

USCIB: 23/59

29 May 1953

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Report of Ad Hoc Committee on Allied (NATO) Communications Security.

Reference: USCIB 23/55 dated 20 May 1953.

1. USCIB met in special session on 28 May 1953 and reviewed the report of its ad hoc committee on the problem of Allied (NATO) Communications Security as contained in the reference. The Board accepted the report, subject to the incorporation of a few changes made during the meeting. Certain other portions have been excised at the direction of the Board.

2. New pages containing these changes and excisions are forwarded herewith. It is requested that these new pages be inserted in the subject report and the superseded pages removed and destroyed. In addition, page 11 of the Introduction is to be removed and destroyed.

3. It is particularly important that these new pages be inserted in the copies of the report now in circulation, prior to the first session of the U.K.-U.S. Conference.


for RUFUS L. TAYLOR
Captain, U. S. Navy
Executive Secretary, USCIB

Enclosure

- New pages 1, 7, 9, and 10 of Introduction.
- New page 2 of Tab C.
- New page 2 of Exhibit 3.

USCIB: 23/59

~~TOP SECRET SECURITY INFORMATION CANOE~~

18 May 1953

REPORT OF AD HOC COMMITTEE ON EXAMINATION
OF TELECOMMUNICATIONS OF NATO NATIONS

PROBLEM:

1. To examine the available telecommunications traffic of NATO members in order to measure (a) the incidents of violations of NATO communications security regulations; and (b) the extent of potential damage to US interests resulting from leakage of valuable information through weak national crypto-systems and poor communications security practices.

SCOPE AND METHOD OF THE INVESTIGATION:

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

2. This Committee was established at the 82nd meeting of USCIB on 13 February 1953 to examine the problem of communications security violations by NATO members. The Committee filed a report dated 30 April 1953 which set forth certain findings pertaining to security

[REDACTED]

the period of this initial study, arrangements were made to hold a BRUSA conference on the entire problem of NATO communications security. With that fact in mind, USCIB decided at its 84th meeting on 8 May 1953 that this Committee should continue its investigation on broader lines which would include not only a consideration of security violations but also an effort to determine the extent of potential damage to US interests resulting from leakage of

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~

-7-

appraise, especially in hindsight. The Committee has made every effort to be accurate as well as objective in examining this traffic but the number of examples found in this survey cannot be presented as an absolute figure. Nevertheless, when one takes into account the huge number of messages examined by all the evaluating agencies in the course of their normal operations during the test period chosen for this survey, and the intensive effort on the part of the representatives of these agencies meeting in committee to identify examples of information leakage injurious to US interests, it is evident that the leakage, insofar as quantity is concerned, is very small.

6. Despite the quantitative insignificance of the foregoing examples, the potential for damage which is inherent in the cryptographic weakness of some of the systems in use by NATO nations remains. This survey has brought out a reasonably comforting fact in the sense that few damaging examples were uncovered, but this must be balanced against the possibility that at any moment critically damaging information could appear in the same type of traffic. The latter aspect of the situation is covered in the section immediately following.

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~

-9-

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

7. An effort to improve national cryptographic and communications practices could reduce appreciably the total communications security problem under consideration and should be made prior to any effort to improve systems or to encourage the use of more complicated cryptographic equipment.

8. A substantial improvement in the general situation might result from the institution of a security demonstration among the NATO countries.

E. Other conclusions:



2. As long as certain NATO countries employ weak cryptographic systems or vitiate good systems through poor procedures and careless practice, there is a potential for very serious damage whether through security violations or leakage of valuable information.

3. The evidence brought out in this investigation does not indicate that serious damage has occurred during the period covered by this survey. However, such damage has occurred in the past and may occur again in the future.

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~

-10-

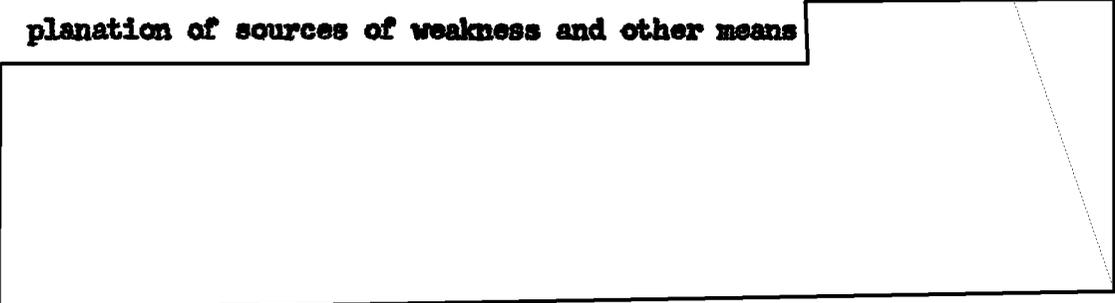
EO 3.3(h)(2)
PL 86-36/50 USC 3605

4. A continuing effort to analyze the communications and communications practices of NATO nations is necessary and should be undertaken jointly with the British.

RECOMMENDATIONS:

1. The US-UK authorities in NATO should be fully informed of the security violations with respect to NATO matters for the purpose of developing a program of strict observance of the NATO communications security regulations.

2. An effort should be undertaken jointly with the British to improve the national cryptographic and communications practices of the NATO countries by a demonstration of proper techniques, explanation of sources of weakness and other means



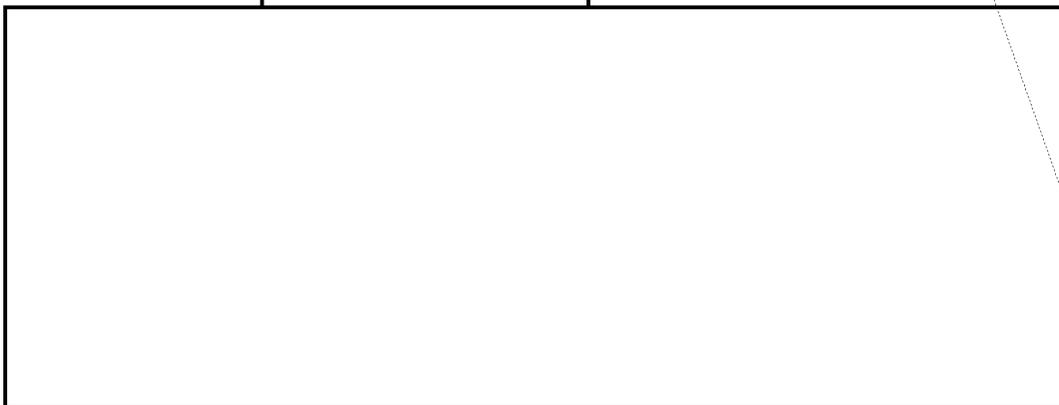
3. Machinery should be established jointly with the British for the continuing examination of the traffic of NATO countries and for the analysis of their communications practices in order to supplement this survey, to judge the effect of the efforts to improve their security and to provide a basis for future action.

~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~

of this report⁷ were checked by the Committee under the terms of reference mentioned in Paragraph 1 above.

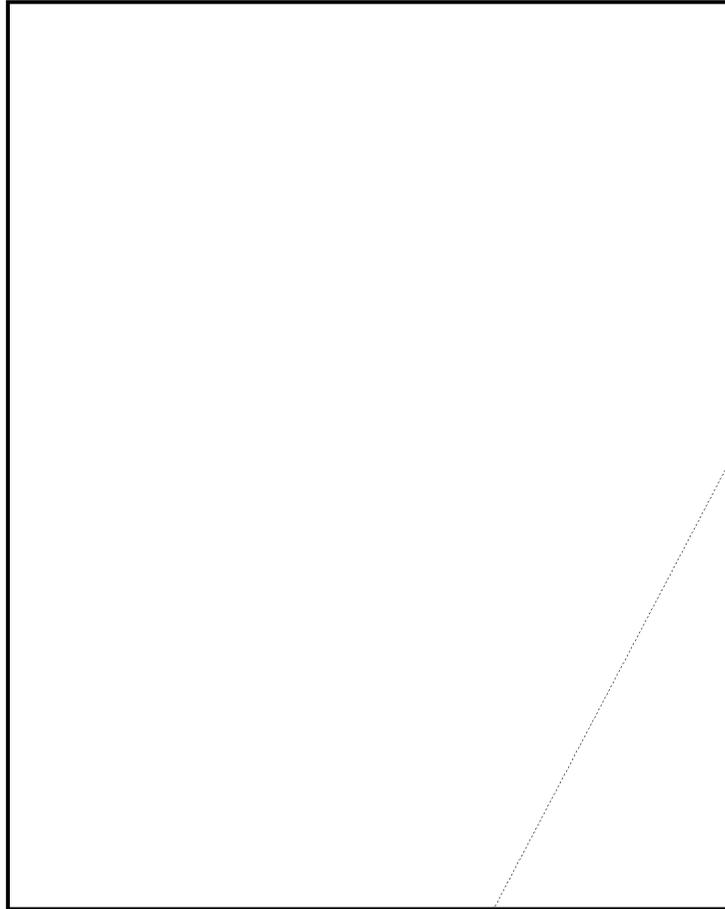
(c) The military representatives on the Committee submitted a further list to Special Projects Staff, Department of State for examination as the damaging nature, if any,



3. On the basis of investigating the four categories noted in the paragraph immediately preceding, the Committee accepted the evaluations of the various specialist panels to the effect that there were messages containing information whose "leakage" to the USSR made them potentially damaging to US interests. The messages are listed in Exhibit 3 of this report.

PL 86-36/50 USC 3605
EO 3.3(h)(2)~~TOP SECRET SECURITY INFORMATION CANOE~~

~~TOP SECRET SECURITY INFORMATION CANOE~~



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

~~TOP SECRET SECURITY INFORMATION CANOE~~