T O P S E C R E T

T 3.6..

Your Honor's assertion that almost all cipher telegrams can be deciphered is untenable. If the matter were so easy, the German radio sections would probably not fail to decipher the Russian, English and French radiograms which they intercept. To my knowledge the German radio sections have only succeeded in partially deciphering the Italian radiograms; this may be explained by the fact that they had material supplied by the Austrian-Hungarian army to serve as basis. Without such an aid, the decipherment of unsystematic ciphers is out of the question. That the General Staff is at present not in a position to decipher Russian diplomatic cipher despatches, is best shown by the fact that Major Nicolai recently requested that we turn over our Russian cipher material and the Communications officer in the General Staff of the Field Army recently repeated this request.

In the case of ciphers of the Foreign Office a distinction must be made between antiquated and new ciphers. Of the former there are usually one or two copies in each mission for the transmission of unimportant reports or identical messages, or - since these are already compromised - for sending out misleading information. In radio communication with Spain, for instance, several bogus telegrams have been sent in a cipher known to our enemies. That the decipherment of such radiograms causes no difficulty is clear. It is different with telegrams enciphered in the unsystematic secret ciphers of the Foreign Office, especially when used with constantly changing keys. Decipherment of these telegrams is simply impossible even for the most clever specialists. It can only result if the entire cipher is betrayed or essential parts and keys come to the knowledge of a foreign government. Of course, there is no absolute security against betrayal and the only aid is the frequent change of cipher and of keys, which is abundantly provided for here.

During the war the Foreign Office has had radio communication chiefly with the embassies in Madrid and Washington and with the mission in Persia. The embassy in Madrid has independently and constantly safeguarded its ciphers by the most intricate systems. However, since the cipher itself could not be changed during the war, it is conceivable, though highly improbable, that radiograms to Madrid could in part be deciphered, always assuming that the literal key employed was betrayed.

For Persia too a secret key is employed for important telegrams. The radiograms to Washington could be read by our enemies since they had to be enciphered with a cipher which is in the hands of the American censors in Tuckerton and Silvess. Perhaps the observations of the General Staff are based in the main on these telegrams. It would interest me, however, to be informed of these observations in detail.

In my conversation with Major Nicolai he requested the sending of a representative of the Foreign Office to a conference which should discuss an exchange of information regarding cipher material of hostile states now in the hands of the Admiralty Staff, General Staff and Foreign Office. In this way

the decipherment of foreign enciphered correspondence should be furthered so far as possible and at the same time our own cipher system be benefitted. The representative of this office did not give any assurance regarding the turning over of used German ciphers of the Foreign Office for the purpose mentioned by Your Honor and, therefore, could not take back that assurance. Instead, the Communications Officer, Capt. Grabau, was informed that it would be well to turn over to the Foreign Office the intercepted radiograms between St. Petersburg and Russian diplomatic missions abroad, since the Cipher Bureau - on the basis of the older Russian cipher material at its disposal and its long experience deciphering Russian cipher telegrams - might be in a position to decipher them, whereas this was simply impossible for the General Staff. Your Honor will bring up this suggestion most emphatically with the appropriate office.

Our representative expressed himself in general terms at the above mentioned conference respecting the cipher systems used in the Foreign Office and the measures taken for their security. The Foreign Office itself has the utmost interest in safeguarding its telegraphic traffic.

I will say further that in the past year word came from Holland - word which has been repeated several times - that all German cipher telegrams were being read by especially clever enemy agents. Thereupon, 12 sample postal ciphers were given the representative supplying the information, these he was supposed to be able to get into the hands of the agents and also to learn what results they had with decipherment. To date no report on this matter has been received. This shows the value of such reports.

I leave it to Your Honor to use the foregoing in friendly fashion in the proper quarter. I have not the slightest doubt of the loyalty of the Army Supreme Command in the question.

Representative of the Foreign Office
at Grand Headquarters Nr. 158, Secret.
General Headquarters, 23.III.17.

I bring to Your Honor's attention the foregoing letter of the Secretary of State of the Foreign Office to me. Please treat as confidential.

(Signed) Baron V. Lersner

~~TOP SECRET~~

To the Chief of Field Telegraphy.

Chief of Field Telegraphy
Grand Headquarters. Received: 7 May 1917.
Section IV Nr. 49414 Secret.

Sent 10 May 1917 with a draft.

Chief of General Staff of the Field Army 10. May 1917
Chief of Field Telegraphy
Section IV Nr. 49414 Secret

To I C Nr. 3119 Secret of 7 V 17
Re: Security of the Codes of the Foreign Office.

To Chief of the General Staff of the Field Army.

I agree with the view of the Chief of the Admiralty Staff of the Navy The requested draft of a letter to the Foreign Office is enclosed.

On behalf of the Chief of Field Telegraphy

1 enclosure. (Signed) von Massow.

DRAFT

Through a letter of the Admiralty Staff of the Navy I am made acquainted with the fact that four systems of secret communication supplied by the Foreign Office during the course of the war have not proven adequately secure. The Admiralty Staff has found itself forced to order the withdrawal of these codes from all Naval offices (attaches) equipped therewith.

The fact that these codes were furnished to the Navy for use during the war leads to the conclusion that the codes of the Foreign Office are composed on the same principles and therefore do not afford adequate security.

In view of the extraordinary importance which the security of the codes of the Foreign Office has for the collective [illegible] of the nation, I can not fail to suggest once again to Your Excellency subjecting the codes used by the Foreign Office to an examination by experts who had no part in the production of these codes.

The art of decipherment has developed into a science during the war.

Under the Chief of Field Telegraphy there is an office which is exclusively occupied with the decipherment of foreign systems and which has succeeded in breaking nearly all field and naval systems now in use as well as several diplomatic systems. Even unsystematic ciphers with changing decipherment have been solved by this office without any aid from other sources.

I propose therefore that Your Excellency utilize the rich

[redacted]

Chief of the Admiralty Staff of the Navy
II

Berlin, 14 April 1917.

Very Secret.

Pursuant to my letter D 2584 II of 22 March I have had the codes of the Foreign Office Nr. 200, 604, 2505, and 1303 which were turned over to the Navy subjected to a brief examination. The result of this examination which is enclosed, has convinced me that these codes are not suitable to guarantee adequate security over any considerable period of time. I have therefore ordered their withdrawal from all Naval Offices [illegible] at present supplied therewith.

Signed Signature

To Imperial Privy Counsellor, Secretary of State of the Foreign Office, Mr. Zimmermann, Excellency, Berlin.

Chief of the Admiralty Staff
of the Navy
D 2908 II.

Berlin, 14 April 1917.

Very Secret.

To the Royal Field Marshall General, Chief of the General Staff of the Field Army, Mr. von Beneckendorff and von Hindenburg, Excellency, Grand Headquarters.

Enclosed I send Your Excellency for your information a copy of a letter to the Secretary of State of the Foreign Office.

Even though it is impossible to judge here whether the other secret means of communication used by the Foreign Office afford greater security, the results of the investigation of four codes turned over to the Navy during the course of the war for its use - which therefore were evidently regarded by the Foreign Office as sufficiently secure - make it imperative to use caution in transmitting secret material through the mediation of the Foreign Office.

(Signed) von Holtzendorff

Chief of the General Staff of the
Field Army
I G Nr. 3119 Secret

Grand Headquarters
7 May 1917.

Only by Officer.

Through the letter of the Chief of the Admiralty Staff D 2908 II of 14 IV it has come to my attention that individual secret codes of the Foreign Office are not absolutely secure.

Should this be true, I request, that a suitable draft of a letter to the Foreign Office be prepared for me.

I enclose the material at hand for your confidential use.

By Order
Ludendorff

5 enclosures

~~TOP SECRET~~

experience of this office and have the codes in question checked by an officer of this office. Details could be arranged with the Chief of Field Telegraphy

Chief of the Admiralty Staff
of the Navy

Berlin, 28 VII 1917

5749 II

Very Secret.

In connection with D 2980 II of 13 April (I beg to inform you) that for special reasons the telegraphic communications of the Foreign Office with the Imperial Embassy in Madrid has been subjected to a study of its security. This investigation has confirmed the previous opinion respecting the codes constructed on the model of 2505, inasmuch as all enciphered telegrams could be deciphered in 14 days. With respect to the so-called Lotteria Cipher employed for more important matters, investigation showed that this did indeed involve greater difficulty in solution but nevertheless would only assure adequate security if certain defects were eliminated and if a number of codes were available for use at the same time.

(Signed) von Holtzendorff

To the Royal Prussian Field Marshal General,
Chief of the General Staff of the Field Army
Mr. von Beneckendorff and Hindenburg,
Excellency,

Grand Headquarters.

R. Chief of Communications
with request for opinion.

by order
P. L.

Chief of the Communications Service
Section IV f Nr. 74284 Secret

Grand Headquarters 1 VIII 17.

I agree with the view of the Admiralty Staff. Here too traffic of the Foreign Office with Madrid is intercepted and worked on. One of the codes used between the "Minister of Foreign Affairs" Berlin and Madrid was solved after 14 days. The Chief of the Communications Service made personal report of this to the Quartermaster General. Telegrams from this traffic are enclosed.

A check of the codes of the Foreign Office for solubility by experts is considered absolutely essential, as already reported.

By Lotterie Cipher is understood a code in which the groups are not arranged in alphabetical order but distributed in random fashion after the manner of a lottery.

V. S. d Ch. d. N.
U. Ch. d. G.
(Signed) von Massow

~~T O P S E C R E T~~

Foreign Office
Pol. B. 768
g. Nr. 18931
11 enclosures

Berlin, 11 August 1917.

Very Secret.

I am returning to Your Excellency the telegrams enclosed with your letter of 6th inst. M. J. Nr. 21625 with the obedient remark that they did not originate with the Foreign Office but from the Admiralty Staff, or were destined for the latter, and that they are enciphered with the Naval communications book and the Naval keys. Only the beginning of Tel. Nr. 26 of 2 March (Sheet 6) is given in a cipher of the Foreign Office and not enciphered.

I leave it your judgment whether to inform the Chief of the Admiralty Staff of the foregoing

So far as the decipherment by the Admiralty Staff of the telegrams of the Foreign Office enciphered after the model of the antiquated code 2505 is concerned, it may be remarked that this was only possible due to the exact knowledge of the Foreign Office cipher material available at the Admiralty Staff and on the basis of actual decipherments of telegrams supplied from here since sent for that department. Decipherment of telegrams in the Lotterie Cipher has not yet been undertaken by the Admiralty Staff here.

The Foreign Office adheres, first and last, to the point of view that its new Lotterie Cipners, especially when reenciphered, can only be regarded as not absolutely secure if betrayal or careless use of the ciphers or of the enciphered correspondence occurs.

(Signed) Signature.

To the First Quartermaster General,
General of Infantry,
Mr. Ludendorff, Excellency,
Grand Headquarters.

Chief of the General Staff of the
Field Army
I C Nr. 4291 Secret
P. Chief of Communications

14 VIII 17

Reference your IV f Nr. 74284 secret with request for opinion.

by order and acting

(Signed) von Bockelberg.

~~T O P S E C R E T~~

TOP SECRET

Chief of Communications Service
Section IV f Nr. 74284
In: 14 VIII out 17 VIII 17

It was assumed here that the traffic with the inscription Minister of Foreign Affairs Madrid" and "Minister of Foreign Affairs Berlin" was conducted by the Foreign Office or at least enciphered there. From the above communication from the Foreign Office, as well as from solution of another system in this traffic which has been made meanwhile (Political Section O.H.L.) it appears that this is not the case. The various, as yet unsolved systems from this traffic, among which that of the Foreign Office must be found, are being worked on further.

11 enclosures.

V. S. d. Ch. D. N.
d. Ch. d. G.
(Signed) von Massow

Foreign Office
Ch. B. 545
J Nr. 19241
In reply to letter of 11 May of this year.
I G Nr. 3119 Secret
1 enclosure
Very Secret

Berlin, 17 August 1917

Representative of the Foreign Office in Grand Headquarters
Nr. 654
through: 19 VIII 17
signed Baron von Lersner

Your Excellency's assumption that the ciphers assigned to the Navy were considered by this office to be sufficiently secure, is correct. The Foreign Office still takes the point of view that the other ciphers too - especially the Lotteria Ciphers with recipherment according to new principles, are absolutely secure so long as there is no betrayal or careless handling of cipher material or enciphered correspondence. Too long a use of the code is, of course, likely to shake faith in the code and we have always taken care to change codes and keys frequently. Unfortunately it has never been possible to change the frequently used codes in Madrid as we should have liked, due to the war, however frequent change in encipherment has been made.

To the statements of the Admiralty Staff regarding decipherments of telegrams of the Foreign Office to and from Madrid, I have stated my position in my answer of 17th inst., and have the honor to send Your Excellency a copy herewith.

Copy of Ch. B. 750

(Signed) von Kuehlmann

To the First Quartermaster General,
General of Infantry,
Mr. Ludendorff, Excellency.

TOP SECRET

~~TOP SECRET~~

[illegible].
[illegible]. 750
[illegible]. 19342
Very Secret

Berlin, 17 VIII 1917

In reply to letter of 27th u't.
D. 3749 II

With the intimate service relations which have always obtained between the Admiralty Staff and the Foreign Office the latter has never hesitated to place at the disposal of the Admiralty Staff its cipher material, just as the Admiralty Staff has turned over its codes (Traffic and despatch books) to the Foreign Office. In this way the Admiralty Staff gained insight into our cipher systems. Since the land line communication with Spain has been blocked all telegrams of the Foreign Office to and from Spain have passed through the war central office of the Admiralty Staff. Telegrams arriving here from Madrid, which are destined for the Admiralty Staff, have hitherto been passed on to the latter in clear without any change so that both cipher text and plaintext were available together. Even new keys have been sent from Madrid in [illegible] code. Thus, the opportunity for decipherment was provided. Under like circumstances other codes could be read too.

In the telegram decipherments submitted the Lotterie Cipher was not employed in a single case. The Foreign Office therefore sticks to the point of view that its new Lotterie codes are perfectly secure provided no possibility of unauthorized decipherment is given by betrayal or lack of caution in their use.

In judging the Madrid Ciphers consideration must be given to the unavoidable circumstance that they could not be changed during the war, otherwise the series to which 2505 belongs would have been replaced long since by the Lotterie Cipher. As stop-gap serve the variations of the ciphers used by Madrid, these changes are frequent and, in part, very serviceable. For instance the system of the Naval codes with alidable, frequently changing keys is used there.

For the rest, we are working unceasingly to attain the utmost possible security of our enciphered correspondence by frequent change of codes and recipherments.

(Signed) Kuehlmann.

For the Chief of the Admiralty Staff of the Navy.

Ch. B. 960 25 IX 17
Chief of the Communications Service
Section V Nr. 79141

Grand Headquarters of His Majesty,
23 IX 17.

To the Chief of the General Staff of the Field Army.

Enclosed are enciphered radiograms of a circuit Koenigwusterhausen - Madrid which have been solved by my evaluation center in Grand Headquarters. It appears to be a question of a secret traffic of the Foreign Office in Berlin with its representatives in Spain.

~~TOP SECRET~~

It is requested that one ascertain whether the solved messages agree with the originals.

3 enclosures (Signed) Hesse

U. R. Secretary of State of the Foreign Office with a request for prompt statement.

(Signed) Ludendorff.

U. Chief of Communications Service

Foreign Office informs that the Cipher Service of the Foreign Office is being reorganized.

(Signed) von Bartenwerffer 8 X.

Radio Section O.H.G. (A.) G. 459 Grand Headquarters of His Majesty 22 IX 19.7

Result of Investigation of Cryptographic Systems used in Radio Traffic between Berlin and Madrid

The various types of radiograms observed here in traffic Berlin - Madrid, signed on the one hand by Zimmermann, Kuehlmann, Stumm, Busche and on the other hand by Ratibor, Bassewitz, Hevse beyond doubt belonging to the telegraphic communications of the Foreign Office with the Imperial Ambassador Prince Ratibor in Madrid, can be divided essentially into two main groups:

1. Telegrams which have at the beginning the indicator groups 27082, 18470, 21894, 1777, 12444 with 4 and 5 digit groups up to 30900 and rare groups above 30900.

2. Cipher telegrams with the indicator groups 0053, 5003, 5300, 0000, 4343, 1357, chiefly with 4 digit groups.

The investigations were made on the basis of intercepted radiograms, i.e., with the same means which - at the very least - would be available to an unauthorized, hostile decipherer.

The results are as follows:

To 1. Work on telelgrams with indicator group 27082 showed that:

a. the telegrams are encoded but not enciphered.

b. the code used is systematic; the code groups are composed of 2 and 3 place heading numbers and 2 place column numbers. Groups with the same heading number lie near together in the alphabet.

Since there is no doubt about the possibility of solving an unenciphered systematic code, and since furthermore from a solved cipher telegram the relationship of the systems 27082, 21894, 1777, 12444 was evident, work was not carried further with these systems. (Cf. Radiograms read - Supplements 11 and12).

To 2. Investigation of the telegrams with indicator 0053, 0000, 4343, 1357 yielded the following results:

a. the telegrams encoded with a code and encipherment by several methods. In 0000 encipherment is by simple transposition of the digits of the groups, in the other telegrams by addition and substitution according to frequently changing keys. (Supplement 1)

The discovery of the types of encipherment and thus the reduction of all these types to one basic type was carried out by one operator in 3 weeks.

b. The code thus discovered is entirely 4 place; the fifth digit prefixed to many groups is a blind. No system was found in the structure of the code. The code turned out to be the completely irregular so-called "Lotteriechiffre". Contrary to the opinion of the Foreign Office which "adheres first and last to the view that the decipherment of the Lotteriechiffre is absolutely impossible" two workers were able in 4 weeks to reach the state of decipherment shown in the appended telegrams (Supplements 2 - 10). According to our experience with other Lotteriechiffres in diplomatic traffic (e.g., Italian K. 19) it would be possible in a few weeks to carry the work to a point where almost every telegram could be solved for practical purposes.

The preceding proves that system 0053, 0000, 4343, 1357 can be solved and is therefore open to criticism.

Regarding the appended solutions of messages it may be said that:

1. The 3 place groups in the heading generally show number and date of the message. These are enciphered by a special table for numbers and dates which was solved here.

2. It lies in the nature of a non-alphabetic code (Lotteriechiffre) that the recovered values of cipher groups do not always agree in wording with the meadings in the original code and that words or rare occurrence can only be deciphered with limited certainty.

I. V.
(Signed) Stuetzel
Lt. of the Reserve.