24

USCIB: 29.1/26

~~APPENDED DOCUMENTS CONTAIN CODEWORD MATERIAL~~

28 June 1954

~~TOP SECRET~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Program to Improve Communications Security of NATO Countries.

1. The following documents regarding the Program to Improve the Communications Security of NATO Countries have been received from the Chairman of the USCIB Ad Hoc Committee handling that program and are forwarded for your information:

a. A report of the USCIB Ad Hoc Committee on the recent approach to the French, prepared in compliance with the decision of USCIB at its 103rd Meeting.

b. English text of the Standing Group Memorandum agreed to at the technical talks.

2. A copy of the French text of the Standing Group Memorandum and a copy of the report of the U.K. technical delegates have been filed in the office of the Executive Secretary, USCIB, and are available to any member who wishes to examine them.

3. In general, the U.K. report agrees with the conclusions and observations of the U.S. technical delegates except that the U.S. delegates did not encounter the examples of physical insecurity noted in the U.K. report.

4. The Standing Group Memorandum as agreed at the technical talks is substantially the same as that approved by USCIB with the addition of an appendix on general security practices proposed by the French and of a provision for issuance of the memorandum through the NATO Council. This memorandum has been introduced into the NATO Standing Group.

H. D. JONES
Deputy Executive Secretary, USCIB

Enclosures
a/s

~~APPENDED DOCUMENTS CONTAIN CODEWORD MATERIAL~~

USCIB: 29.1/26

~~TOP SECRET FROTH~~ 10 June 1954

USCIB AD HOC COMMITTEE REPORT
OF THE US-UK APPROACH TO THE FRENCH ON THE SUBJECT
OF FRENCH AND NATO COMSEC.

A. General Chronology and Summary, 17 March - 1 May.

1. On 17 March US Ambassador Aldrich in London was briefed on the project so that he would be in a position to deal with the Foreign Office if the need arose for exchanges on this topic.

2. On 18 March US Ambassador Dillon in Paris received Mr. Polyzoides and resumed preparations for the approach to the French.

3. On 19 March Ambassador Dillon received a full briefing on the entire project. During this conference, it was decided that the program should be reviewed with the British Embassy in order to clarify any last-minute problems and in order to assure a fully coordinated joint approach to the French Foreign Ministry. It was also suggested that Ambassador Dillon meet with British Ambassador Sir Oliver Harvey prior to their joint approach.

4. On 20 March US Minister Joyce--who was acting in place of US Minister Achilles--and Polyzoides met at the British Embassy with Minister Patrick Riley and Mr. Richard Owen who had been designated as the British delegate to the proposed

24 318#44

Tripartite Security Working Group (TSWG) phase of the projected operation. The general approach was discussed fully and some adjustments were made in a French text which summarized the English text of the Aide Memoire and which the British Ambassador, Sir Oliver Harvey, proposed to read at the time of the joint approach. It was agreed at this meeting that Ambassador Dillon would join Sir Oliver at the British Embassy prior to their departure for the French Foreign Ministry, that M. Alexandre Parodi, Permanent Secretary General of the Ministry of Foreign Affairs, was the most suitable person to visit in the Ministry, and that every effort would be made to meet Parodi as we had initially planned on Monday, 22 March. This date was later changed to 24 March.

5. On 24 March, the meeting with Parodi took place. Immediately after that meeting, Ambassador Dillon described the principal results to Mr. Polyzoides, as follows:

a. Parodi had given a visible expression of awareness of the true meaning of the Aide Memoire which Sir Oliver Harvey had read to him in the form of the summary in French which had been prepared at the British Embassy as noted in Paragraph 4, above.

b. Parodi's initial comment was to ask whether the operation described in the Aide Memoire was directed mainly toward France. He was informed, of course, that such was not the case.

c. Parodi agreed that the matter was serious, that he was in general agreement, that he would give it "serious consideration" and that he "saw no difficulty in reaching agreement" within the terms of the Aide Memoire.

It was learned that the British Ambassador had received, in essence, the same impressions.

6. On 31 March contact was renewed with the Foreign Ministry through the British Embassy. At that time the French promised action within 48 hours and on Friday evening, 2 April, they informed the US and British Embassies that a M. Jean Marc Boegner had been named to the TSWG group. Since this man was head of the section on NATO matters within the French Foreign Ministry, it was quite apparent that our deliberately obscure Aide Memoire had been attractive to the Foreign Ministry primarily in its NATO interpretation. After further discussions with Ambassador Dillon, Mr. Achilles and British

Minister Riley, it was decided to meet with Boegner and to make an effort at that meeting to draw the operation back within the planned TSWG format.

7. On 6 April Minister Achilles, Mr. John C. Elliott of the Department of State, British Minister Riley, and Mr. Owen of the British Embassy met with M. Boegner and M. Christian Auboyneau* of the French Foreign Ministry. The French opened this meeting by declaring that they had no specific objections to the plan as noted in the Aide Memoire but that for a variety of reasons they felt, in effect, that handling the matter through the NATO sections of the Foreign Ministries involved seemed desirable. The US-UK representatives countered with a full and vigorous exposition of the reasons for choosing the TSWG mechanism as the initial means for developing the technical conference. The French were persuaded to accept this view; Boegner withdrew; and Auboyneau and M. Adrian Guillerme (also attached to the Secretariat of the National Defense Ministry) were named to meet with Elliott and Owen in order to complete the TSWG phase of the operation.

*Diplomatic Counselor to the Permanent Secretary General of the Ministry of National Defense.

8. On 8 April the TSWG group as described in the preceding paragraph met formally for the first time. Further meetings were held and on 12 April this phase of the operation was concluded to the satisfaction of the US and British members. The technical talks were scheduled to begin on 22 April at the Invalides.

9. Meanwhile, Mr. Polyzoides left Paris and arrived in London on 13 April where he consulted with Messrs. Austin and Raven of NSA.

PL 86-36/50 USC 3605

10. On 14 April, Major General Ronald C. Penney, Chairman of the Cipher Policy Board, was host at an informal and very satisfactory conference attended by [redacted] of GCHQ, and Messrs. Austin, Raven and Polyzoides. The progress of the Paris operations was described and final arrangements were made for the departure of the technical conferees.

11. On 17 April the NSA members proceeded to Paris.

12. On 22 April the technical talks were started as scheduled and were concluded on 1 May.

PL 86-36/50 USC 3605

B. Summary of the Technical Proceedings, 22 April - 1 May.

1. The American representatives met with the British representatives, [redacted] in London from 12-15 April to smooth out differences in the minimum standards paper and to prepare detailed procedure for the meetings with the French. These meetings were successful.

2. Ten meetings with the French were held from 22 April to 1 May in Paris. The four French representatives were:

Mr. Viala - Head of Foreign Office Department of "Transmission et Chiffre"

Capt. Muller - Head of "Service Technique Central des Chiffres" the permanent secretariat of the Interministerial Commission on Cipher

[redacted]

Capitaine de Corvette Rault - Ministry of Defense

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

In addition, Lt. Colonel Arnaud of the French Army and an assistant were present at one meeting.

3. The ostensible purpose of the talks, the preparation of a memorandum for the Standing Group to issue

in order to correct poor practices in the national communications of NATO nations, was quickly and quite easily accomplished. The memorandum, which was prepared in final French and English texts, is addressed to the NATO Council, with the request that it be forwarded to the nations. The French proposed an acceptable addition, an appendix concerning general physical security as applied to cryptographic operations and the handling of message texts. It was agreed that SECAN would inform the French and British of the results of the Standing Group memorandum, and also that subsequent events might require another meeting. Significant in the discussions of the Standing Group memorandum was the obvious indication that Muller intends to use the memorandum to strengthen his own position and that of the Interministerial Commission in the control of French COMSEC.

[redacted] This paper resulted

in considerable discussion particularly on the Hagelin B211, the latest model of which was demonstrated.

5. It is felt that the UK/US delegates got through to the French on the need for improvement. This was made evident in a private session which Mr. Austin had with Mr. Viala and Capt. Muller, called by Mr. Viala to discuss the ASAM 2-1 which Austin had demonstrated to him in Washington. At the close of the discussion Viala made a short speech, slightly emotional, of thanks and appreciation and ended by saying (these are his exact words as nearly as can be remembered) "Be assured that we believe and understand everything that you told us and also what you did not tell us. This is a delicate business, but believe that we do understand." This remark was repeated more or less by Muller. Then, when Muller had left the room, Viala told Austin, "I have only been in this job for a short time, but already I have found much that is bad. Believe me that I have been doing everything that I can, and now I will renew my efforts."

6. The U.S. representatives in addition, as authorized, revealed the principles of the AFSAM-7 to the French. There was

also some discussion of the ASAM 2-1 and its modification. Viala brought up, with some slight reluctance, and after some urging, the French request to the U.S. for aid. A British offer of possible help was politely received but not discussed in any detail.

7. It is possible to draw these conclusions:

a. A better group of French could not have been found. Amongst them they had the technical ability, the administrative positions, and the sincere desire to improve security that were necessary to the success of the talks.

b. The main purpose of the talks were achieved. It will be some time before it is known whether improvements in French COMSEC will actually result, but there is little doubt that a sincere attempt will be made.

c. The French are, up to a point, technically competent and knowledgeable in the field of COMSEC. They appear to have only a naive concept of the capabilities of machine analysis; other than this they are good.

d. They are handicapped by the lack of a centralized organization to deal with COMSEC matters; and

by the lack of the authority necessary to inforce such regulations as they promulgate. The regulations themselves are good.

e. They are also handicapped by a lack of knowledge as to how their systems are actually being used, and abused, in the field. Time and again they insisted they would not tolerate certain usages which are nevertheless known to be current.

f. The relationships among the various French departments engaged in COMSEC work, while cordial, are not at all intimate or even candid.

g. Although not discussed, renewed requests for material aid are to be expected.

~~TOP SECRET~~

MEMORANDUM FROM THE STANDING GROUP TO THE NATO COUNCIL

1. Regulations at present in force (DC 2/7 (Final) and STAND 474 as amended by STASECS 1508, 1535 and 1588) ensure that all COMSEC telegrams and all NATO TOP SECRET and SECRET telegrams, whether they are national or international, are encyphered in cryptosystems authorized by the Standing Group. But all nations of NATO are also originating and transmitting in their own national cryptosystems a quantity of telegrams both civil and military which, although they are the private concern of the nation in question, must be expected to contain information which affects NATO as a whole and the loss of which to a non-NATO nation harms the security of NATO.

2. Further STAND 474 allows NATO telegrams graded CONFIDENTIAL or RESTRICTED to be encrypted in national systems, and it is highly undesirable that information of such grading should become available to nations outside NATO.

3. The Standing Group therefore feels considerable concern at the potential danger to the security of NATO which may arise from the insecurity of the national communications of individual nations: the insecurity of one can endanger the security of all.

4. The Standing Group has had prepared two papers, one of which enumerate examples of cryptographic and communications practices and procedures which endanger security, and the other, general security considerations. These papers are attached as appendices A and B. The Standing Group

~~TOP SECRET~~

urges the NATO Council to request each member nation to examine these papers and take action to ensure that its own communications are free from the practices and procedures mentioned in appendix A, and that the principles of appendix B are applied.

5. Further the Standing Group urges that each NATO nation be requested to designate or establish a Communications Security Agency which shall be authorized to communicate on communication security matters both civil and military direct with the Standing Group Communications Security and Evaluation Agency Washington (SECAN).

6. The Standing Group also urges the NATO Council to invite any member nation, which requires advice and technical assistance towards the improvement of the security of its national cryptographic and communications practices and procedures whether civil or military to apply through their Communications Security Agency direct to the Standing Group Communications Security and Evaluation Agency Washington. It may subsequently be found more convenient that SECAN arrange for discussions arising out of this first approach to be held with appropriate authorities in Europe.

~~TOP SECRET~~

APPENDIX A

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. They are only acceptable in special cases for Armed Forces communications 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. It follows that such codes must be changed at very frequent intervals.

II. ADDITIVE SYSTEMS.

2. Any additive (or subtractor or minuend) system is dangerous unless special precautions are taken in the construction and method of employment of the additive itself. Many "special precautions", however, 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.

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

5. In general, polyalphabetic substitution systems whether actually additive in nature or not, are subject to the same dangers as are additive systems.

~~TOP SECRET~~

III. NON-ADDITIVE HAND SYSTEMS.

6. There are many hand systems of encipherment that do not employ additive. Very few of these can be guaranteed to be secure, even though they may be very complex and apply both substitution and transposition to code or plain language.

IV. MACHINE SYSTEMS.

7. 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" of the old "C" series (see para 8 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.

8. Special attention is drawn to the dangers inherent in the use of the Hagelin "Cryptoteknik" machines of the "C" and "CX" series:

a. Since the encipherment is essentially by additive, it follows that if the same or a neighboring message setting is used more than once the internal set-up can be recovered on the overlap; a single mistake by an operator using a message setting a second time can thus compromise the machine set-up.

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 some of these machines can give adequate 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 these machines are especially urged to consult SECAN.

V. TRANSMISSION SECURITY.

9. Ciphers, however good individually, are not enough to ensure communications security. Transmission techniques and message formats can in themselves provide valuable intelligence to a traffic analyst. Although there are practical limitations, the ideal to be striven for is that the traffic neither of any type (e.g., naval, air force, etc.) nor of any 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 attention be paid 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 messages and suppression of plain language chatter.

~~TOP SECRET~~

APPENDIX B

GENERAL SECURITY CONSIDERATIONS

I. PERSONNEL SECURITY AND TRAINING.

1. In addition to the security of cryptographic systems themselves, the security of cryptographic personnel must be considered an essential part of cryptographic security. It is no use having a secure cryptosystem and special conditions of physical security if the personnel responsible for such tasks as the printing of documents and the typing of cryptographic instructions are not themselves completely secure.

2. Personnel employed in communication security matters, and this includes cipher staffs, must be thoroughly investigated. Their instruction must be as complete as possible; mistakes by cipher clerks, and even operators' "chat", often result in compromise of security.

3. In short, personnel must be guaranteed to be competent, loyal, and trustworthy.

II. SECURITY OF CLASSIFIED MESSAGES BEFORE ENCIPHERMENT AND AFTER DECIPHERMENT.

1. If security of classified messages is to be achieved, it is not enough to encrypt and transmit them securely. It is necessary to follow strictly the general security rules which apply to all classified documents, both before and after encryption. Special measures must be taken in the processing of messages, in their reproduction, distribution and storage.

~~TOP SECRET~~

2. Originators and addressees of messages must have impressed upon them the fact that their carelessness or indiscretion can result in compromise of not only message texts, but also, and as a consequence, on the cipher systems used to encipher the message texts.

3. It is essential:

a. To destroy carefully all rough drafts of messages, and all work sheets.

b. To reduce to a minimum the number of people who handle a message between its origination and encipherment.

c. To deliver message texts, before encipherment and after decipherment, securely wrapped and by safe hand.

d. To use only cleared personnel for typing and otherwise processing message texts.

e. To restrict the dissemination of the plain texts of encrypted messages to those who have need to know their content.

f. To insure careful and secure storage of the plain texts of encrypted messages.