define a role does not create any presumption that it should be a continuing one or one frequently played, or that it cannot be well played by existing instrumentalities.) Perhaps the outsider's role is to take responsibility for the guesses that the cryptanalysts should not be compelled to make. If those who have been working for years and who face more years of work in a massive attack on a cryptographic system are pinned down to estimating the chances of a specified degree of accomplishment in a specified time, they are bound to be torn between two temptations. One is to express the optimism that will justify continuation and even expansion of the attack and the other is to avoid the risk of having promised too much by

~~TOP SECRET~~ LIMITED DISTRIBUTION [REDACTED]

~~TOP SECRET~~ [REDACTED]

expressing a relatively pessimistic view. There are obvious reasons for relieving the professional cryptanalysts themselves from the necessity of committing themselves to such an estimate in any formal fashion. The outsider, however, can listen to them, set down as faithful a reflection as he can of their composite judgment, and assume the responsibility for it. It must be emphasized, however, that the only advantage he possesses is a detachment from the activity which may make it easier for him to be disinterested and to accept a risk. The composite judgment that he records can be nothing but a kind of average of those that have been expressed to him or which he had inferred to be in the minds of the professionals. It remains a discouragingly shaky basis for decisions involving the massive commitment of resources.

There is another difficulty encountered in evaluating an as yet unsuccessful cryptanalytic effort. Viewed as an investment, this activity is expected to yield two future benefit streams: one of these is the flow of intelligence that will be forthcoming if it is successful; the other is a growing competence in cryptology, that is, a series of improvements in the state of the art of cryptanalysis (some of which may also be of value in cryptography). Enjoyment of the latter type of benefit is by no means necessarily dependent on the kind of success which ultimately yields a flow of intelligence. A number of new chapters in cryptology have emerged from cryptanalytic attacks

~~TOP SECRET~~ [REDACTED]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~ [REDACTED]

that are still unsuccessful. Thus the investment represented by the efforts against the [REDACTED] high-grade ciphers has already improved the capability of the United States to solve other cryptanalytic problems, and it can confidently be expected that this will continue to be true. Not only are the improvements in the state of the art that are generated in this fashion applicable to other targets, notably lower-grade [REDACTED] traffic and the traffic of other governments, but they will improve our chances of success with new [REDACTED] systems in the future. A most important special case is the contribution this experience will make to our ability to read enemy traffic in the contingency of war, when it is realistic to expect that many mistakes will be made in the handling of cryptographic systems under stress and when, therefore, the prospects for current exploitation of encrypted traffic would presumably be much greater than in peacetime. These improvements in the cryptanalytic state of the art also provide significant assistance to the design and protection of our own cryptographic systems.

An evaluation must, therefore, endeavor somehow to weigh not only the prospects for a future flow of intelligence but also the benefits to cryptology. The reason this is cited as a further difficulty is, of course, that the latter simply defy quantification. It is possible to acquire some "feel" for the progress of cryptology in recent years and to recognize that a major

- 7 -

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [redacted]

part of this has been achieved in the course of the attack on the more difficult [redacted] systems. This is not to say that a good deal of the progress could not have been achieved if the same resources of brain power had been at work on other cryptanalytic problems, but it is the view both of the cryptanalysts in NSA and of informed outsiders that the most sophisticated advances in the state of the art are apt to be those generated in [redacted]. The very fact that (with the possible exception of the [redacted] [redacted] confront us with the most advanced and best operated secure cryptographic systems suggests that the attack on these is the best preparation for handling the problems we will increasingly encounter in other parts of the world. This consideration must therefore be treated as an important one but it can be taken into account only qualitatively.

(b) (3) - P.L. 86-36

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36

~~TOP SECRET~~ [redacted]



~~TOP SECRET~~

(b) (1)

(b) (3) -50 USC 403

(b) (3) -18 USC 798

(b) (3) -P.L. 86-36

3. The Background of the Problem

Proceeding from these introductory remarks on the scope of this report, the nature of the judgments required for the evaluation of cryptanalytic efforts, and the difficulties in making these judgments, it is useful to refer to certain features of the background against which any current evaluation must be made. The obvious place to begin is with the so-called Baker Report of 1957. This was the result of an investigation-in-depth on the whole communications intelligence program of the United States by a group of scientists of outstanding technical competence. Their report must be regarded, therefore, as by all odds the most authoritative independent commentary on the communications intelligence program that has been prepared since [redacted]

[redacted] That report covers many matters beyond the scope of this paper (including notably certain aspects of internal NSA organization, the whole collection effort, data processing, and research and development). In its treatment of cryptanalysis, and more especially efforts against the [redacted] high-grade systems, the major general conclusion of the report is that the enormous technical advances of the last 15 years in cryptology favor a more rapid advance for cryptography than for cryptanalysis. "Technology is irresistably making the situation worse rather than better." (It is to be noted, however, that despite this conclusion, the Report advocated increased rather

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~ [redacted]

than decreased cryptanalytic efforts, including those directed against [redacted] high-grade systems.)

Understandably, this sweeping assertion is challenged in the cryptanalytic community and the experience of the seven years since the Baker Report was written gives considerable support to the arguments that are advanced in opposition to such generalized pessimism. The rebuttal is apt to start with the suggestion that it is easy for an informed U.S. observer to credit the opposition with an ability both to devise unbreakable cryptographic systems and to avoid mistakes in their use except under special circumstances. To make this assumption about [redacted] performance is to pit the American cryptanalyst, operating within acknowledged constraints, with analytic skills which, though of a high order are less than perfect, who must contend with bad luck as well as good luck on occasion, against an almost perfect cryptographic effort. This way of looking at the future, it is argued, inevitably tips the scales against U.S. cryptanalysis and this is the intellectual trap into which it is alleged the Baker Panel fell.

In support of this rebuttal, certain encouraging observations can be made that reflect the experience of recent years. First, it is still true that the [redacted] typically make numerous and serious [redacted] when a new system is introduced. By being alert to the appearance of new systems, therefore, and by ensuring adequate intercept of early operational traffic, there is good

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

~~RESTRICTED INFORMATION~~  
~~TOP SECRET~~

reason to expect that raw material will be acquired which will greatly assist an attack on the new system. Second, it continues to be true also, that a significant number of [ ] are made, month in and month out, in the operation of even well and long established cryptographic systems, like [ ]. One need not, therefore, be wholly pessimistic about the prospects for acquiring and accumulating a significant volume of inputs for the cryptanalytic attack, or for at least fragmentary opportunities for the exploitation of a machine if it can be recovered. A third observation is that the [ ] when they introduce new machines do not in all cases proceed at once to the optimum design (from the standpoint of their communications security) that is presumably within their technical competence. [ ]

[ ]

[ ] It is obvious too, that the [ ] continue to be constrained in altogether understandable ways by such considerations as their large investment of both resources and experience in established systems, which argue against the too rapid introduction of new ones, by the rapid growth in the total volume of communications which compels continued major reliance on radio links, and by the shortage of really skilled and disciplined operators, which presumably plagues all communications systems everywhere.

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

~~TOP SECRET~~ [REDACTED]

Clearly, then, the defense that must be overcome is not a set of idealized systems embodying the most advanced technology in design, the most secure cryptographic practices, and the most skillful and disciplined operational handling of which the [REDACTED] are theoretically capable. It is, rather, a set of systems built by human beings who are subject to familiar kinds of constraints, who do not always push their technology to the limits of the state of the art, who sometimes make bad technical choices in the design of systems, and who can be depended on to operate carelessly some fraction of the time.

More impressive even than these observations as evidence which challenges the pessimism of the Baker Panel are the very substantial results that have been achieved since it completed its study. The notable accomplishment, of course, has been completion of the diagnosis of the [REDACTED] the development of techniques for recovery of the machine in each crypto period, and of techniques for entering a small but still significant fraction of the traffic by taking advantage of [REDACTED] New special purpose equipment which will soon be operational will enable a sizeable increase in the size of this fraction. It is confidently anticipated that NSA will read approximately [REDACTED] messages transmitted through this [REDACTED] this year and it expects to exploit a sufficient volume of traffic to yield about [REDACTED] message a year thereafter. With a similarly high confidence factor, the Agency expects to be current about half the time, that is, to have recovered the machine as use

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~

in a given net about half-way through the typical two-year crypto period, on the average. When the cryptanalysts are in this sense "current," messages of [redacted] links can be read within [redacted] which means that the average time lag from intercept to decryption can be of the order of [redacted]. For messages that are intercepted during the earlier part of a crypto period when NSA has not yet recovered the machine on which they are transmitted, the time lag between intercept and decryption is of course set by the date on which the machine is recovered. Although an average delay has little meaning, it would in fact be of the order of six months.

Anyone who has been exposed to the history of the cryptanalytic achievement represented by this exploitation capability is bound to be impressed by its magnitude. Yet it illustrates the limitations on what we can hope to accomplish against high-grade systems. Despite the impressive absolute volume of [redacted] traffic that NSA expects soon to be exploiting, we will be reading only [redacted] of the traffic that is intercepted. The time lag between interception of the message and its receipt by the intelligence analysts will half of the time be as little [redacted] the time will run to [redacted] and be essentially unpredictable. Above all it must be emphasized that the [redacted] sample of intercepted traffic which turns out to be decipherable is determined by the incidence of [redacted]

LIMITED DISTRIBUTION

~~TOP SECRET~~

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

carelessness and of machine malfunctions so that the selection is one over which we have no control.

Although, it is conceivable that techniques might be devised for entering [redacted] traffic "on cipher," that is, for decrypting traffic on days and links of our selection rather than those on which [redacted] occur, this would probably be so costly a mode of exploitation in terms of cryptanalytic time and machine time (even after the capability had been developed) that it could be used for only a very small percentage of the total traffic intercepted. It is doubtful whether large resources should be invested in the attempt to develop this capability, especially since the traffic entrusted to the [redacted] is not as rich in intelligence as that which is handled by other systems. [redacted]

[redacted]

[redacted] Only [redacted] of the messages are [redacted] at all, the [redacted] bulk are [redacted]

[redacted]

[redacted] Presumably, however, more will be known about both the prospects of success in such an undertaking and its costs before a final decision will have to be made.

It is relevant to the Baker Panel's pessimism that the achievement of the results characterized above, limited as they are, took some [redacted] after [redacted] came into reasonably extensive operational use. To be sure,

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

much of this time was required to develop the whole system of intercepting, storing, and processing [redacted] traffic, a developmental activity which has not had to be repeated for the other [redacted]. The more narrowly defined cryptanalytic effort occupied only a portion of the [redacted]. Nevertheless, a massive intellectual effort was required over a number of years.

What is one to conclude from the experience of the [redacted] and more particularly from the success against [redacted] and the progress against a number of other high-grade [redacted] systems? Does the rebuttal successfully destroy the proposition advanced by the Baker Panel that technology is tending to shift the balance of advantage from cryptanalysis to cryptography? Although this may not be a useful question to explore because their broad generalization has little immediate relevance to policy, the opinion will be hazarded here that the answer should be negative, that in long perspective their pessimism is justified.

The apparent purpose of the Panel in advancing the generalization was to draw a sharp contrast between the brilliant and massive cryptanalytic wartime successes against the Japanese and Germans, and significant success later against the [redacted] which characterized our experience up [redacted] and the very much bleaker prospects we faced in [redacted] for the actual exploitation of high-grade [redacted] traffic, even on the most optimistic assumptions.

~~TOP SECRET~~ [REDACTED]

Perhaps the wartime accomplishments were exaggerated in retrospect. Yet nothing has happened since that report was written which calls into question the view of its authors that much more modest results were the most that could be hoped for in the future and that attitudes and hopes should be adjusted accordingly. What can be said, however, is that we are probably doing better today against the high-grade [REDACTED] systems than the Panel expected we could; that visible progress is being made and promising approaches are being exploited; and that the new kinds of [REDACTED] systems which the cryptanalysts have so far encountered do not appear to them at the present stage of their exploration to be invulnerable to attack. If the acquisition of timely intelligence from high-grade systems on the World War II scale would appear to be out of the question, the prospects for more modest results are better than they appeared [REDACTED]

- (b) (1)
- (b) (3)-50 USC 403
- (b) (3)-18 USC 798
- (b) (3)-P.L. 86-36



(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

~~TOP SECRET~~

4. The Prospects for Success in the Next Few Years

Against the background of the foregoing discussion of the Baker Panel's arguable general conclusions concerning the progress of the attack on the [redacted] high-grade systems, the time has now come to bite the bullet by considering the prospects of the various systems against which no success has been achieved comparable to that with [redacted] and from which, therefore, no continuing flow of finished product in the form of intelligence is yet being derived. It must be repeated in starting this section of the paper that the timing and degree of success that may be achieved is inherently most unpredictable, except perhaps with respect to those systems that have already been worked on for many years, and, therefore, that the judgments herein set forth are unreliable as bases for policy. The reader must also be reminded that these can only and do represent the synthesis by the reporter of views expressed by a number of more deeply informed and more highly qualified analysts. His role is limited to that of synthesizing, reporting, and thereby hopefully reducing the pressure on the analysts themselves to make commitments they would prefer to and probably should eschew. These comments will be organized around [redacted] together with [redacted] are listed below.

It is useful as background for the discussion to give at this point some measure of the effort that is being expended on each of these. Probably the

~~TOP SECRET~~

[Redacted]

most significant measure is given by the assignment of the top-level cryptanalysts in the Agency. To do so requires the identification of the category of people regarded as falling in this group. To avoid extraordinary arbitrariness, NSA was asked to identify first a very limited group, which turned out to be [Redacted] in number, who obviously constitute the elite of the profession, and, second, a larger category (additional to the first) of less senior but still highly competent analysts, which came to [Redacted]. The first column in the following table shows the assignment of the first category and the second column that of the larger.

Across the Board	
[Redacted]	(b) (1)
[Redacted]	(b) (3)-50 USC 403
[Redacted]	(b) (3)-18 USC 798
[Redacted]	(b) (3)-P.L. 86-36
More Than One Area Not in Cryptanalysis	
Total	

Turning to the other measure of effort, dollar costs, an analysis has been made by NSA for the purpose of segregating the costs of the cryptanalytic

[Redacted]

effort as a whole within the [redacted] and of the current attack on the high-grade [redacted] systems within the over-all cryptanalytic effort. The Agency's analysis is appended as a separate annex. The grand totals which stand out indicate that the whole cryptanalytic effort is costing in the current fiscal year [redacted] and is employing some [redacted]. The comparable figures for the effort against the [redacted] high-grade systems are [redacted]. A breakdown by functional headings of the approximately [redacted] total is given in the following table for the current fiscal year and for [redacted]. Beyond [redacted] all the way through [redacted] the numbers show little change with the exception of a gradual increase in the estimated cost of machine processing and, in [redacted] of crypt-analysis itself.

Collection
Processing
Cryptanalysis
Subtotal
Research & Development
Machine Processing
Procurement
Operation and Maintenance
Total

(b) (1)
(b) (3) -50 USC 403
(b) (3) -18 USC 798
(b) (3) -P.L. 86-36

Another breakdown is given in the following table which shows, for the [redacted] programs, the first three categories of costs (collection,

~~TOP SECRET~~ [redacted]

processing, and cryptanalysis), allocated by target system. The totals for R&D, machine processing and procurement cannot be directly allocated in this fashion, but over [redacted] of these are incurred in the efforts against the

[redacted]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

Both the dollar figures and those for assignment of senior cryptanalysts show a heavy concentration of effort on [redacted] with the second largest on [redacted]. The budgetary figures also indicate the high cost of both R&D and machine processing. It should be said, however, that the size of the former of these is primarily a measure of the degree to which the work in progress in [redacted] is the Agency's pioneering effort. It is in the attack on the high-grade [redacted] systems that new technology is having to be developed, some of which is already applicable to [redacted] targets and much of which someday will be.

With these rough indications of the magnitude of the several efforts, the [redacted] identified in the above list (omitting [redacted]) will be discussed in turn.

(b) (3)-P.L. 86-36

~~TOP SECRET~~ [redacted]

UNCLASSIFIED

~~TOP SECRET~~

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [redacted]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

Despite these efforts, only about half of the machine has been recovered, and this as a result of work done more than [redacted] In the last few years little further progress has been made. Currently [redacted] new

~~TOP SECRET~~ [redacted]

~~TOP SECRET~~

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

attacks are in preparation, both of them requiring [redacted]

[redacted] Thereafter it will require something on the order of up to [redacted] a period determined by the capacity of the machines - fully to exploit the potentialities of these attacks. In the meanwhile, additional traffic is being converted for machine processing at a rather moderate rate.

The status of this cryptanalytic effort may, therefore, be summarized as follows. The attack has not yet come up against a stone wall; there are at least [redacted] further specific approaches to be explored.

While these explorations are in progress, rather [redacted]

[redacted] will be tied up but very little top-grade cryptanalytic brain power will be used. An outsider's estimate of the prospects of success is that they are very remote. With the investment already made, the cost of carrying out the operations planned for the next [redacted] is small and there would appear to be little reason to question the wisdom of so doing. The NSA position is, however, considered sound; that there be no further investment, whether of money and equipment or of the time and energy of highly qualified cryptanalysts on [redacted] beyond the [redacted] attacks mentioned above, unless significant new data becomes available from

[redacted] or other sources that justify it.



~~TOP SECRET~~

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

[redacted] Not enough work has been done on this problem to give any indi- : . :  
cation of the number of systems included or of their degree of invulnerability.  
At least a modest exploratory effort would therefore seem to be indicated.  
NSA has reactivated the cryptanalytic attack on [redacted] which  
has already achieved significant progress. A [redacted] has recently been identified  
which ranks as one of the major finds of recent years. Nevertheless, an out-  
sider's estimate must be that the possibility of success up to the point of  
even limited exploitation is low.

LIMITED<sup>25</sup> DISTRIBUTION

~~TOP SECRET~~

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~

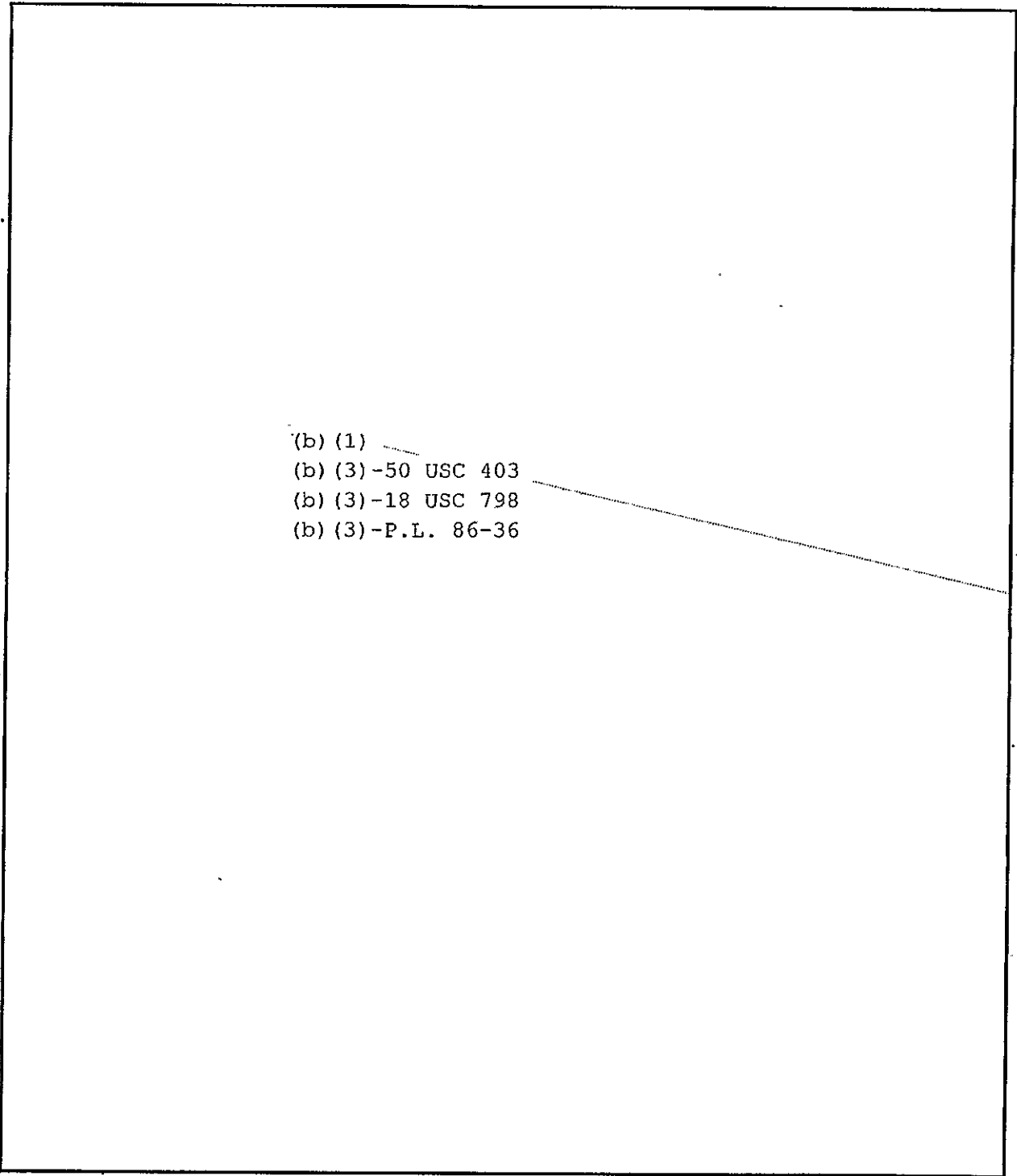
~~TOP SECRET~~

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

With respect to this system as to the others it is possible for an outsider to record only an impression. One well-informed analyst's estimate of the prospects for success that has been quoted is a [redacted] likelihood of recovering the machine within [redacted]. A second, considerably more pessimistic, is a [redacted] likelihood of recovery in such a period, and a third estimate, although expressed with less numerical precision, was inferred to fall about [redacted]. Presumably all analysts would agree that the probability rises with the length of time allowed for the effort, though those at the pessimistic end of the spectrum would allow it to rise only slowly. In short, it would appear reasonable to estimate a [redacted] chance of recovery within [redacted] rising to considerably better than an even chance in [redacted] and also to assign a better [redacted] probability that recovery, if accomplished, would permit the exploitation of a larger proportion of the traffic intercepted than the [redacted] characteristic of [redacted]. If this "average" opinion is accepted, the prospects for success in attack on [redacted] are brighter and the prize to be gained thereby more valuable than for any of the other targets under consideration.

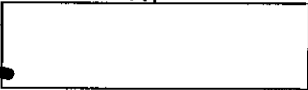
(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

~~TOP SECRET~~



(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~



~~TOP SECRET~~ [REDACTED]

[REDACTED]

The [REDACTED] systems are new enough, both in their concept and in their usage, that cryptanalysts cannot easily be tempted into giving quantitative estimates of the likelihood of success against them. Certainly, however, they do not feel that they are up against a stone wall; there are approaches to the problem which are being explored. It is a safe prediction that the state of the art of cryptanalysis will be advanced in this effort. Until a good deal more work has been done on these machines, perhaps for several years, it is suggested that the assumption of about the same degree of optimism as is applied to the [REDACTED] is appropriate for planning purposes.

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

LIMITED DISTRIBUTION

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

g. Summary

The foregoing paragraphs contain an outsider's synthetic appraisals of the status of the attacks against the various [REDACTED] high-grade systems and their prospects for success. They can be summarized as follows:

- (1) Virtually no hope for the [REDACTED] high-grade systems.
- (2) Very little hope for [REDACTED] too little known as yet about [REDACTED] to support an estimate but a case for an exploratory effort.

~~TOP SECRET~~ [REDACTED]



(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

~~TOP SECRET~~

(3) High degree of confidence in the exploitation of [redacted]

[redacted] of intercepted [redacted] traffic, amounting to [redacted]

[redacted] messages a year.

(4) Pessimism with respect to [redacted] perhaps a [redacted]

chance of recovering the machine within [redacted] and poor

prospects for exploitation if recovered, unless cryptographic usage

turns out to have unexpectedly favorable aspects.

(5) Moderate optimism with respect to [redacted] this defined

as a [redacted] of recovery within [redacted] multiplied by

a better than [redacted] of exploiting [redacted]

considerably more of intercepted traffic if recovered.

(6) With respect to [redacted] there is enough known

to convince the cryptanalysts (a) that whatever the future may hold,

they have not as yet seen anything in these systems that is especially

terrifying or that suggests they will prove to be invulnerable; (b) that

there is promising work to be done in learning more about them; in no

sense have the investigations reached dead ends.

(7) With respect to the [redacted]

[redacted] considerable success already achieved; insufficient

work as yet on the comparatively new [redacted] system to justify an

estimate but moderate optimism seems justified on the basis of progress

on the older systems with [redacted]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~

5. The Value of the Raw Intelligence Obtained and Its Cost

This is believed to be as close as anyone can come (and probably closer than a wise man should) to an estimate of the stream of benefits in the form of raw intelligence that is to be hopefully anticipated from the massive investment currently being made. Logically the next question to which some sort of answer should be attempted concerns the value of the kind of fragmentary intelligence that is all that can be hoped for even in the event of what has here been described as cryptanalytic success against any of the high-grade  systems. Unfortunately, this question is unanswerable in quantitative terms and a qualitative answer would require an inquiry on a scale and of a duration well beyond the scope of this report.

There are both philosophic and practical reasons why this is so. As a starting point, it may be said that no one has ever found an altogether rational way of evaluating a particular flow of intelligence in dollar terms. Pragmatically, the only way the value to the nation of "intelligence" as a whole (like "national Security") is established in money terms is through the normal budgetary process. The government is the only buyer of these commodities. What it pays for them is the only price they carry. The only figure that can be quoted as a measure of what the whole flow of intelligence turned out by the intelligence community is worth in dollars is whatever amount has been appropriated each year. Obviously, this number which is the cost of an

~~TOP SECRET~~ [REDACTED]

activity and which reflects past evaluative judgments about it, gives no indication of whether these past judgments were correct, that is whether the "value" (in some undefined sense) of the intelligence produced has turned out to be at least as great as its cost.

The question "what is intelligence worth," can elicit only an arbitrary answer but it should be possible to arrive at a meaningful comparative evaluation of particular flows or bodies of intelligence. One should be able to ask the users whether one series of reports is worth more or less than another. If the judgment could be expressed cardinally (that is if the users would indicate by what factor the value of Series A exceeds that of Series B), and if the cost of each series could be ascertained, it would then be possible at least to determine which of two collection activities or sources had the more favorable cost effectiveness ratio.

There are many reasons, however, why this procedure does not seem to be employed frequently or systematically. One is that the relative value of two flows of intelligence may change frequently through time as requirements for information on different countries and different subjects change. Another is that each intelligence collector, like NSA, has many consumers who have legitimately competitive requirements and, therefore, legitimately differing views concerning the usefulness of a given body of intelligence. Since it is scarcely feasible for the users to bid against one another in a free

~~TOP SECRET~~ [REDACTED]

- (b) (1)
- (b) (3)-50 USC 403
- (b) (3)-18 USC 798
- (b) (3)-P.L. 86-36

~~TOP SECRET~~ [redacted]

market, a collective comparative evaluation would have to be arrived at by arm's length negotiation. This procedure is not conducive to either clear-cut or subtle evaluation. Still another reason is the reluctance of both the collectors of raw intelligence and the analysts who use it to make comparisons which are bound to be invidious and could cause one or another collection activity to be curtailed. The whole community is in the habit of pressing for more intelligence from all sources; it is not well organized to make comparisons, especially as between the outputs of major collection systems. For all these reasons, evaluations are generally speaking purely qualitative and non-comparative. The body of intelligence under consideration is characterized by such terms as "vital," "useful," or if the evaluator really thinks it is unimportant "corroborative of other sources."

Despite these difficulties, there is little doubt that a useful qualitative evaluation of the intelligence to be expected from, say, the exploitation of [redacted] could be arrived at. Probably the simplest way of so doing would be to take a sizeable sample of raw intelligence derived from [redacted] to find out who in the intelligence community has used this material for the production of finished intelligence, how useful they have found it to be, to what extent its value has been limited by its fragmentary and accidentally selected character and, for much of it, its lack of timeliness. Such an appraisal would then need to be arbitrarily corrected to allow for the almost certainly interesting and informative character of the traffic carried on [redacted]

UNCLASSIFIED  
~~TOP SECRET~~ [redacted]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~ [REDACTED]

The judgment of a few intelligence analysts arrived at in this way would probably constitute as useful an evaluation as it is feasible to undertake but, to repeat, it would not be an estimate of what an assumed success would be worth either quantitatively in dollars or comparatively by reference to some other identifiable body of intelligence.

Unfortunately, this sort of investigation has not in fact been carried out. Its results would presumably have little standing unless it were undertaken on behalf of the whole community and with the participation of more than one intelligence agency. Moreover, such an evaluation would require major support by NSA, if only because a significant fraction of the [REDACTED] traffic that is decrypted is not identified [REDACTED] when it leaves NSA so no one outside of that Agency can assemble a representative sample of the traffic for evaluation. One of the suggestions at the end of this report is that such an evaluation be undertaken.

Lacking quantification in dollar terms of the future benefits that it is legitimate to expect (or assume) for planning purposes from the attack on the high-grade [REDACTED] systems, there is obviously no rational way of demonstrating that they are either greater or less than their dollar costs

[REDACTED] Moreover, the tools available for budgetary analysis of cost and effectiveness in cryptology are and will remain extremely crude.

It will never be possible to estimate the effect of changes in the input of

~~TOP SECRET~~ [REDACTED]

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [REDACTED]

resources on the future output of intelligence except with large margins of uncertainty. The placing of a dollar value on an assumed future flow of intelligence will always involve an essentially arbitrary act of judgment. It is going to be a long time before even cost effectiveness comparisons can be made between radically different intelligence collections activities (such, for instance, as cryptanalysis, [REDACTED] reconnaissance, and [REDACTED] [REDACTED] since this analysis would require not only quantitative estimation of the output that would be produced by an increment of resources in each collection activity but also the sort of cardinal comparative evaluation of alternative flows of intelligence which the intelligence community finds it difficult to make for reasons alluded to above. In this situation, decisions about the scale of major and sharply differentiated sectors of intelligence activity have to be based on rough, broad appraisals, not on refined cost benefit comparisons. Wise judgments rather than detailed quantitative calculations must be the basis of a determination that more or fewer dollars (resources in general) should be devoted to cryptology (or to reconnaissance or [REDACTED])

On the other hand, it is both intellectually and administratively feasible to apply a rather more refined calculation to decisions concerning the allocation of resources within one major sector of activity. Intellectually, this is a more manageable process because both the resources employed and the

UNITED STATES GOVERNMENT  
~~TOP SECRET~~ [REDACTED]

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [REDACTED]

products produced by different programs within one sector are more homogeneous. Cryptologists can be shifted from one target to another (as can the engineers who develop reconnaissance systems and the staff members who conduct [REDACTED] COMINT from one source is more readily comparable with COMINT from another source than either is with, say, photography. Administratively, the comparisons involved are easier to make because there are managers who have to make them in the process of determining what is the best allocation of resources. (It is for just these reasons, especially the greater homogeneity of "product" or mission, that cost effectiveness comparisons can be more accurately made between, say, two missile systems than between a missile system and a manned aircraft system and are virtually meaningless as between a strategic missile system on the one hand and an infantry unit on the other.)

The purpose of these remarks is to explain, by way of a reminder, why it is that decisions can be made in one way, that is with one degree of refinement, about the allocation of resources to major sectors of governmental activity and in a rather different way, relying more on meaningful cost-effectiveness comparisons, about the allocation of resources within each sector.

The distinction has implications for the subject matter of this report. When one looks at a particular part of the cryptologic effort there are two

~~TOP SECRET~~ [REDACTED]

different tests one can try to apply in deciding whether the current allocation of resources is just as it should be. One is to ask whether more or less money should be budgeted for these particular programs, but this question invites only the same sort of broad judgment and essentially arbitrary answer that can be made about the sector as a whole. The other relevant question is whether a larger or smaller portion of the whole pool of cryptologic resources should be allocated to these programs. This question should be susceptible of a less arbitrary answer, one to which cost-benefit calculations could contribute far more. It is, therefore, convenient to arrive at a conclusion about the magnitude of the effort against the high-grade [REDACTED] systems in two stages: first with respect to the scale of the whole cryptologic capability and second with respect to the allocation of cryptologic resources to the particular programs here under discussion. Opinions on both are discussed in the concluding section of this report, where some of the judgments on which they rest are enumerated.

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [REDACTED]



- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~

6. The Allocation of Cryptologic Resources

In a sense, the latter of these topics is beyond the scope of the present report which is confined to the [redacted] systems. Yet, as a practical matter the kind of review that has been attempted here probably has more bearing on and relevance to allocation than to budgetary decisions. The actual consequence in 1956 of the decision to give top priority attention to the high-grade [redacted] ciphers was a shift of people (and other resources) away from other cryptologic tasks. Even if there had been a willingness to fund this additional effort entirely as an increment to the dollar budget, its short-run impact would have been on the allocation of manpower, machine time, and the other scarce resources the pool of which can neither be augmented nor greatly reduced overnight.

Something must, therefore, be said about the possible other uses of cryptologic resources. One must try to learn how badly senior cryptanalysts are needed in other NSA programs, what contributions they could make there, and to what extent it would be feasible to reallocate them in this fashion, if it should prove desirable, given their long specialization on certain problems, their particular linguistic skills, and the other constraints on freedom of movement. Without pretending to have had the benefit of more than a few scattered conversations on this matter, the resulting impressions will be mentioned here, if only because they inevitably influence the conclusions of the report.

~~TOP SECRET~~ [redacted]

(b) (3) - P.L. 86-36

To begin with, there is no question that other programs of the Agency would benefit from the availability of some additional high caliber cryptanalysts with appropriate other resources. Not only would these individuals contribute directly the results of their own analytical work but it was emphasized that in a number of areas of Prod outside of [redacted] the able cryptanalysts are spread so thin that the capabilities of other elements of the staff cannot be utilized as effectively as they might. In other words, additional senior cryptanalysts in these areas would render the efforts of the rest of the staff more productive.

No firm opinion will be offered here as to the specific areas where the need is greatest. [redacted]

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36

[redacted] With respect to [redacted] the limiting factor

would appear to be collection and topflight traffic-analytic personnel rather than cryptanalytic effort at this time. Another set of targets which should be mentioned are the [redacted] It has also been suggested that a few additional first-rate cryptanalysts could contribute significantly to traffic analysis.

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~

Beyond these general and qualitative comments on the need for cryptological resources in other programs, it would be improper to go. Clearly, they are not sufficient to support a judgment that the resources concerned would contribute more or less if there were a modest change in their allocation. The management of NSA undoubtedly tries to allocate resources in a way that will maximize their contribution, given the priorities on different intelligence sources that are established by the intelligence community.

This kind of calculation cannot, however, be an easy one. For instance, it would be hard to pin down the responsible supervisors in NSA to any estimate of the degree to which progress on the high-level cryptanalysts included in the elite of [redacted] together with appropriate supporting resources, to other targets. It would no doubt be equally difficult to pin down the senior professionals responsible for the other areas to an estimate of the degree to which the shift would accelerate the progress of their work. When it is so difficult to estimate the effect on the present and future flow of intelligence of a modest shift out of one risky investment into another (perhaps less risky), there is little incentive to define, study, and evaluate several different options with respect to the use of resources in an effort to refine the way in which their allocation is optimized.

It may be worthwhile at this point to comment in rather theoretical terms on the optimization process. If the present allocation of well over half the top-level cryptanalytic manpower, and of about two-thirds of the

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [REDACTED]

cryptanalytic effort measured in dollars, to the attack on the high-grade [REDACTED] systems is taken as one option, at least two other sets of options could be defined. One is that which would result from a shift of resources to less difficult cryptanalytic problems, already well known and identified as such. It is legitimate to expect that this action would in due time give rise to a larger total flow of decrypted material but would do so at the expense of a longer delayed and ultimately smaller flow of decrypted high-grade [REDACTED] traffic. The other set of options is that which would result from a shift of resources to developmental activities, essentially exploratory investigations to learn more about the characteristics of newly encountered systems, to assess the current state of cryptographic practices in various countries, and generally to seek to identify the targets which are technically promising for any one of a number of reasons (including successful [REDACTED]). Stated more succinctly, it should be possible by accepting a somewhat more pessimistic outlook for the exploitation of the high-grade [REDACTED] systems (together with the associated sacrifice of education and of contributions to the state of the art) to buy either a larger, more timely, and more predictable flow of COMINT from all sources taken together (with a smaller proportion being [REDACTED]) or more flexible and extensive developmental activities.

The purpose of identifying these three options (the present allocation and the two alternatives thereto) is, of course, to say something about the character of the choices they present. Consideration of either of the two

UNITED STATES DEPARTMENT OF DEFENSE

~~TOP SECRET~~ [REDACTED]

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [REDACTED]

alternative options would, for one thing, require an assessment of the degree to which the traffic carried on the high-grade [REDACTED] systems must be presumed to be richer in intelligence than any other COMINT. Moreover, such a shift would involve some diversion of resources from capital formation, that is from the process of advancing the state of the art of cryptology, either to the production of a larger near-term output of useable intelligence (if the first of the alternative options were adopted) or to developmental activities, which constitute, at least in part; a different form of capital formation. Thus, the issues concern the relative values of COMINT from different sources and the proper balance either between long-term investment and near-term output or between two kinds of investment.

There are other kinds of options that could be defined and other choices that could be posed. The foregoing discussion is intended only to illustrate the point that, in an ideal world, several possible allocations of resources, and the different results (future flows of intelligence) that might be expected to result therefrom, could be presented for evaluation. The community could be made explicitly aware of alternatives and could help both to judge which communications nets in which countries might be expected to be carrying intelligence of the highest value and to make the choice between current output and possible future output (the investors' choice).

In the real world, however, there are obvious reasons why such rational decision making can be approximated only very roughly if at all.

~~TOP SECRET~~

(b) (1)

(b) (3)-50 USC 403

(b) (3)-18 USC 798

(b) (3)-P.L. 86-36

For one thing, it would be extremely difficult (as pointed out above) to systemize the definition of available options, that is to tell the customer what the consequences of each of several different allocations of resources would be. There is, too, the more fundamental difficulty that consumers naturally wish to have the flow of intelligence to them maximized in the present and near future and are in no position to assess the price they would have to pay in the longer run in the form of a reduced cryptologic capability. Inevitably NSA itself must be the guardian of the future; it must be the claimant for adequate resources for investment in the form both of the education that is acquired through the attack on sophisticated systems and of the exploratory activities referred to above. Yet another practical difficulty is that the consumers might find it difficult to sort out their priorities to the point where they could rationally make these choices. There are many consumers whose requirements are at least in part competitive and there is always the difficulty of knowing in advance how valuable the decrypted traffic from a particular source will be.

In practice, these immensely difficult managerial decisions concerning the allocation of resources have been made easier for the NSA by the overriding priority which the intelligence community has placed on the [redacted] high-grade traffic as a potential source of intelligence. The priority has been interpreted to mean that all well-defined needs of [redacted] for top-level professionals should have priority over other requirements for personnel, except as

(b) (3)-P.L. 86-36

- 46 -

~~TOP SECRET~~

~~TOP SECRET~~

modified by such circumstances as the temporary but highly urgent priorities that grow out of political crises and the very promising technical opportunities that occasionally spring up in other areas and justify the temporary diversion of personnel. (Such temporary diversions can rarely produce any significant product from cryptanalysis because of the lack of continuity and the lead time needed.) An outsider is left with the impression that, in the shadow of this priority, the attempt has not been made, at least for some years, systematically to weigh against one another various patterns of resource use in the light of estimates of their yields and consumers' evaluations of those yields. A suggestion put forward below is that such a confrontation of needs and opportunities might well be undertaken.

~~TOP SECRET~~ [redacted]

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

7. Conclusions and Concluding Comments

Given the scope of this inquiry as determined both by its terms of reference and by the effort that could be devoted to it, the conclusions that legitimately emerge from it are disappointingly limited. Almost certainly the most useful findings are those concerning the prospects of success against the [redacted] high-grade systems, as summarized on pages 21 to 33 above. These can be described as "findings" in that they are syntheses of the judgments of a number of individuals far better informed than the author of this report, from both within and outside the cryptologic community. Various observations about the evaluation of intelligence and possible procedures for reviewing the allocation of cryptologic resources have perhaps the same degree of validity.

In the course of such a review as this, however, the inquirer inevitably arrives at certain broad conclusions which, as it were, go beyond anything supportable by hard evidence. The concluding comments set forth below are of this character. They are offered in the belief that one individual's impressions on what are admittedly complex policy issues may be of value and that the report would be incomplete without them.

a. There should be no reduction in the over-all cryptologic effort of the United States. Indeed, it is evident that the limitation on the number of really first-class cryptanalysts is more serious than any other single

~~TOP SECRET~~ [redacted]



(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~ [REDACTED]

constraint in pacing our progress and and a strong case can be made for the kind of training provided by the Junior Mathematicians Program which is designed to increase their number. It seems equally clear that if we are to maintain, and hopefully augment, the corps of highly able people, they should be given the full support they require, especially in [REDACTED] equipment and in the supporting staffs required for data processing of various kinds that permit the cryptanalysts to get a hold on their problems. After all, the major technological advance that has favored cryptanalysis over cryptography, at least up to this time, has been the introduction of [REDACTED] [REDACTED] and of improved practices in data processing.

Expensive as such resources are, these technical possibilities must be exploited to the fullest if we are to have any hope of keeping up with the advances of cryptography.

Enough has already been said in this report to make clear that this strongly stated conclusion cannot and does not rely for its support on quantitative comparisons of costs and benefits (if only because no attempt was made to evaluate the whole cryptanalytic effort). The cryptanalytic community cannot estimate with any confidence or any pretense of accuracy what it will be able to produce. The intelligence community has never solved the problem of placing a dollar value on a given flow of raw intelligence, except pragmatically year by year. The most elaborate calculation is

LIMITED DISTRIBUTION  
~~TOP SECRET~~ [REDACTED]

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [redacted]

unlikely to improve this situation greatly. Accordingly, the decision to support the cryptanalytic effort to the tune of [redacted] will continue to be based on essentially broad qualitative judgments. Those that underlie the above conclusions are the following:

COMINT as a whole is still an enormously important form of raw intelligence. For reasons elaborated in the Baker Report and referred to briefly above, one may expect the yield of decrypted traffic from high-grade systems to show a slowly declining trend over the years. On the other hand, this can be a very gradual process and there is an excellent likelihood that there will be at least periods of perhaps some years duration during which the yield (taking account of both quantity and quality) will increase. For instance, we are deriving more COMINT from [redacted] traffic today than we were from all the [redacted] high-grade ciphers a few years ago and the level of exploitation of this whole group of [redacted] will show a further significant rise if the attack on [redacted] in due time meets with some success.

Looking elsewhere in the world, there is in process a steady increase in the total volume of encrypted traffic [redacted] Although in one sense this means that new obstacles to intelligence acquisition are being placed in our path, it remains true that for the next [redacted] our reliance on COMINT in parts of [redacted] may be on the increase and greater than in the recent past.

~~TOP SECRET~~

~~TOP SECRET~~ [REDACTED]

If this prospect is accepted, it follows that our cryptologic capability should be regarded as a major national asset which will have if anything an expanding volume of highly useful work to do at least for some time. Whatever degree of pessimism about the long-run is justified by the shifting of the balance of advantage on high-grade systems from cryptanalysis toward cryptography, even if it be concluded that ultimately the volume and value of COMINT will contract and the scaling down of this capability would be appropriate, there are cogent reasons for believing that many years, probably decades, will elapse before such a situation materializes.

There is another consideration that lends further support to the broad conclusion stated above. It is that lead times are very long in this business so any decision taken today to reduce the scale of the national cryptanalytic effort would not be readily or quickly reversible. An effective effort requires brains, experience, machines, and supporting staffs, together with continuity in the sense of both accumulated raw material and current knowledge of the opponent's cryptographic practices. None of these elements could be quickly found and assembled if it should become desirable to expand a program once a curtailment had actually taken effect.

Although the above conclusion has been expressed negatively that the scale of the cryptologic effort should not be reduced, a stronger positive view will be added here on one activity of the NSA: its Junior Mathematicians

~~TOP SECRET~~ [redacted]

(b) (1)

(b) (3)-50 USC 403

(b) (3)-18 USC 798

(b) (3)-P.L. 86-36

Training Program. If the whole cryptologic effort is to be maintained in scale, and hopefully strengthened in effectiveness, the Agency must engage systematically in the recruitment and training of additional top-level analysts. Dramatic proof of the potential effectiveness of this activity is the fact that a number of the ablest senior professionals in this group today were brought into NSA by way of an organized program that was conducted for only one year in the early fifties. The current program, reactivated two years ago, has been successful in attracting over [redacted]. It seems a safe prediction that men of the caliber of the [redacted] was summarized earlier in this report, will be in short supply relative to the need for them for the foreseeable future. Moreover, these trained people represent the resources with the longest lead time of any in this business. Unless drastic curtailment across-the-board is contemplated, this effort should be pressed; it should be one of the last candidates for any economies that have to be effected.

b. What should receive serious consideration (rather than the scale of the over-all effort) is the desirability of some reallocation of cryptologic resources as between the attack on the high-grade [redacted] systems and other cryptanalytic problems.

As to where the resources should come from, anything purporting to be a definitive or solidly-based judgment would be presumptuous. All

~~TOP SECRET~~ [redacted]

~~TOP SECRET~~ [redacted]

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

that can be recorded is an impression that the work on the data systems is going well and probably should not be disturbed, that it would be dangerous to reduce the effort on [redacted] and similar systems, and that the reactivated effort on [redacted] should continue, at least for a time. What this implies is that the resources would have to be taken from the efforts on the [redacted] with [redacted] certainly having the lowest priority for reasons discussed above. As to where additional resources might best be used, an even more superficial impression has been formed that the most urgent need is for a larger pool of resources to be used flexibly for developmental work on [redacted] systems and possibly on lower-grade [redacted] traffic.

With slightly more confidence, it is suggested that the way in which allocation decisions are made may be susceptible of improvement. A continuing dialogue is of course conducted between, on the one side, the cryptologic community and, on the other side, the producers of finished intelligence who are the consumers of what is usually classified as raw intelligence produced by NSA in its role as a collection agency. Nothing has been discovered in the course of this inquiry which would suggest the need for additional or different formal machinery for the conduct of this dialogue. On the other hand, it may be that the content of the dialogue could be modified

~~TOP SECRET~~ [REDACTED]

in ways which would make it more useful as a source of guidance to NSA.

Presuming that NSA's customers are the final judges of the usefulness of the intelligence they receive from the Agency, it is plainly desirable that they be as well informed as feasible about what it is possible for the Agency to do and that they in turn rank the various possibilities in order of desirability. The essence of a procedure to accomplish this result would be the definition by the cryptologic community of several different options, as suggested above, and the estimation (as best it could be done) of what it would be reasonable to expect from each option in the way of a flow of intelligence at some point in the future. The presentation of such options would serve to inform the consumers about capabilities and technical opportunities in a form which would put pressure on them to make choices and not merely to assert the immense value of virtually all the intelligence they receive.

Such a procedure would have its dangers as well as its intellectual difficulties. To begin with, it would be unwise to conduct such an effort too often. The cryptologic effort simply cannot produce results in a hurry; it cannot shift resources around in response to frequent or short-term changes in priorities. Yet there will always be a natural tendency for consumers to wish to try to turn the flow of intelligence off and on in response to the pressures of the moment. A more useful contribution they could make to

- 54 -

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

optimizing the use of resources would be to give their views as to which targets will decline in importance in the long-run and which will acquire higher priorities.

Another somewhat analogous danger is that the procedure here proposed could whet the appetites of the consumers to attempt to impose rigid and specific allocations on the NSA. It can only be said that this should be explicitly made contrary to the rules. There is no intention to suggest dilution of the authority of NSA's top management. Indeed, it must be repeated here for emphasis (even though this inquiry has not attempted to deal with questions of organization) there is every presumption against the creation of any additional committee structure or the multiplication of review procedures. There is ample machinery for keeping NSA informed of customers' requirements, its management must retain appropriate freedom of action in meeting them. The intent of the suggestion here under discussion is only to make those consumers more clearly aware of alternative opportunities for the use of cryptologic resources, and of the implications of those opportunities, so they may be in a position to give guidance which is subtler and therefore more helpful than can be contained in a simple statement of priorities.

These concluding comments on the process of optimizing the allocation of resources are in no way intended to imply that the total resources devoted to cryptology should remain rigidly constant. Obviously, everyone

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [redacted]

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

concerned with this part of the intelligence business would like to expand the effort against [redacted] lower-grade systems while continuing the attack on the high-grade [redacted] systems with undiminished resources.

The problem of allocation, that is of choice, cannot, however, be evaded, even through budgetary liberality. Whatever the scale of the whole cryptologic effort, it will still be important to optimize the use of resources and this will inevitably require the exercise of choice as to where they are to be used. Decisions of this kind are bound to be touchy and there is a legitimate reluctance to consider them in too wide a circle. What is argued here is that they should not be swept under the carpet; more specifically that the maintenance for many years of an overriding priority should not be treated as if it rendered systematic review from time to time unnecessary.

c. As suggested in the body of this report, consideration might well be given to a more systematic evaluation than is now available, on behalf of the whole intelligence community, of the raw intelligence that may in time be produced through the successful exploitation of [redacted] and of other high-grade systems. It is suggested that this neither requires nor could be effectively done by too large a committee or too formal a procedure. It would seem that the logical starting place for the evaluation would be with the material now being derived from [redacted] traffic, and an evaluation of this flow of intelligence would be useful in itself. Its particular utility as a sample of what may be derived through success against other systems in

~~TOP SECRET~~ [redacted]

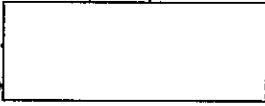


~~TOP SECRET~~ [REDACTED]

the future is that it will exemplify the fragmented, accidentally chosen character of COMINT derived from a high-grade system and also the time lags typically encountered (at least in peacetime) in deriving COMINT from this kind of source. It would be presumptuous to suggest just how this evaluation might be done, except to say that the evaluators should concern themselves with the way in which the sample of [REDACTED] traffic is selected. Presumably, they should be aware of NSA's procedures with respect to the selection of relevant material, the sanitizing of some of it, and its circulation. It is not to be expected that anything other than a qualitative evaluation will be possible but this in itself might be worth a few man months of effort.

- (b) (1)
- (b) (3) - 50 USC 403
- (b) (3) - 18 USC 798
- (b) (3) - P.L. 86-36

~~TOP SECRET~~



ANNEX

ESTIMATE OF CRYPTANALYTIC COSTS

SC-01287-65  
Cy 15 of 15 Cys

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~TOP SECRET~~ [REDACTED]

1. The attached charts present a cost and manpower estimate of that portion of the Cryptologic Program which is allocable to the cryptanalytic functional area. The estimate includes the cryptanalytic effort and the processes required for its support. The support area serves other analytic functions as well; consequently, cost estimates of other functional areas would encompass many of the resources described in this paper as supporting and necessary to cryptanalysis. In these terms, the total cryptanalytic effort for [REDACTED] is approximately [REDACTED]. Over [REDACTED] of this total is allocable to the [REDACTED] High Grade Cipher effort. The total cost of the High Grade Cipher effort [REDACTED]. The costs during the ten year period, [REDACTED]. FY-65 costs are [REDACTED] and the projected costs for the [REDACTED].

2. Only directly allocable resources and dollars have been included in this estimate which represents an NSA judgement of the order of magnitude of the cryptanalytic effort and the supporting processes. As these figures relate to the target [REDACTED] they are considered to be a reasonable indicator of the role of cryptanalysis in the exploitation, or anticipated exploitation, of target communications. Costs of unallocable [REDACTED] such as communications, training, construction, etc., are not reflected in these figures.

3. The [REDACTED] figures for machine processing show that approximately [REDACTED] resources devoted to cryptanalysis are used by the [REDACTED] High Grade problems. To estimate the costs of machine processing in direct support of cryptanalysis by fiscal year an NSA planning technique of [REDACTED]

[REDACTED] Cost factors have been developed based on experience and include maintenance, programming, operating, procurement and O&M. Cryptanalytic requirements for machine support are expressed to [REDACTED] by the Analytic Offices, in terms of a basic [REDACTED]. The projected costs in Chart 2b are computed by costing the cryptanalytic requirements over the program period with a diminishing cost per machine hour predicated on anticipated system improvements. Although this is essentially a level program after [REDACTED] the total machine capacity is expected to increase by approximately [REDACTED].

4. The direct assignment of a major portion of NSA's R&D effort to [REDACTED] cryptanalysis could be misinterpreted. This assignment results primarily from the fact that new developments in communication and cryptographic

UNCLASSIFIED

~~TOP SECRET~~ [redacted]

techniques among the target countries have generally been first encountered on the [redacted] problem. A significant part of the [redacted] R&D cost lies in the development of equipment and techniques to collect and prepare material for cryptanalysis. Once developed, equipment and techniques have application to other target countries. For example, some of the [redacted] processing equipment developed for [redacted] processing is now being used to process [redacted]

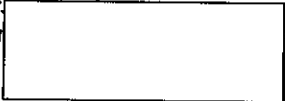
5. Not covered by charts, but a significant factor in the planning for utilization of collection, support and cryptanalytic processes, is the increasing resource requirements of the effort against the [redacted]. The impact is felt in two ways; first, there is increased pressure from consumers for a wider scope of coverage and second, the increasing sophistication of target communications and cryptography requires a greater effort to maintain the present level of coverage and exploitability. The [redacted] programs, as is the case for [redacted] programs, are based on a continuation of existing problem status with many of the targets outside of the [redacted] areas being currently exploitable by cryptanalytic techniques. Notable trends in the [redacted] area are; the increase in the number of [redacted] the gradual increase in sophistication of target communications equipment and cryptography, and, in the [redacted] increased susceptibility to cryptanalytic attack as the result of decreased [redacted]. The existing resource programs are not fully adequate to cope with these trends for a variety of reasons among which are problems in [redacted] and relative priorities as assigned by consumer agencies which determine the allocation of resources within approved ceilings.

6. The projection of future efforts on the [redacted] problem is based primarily on a continuation of present efforts. Any major successes in this area would require reprogramming of resources based on the techniques required and the volume to be handled. This program provides a level of collection and diagnostic effort which is considered adequate for success against those problems which have been selected for cryptanalytic attack. Success cannot be guaranteed, nor can the resource impact of success be predicted at this time.

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [redacted]

~~TOP SECRET~~



SUBSTANTIVE CRYPTANALYTIC EFFORT

Chart. 1a

- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~ [REDACTED]

Comments on Chart 1a

1. The figures for FY-65 are considered to be the approximate dollar and manpower numbers for the cryptanalytic effort within the amounts approved in the CCP.

2. The manpower estimates for [REDACTED] include the field collection and cryptanalytic efforts in addition to the NSA manpower since these costs are directly identified with the cryptanalytic process. In [REDACTED] only the field collection effort identified to the data systems has been included. The remainder of the [REDACTED] receive their raw materials in varying amounts from a large number of diversified collection positions. It is impossible to identify these collection costs to the [REDACTED] cryptanalytic effort for the purposes of this study. Therefore, only the field manpower assigned to cryptanalytic functions are included in those [REDACTED]. The NSA manpower for cryptanalysis in support of [REDACTED] are programmed in [REDACTED] and are costed there in this study.

3. The [REDACTED] figure includes all of the manpower on the [REDACTED] since the effort is primarily in satisfaction of the cryptanalytic requirements which are predominantly [REDACTED].

4. The [REDACTED] costs are directly allocable NSA expenditures only and do not contain [REDACTED] costs since they are not applicable.

5. The machine processing cost estimates for cryptanalysis include identifiable and allocable technical manpower, procurement, T&E and O&M.

6. There are few major procurement actions programmed for FY-65 that are attributable to the cryptanalytic operation. The [REDACTED] estimate is a combination of SCA and NSA procurement scheduled for [REDACTED].

- (b) (1)
- (b) (3)-50 USC 403
- (b) (3)-18 USC 798
- (b) (3)-P.L. 86-36

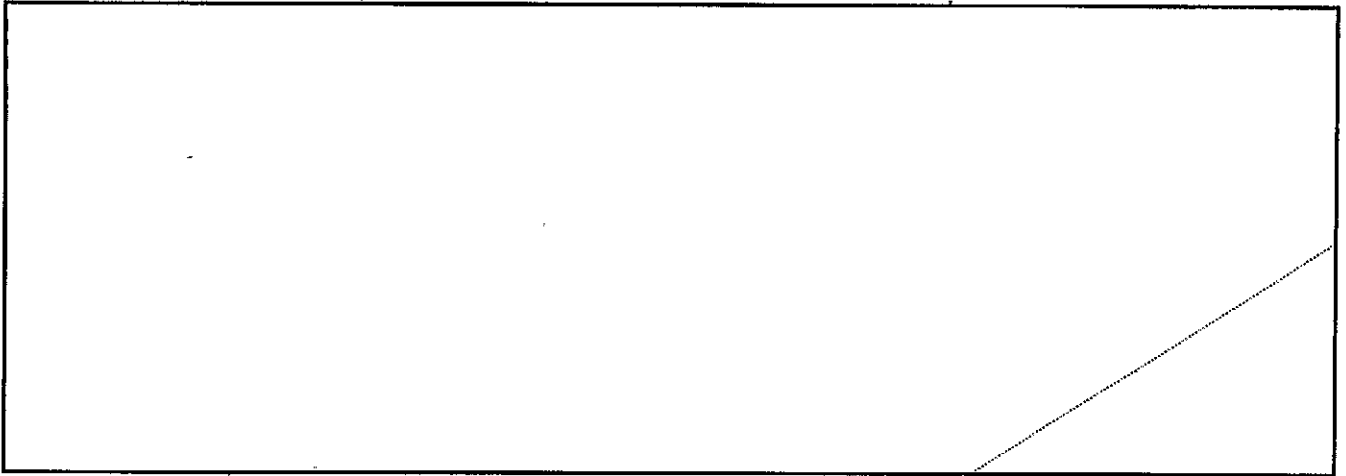
~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

SUBSTANTIVE CRYPTANALYTIC EFFORT

Chart 1b

[REDACTED] HIGH GRADE CIPHER SYSTEMS



Comments on Chart 1b

1. The entire cost of manpower in [REDACTED] is charged to the [REDACTED] High Grade systems. The manpower in [REDACTED] is that portion of the manpower identifiable to high grade system cryptanalysis.
2. The Research and Development costs are only those projects from Chart 1a in direct support of the [REDACTED] High Grade ciphers.
3. The machine processing costs are further identification within the [REDACTED] for support of the total cryptanalytic effort. High Grade cryptanalysis especially on the [REDACTED] absorbs the major portion of the total effort.
4. Identifiable and allocable technical procurement and O&M costs are primarily in the [REDACTED]

(b) (1)

(b) (3) - 50 USC 403

(b) (3) - 18 USC 798

(b) (3) - P.L. 86-36

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [redacted]

Chart 1c

APPROXIMATE COSTS OF  
CRYPTANALYTIC EFFORT ON [redacted] CIPHER SYSTEMS

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

Comments on Chart 1c

1. Personnel costs include collections, processors and cryptanalysts at NSA, and overseas, both military and civilian. Generally about [redacted] of the manpower and capital investment costs have occurred during the [redacted]

2. The operations and maintenance costs are for magnetic tape, traffic paper and TDY in support of cryptanalysis.

3. The research and development costs include those readily identifiable large investments over the last ten years in areas such as the [redacted] processing equipments, [redacted] cryptanalytic research and a variety of collection developments.

4. The heaviest investment in procurement dollars during this period was the initial buy of [redacted] collection [redacted] in FY-65; a modernization of the [redacted] collection [redacted] and finally the [redacted] collection [redacted] reconfiguration now underway. Major investments in special analytic equipments for cryptanalytic attack are also included.

~~TOP SECRET~~ [redacted]





~~TOP SECRET~~ [redacted]

Comments on Chart 2a

1. The functional breakout by system for support, collection, processing and cryptanalysis is a combination of manpower [redacted] and at NSA from [redacted]. It is not possible to equate Research and Development or Machine Processing manpower to a specific high grade system. However, the distribution of effort can be approximated in that over [redacted] of both Research and Development and [redacted] efforts on [redacted] High Grade Ciphers is expended in the [redacted] area and can be further identified as primarily supporting two major systems, [redacted].

2. Identifiable and allocable technical procurement, operations and maintenance costs can also be primarily assigned to the [redacted] area. [redacted]

- (b) (1)
- (b) (3)-50 USC 403
- (b) (3)-18 USC 798
- (b) (3)-P.L. 86-36

~~TOP SECRET~~ [redacted]

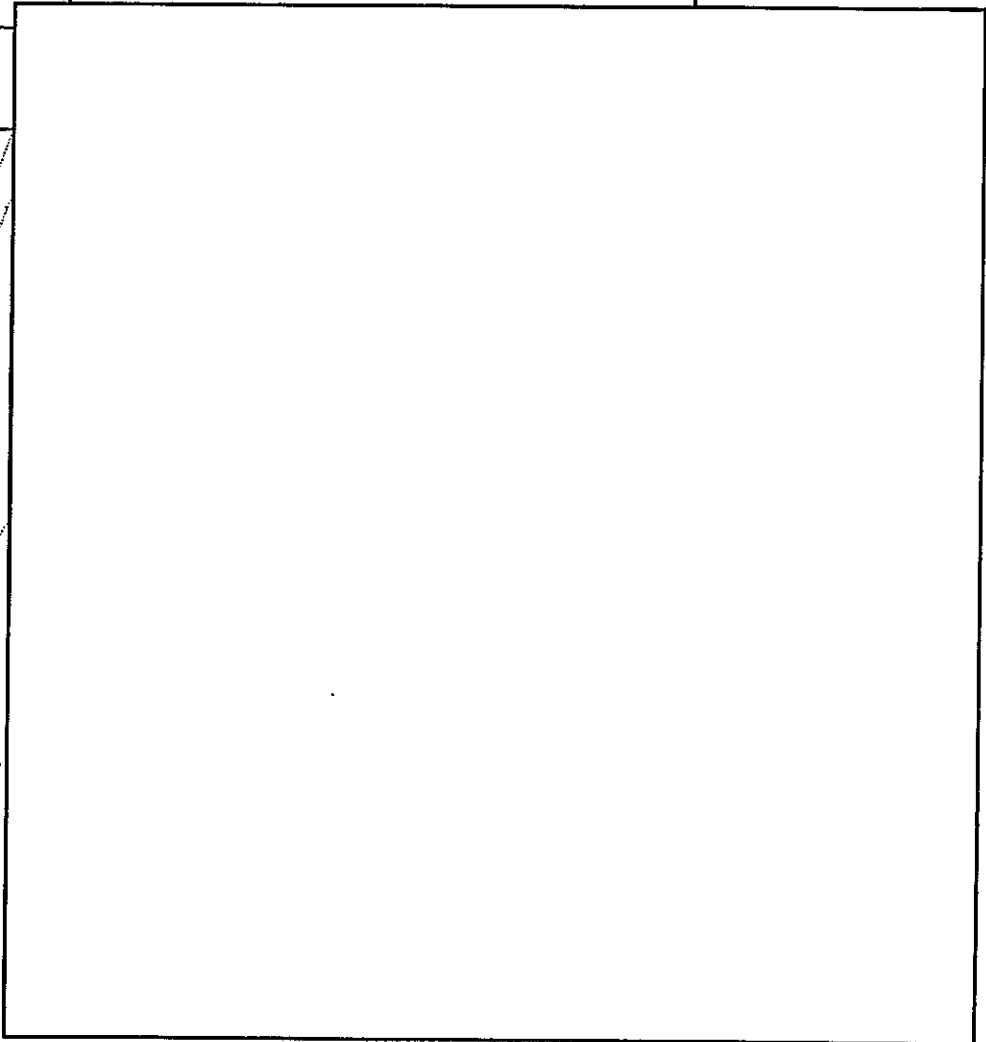
~~TOP SECRET~~ [Redacted]

Chart 2b

CRYPTANALYTIC EFFORT

[Redacted] HIGH GRADE CIPHERS

Category of Function
Collection
Processing
Cryptanalysis
Research & Development
Machine Processing
Procurement
Operation & Maintenance



- (b) (1)
- (b) (3) -50 USC 403
- (b) (3) -18 USC 798
- (b) (3) -P.L. 86-36

~~TOP SECRET~~

~~TOP SECRET~~ [Redacted]