~~TOP SECRET~~
~~SECURITY INFORMATION~~

USCIB: 23/65

24

30 June 1953

~~APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL~~

~~TOP SECRET - SECURITY INFORMATION~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Final Report and Papers of the U.K.-U.S. Conference on the Communications Security of NATO Countries.

1. The subject documents are forwarded for review, prior to formal consideration at the next regular meeting of USCIB.

2. Copies of these papers have been forwarded to SUSLO for delivery to the Secretary, LSIB.

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

Enclosure
Subject Report
and Papers.

USCIB: 23/65

~~APPENDED DOCUMENTS CONTAIN CODE WORD MATERIAL~~

~~TOP SECRET CANOE - SECURITY INFORMATION~~ 24

REPORT

TO

THE LONDON SIGNAL INTELLIGENCE BOARD

AND

THE UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD

ON

THE U.K.-U.S. CONFERENCE ON THE COMMUNICATIONS SECURITY OF NATO COUNTRIES

HELD AT WASHINGTON, D. C. - 5-12 JUNE 1953

1. As the result of an LSIB proposal of 26 February 1953,* and the USCIB acceptance thereof, communicated to LSIB by letter dated 18 April 1953,** a UK-US Conference to consider the improvement of the communications security of NATO countries was held in Washington commencing the 5th of June, 1953.

2. The detailed conclusions and recommendations of the Conference, which were agreed by the conferees at their final meeting on the 12th of June, 1953, and which are set forth in the accompanying report, are submitted for approval by the London Signal Intelligence Board and the United States Communications Intelligence Board.

3. Both Delegations recommend that a copy of the Report be forwarded to the appropriate Canadian authorities, since the communications security of the non-CANUKUS NATO nations is of as vital concern to the Canadian Government as it is to the Governments of the US and the UK. It is felt that at the same time the Canadian authorities should be informed that the Conference gave no consideration to the security of Canadian communications, either those dealing with NATO affairs or those of a purely national character, since the cryptosystems and practices of the Canadian Goverrment are of equal security with those of the US and the UK Governments.

[redacted]

Chairman, U.K. Delegates

William F. Friedman

WILLIAM F. FRIEDMAN
Chairman, U.S. Delegates

*DGC/32142
**CIB/00045

FCC53/EK/A TOTAL
011

12 June 1953

REPORT OF THE

UK-US CONFERENCE ON THE COMMUNICATIONS SECURITY OF NATO COUNTRIES
HELD IN WASHINGTON, 5-12 JUNE, 1953

THE PROBLEM

1. To consider the insecurity of NATO communications and of the national communications of NATO countries, including a review of the conclusions of the 1951 US/UK Conference on the Security of French Communications, in order:

a. To determine whether the NATO Governments should be approached with a view to improving their communitions security;

b. To assess the advantages and disadvantages of such an approach;

c. To develop, if such an approach should be made, (1) a specific plan for improving the security of NATO communications and of the national communications of NATO countries and (2) a specific plan for approaching the NATO Governments.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

I. ASSUMPTIONS AS TO THE COMINT CAPABILITY OF THE USSR

2. This Report is predicated upon the assumption that:

a. The capabilities of the USSR to intercept and exploit radio communications are at least equivalent to those of the US and UK.

b. The USSR monitors all landline communications passing through its own or satellite territory. The possibility that it has access to other communications passed solely by landline cannot be excluded, but there is no evidence to assess the extent of this possibility. Any traffic obtained by the USSR from landlines can be exploited to the same extent as traffic obtained from radio transmissions.

II. VALUE TO THE USSR OF COMINT DERIVED FROM THE COMMUNICATIONS OF NATO COUNTRIES (see Footnote 1)

3. Diplomatic Communications in peace time.

a. Although the US and UK views differ as to the current value of this COMINT to the USSR in the light of recent and current appreciations of [redacted] (see Footnote 2), both the US and UK agree that intelligence derived from these communications may, at any time, be of high-or indeed critical-value to the USSR.

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

Footnote 1.

It should be noted that the security system of NATO provides sufficient protection for "COSMIC" and "NATO" communications passed electrically. However the NATO security system does not provide protection for national communications carrying related information, nor do all the NATO countries confine "NATO" and "COSMIC" communications to approved channels. [redacted] There is no evidence on which to conclude whether or not other NATO countries observe the NATO procedures.

Footnote 2.

The US view is that the diplomatic communications of NATO countries are essentially tactical and "perishable" in that they normally relate to the conduct of current negotiations and arrangements involving these countries, rather than to the broad policies and long-range objectives or capabilities of these countries. They are of optimum value when obtained promptly and brought to bear directly, rather than indirectly, on these events. It is considered, therefore, that COMINT from the communications of NATO countries is of value to the USSR to the extent that the USSR participates in, or can affect directly, the events which they concern. The US is of the opinion that these communications have not generally been of a character which the USSR could exploit in this manner.

The UK view is that the information must be of positive value to the USSR both for short-term and long-term purposes. In the short term it gives a clear picture of the inter-relationship of the NATO countries and of exchanges between them concerning mutual difficulties. This provides a basis for the tactical conduct of negotiations with the West over questions such as the Austrian Treaty, and also for the direction of propaganda. In the long term it provides intelligence on NATO and particularly SHAPE war plans, specifically on the contribution expected from countries such as Portugal and Turkey and on the general progress of SHAPE war planning and the extent to which the plans are being realised.

b. The value to the Russians of the COMINT derived from the communications of individual NATO countries will vary directly with both (1) their vulnerability and (2) the extent to which they contain information, the compromise of which would be damaging to the US or the UK.

(1) In these terms, the communications [redacted] are the least vulnerable and are on this basis alone thought to represent no current or predictable source of valuable intelligence to the USSR.

(2) Communications of [redacted] are agreed to be the most vulnerable but, due to the limited volume of their communications and the relatively slight participation of these countries in matters which would involve critical information, are also thought to represent no current or predictable source of valuable intelligence to the USSR.

(3) The communications of [redacted] are very vulnerable and, because of the significant participation of these countries, are considered to represent a potential source of valuable intelligence to the USSR.

(4) The communications of [redacted] although less vulnerable than those of [redacted] and [redacted] are also a potential source of valuable intelligence to the USSR.

[redacted]

4. Diplomatic communications in wartime.

It is considered that on outbreak of active hostilities the value to the USSR of the information derived from the communications of NATO countries would be greatly increased.

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

5. Armed Forces communications in peace and war.

a. US and UK information on the vulnerability of the National Armed Forces communications of NATO nations is limited [redacted] It has however been established that French military systems used in Indo-China are highly vulnerable and are presently carrying intelligence that ought to be denied to the Communists.

b. In general it is thought that under peace time conditions Armed Forces communications are unlikely to be an important source of valuable intelligence to the USSR. In cases of limited hostilities, such as the present war in Indo-China, it is, however, considered that vulnerable Armed Forces communications are a menace to the national interests of the UK and the US and in the case of general hostilities would become a real danger.

III. VALUE TO THE USSR OF INTELLIGENCE ON NATO COUNTRIES DERIVED FROM NON-COMINT SOURCES.

6. Clandestine Sources.

a. Non-COMINT clandestine means of obtaining intelligence cannot be regarded as a complete substitute for COMINT as a source of intelligence. In particular, in areas where COMINT is effective, clandestine intelligence is generally less timely, less complete and less authoritative than COMINT. Information from clandestine sources needs a sometimes difficult process of evaluation before it can be accepted; is dependent on the availability of communications; and is frequently subject to considerable delay before it is received by the user agency. Further, the value of intelligence from clandestine sources can frequently be greatly increased by correlation with COMINT. Moreover, the capacity to sustain successful clandestine arrangements to obtain intelligence often depends upon information derived from COMINT.

b. Although it must be presumed that penetration of NATO nations by agents of the USSR exists and will continue to exist, it is considered that, at least, so far as the US, UK, and France are concerned, this is becoming increasingly difficult.

(1) In the case of France, there has been a definite improvement in the overall security situation, and further improvements are planned. In the Armed Forces and security agencies specific steps have been taken to place in effect a security system which is acceptable to the US and UK. However, in other sensitive agencies, such as the MFA, these steps had not been initiated as of the completion of the last Tripartite

Security Survey of December, 1952, and there remain significant handicaps--political and administrative--to improvement. The level of overall security in France remains considerably below that of the US and UK. In the light of these developments it cannot be assumed that clandestine sources of intelligence for the USSR will be significantly reduced in France in the near future. Nevertheless, the operation of clandestine sources is expected to become increasingly difficult, and, therefore, it is felt that the USSR could not find adequate compensation for the loss of potential COMINT through increased clandestine activity.

(2) As regards other NATO countries from which the potential value of COMINT is estimated to be high there is insufficient collated evidence available to this conference to assess the state of their security. In particular there is not available any report such as that produced by the Tripartite Security Working Group which covered security conditions in France. In the absence of conclusive evidence it is not considered safe to assume that the level of overall security is higher than that of France as described above.

c. In time of war, due to the introduction of security measures which are not possible in peacetime, clandestine operations become much more difficult. The ready means of communication afforded by diplomatic missions and consulates are also no longer available. It is therefore considered that the value of information from clandestine sources will be substantially diminished at least initially by an outbreak of hostilities.

7. Other Sources

a. It is difficult to assess to what extent open sources (newspapers, trade publications, public documents and statements, etc.) or diplomatic reportage could be a substitute for COMINT. It is however agreed that COMINT derived from readable communications of NATO countries does produce intelligence not available to the USSR from other sources and that, even during peacetime, this intelligence may increase substantially in volume and value at any time. In wartime, censorship and other extraordinary security measures, will reduce drastically the flow of intelligence from such sources, and the value to the USSR of any available COMINT will be correspondingly increased.

b. It should be noted that, as in the case of clandestine sources, the value of intelligence from other sources can be greatly increased by information derived from COMINT.

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

[redacted]

V. SECURITY AND INTELLIGENCE FACTORS AFFECTING ACTION TO BE TAKEN

10. The nature of any action taken to reduce the potential damage to the national security of the US and UK created by the vulnerability the communications of NATO countries will be determined largely by technical considerations. From the point of view of intelligence and general security consideration, however, such action must:

a. be designed to rectify effectively inadequate communication security practices of NATO countries throughout.

[redacted]

c. not lead, without prior agreement of the US and UK in each case, to a disclosure of cryptanalytic techniques over and above those already published in commercially obtainable literature or known to be within the capacity of the cryptanalytic organization of the NATO nation concerned.

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

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

d. be designed to prevent any leakage of communications security principles and procedures [redacted]

In particular it is of the greatest importance that any action taken should not lead to the commercial improvement of cipher machines such as those produced by A. B. Cryptoteknik, Stockholm and Crypto A. G., Zug, Switzerland which may then be made available to non-NATO countries. The means by which this is to be achieved are for further consideration.

[redacted]

VI. TECHNICAL FACTORS AFFECTING ACTION TO BE TAKEN.

11. Inasmuch as it appears to be impractical to attempt corrective action by provision of new equipment, action should initially be aimed at the improvement of available cryptosystems and communications practices wherever possible. It is considered that such improvement can be effective.

12. No matter what initial approach is agreed the proper authorities for handling issues of this nature are the communications security agencies of the NATO nations concerned. This consideration is re-inforced by that stated in paragraph 11 above. It is therefore important to associate the communications security agencies with the action proposed at as early a stage as possible. The same reasoning applies to the use of communication security authorities to originate the action. Further factors in support of these considerations are that:

a. The security and intelligence factors enumerated in paragraph 10 above make this the safest procedure.

b. For reasons of economy it is desirable that existing agencies be used wherever possible. At least the US, UK and the Standing Group have already in existence appropriate communications security agencies.

c. There have already been several instances in which NATO countries have requested advice and assistance in improving national, as well as NATO, communications security through communications security channels. Two examples of such instances are enclosed herewith as Appendix A.

13. The interrelationships between transmission security and cryptosecurity are such that a completely successful program to improve communications security must deal effectively with both.

14. It is considered that there is no way to deal effectively with disregard of "COSMIC" and "NATO" communications security regulations [redacted] except through the improvement of the overall communications security attitude and practices of the offending countries.

VII. OUTLINE OF THE PROPOSED ACTION.

15. The Conference is agreed that the factors enumerated in paragraphs 10 through 14 above can best be met by using the existing communications security machinery of the Standing Group. It is realized that the Standing Group cannot issue directives about matters outside the scope of the military aspects of NATO, but it would seem right to use existing Standing Group machinery in an advisory capacity, since the security of NATO is jeopardized by insecure national communications.

16. It is thought, however, in view of (a) the position of France in NATO, (b) the need to achieve wholehearted cooperation of the French, and (c) the special urgency of the French problem, that the French should be approached first and that this should be done directly rather than through the Standing Group.

17. In order to avoid embarrassment, to ensure maximum cooperation, and to adhere to the security and intelligence factors enumerated in paragraph 10 above, any action with an individual country should be as inconspicuous and private as possible.

VIII. THE DETAILED APPROACH AND SUBSEQUENT ACTION.

18. The French Government should be approached, at a level and by a means to be determined and agreed by cognizant US and UK authorities, with a view:

a. To obtaining French assent to a proposal to attempt improvement of the diplomatic and military communications security of NATO countries through the Standing Group mechanism.

b. To establishing discussions on the communication security technical level to bring French communication security up to a standard agreed by the US and UK to be satisfactory. These discussions will be governed by the principles enumerated in paragraph 10 above, and should be continued to the point where the UK and US have received, to their satisfaction, evidence that the French are in fact taking effective steps to improve their communication security.

19. Upon receipt of the assent of the French to the use of the Standing Group as the NATO mechanism to improve the communications security of the other NATO nations and after successful initiation of the discussions described in 18b above, the Standing Group will issue a memorandum to all member nations which will:

a. Express disquiet at the potential danger to overall NATO security of the insecurity of the national communications, either diplomatic or military, of NATO nations, pointing out that the security of NATO as a whole depends upon the security of each individual nation.

b. Forward a list of examples of dangerous cryptographic and communications practices and procedures. This list will be finally agreed beforehand by the cognizant UK and US authorities along the lines of Appendix B hereto.

c. Advise each nation to examine this list to ensure that its own communications are free from such practices and procedures.

d. Request the NATO nations to designate or establish Communications Security Agencies, such agencies to be authorized to communicate directly with the Standing Group Communication Security and Evaluation Agency, Washington (SECAN) and the European Security and Evaluation Agency of the Standing Group (EUSEC).

e. Invite any nation that requires advice and technical assistance in such matters to apply, through their national communication security agencies, to SECAN.

20. As the NATO countries respond to the invitation of the Standing Group advice would be given separately to each enquiring country either by correspondence, or at a meeting of communications security experts, as may be appropriate. EUSEC would act as may be necessary as the European agency of SECAN; and may, by reason of its location, be the more convenient body for action necessitating meetings with the communications security experts of the European NATO countries.

Representatives of both the US and UK may participate in such meetings and actions.

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

21. For the purpose of providing guidance to SECAN and EUSEC and for establishing a basis for giving advice to each country, the UK and the US will formulate agreed and detailed minimum communication security standards applicable to the national systems and procedures of the NATO countries.

22. All technical correspondence and discussions of SECAN or EUSEC with NATO countries will be designed to effect compliance with these minimum communications security standards and will be governed by the principles enumerated in paragraph 10 above.

23. Wherever a country fails to respond adequately to the invitation of the Standing Group or to the advice tendered by SECAN/EUSEC, further steps may be necessary. The nature of these steps will be decided in consultation between the US and the UK in the light of the individual cases.

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

24. The approach described above involves complicated issues which raise intelligence and political, as well as communications security, problems. These will require special attention and rapid coordination between the US and UK until the precise direction and success of this program have been assured. Among the several liaison arrangements which exist now in these fields there does not exist the specific informal mechanism which would afford the representation and flexibility required for this purpose. It is considered that the need would be met by the setting up in Washington of a small combined working group representing intelligence and political as well as technical interests, the exact composition and terms of reference to be decided by consultation between the cognizant US and UK authorities.

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

CONCLUSIONS

[redacted] valuable intelligence for the USSR. [redacted] there is no evidence to assess to what extent national armed forces ciphers of NATO countries are vulnerable. If vulnerable however they also constitute a potential source of highly valuable intelligence for the USSR.

26. Despite the inadequate level of overall security in France, and the absence of assurance that the overall security of other NATO countries is any better, the USSR could not compensate adequately for the loss of COMINT as a potential source of timely and authoritative intelligence of high value through other sources of information.

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

[redacted]

28. Action should be taken immediately to rectify all vulnerable communications security practices of NATO countries.

EO 3.3(h)(2)
PL 86-36/50 USC 3605 29. Intelligence and security considerations require that any remedial action taken, while designed to be effective, should not lead to a direct disclosure [redacted] of cryptanalytic techniques beyond those permissible under paragraph 10c above. Also, [redacted] the actions taken should be calculated to prevent the leakage of effective communications security principles to non-NATO nations.

30. Certain technical factors and general considerations require that the action taken should:

a. Attack violation of NATO communications security regulations through improvement of the overall communication security attitudes and practices of offending NATO countries.

b. Deal first with the French Government directly on the problem of French national communications.

c. Utilize the machinery of the Standing Group of NATO as the instrumentality for improving the security of the national communications of other NATO countries.

d. Be taken through communications security channels, using existing communications security agencies wherever possible.

e. Be aimed at the improvement of available cryptosystems and communications practices rather than at the provision of new equipment.

f. Afford maximum privacy in dealing with individual NATO countries.

31. The course of action outlined in paragraphs 18 through 24 above meets the foregoing considerations and is feasible.

32. Upon approval of this report the following preliminary steps must be taken:

a. Determination between the cognizant US and UK authorities of the nature of the first approach to the French (see paragraph 18);

b. Preparation by the cognizant US and UK authorities of a brief for the US and UK representatives at the communication security technical discussions with the French (see paragraph 18b);

[redacted]

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

d. Formulation by cognizant US and UK authorities of detailed minimum security standards applicable to national communications systems and procedures of the NATO countries (see paragraph 21);

e. Agreement on the terms of reference and composition of the Combined Working Group to be set up in Washington to facilitate coordination of this action (see paragraph 24).

33. It will be necessary to continue examination of the communications of NATO countries in order to provide guidance to SECAN and EUSEC in their contacts with authorities of other NATO countries, and to assess the effectiveness of action taken. [redacted] arrangements to coordinate this examination and the drawing of lessons from it are adequate, and no further liaison machinery is required.

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

RECOMMENDATIONS

34. It is recommended that:

a. The foregoing conclusions be approved and supersede those of the 1951 UK-US Conference on the Security of French Communications.

b. The program in paragraphs 18 through 24 be undertaken in accordance with the conclusions and, in particular, hat the steps enumerated in paragraph 32 should be undertaken immediately.

FSC53/EX/R FINAL
011

12 June 1953

APPENDIX A

Examples of Recent Instances in which NATO Countries Have Requested Advice and Assistance Regarding Their National Communications Security

1. A Belgian request to NATO in February 1953.
2. An Italian request to NATO in April 1953.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL
011

Ministere de La Defense Nationale
- - - - - - - - - - - -
- - - - - - - - - - - -

Brussels, 21 February 1953

Dear Sir:

Subject: Ciphering System - 1) Nato 3rd Level - 2) National

* * * * * * * * *

2. Could a system derived from Natex - - - - be authorized - - - - - as National cipher.

* * * * * * * * *

5. What would be the delay and eventually the price for the delivery of such machines (ACP 212), to Nato Nations for National use.

Sincerely yours,

F. L. Lambeau
Cap. Commandant
Belgian Representative

(This correspondence was addressed to the Chairman, Communications Security Panel, Shape Communications Electronics Board, who relayed it to the Standing Group.)

~~TOP SECRET CANOE - SECURITY INFORMATION~~

FSC53/EX/R FINAL
011

Italian Military Mission
Washington, D. C.

0927/SRP

April 30, 1953

TO THE SECRETARIAT OF THE STANDING GROUP

SUBJECT: Telecipher Machines
Reference SGM-212-53 dated February 11th, 1953

The Italian Code Teleprinter T2-ZK is being considered for adoption by the Italian Armed Forces for its internal national communications.

In consideration of the fact that as stated in SGM-212-53 the a/m teleprinter does not meet Nato requirements, the Italian General Staff would greatly appreciate being informed of the technical reasons which induced the Standing Group experts to make such a statement.

The Italian General Staff would furthermore appreciate any information on the type of teleprinter which is being considered for common Nato use.

Cesare Grandini
Lt. General, Italian Army

APPENDIX B

LIST OF EXAMPLES OF DANGEROUS CRYPTOGRAPHIC AND COMMUNICATIONS PRACTICES AND PROCEDURES

I. UNENCIPHERED CODES

1. Unenciphered codes are totally inacceptable in diplomatic use for transmission of classified information. In Armed Forces communications they are acceptable only when changed at very frequent intervals and when it is not considered essential to maintain the security of the information for more than two or three days from the introduction of the code.

II. ADDITIVE SYSTEMS

2. Any additive (or subtractor or minuend) system is dangerous unless special precautions are taken in the construction of the additive itself. Many procedures that may be regarded as "special precautions" are deceptive as to security and may even in themselves create weaknesses.

3. Encipherment by additive can only be guaranteed to be secure when the additive is used on a strictly "one-time" basis, and systems that permit depth gain little or no security from the additive.

4. Encipherment by non-one-time additives is highly dangerous, but can be acceptable in certain circumstances for limited traffic provided that precautions are taken to minimise overlap and to prevent cryptanalysts from finding any overlap that may arise.

III. NON-ADDITIVE HAND SYSTEMS

5. There are many hand methods of encipherment, not employing additive, but few of these can be guaranteed to be secure.

IV. MACHINE CIPHERS

6. Machine ciphers vary greatly in the amount of security they afford. Failure to observe in every detail proper instructions for

operation may lead to compromise even with the best machines. Others, such as the well-known Hagelin "Cryptoteknik" (see para. 7 below) are insecure unless precautions are taken over and above those recommended by the manufacturer. Others, again, are basically insecure and should in no circumstances be used.

7. Special attention is drawn to the dangers inherent in the use of the Hagelin "Cryptoteknik" machine:

a. Since the encipherment is essentially by additive it follows that if a message setting is used more than once the key can be recovered on the overlap; a single mistake by an operator using a message setting a second time can thus compromise the machine setting.

b. The additive generated by the machine is never truly random and there are circumstances in which this fact can be used to recover the machine setting, even though no message setting is repeated.

c. With proper precautions this machine can give very good security for a limited amount of traffic, but in view of the number of different dangers that can arise in varying conditions of use, for which it is impossible to legislate in advance, member nations who wish to make use of the "Cryptoteknik" are specially urged to consult SECAN.

V. TRANSMISSION SECURITY

8. Ciphers, however good individually, are not enough to ensure communications security. Transmission techniques and message formats can in themselves provide considerable intelligence to a traffic analyst. Although there are practical limitations, the ideal to be striven for is that the traffic neither of any one type (e.g. naval, air force,

etc.), nor of any one nation should be distinguishable by external characteristics. Again, intelligence can be gained by study of the organization and procedure of radio networks and by use of radio direction-finding. In many cases, especially in Armed Forces communications, a skillful enemy can obtain valuable intelligence by collation of apparently uninformative message texts. It follows, therefore, that full communications security demands that special precautions be observed in such matters as the judicious employment of indicators, the selection of call signs and of frequencies, radio procedures, and the restriction of the use of plain language.