Description of document:	Precis of the Bissell Report - Review of Selected National Security Agency (NSA) Cryptanalytic Efforts, 18 February 1965
Requested date:	29-March-2016
Released date:	08-August-2018
Posted date:	01-October-2018
Source of document:	FOIA Request National Security Agency Attn: FOIA/PA Office 9800 Savage Road, Suite 6932 Ft. George G. Meade, MD 20755-6932 Fax: 443-479-3612 (Attn: FOIA/PA Office) Online FOIA Request Form

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 84064
8 August 2018

This responds to your Freedom of Information Act (FOIA) request of 29 March 2016 for "Precis of the Bissell Report- Review of Selected NSA Cryptologic Efforts, 18 February 1965, NSA/CSS Archives, ACC 290Z, 199104" . A copy of your request is enclosed. Your request has been processed under the FOIA and the document you requested is enclosed. Certain information, however, has been deleted from the enclosure.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified TOP SECRET as provided in Section 1.2 of Executive Order 13526. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)). The information is exempt from automatic declassification in accordance with Section 3.3(b)(1of E.O. 13526.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in this document. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

FOIA Case: 84064

NSA FOIA/PA Appeal Authority (P132)
National Security Agency
9800 Savage Road STE 6932
Fort George G. Meade, MD 20755-6932

The facsimile number is 443-479-3612.
The appropriate email address to submit an appeal is FOIARSC@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877-684-6448
(Fax) 202-741-5769

Sincerely,

Paul K
for

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

PRECIS OF BISSELL REPORT

SUBJECT AND NAME

Review of Selected NSA Cryptanalytic Efforts, 18 February 1965

AUSPICES AND PURPOSE OF THE REPORT

The Bissell Study was undertaken at the request of The Honorable John A. Bross, Deputy Director for National Intelligence Programs Evaluation, Central Intelligence Agency. The focus of Mr. Bissell's report was "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." Assisted by NSA, Mr. Bissell examined certain high-grade [redacted] systems in an attempt to determine the probable expected cryptanalytic success against them, and to evaluate the level of effort appropriate for investment against those systems.

MAIN FINDINGS

1. Summary of main findings:[1]

[redacted]

1 - By letter to the Honorable John S. Bross, Deputy Director (CIA) for National Intelligence Programs Evaluation, dtd 29 Jul 65, the Director, NSA, recommended revision to certain technical statements made in the Bissell Report. Recommended changes are attached as Incl 1.

~~TOP SECRET~~ TRINE

~~TOP SECRET TRINE~~ - LIMITED DISTRIBUTION

[redacted]

ANY UNRESOLVED ISSUES THE REPORT LEFT FOR LATER WORK

Mr. Bissell suggested that a simple qualitative evaluation of the level of effort on [redacted] high-grade systems be undertaken 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. It was further suggested that the proposed evaluation could not be undertaken as part of the current inquiry, and that a number of agencies in the intelligence community would need to be involved.

KEY PASSAGES AND IDEAS IN REPORT BODY

1. "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 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 reassembly or reconstitution would require very long lead times indeed. The recruitment and training of additional top-level analysts should be pushed vigorously." (p.6)

2. "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 definitions 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 try to produce results in a hurry." (p. 7)

3. "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 of the whole cryptologic effort and the allocation of cryptanalytic resources that now exist." (p. 7)

4. "It must be made explicit that neither of the two preceding recommendations (items 2 and 3 above) is intended to imply that there should be changes in organization, especially in the form of an additional committee structure, or that the authority of the NSA top management should be diluted." (p. 8)

5. "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

6. "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 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."

7. "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 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, overhead reconnaissance, and covert operations), 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 covert collection)."

8. "When one looks at a particular part of the cryptologic effort there are two 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." (pp. 39-40)

9. "If this project 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." (p. 51)

10. NSA provided information on costs and manpower estimates for that portion of the Consolidated Cryptologic Program which was allocable to the cryptanalytic functional area, including support. Cost information was included as an Annex to the Bissell Report.

RESULTS ATTRIBUTABLE TO THE REPORT

None

LIST OF PROPOSED CHANGES TO

THE BISSELL REPORT

This Inclosure contains
8 pages

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Page 3

Line 3

[redacted]

Amend to read

[redacted]

Line 8

[redacted]

Amend to read

[redacted]

Line 5

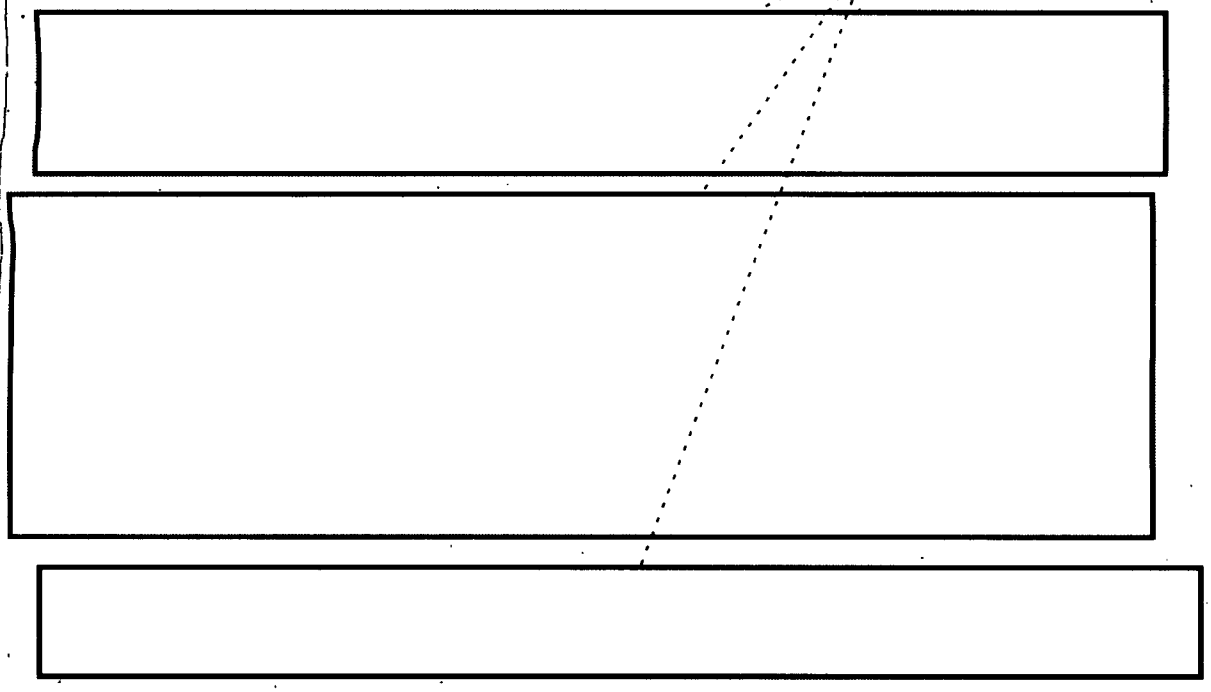
[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Page 22

Line 6, et seq



Page 23, last 3 lines, and all of Page 24
except the last line

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Suggest the following wording:

These efforts resulted in recovering about half of the machine some [redacted] In the last few years further progress has been made, with the result that [redacted] new attacks are in preparation, both of them requiring [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] will be tied up but very little top-grade cryptanalytic brain power will be used. An informed estimate of the prospects of success is that they are about even. With the investment already made, the cost of carrying out the operations planned for the next [redacted] s small and there would appear to be little reason to question the wisdom of so doing. The NSA position is 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] r other sources that justify it.

TOP

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

Page 25

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Line 8

[redacted]

I do not know where this notion comes from - certainly not from anyone in [redacted] It should read:

[redacted]

~~TOP SECRET~~

Page 32

Last 3 lines

[redacted]

Amend to read

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Line 4

"(4) Pessimism with respect to [redacted]

Would suggest the following wording:

(4) Pessimism with respect to [redacted] perhaps an even chance of recovering the machine within [redacted] but poor prospects for exploitation if recovered, unless cryptographic usage turns out to have unexpectedly favorable aspects.

Page 36

Line 12

[redacted]

In view of this, I suggest elimination of the paragraph beginning on page 36 and following paragraph on page 37.