A STUDY

OF

FRENCH COMMUNICATIONS DOCTRINE AND PRACTICE

9 April 1951

9 April 1951

A Study of French Communications Doctrine and Practice

A. Statement of the Problem.

In order properly to evaluate the state of security of French communications, the history of French cryptographic practice must be studied with the purpose of finding answers to four questions:

1. Do the French know what constitutes sound COMSEC doctrine?

2. Do their cryptographic practices demonstrate that such knowledge is indeed applied?

3. Do they supervise communications in order to detect compromises and take corrective action?

4. Do they use cryptographic systems that guarantee adequate security?

Answers to these questions have been sought from two sources: the actual published documents of French Cryptographic Services, and the history of French practice as it is known to AFSA.

B. Facts Bearing on the Problem and Discussion.

This discussion will be concerned primarily with the communications of the Army and the Foreign Ministry because it is in these two fields that there is most current information available.

1. Do the French know what constitutes sound COMSEC doctrine?

The most recent explicit statement of French COMSEC doctrine available is the "Instruction relative à l'organisation et au fonctionnement du service de la correspondance chiffrée", issued in 1941 by the Secretariat of State for War, General Staff of the Army, Deuxième Bureau. Following is a translation of Chapter 1, "Cryptographic Secrecy", of Section II, "Cryptographic Security".

"Cryptographic secrecy demands a strict observance of precautionary measures which are sometimes neglected: certain imprudences, which seem at first sight harmless, are capable, indeed, of gravely compromising the security of cryptographic systems.

NO CRYPTOGRAPHIC SYSTEM IS PROOF AGAINST CERTAIN IMPRUDENCES, ESPECIALLY WHEN THEY ARE REPEATED."

Maintenance of the security of cryptography is, consequently, the primary condition of its employment. It demands on the part of the cryptographer the rigorous observance of the rules, called "General Security Measures," enumerated in Chapter II following, which are the result of numerous experiences.

"It is important then that in all echelons the regulations concerning encryption be scrupulously observed".

The document cited, other related documents, plus files of correspondence of the Cryptographic Section of the Army General Staff, prove conclusively that the French Army, at least during the War, recognized the need for maintenance of communication security, that it expended

considerable effort in the years preceding the last war in training cryptographers, and that it was amply aware of the ways in which communications security could be maintained. Pertinent quotations from documents on the subject will be found in Tab A.

The only documentary evidence on Diplomatic doctrine is found in the prefaces to certain captured codes. These prefaces give instructions for the use of the system, and also set forth some general security rules. These rules indicate that the Foreign Ministry cryptographers, too, were aware of the dangers of poor COMSEC practice and tried to instruct the users of systems in ways to avoid compromising their security.

Army, Navy, and Diplomatic doctrine are generally the same on matters like physical security, avoidance of compromise by plain-text reference to code messages, need for paraphrasing when communicating code text to a third person, and varying of indicators in enciphered code telegrams.

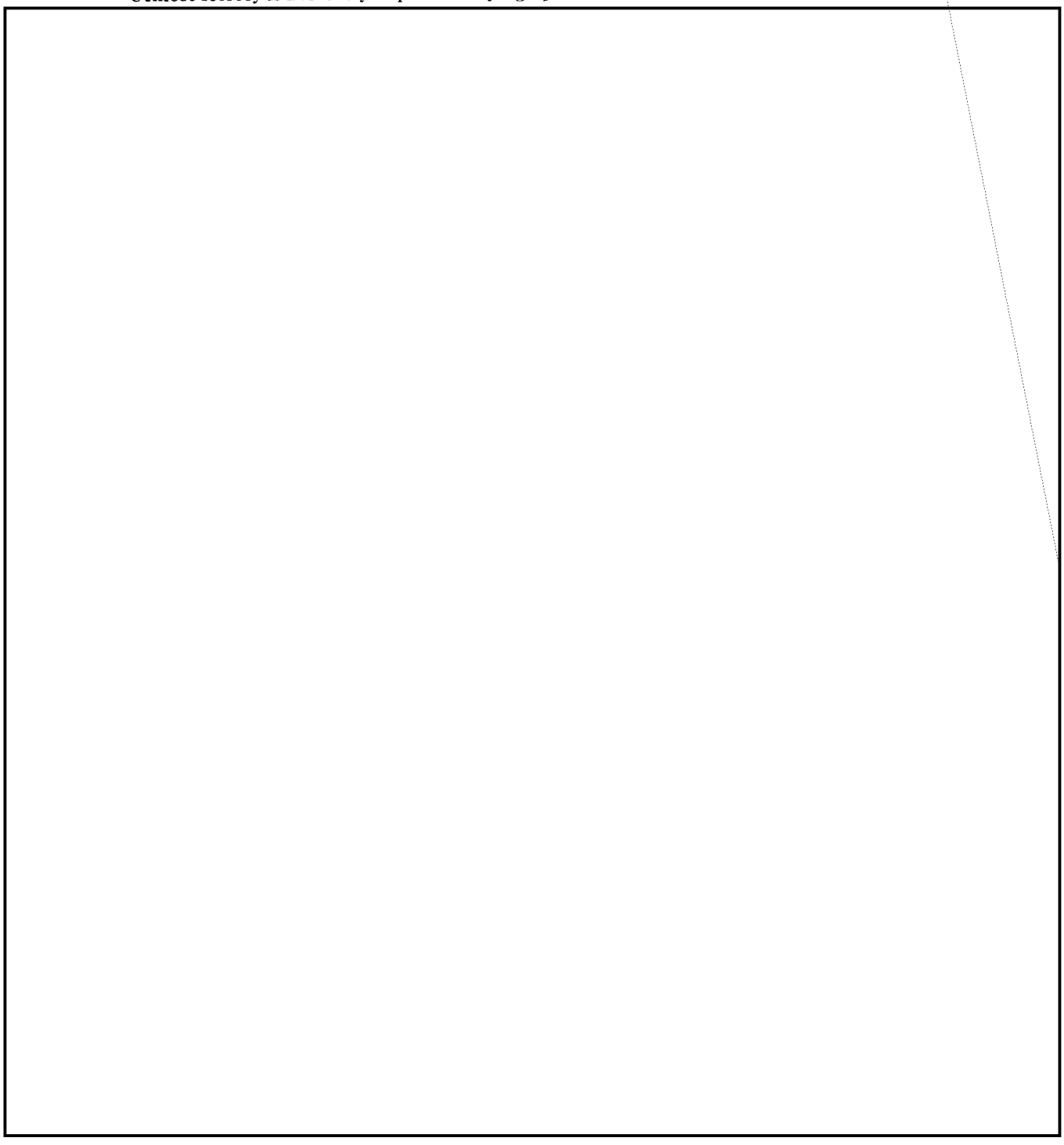
EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted] offer sufficient evidence of the fact that the laws of COMSEC are known to the authorities. As deduced from these [redacted] the French rules are very similar to those of the U.S. Army. Most of the rules are apparently known, also, in at least some quarters of the Diplomatic service. For example, the principle that a given system should be used for correspondence of a certain classification is not unknown.

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

[redacted]

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.



While there are many similarities in Army, Navy and Foreign Ministry doctrine with respect to cryptographic practice, there are certain differences, some of which appear traceable to mere lack of a specific doctrine on the part of the Foreign Ministry.

There is noted one major doctrinal difference: the Foreign Ministry allows the use of unenciphered code. Furthermore, although some highly classified codes are accompanied by the warning that they must never be used unenciphered, others have been officially used both enciphered and unenciphered, thus affording an excellent opening for cryptanalytic study. The Army's position, as deduced from several statements in instructional documents, is that the originator decides whether a tele-- gram is to be enciphered or not. If it is to be enciphered, however, "Simple encipherment is, in general, insufficient to insure the security of the texts". Plain codes, the doctrine runs, are susceptible of analysis, especially if widely used, and furthermore, codes can be secretly photographed. Therefore, "all radio-telegrams must be in enciphered code. It is absolutely forbidden to send radio-telegrams in unenciphered code." As a result of the application of these opposite doctrines, there is no case known of Army use of plain code, whereas

[redacted]

Army doctrine recognizes the problem of repetition of stereotyped expressions (especially at beginnings and ends of messages) and urges the use of nulls and variation in placement of internal numbers, addresses, message references, etc. Diplomatic awareness of this problem,

[redacted]

is limited to the problem of stereotypes at the breaks in message parts.

Army and Navy instructions urge the systematic use of variants where they exist; no Diplomatic mention of this point is found.

"Never send the same text in two telegrams, one in clear and the other in code or one encrypted with one code and the other with another code, or even with another key." This law is laid down in the "Instruction Secrète du 3 février 1936 relative à l'organisation et au fonctionnement du service de la Correspondance Chiffrée dans l'Armée en temps de paix et en temps de guerre" issued by the Cryptographic Section of the Army General Staff. It is added that, where necessary, the same substance, paraphrased and otherwise altered, may be sent in two systems. The same rule can not be found in any Foreign Ministry instructions, although the obvious ban on sending the same text in code and in clear seems to be implied [redacted] cited above. There is no evidence, however, either in writing or practice of the existence of a ban against repeating the same text in two different codes.

2. Do French cryptographic practices demonstrate that their knowledge of sound doctrine is applied?

In the years since 1941, the French have been notoriously lax in their cryptographic practices. This statement applies especially to the Foreign Ministry, but the indictment of the Military services can be only slightly less strong. Whatever real security is enjoyed by French communications results directly from the use of a few inherently good systems. Short of physical loss, it is difficult to compromise completely a true one-time pad. But if the system itself is at all

vulnerable, the French can almost be counted upon to endanger it by violating the most important rules of COMSEC.

French violations of security fall under three headings. (1) improper construction of system, (2) improper composition of cryptograms (3) failure to observe the rules against encipherment of the same text in two systems.

A few examples of each kind of violation will suffice to illustrate the case:

(1) Improper construction.

(a) Both one-part and 2-part codes are re-generated one from another by simple re-pagination and re-lineation.

(b) Additive key is systematically generated.

(c) The same key is used to encipher several codes. (The Army has been especially derelict in this respect).

Under this head might also be mentioned the fact that it has often happened that the compilation authorities have issued instructions for use of systems in an attempt to improve security, only to have their procedure provide new weaknesses for the analyst to exploit. Such a case was the instruction that the groups for indicating the parts of a multipart message cease to appear in clear at the end of the part, and be enciphered somewhere in the body of the text. At the time this change was made, it took three code groups to indicate the part. Many

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

(2) Improper Composition.

(a) Stereotyped beginnings are regularly employed.

(b) Plain-text addresses are often repeated, enciphered, in the text.

(c) When variants are available, certain ones are over-used.

(3) Re-encipherment

Of all rules of security, this is possibly the most important. It is also the one that has been violated the most flagrantly and with the most dire results. The Foreign Ministry is by all odds the chief offender on this score, although the Military are by no means free of guilt. Re-encipherments usually come about for one of two reasons.

3. Do the French supervise communications in order to detect compromises and take corrective action?

There is some attempt to catch errors and see that they are not repeated, but it can not be seen that this surveillance is either systematic, consistent or effective.

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

The violations that are caught and reported are generally of a secondary importance.

[redacted]

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

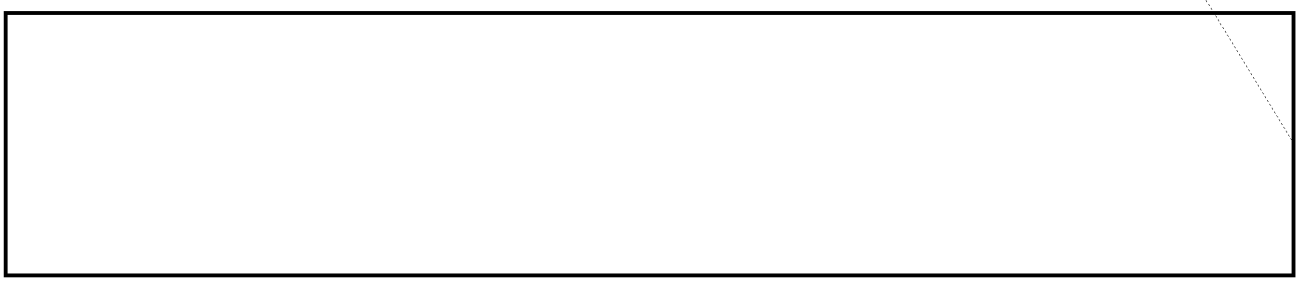
[redacted]

Physical compromises of military systems have been reported from time to time and the necessary action has been taken.

[redacted]

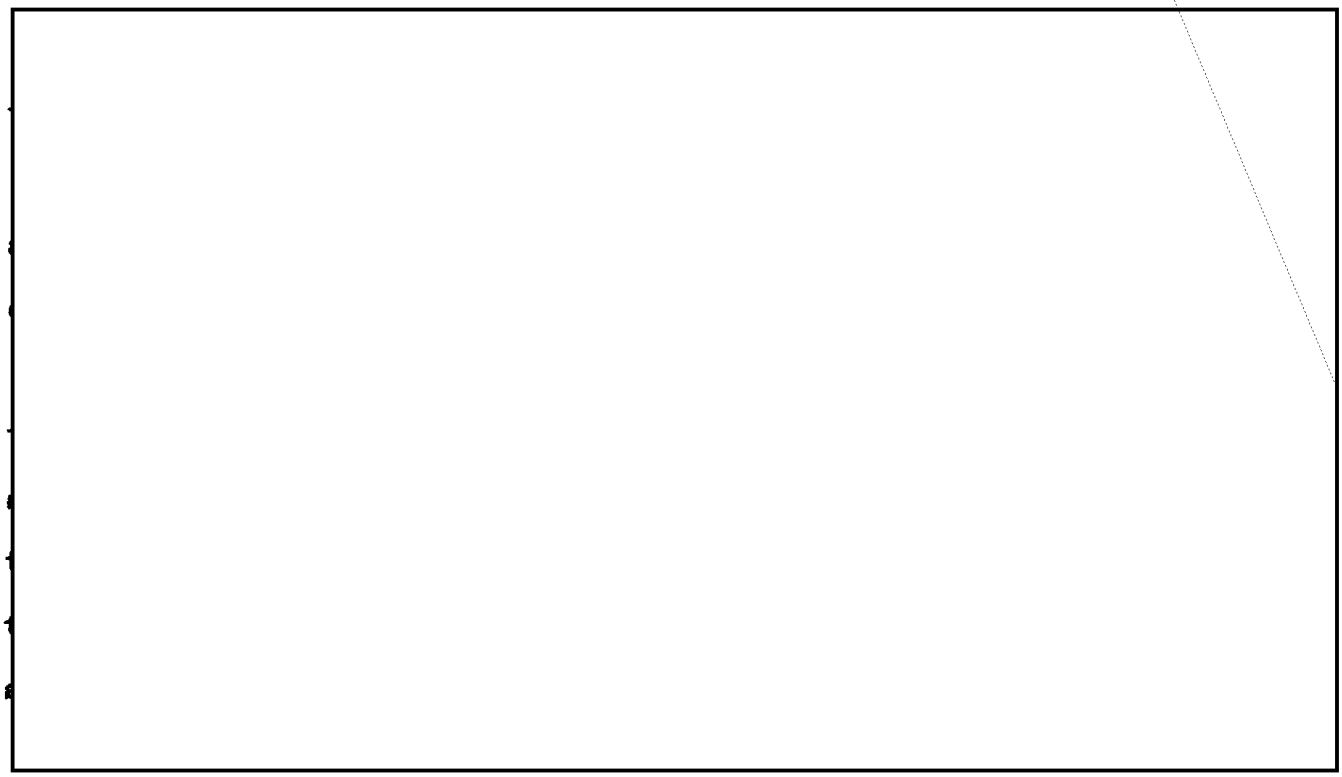
But most compromises resulting from blunders in communication seem never to be caught. There have been few instances recently of military systems so endangered, but the history of 1947 and 1948 is full

[redacted]



The conclusion can be only that the security monitoring system of the French - if a formal one exists - is not doing its job.

4. Do the French use adequately secure cryptographic systems?



This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

CONCLUSIONS

The French Cryptographic Services, both Diplomatic and Military, may be fairly presumed to understand the rules of communications security. However, the rules are too often violated by the operating personnel and the errors too often go unnoticed by the authorities. These circumstances, coupled with the fact that most traffic is sent in

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

systems [redacted] or which are weakened by unwise methods of use, result in a communication operation in which the elements of insecurity considerably outweigh those of security.

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

TAB A

Quotations from Military Statements of Crypto-Security Doctrine

I. Source. "Instruction sur les conditions d'emploi du chiffre", 3 March 1940. Commandement en Chef des Forces Aerienne, Etat - Major General.

Chapter II, 7.

Any encrypted message sent by radio-telegraph of radio-telephone can be intercepted by monitor stations and thus constitute an element for study handed over to the enemy Cryptanalytic Services.

The results that they can expect from their labors are, in general, proportional to the number of documents available to them.

Chapter III, 8.

A cryptographic system may be compromised:

Directly:

When the methods of encryption become known to the enemy as a result of theft of a document or a machine, loss or photographing of codes or keys, espionnage, indiscretions of cryptographic personnel concerning methods in use, etc. (It isn't necessary that a document disappear for it to be compromised.)

Indirectly:

As the result of cryptographic studies that the enemy may undertake on encrypted messages which have fallen into his hands .....

These studies can be considerably facilitated by:

Technical errors by the encryptor.

The weakness of the methods employed.

Abuse of cryptography, especially in lower echelons of the command; ....

Cross-checking resulting from indiscretions by our services, etc.

Chapter III, 24.

It is absolutely forbidden to mix clear and cipher in the same message.

Chapter III, 25.

It is recommended that one avoid enciphering identical texts by means of different codes.

II. Source. "Instruction relative à l'organisation et au fonctionnement du service de la correspondance chiffrée, Ière Partie, Memento du Chiffreur", Secrétariat d'Etat à la Guerre, EMA, Deuxième Bureau, 1941".

The present Memento annuls and replaces the "Notice sur les Procédés de Chiffrement dans les Petites Unités" of 15 November 1929.

Part II Chapter II, General Measures of Security

1. Use of Cryptography

Encryptment is to be used only in cases of necessity.

It is not to be used if there are no serious disadvantages to transmitting the telegram in clear, or if the information to be sent or to be received can stand the delays of transmission by ordinary mail.

It is up to the authority sending the telegram to decide whether it is to be encrypted or not.[a]

Do not forget that indiscretion concerning a telegram the contents of which present only a relative importance can have repercussions with respect to more important telegrams.

Experience has demonstrated that it was relatively easy to procure texts of code telegrams, even when they pass only over national lines; it is therefore indispensable to take the precautions prescribed in the present Memento, even when the communications personnel is above any suspicion.

****

a. The "Instruction Secrète du 3 février 1936 relative à l'organisation et au fonctionnement du service de la correspondance chiffrée dans l'Armée en temps de paix et en temps de guerre", whose section on cryptographic security is for the most part identical to this one, inserts the following paragraph at this point: "As a rule, correspondence transmitted on French lines or going by French stations will be encoded by simple code; variants will be provided in order to increase the security of this coding procedure (change of codebook, change of encoding)."

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

2. Code Room

Let no unqualified person enter the rooms where encrypting takes place, at any rate while encrypting is going on. Do not encrypt in a room where there are non-French persons, whoever they may be, and do not install the Cryptographic Service in an office to which foreigners regularly have access.

3. Cryptographic Operations

Unless absolutely impossible, use only officers in encrypting and decrypting; do not entrust cryptographic operations and cryptographic documents to personnel which is constantly changing, is little or not known by the head of the Service, or does not inspire absolute confidence in him.

4. Safeguarding of Documents

All equipment and documents relative to encrypted correspondence must be preserved with the greatest care in a secure place, insofar as possible in solid pieces of furniture, provided with secret locks.

Do not let the codebooks be seen by persons who do not have to use them. Their dimensions, in fact, would give indications on their structure and the size of their vocabulary. The changing of a codebook, revealed by the change in color of the cover, is a valuable indication for unauthorized persons. Same precautions, of course, for secret instructions and papers which have served in the encryptment.

Open the cipher machines only for ciphering operations. Then lock them during periods of non-use. Do not leave the machines "on key" during their moving.

If a machine is damaged, never entrust the repair of a part to a non-qualified person (a civilian worker, for example). Request the exchange of the machine for a machine in good condition.[a]

It is strictly orbidden to keep information or documents concerning encrypted correspondence on one's person or in personal articles of furniture. It is absolutely forbidden to make extracts from codebooks under the pretext of collecting frequent words. Loose sheets are the sort of thing that can become lost or are in danger of being sneaked away more easily than documents.

5. Cryptographic Worksheets

All papers which have served in encrypting and decrypting are secret documents, of the same importance as the codebooks and machines themselves.

These worksheets must be burned (and not only torn up) as soon as they as they are no longer useful.[b]

6. Use of the telephone

Give no information by telephone relative to cryptographic operations or explanations on a cryptographic system. Everyone has had the experience of hearing others in conversation over the telephone. It is therefore a very insecure way of corresponding.

7. Wording of telegrams. Discretion to be observed.

It is forbidden anyone having knowledge of an encrypted telegram to speak of it to any person whomsoever who is not qualified

a. The preceding two paragraphs do not appear in the "Instruction Secrète" of 1936.
b. The "Instruction Secrète" of 1936 adds the following paragraph: "Burn the old key as soon as the new one is put into service".

to know about it.

Any indiscretion, however insignificant it may appear, is in fact of such nature as to compromise, sometimes irremediably, the secrecy of a document.

8. Paraphrasing of telegrams

It is forbidden to reprocuce textually and explicitly an encrypted telegram in a report, even if it is a secret one.

When the receipt of an encrypted telegram obliges any authority whatever to give orders or instructions relating to it, or to make a communications to another Department or to the press, all provisions must be made so that these orders, instructions or communications never permit the reconstruction of the telegram by anyone whomsoever.

The paraphrasing of the communications to the press must be done with the greatest care, that is, the text must undergo such changes of form that, all the shades of meaning being respected, the initial wording could not be recognized or reconstructed (change the words, especially the beginnings and ends, bring together into a single copy, the parts of the same telegram, etc.)

This precaution is of capital importance and the author of the communication is accountable if it is not carried out.

Chapter III. Technical Security Measures

1. Drafting of telegrams

Cryptanalysts base their work upon repetitions of groups. Consequently, have the authorities who draft the telegrams adopt, if possible, a restrained style, stripped of useless formulas, approaching what is called telegraphic style.

The Cryptographic Service does not have the right to change a wording unless it has been expressly authorized to do so by the authority from which the telegram emanates. But it has the right to propose to that authority any changes in wording susceptible of avoiding lengthiness, spell groups, repetitions of groups, in a word, everything that can afford an opening for cryptanalytic study.

The Cryptographic Service is, however, qualified to make slight changes in form such as the transferring of the number and references, which the drafters usually place at the beginning of a telegram, to the end.[a]

2. Encrypting of telegrams

(a) Be well acquainted with the cryptographic documents. Apply strictly the cryptographic rules which indicate the way to use them. When the encrypting system chosen involves the use of a codebook, the telegram must be encoded in such a way as to utilize to the fullest the facilities afforded by that codebook through the use of

a. This paragraph does not appear in the "Instruction Secrète" of 1936.

sentences or expressions which appear in it, and to avoid repetitions or spell groups. Thus several groups are gained in a telegram.

(b) When a word does not exist in the codebook, spell it out in syllables or letters which are encoded successively.

Several consecutive words thus encoded by their consecutive parts are separated from each other by a null group when this precaution seems necessary for the clarity of the translation. Use the group "Separation of spell groups" if that group appears in the codebook.....

(c) Encoding of repeated words.

If a repeated word has several variants in the codebook use them in turn.

If it has no code group and must be spelled by syllables, spell it in a different manner each time it recurs.....

(d) Stereotyped formulas.

Avoid the frequent use of set textual formulas, called stereotyped, such as "I have the honor of reporting to you", "in reply to your telegram", etc.

These formulas give rise to series of groups in which repetitions frequently arise.

(e) Use of null groups

To conceal repetitions of groups in the formulas often employed. such as the stereotyped formulas referred to above, it is recommended that they be disguised by the null groups. These are interspersed among the words or syllables or else, in short telegrams

of one or two groups, placed at beginning or end.

Null groups are also advantageously employed under the following conditions: Placed at the beginning or end of an encrypted text, they prevent the cryptanalyst from making hypotheses on the beginning or end of the telegram, hypotheses which practice often shows to be fruitless.

Interspersed between two letters or two syllables which are repeated in a spelled word, they hamper the work of the cryptanalysts.....

Finally, used to represent punctuation in place of groups specially designed for that use, they avoid the repetition of those groups.

(f) Use of punctuation and grammatical formulas

Suppress unnecessary articles and conjunctions in the process of encrypting.

Use punctuation and grammatical formulas only in case of absolute necessity, when their use is indispensable for the understanding of the text.

The observance of these rules presents the double advantage of reducing the length of the telegram and of avoiding repetitions.

In general a verb in the present tense is given through its infinitive, and a past participle after an auxiliary by the infinitive.

.....

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

(i) Never send two telegrams with the same text, either one in clear and the other in cipher, or one encrypted with one codebook and the other with another codebook, or even with another key. If a telegram is intended for two authorities who do not have the same materials for corresponding, introduce null groups at beginning and end. The length can be changed by introducing prepositions and articles, and by encoding in separate words the formulas which appear ready made in the codebook, or again by dividing the two telegrams into parts in an altogether different way.

3. Dividing of telegrams

When the draft of a telegram is very long or when, because of many null groups, the number of groups must be increased, it is advisable to divide that telegram into several distinct telegrams.....

Each of the parts must then be encrypted by means of a different key if the encrypting system permits.[a.]

a. This is followed in the "Instruction Secrete" of 1936 by:

"4. Precaution to be observed in the use of radio.

"The intensive use of radio, an insecure means of transmission, imposes an even stricter discipline in the matter of encrypting in that, since the waves can be intercepted by any unauthorized person, the information entrusted to radiotelegraphy can be exploited by foreign intelligence services.

"Consequently, it is important to apply strictly all the regulations on the subject of precautions to be taken:

"a. To preserve the secret nature of all the cryptographic documents;

"b. To let these documents be used only by absolutely qualified persons, as a rule officers, who are alone responsible for the documents which are entrusted to them (Codes and Methods of using them.).

"All radio-telegrams must be superenciphered. It is absolutely forbidden to send radio-telegrams in unenciphered code."

Chapter IV. Errors, Repetition and Verification of Telegrams.

.....

3. Reply to Verification Requests

Any Cryptographic Service which receives, by encrypted telegram, a request for verification of a cryptogram encrypted by it, must proceed in the following manner:

a. Verify the original encryptment, and, if it is found to be correct, send back exactly the same encrypted text with the same number, without modifications or additions;

b. If the original encryptment is incorrect, or if you no longer have the documents necessary for verification, send a new telegram, modifying the wording as much as possible, above all the beginning and the end, and indicating that it is a verification. Nothing in the new cryptogram must recall the first one.

The new telegram will receive a number different from that of the first.

Date and time will be those of the verification, and not those of the original telegram.

This sheet of paper and all of its contents must be safeguarded with the greatest care.
Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

[redacted]

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

[redacted]

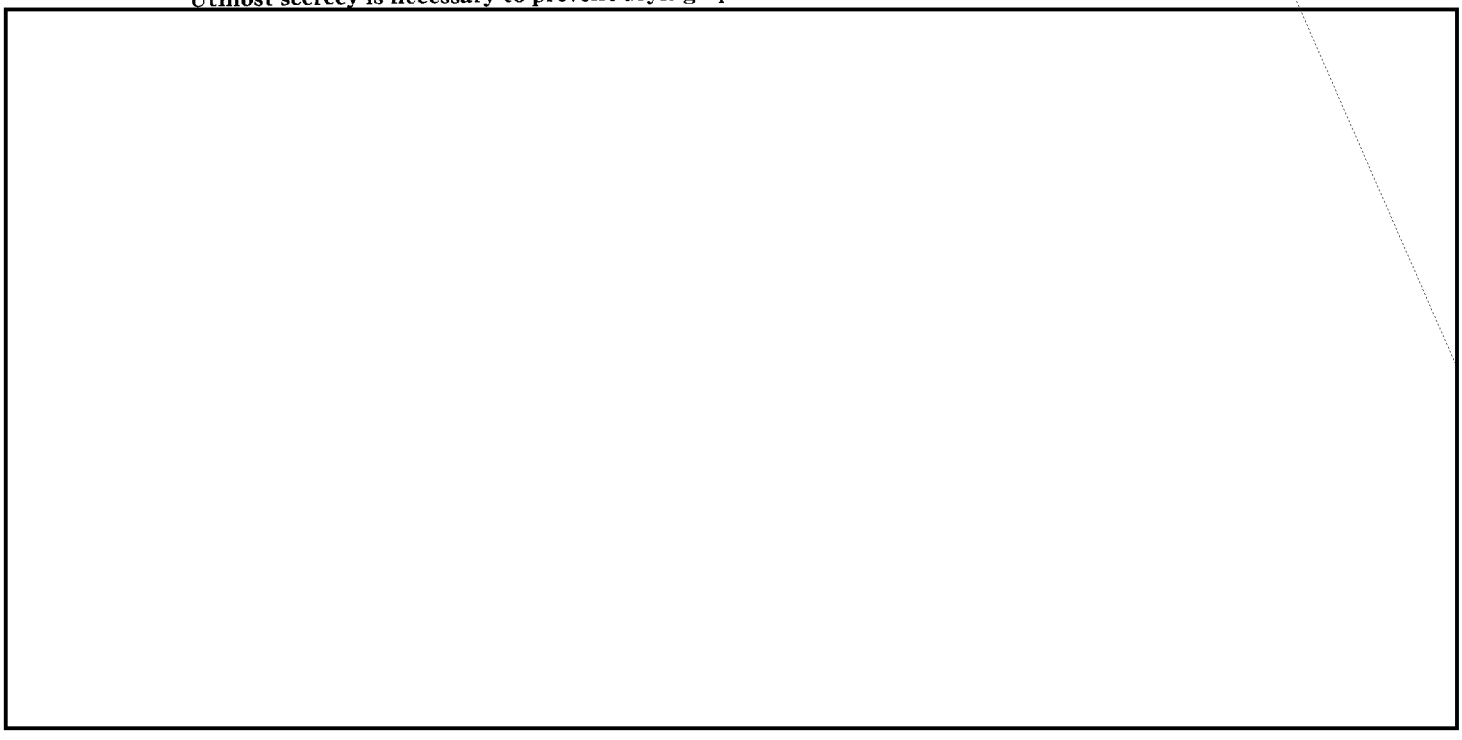
This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

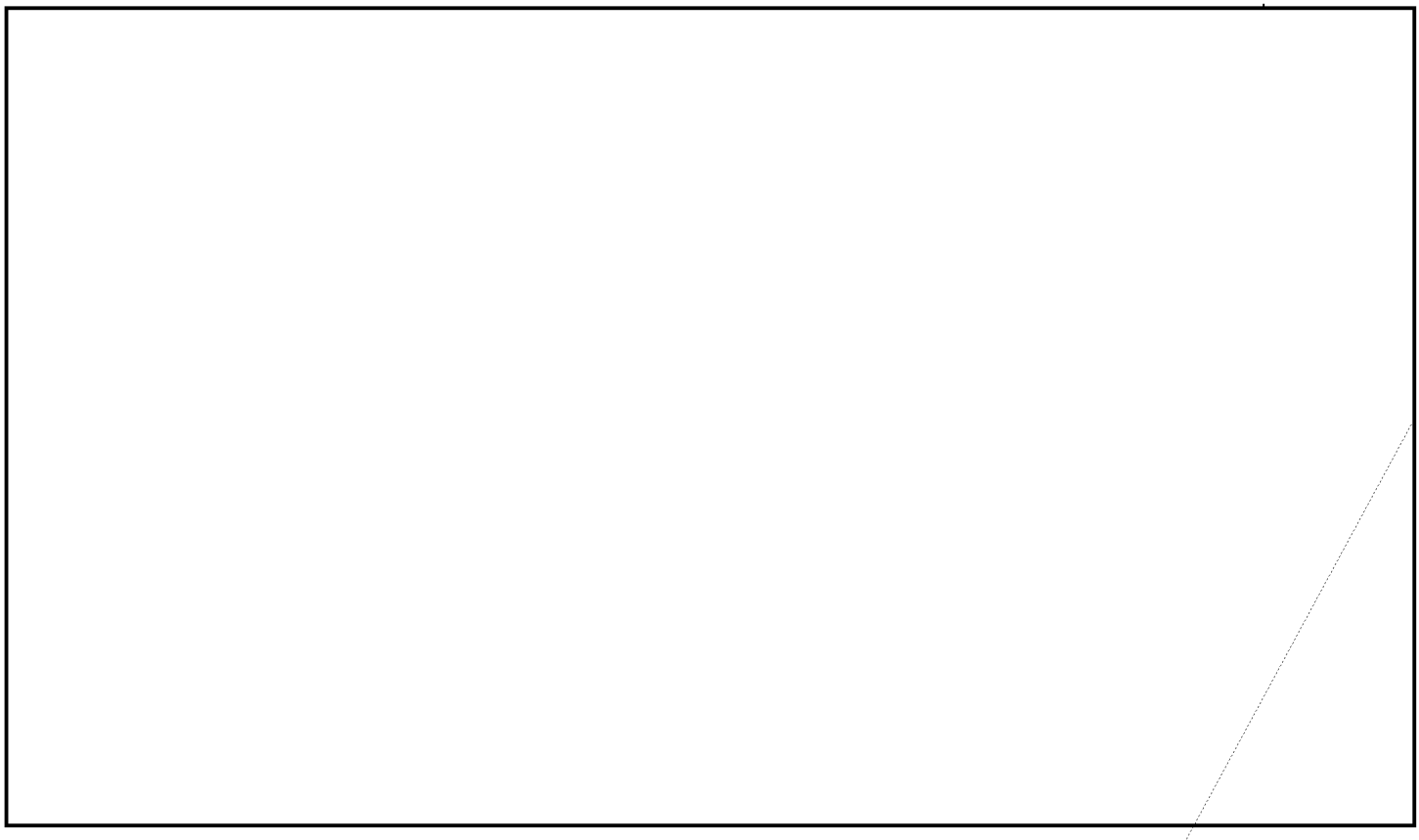
Encl 4

This sheet of paper and all of its contents must be safeguarded with the greatest care.
Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

9 April 1951

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.





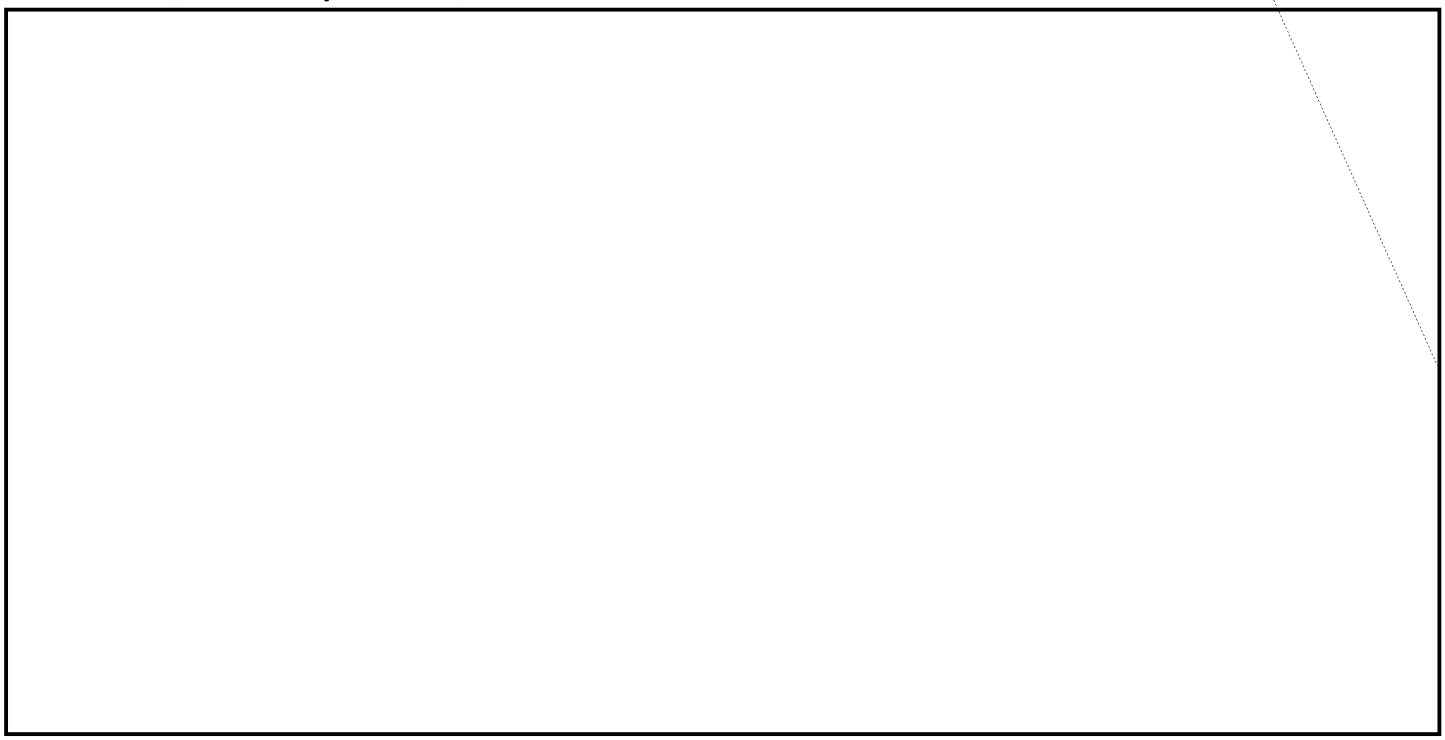
This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

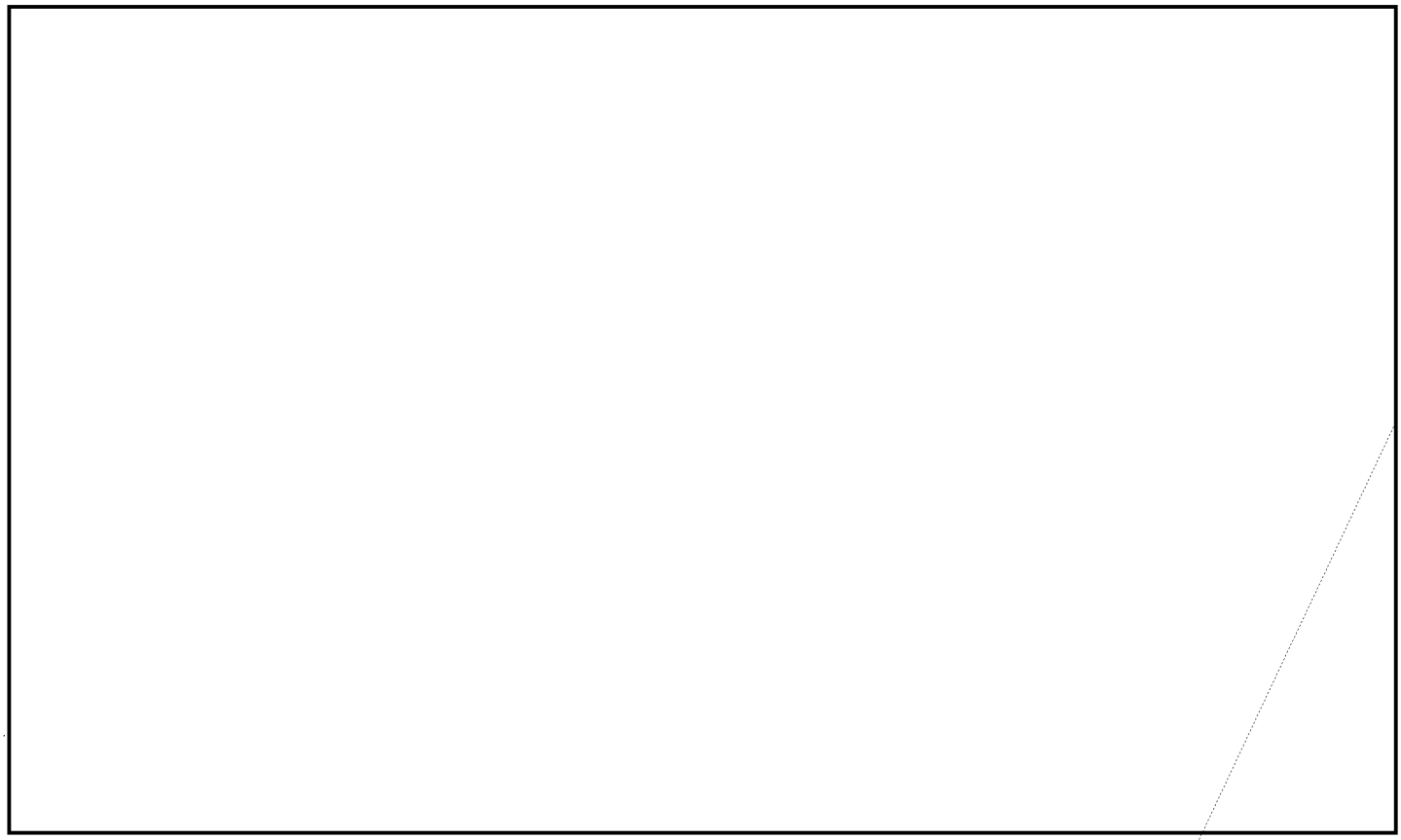
Encl A

This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

9 April 1951

This sheet of paper and all of its contents must be safeguarded with the greatest care.
Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.





This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.