USCIB: 23/51

~~APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL~~

5 May 1953

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Report of the Ad Hoc Committee on Allied Communications Security.

The enclosed report on the above subject is forwarded for information and study with a view to consideration at the Eighty-fifth Meeting of USCIB.

H. D. JONES
Acting Executive Secretary, USCIB

Enclosure
Chrmn, Ad Hoc Cte, Memo dtd 4 May 53, with subject report.

USCIB: 23/51

~~APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL~~

~~THIS DOCUMENT~~

~~CONTAINS CODE WORD MATERIAL~~

TOP SECRET SECURITY INFORMATION

23-123

DEPARTMENT OF STATE
Washington 25, D.C.

4 May 1953

MEMORANDUM FOR THE CHAIRMAN, USCIB

SUBJECT: Report of the Ad Hoc Committee on Allied Communications Security.

REFERENCE: USCIB 23/50

1. Attached hereto is a report by the Ad Hoc Committee on Allied Communications Security.

2. The Committee in this report adhered strictly to the initial terms of reference as set forth in the Eighty-second meeting of USCIB. As a result, the instant report is for the most part confined to considerations of security violations against NATO classification and communications procedures. That portion of this report which deals with instances of possible damage to U. S. interests as a result of "leakage" of valuable information through weak cryptographic systems is relatively incidental to the research conducted on the principal problem as defined by the terms of reference.

3. However, in connection with the above and in response to a request by the Acting Director, NSA, this Committee is currently examining the "leakage" problem as opposed to the question of technical security violations and expects to forward to NSA the results of that survey for possible use by the U. S. delegation to the forthcoming US-UK conference on foreign cryptographic security.

4. It should be noted that the membership of this Committee was expanded beyond that initially planned by USCIB. All USCIB agencies and departments have participated in some phase of this research and this report has been approved unanimously by the Committee.

T. Achilles Polyzoides
Chairman, Ad Hoc Committee

Enclosure:

Report by Ad Hoc Committee
on Allied Communications Security.

Copy No. 25

TOP SECRET SECURITY INFORMATION

TOP SECRET SECURITY INFORMATION

30 April 1953

REPORT OF AD HOC COMMITTEE ON SECURITY VIOLATIONS IN THE TELECOMMUNICATIONS OF ALLIED NATIONS

Problem

1. To determine the importance and frequency of security violations by various Allied nations [redacted]

Discussion

2. At the 82nd meeting of USCIB on 13 February 1953, it was stated that some Allied nations were using such weak cryptographic systems or were following such poor communications practices that important information, especially in respect to NATO, was being compromised. It was suggested, in effect, that more information was being made available to potential enemies [redacted] The Board then decided that an initial investigation should be made to provide a basis for the determination of necessary action. This Committee was established for that purpose.

3. The Board directive requested representatives of the Department of State and the Department of the Army to coordinate with the Director, NSA, in this investigation. The Departments of the Navy and the Air Force, the Central Intelligence Agency and the Federal Bureau of Investigation have also participated in the work of the Committee. This report

represents the unanimous opinion of the representatives of these Departments and Agencies except where otherwise indicated.

4. At the outset of the investigation it became apparent that the Committee could not complete its task in a reasonable time if it examined all communications of all friendly nations. It was also felt that the continuing efforts of many countries to improve their security would invalidate findings in respect to matters occuring some time ago. The necessity of limiting the scope of the Committee's work became evident when it was learned that USCIB wished to have a report which might be helpful in the projected conference with the British in May. Therefore, the investigation was restricted to:

[redacted]

which were brought to the attention of the Committee.

The Committee wishes to emphasize that [redacted] and that the validity of the Committee's finding must be evaluated in the light of this sampling process.

5. The Committee's conclusions must also be qualified by certain assumptions which appeared necessary to permit the focus of attention

[redacted] and to avoid inquiries beyond the competence of the Committee. Thus it was assumed that:

[redacted]

to the fact that the information could have become available to the USSR through landline taps, security leaks or compromises of any other type.

(b) The potential enemy's capabilities are the exact equivalent of our own so that he could intercept any radio transmission and place it in readable form as rapidly but no more so than could be done by NSA.

6. It was also necessary for the Committee to determine what should be considered a security violation. Since the discussion in USCIB had referred specifically to NATO countries, compliance with NATO security regulations was clearly a factor. These regulations forbid "electronic transmission" of COSMIC TOP SECRET* and

*The word COSMIC has been designed as a security warning only. This designation shall, in addition to the appropriate security classification, be placed on all joint and national papers tabled at meetings of any body or committee set up under the North Atlantic Treaty Organization which contain and reveal: (1) Strategic or operational military appreciations, plans or decisions. (2) Political-military appreciations, plans or decisions. (3) Economic planning based on strategic military plans and decisions which could lead to disclosure of such plans and decisions. (4) Classified information of one country tabled or circulated by another country, unless the "owner" country agrees otherwise.

NATO SECRET* information in national systems. Therefore, the Committee considered that the appearance of such information in a national system constituted a security violation without regard to other technical matters affecting the particular message.

7. However, the NATO regulations did not afford a basis for judging messages relating to non-NATO affairs nor did it allow consideration of technical factors affecting the availability of traffic. Therefore,

[redacted]

Policies of the United States were restricted to matters in which the United States was itself taking direct action, such as those relating to NATO, Korea or Trieste. Policies of other countries in which the United States had a less direct interest, such as certain matters relating to EDC or the military discussions between Greece, Turkey and Yugoslavia, were not considered to fall within this standard.

*On all other joint or national documents tabled or circulated within the North Atlantic Treaty Organization the word "NATO" shall appear, together with the appropriate security classification. This "NATO" marking, however, does not require the special handling or accounting provided for "COSMIC" documents, other than as warranted by the security classification, and no special screening (as required for "COSMIC" personnel) is necessary for access to NATO documents.

Conclusions

13. The messages listed in Appendix "C" show that certain nations allied to the United States transmit in national systems information which is highly classified under NATO regulations or which is of importance to United States interests or both. [redacted] Therefore, Allied communications weaknesses and breaches of NATO regulations are resulting in security violations and leakage of information prejudicial to United States interests.

14. The number of security violations and the amount and nature of information damaging to United States interests carried in all [redacted] for a long period cannot be determined unless full-time personnel are assigned to the task or unless a continuous examination has been made in the past. To complete its work in a reasonable time, [redacted] This study is valid [redacted] and only within the defined standards. Damaging information may be passed [redacted] and by other countries than those covered by this report. It may be noted, however, that material damaging to United States policies may be received by Allied nations in such a manner that its transmission [redacted] can hardly be called a security violation

[redacted] although it may constitute a violation or an indiscretion by the original source of the information.

[redacted]

[redacted]

But even if the Committee could have reached such a conclusion, its validity would not have extended beyond the date of the last message examined. These communications might become more insecure, the countries might be entrusted with more detailed information on United States policies or these countries might use the insecure systems for material of a higher level. Any of these changes could increase the danger of damage to United States interests.

Recommendations

18. The proper US/UK NATO authorities should be fully informed of the security violations with respect to NATO matters with the purpose of developing a program of strict observance of the NATO regulations. (Appendix "D" is a statement by NSA on the cryptosystems made available ot NATO countries)

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

19. On the basis of this report alone, no single country should be approached at this time on any plan involving [redacted] The effect of efforts at more strict enforcement of NATO regulations should be determined, and a broader examination of all current Allied traffic should be made to determine all the reasons for the appearance of information damaging to the United States.

20. USCIB should establish machinery for the continuing security examination of Allied traffic by the Departments and Agencies concerned. This would provide an investigation of the effects of the recommended efforts to enforce NATO regulations. It could allow a constant evaluation

[redacted] and thus permit more effective remedial action.

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

APPENDIX "D"

STATUS OF NATO CRYPTOSYSTEMS

A. First level (high military and diplomatic):

1. Typex with Simplex settings.

2. Some one-time pads (approved by standing group)

Date of approval: 20 July 1950.

Made effective approximately August 1950 by France and Italy.

October 1950 by Portugal.

Note: Non-Brusa countries were furnished full technical details for making up their own national Simplex settings but no information is available as to whether they are doing so.

B. Second level (military only - high command to divisions):

1. CCM

Date of approval: 10 November 1951.

Made effective France, Italy, Portugal 1 February 1952.

2. Natex (Back up to CCM).

Date of approval: 25 July 1952.

Made effective by France, Italy, Portugal September 1952.

C. Third level (low echelon):

1. Natex

Date of approval : 25 July 1952.

No systems yet provided.

2. French modified M-209.

Date of approval: Early 1952.

Effective only by France so far.

D. Greece started to use NATO cryptosystems on or about 1 June 1953 on a limited scale and not until the end of the autumn of 1952 had they expanded the nets to a fairly large scale of distribution and usage.

E. Turkey started to use NATO cryptosystems at about the same time as Greece. By approximately 1 January 1953 they had in operation all the crypto nets for which NATO crypto material was available.

F. In addition there are miscellaneous tactical and air-ground codes, authentication systems, etc., approved but not yet effective.