MINUTES OF FOURTH MEETING
US CONFEREES
FRENCH COMMUNICATIONS SECURITY CONFERENCE

1000 TUESDAY, 2 JUNE 1953
Room 19-232B, U. S. NAVAL SECURITY STATION
WASHINGTON, D. C.

Those present were:

Mr. W. F. Friedman, NSA, Chairman
Mr. R. F. Packard (State)
Mr. W. H. Godel (OSD)
Mr. S. D. Ellis (FBI)
Mr. F. B. Rowlett (CIA)
Capt. R. L. Taylor, USN (Navy)
Capt. G. Grange, USN (Navy)
Col. M. L. Sherburn, USA (Army)
Lt. Col. J. M. Anderson, USAF (Air Force)
Lt. K. B. Monypeny, Jr., Secretary (NSA)

NSA Observers

Dr. L. E. Shinn
Dr. H. J. Stukey
Mr. Frank Austin
Mr. F. A. Raven

1. The minutes of the third meeting were considered and paragraph 5 was amended by deleting the last two sentences. The minutes were then approved as amended.

2. The Conference took note of the Memorandum for the Chairman, U.S. Delegation, dated 1 June, 1953, signed by the Executive Secretary, USCIB.

3. The Chairman next placed before the conferees the revised pages of the Polyzoides report and noted the changes made by USCIB. A detailed discussion was held concerning the possible meanings of a "demonstration of proper techniques" (see paragraph 2 of recommendations, page 10, Polyzoides report). It was agreed that Mr. Austin, Dr. Shinn and Mr. Raven would outline the type of demonstration and explanation considered appropriate and that this, after approval by the U.S. Delegation, would be presented to the British during the conference. (Encl. 1) It was further agreed that this demonstration could be detailed to the point permitted by USCIB, which means

that when presented to NATO nations it might be expected to permit [redacted].

4. At 1055 the meeting recessed until 1105.

5. The Chairman then placed before the conferees for review the conclusions and recommendations resulting from the 1951 conference on the problem of French security and the conferees agreed to the following:

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

(Para 3 a.) - The French cryptographic situation has improved, as indicated in Tab D of the Polyzoides report.

(Para 3 b.) - The U.S. position now permits [redacted]

(Para 3 c.) - The Cryptographic Service of the FMA possesses necessary cryptanalytic knowledge to insure provision of systems affording adequate cryptographic security, but it does not possess the ability to enforce rules as to proper usage.

(Para 3 d.) - The US now believes that no drastic reorganization of the FMA is required.

(Para 3 e.) - It is now believed that rather than a drastic shock the French should be given an "educative tour."

(Para 3 f.) - This type of shock [redacted] it is hoped, is not necessary now.

(Para 3 g.) - The situation with regard to infiltration of the French government by disloyal persons has shown some improvement, but not very much. Such improvement noted has been in the military and in intelligence agencies, but not in the MFA or other ministries.

(Para 3 h.) - No change.

(Para 3 i.) - (1) No change.
(2) No change.
(3) No longer a significant factor.

(4) In view of the establishment of a "Y" system in NATO, French pressure for broader Y collaboration will increase.

(Para 3 j.) - The U.S. Delegates feel arrangements for improvement should first be tried through NATO channels. If, in discussions with British, it is shown that an approach to MFA would be more advisable, this view may be accepted. However, an approach to the [redacted] should not be made except as a last resort.

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

(Para 3 k.) - Still true and this reinforces reasons for type of approach now being recommended by U.S.

(Para 3 l.) - The urgency for improving the security of [redacted] communications is such that it warrants the US proposed type of solution to the problem.

(Para 3 m.) - No longer valid.

(Para 3 n.) - No longer valid or possible. Not enough machines available.

(Para 3 o.) - Not applicable.
As to RECOMMENDATIONS of 1951 Conf:

(Para 4 a.) - No longer valid.

(Para 4 b.) - LSIB and USCIB have not agreed.

(Para 4 c.) - No longer valid.

(Para 4 d.) - Still under review.

(Para 4 e.) - Not applicable.

6. Mr. Godel suggested, and it was agreed, that a logical type of approach could be to ask all NATO nations to make an examination to see if COSMIC traffic were being passed in national systems.

7. Mr. Austin pointed out that by using an approach through NATO, it would be possible to correct French insecurity without revealing anything beyond what is in our paper. This would also answer the French complaint, reported in Par. 5 of the LSIB memo of 26 February 1953 to USCIB, concerning insecurity of other NATO nations' cryptosystems, particularly those of the Turks and Greeks.

8. The Chairman stated that there were to be no further meetings prior to the opening of the Conference, and added that the outline referred to in paragraph 3, above, would be distributed to the US Conferees after the Plenary Session. He also stated that the Conferees should be prepared to hold meetings on Saturday, 6 June.

9. There was no further business to come before the meeting. The meeting adjourned at 1230.

K. B. Montpeny, Jr.
Secretary

4 June 53

~~SECRET - SECURITY INFORMATION~~

HOW TO DEMONSTRATE COMSEC WEAKNESSES TO NATO COUNTRIES

1. a. It is believed that NATO countries will recognize it to be to the benefit of all for each to improve his own national communications security. Any action that may be taken by the UK and US must not appear to be an infringement of the national sovereignty of any NATO country or a desire to dictate to any of them. Instead of providing for a detailed examination of national practices, therefore, it is preferable to set up minimum security standards. These should be promulgated by NATO for national use. Each country would be asked to evaluate its own practices against these standards and to assure NATO that that country's security is equal to or better than that which these standards would produce.

[redacted]

Its action would take three forms:

(1) Sponsorship of the program thru Standing Group channels and implementation of it if approved.

(2) Provision of assistance and advice, upon request, to individual countries.

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

(3) Evaluation of the results of the program.

2. Minimum standards can only be worked out in final form after considerable discussion between the UK and the US. Such standards must be set forth in extreme detail and must cover all known national

Incl 1

practices of NATO countries in the whole field of communications security. This paper gives only a bare outline of the fields that must be covered. If this approach is agreed upon by the UK and US, the Conference itself should at least produce an agreed list of topics along these lines which will be the basis for later preparation of detailed specifications.

3. In addition to physical security of cryptomaterial, adequate communications security depends on two principles:

a. The problem of segregating and identifying traffic by nation, net, classification, or system must be made as difficult as possible; and

b. Cryptographic systems must be adequately secure and properly set.

4. As regards the first of these, it will be necessary to set standards in the following fields:

a. Frequency plans: To include minimum standards for frequency allocation and frequency rotation, with attention paid to the interrelation between frequency changes and call sign changes.

b. Format of cipher text: To include the steps necessary to prevent segregation of traffic on the basis of such things as length of cryptoparts, discriminants, indicators, group length, etc.

c. Message externals: To include emphasis on eliminating any external elements that would facilitate the identification of traffic, e.g., steps toward attaining uniform heading procedures, etc.

d. Communication procedures: To include measures for general

SECRET

standardization of communication procedures, for attainment of call sign security, with careful attention to interrelation of call signs and addresses.

e. Plain language transmissions: To include steps toward minimizing transmissions in plain text and procedurally isolating such plain language as must be transmitted.

5. a. The treatment of cryptographic security will include discussion of all systems and equipments known to be in use or available for use by NATO countries other than UK, US, and Canada and will state whether or not they are acceptable; if they are acceptable minimum standards will be prescribed for their use. All systems approved for NATO use will be included in the consideration.

b. The fields now contemplated for discussion are as follows:

(1) Hand systems: To include unenciphered and enciphered codes, Slidex or other tactical codes, transpositions, strips, additives on plain text, etc.

(2) Literal, or off-line machines: To include all known Hagelin types, Enigma types, Kryha, etc.

(3) Teleprinter machines: To include Fish types, Olivetti, Hellschreiber, one-time tape systems, etc.

(4) Key-generation and criteria therefor.