TOP SECRET SUEDE

File

TOP SECRET SUEDE

25 July 1951
AFSA-02T/can

SUBJECT: Forwarding of French Cryptologic Study

TO: AFSA-00T

Forwarded herewith for your information and retention are Copies Number 8 and 9 of AFSA-232 study entitled "History of Collaboration among French Cryptologic Agencies 1909 - 1939."

FRANK B. ROWLETT
Technical Director
Office of Operations

TOP SECRET SUEDE

~~TOP SECRET SUEDE~~ Copy No. 9 ODT

16 July 1951

History of Collaboration among French Cryptologic Agencies 1909 - 1939 as revealed in a file of Ministry of War Correspondence

HISTORY OF COLLABORATION AMONG FRENCH CRYPTOLOGIC AGENCIES 1909-1939 AS REVEALED IN A FILE OF MINISTRY OF WAR CORRESPONDENCE

This paper is based on a collection of documents, dated 1909-1939, from the files of the Section du Chiffre, Deuxième Bureau, Army General Staff, Ministry of War. It is divided into two major sections giving (1) the objectives of the French cryptanalytic services and the proposed methods for achieving those objectives, and (2) a historical account of efforts for closer cryptanalytic collaboration among the various French Ministries, with the results attained. A brief third section contains certain pieces of evidence which seem to have a bearing on the present organization of the cryptologic services in the French Government.

HISTORY OF COLLABORATION AMONG FRENCH CRYPTOLOGIC AGENCIES 1909-1939

I. Objectives of the Cryptanalytic Services and Proposed Methods for Their Achievement

A. Objectives

1. Maximum COMINT results with greatest speed, efficiency, secrecy and economy.

a. Centralization of receipt and distribution of intercepts

b. Liaison on technical cryptanalytic questions

c. Transmission of COMINT to all interested parties

d. Preservation of secrecy of cryptanalytic achievements

e. Central archives and collateral information service

f. Research in complicated cryptanalytic methods (machines)

g. Research in a larger range of languages

2. Preparation for wartime functioning of service

Personnel training

3. Safeguarding of crypto-security

a. Adoption of secure cryptographic systems (including research on new inventions, machines, etc.)

b. Training and supervision of personnel in proper use of systems

B. Proposals

1. Regular liaison among cryptologic service heads

2. Single cryptanalytic bureau

3. Central interministerial cryptanalytic service

II. The Struggle for Closer Collaboration among the Cryptanalytic Services of the Various Ministries 1909 - 1939

A. Pre-World War I Efforts

B. Extent of Wartime Collaboration (1914 - 1918)

1. The first months of the war
2. The situation in 1916
3. The collaboration proposal and failure 1916-17
4. The centralization proposal and the security crisis - 1917
5. The triumph of centralization - 1918

C. Post-War Decline in Collaboration (1918 - 1935)

D. Collaboration Achieved (1938 - 1939)

III. Clues on the Situation since 1940

A. Cryptographic Collaboration

B. Cryptanalytic Coordination

APPENDIX

1. The Single Bureau - from "Note on the Cryptanalytic Service" - 26 July 1916.
2. "Note on a Plan to Reorganize the Cryptanalytic Services" - October 1917.
3. Resolution of the Interministerial Cryptographic Commission on the Subject of Crypto-Security - 20 April 1922.
4. "Plan for Regrouping the Cryptanalytic Services" - 19 February 1938.
5. "Note on the Subject of Interministerial Collaboration in the Matter of Cryptanalysis" (Army proposal) - May (?) 1938.
6. "Central Interministerial Cryptanalytic Bureau" (Navy proposal) 9 May 1939.
7. "Central Cryptanalytic Service" (Air Force proposal) - 24 June 1939.

PART I

Objectives of the Cryptanalytic Services and Proposed Methods of Achieving Them

The principal objectives of the French cryptanalytic agencies, in the view of National Defense specialists, are:

(1) achieving the maximum yield of current communications intelligence with the greatest speed, efficiency, secrecy, and economy,

(2) preparing for wartime functioning of the service, and

(3) (less often stressed) watching over the crypto-security of the national systems.

To achieve these objectives some type of coordination of the various cryptanalytic services was found to be essential. Three types were proposed:

(1) Regular liaison among the heads of the cryptologic services, leaving complete autonomy to the Departmental services,

(2) A single bureau, supplanting the cryptanalytic services of the various Departments and centralizing their activities under an interministerial agency or the Office of the Premier, and

(3) A central interministerial cryptanalytic service, also possibly under the Office of the Premier, devoting itself to coordination of cryptanalytic activities and to "speculative research", leaving a considerable degree of independence of action to the ministerial services.

As will be seen later the first proposal was too loose to be entirely satisfactory, and the second was considered too drastic an encroachment on entrenched positions. The third possibility, combining a strong central directing agency with ministerial autonomy, seems to have gained the most favor.

A. Objectives of the Cryptanalytic Agencies

1. Achieving maximum COMINT results with greatest speed, efficiency, secrecy, and economy.

The attainment of this objective involves:

(a) a centralization of the receipt of all encrypted documents, whether from radio, postal, or telegraphic intercept, or from any other source; and distribution to the proper cryptanalytic section;

(b) the establishing of liaison on technical questions, to permit the sharing of cryptanalytic information and methods;

(c) the regular transmission of communications intelligence to all interested parties;

(d) the reconciling of (b) and (c) with the need to preserve the secrecy of cryptanalytic achievements;

(e) the setting up of a central collateral information service, involving direct contacts with general information sources, press information, and intelligence services, and the establishing of a central library and archives;

(f) the expanding of research to the more complicated cryptographic methods (especially machines);

(g) the expanding of research to a larger range of languages.

Steps (a), (b), (c), and (d) were considered essential from the first by advocates of more efficient cryptanalytic methods. The importance of step (e) was frequently mentioned, but it was not always considered necessary to have a central information service with a library and archives; advocates of liaison did not insist upon it. Step (f) was first advocated in 1938 when the complications of cryptographic methods became a serious problem, revolutionizing the approach to cryptanalytic study. Step (g) was mentioned only once -- in the February 1938 plan for a single bureau.

a. Centralization of receipt and distribution of intercepts

The battle of the intercepts was a hard-fought one, going back to pre-World War I days. In peacetime objections were raised because of the lack of documents for study (many of which were monopolized by the Foreign Affairs Ministry); in wartime it was objected that there was too much scattering of captured or intercepted messages, and that the intercept services were uselessly absorbing many copy and transmission clerks. Besides the

increased danger to operational security engendered by such a practice, there resulted much waste of time both in intercept centers and in cryptanalytic sections, where a duplication of effort often resulted, cryptanalysts of two Ministries working individually on texts of various origins but encrypted with the same systems. In 1938, for example, cryptanalysts in three Ministries -- War, Navy, and Foreign Affairs -- were working on the same Italian diplomatic code without exchanging results.

A single receiving and subsequent distribution center for all encrypted messages was constantly advocated to gain maximum exploitation of all traffic available and to avoid having messages sent to be buried in sections incapable of exploiting them while another section urgently needed them to aid in code recovery. As late as 1938 the complaint was made that this wasteful practice was continuing.

The twin evils of duplication of cryptanalytic effort on some messages and failure to exploit others at all were attributed to the unfortunate practice of the intercept services (both radio intercept and P.T.T.) of distributing traffic purely on the basis of address. Examples were given to show the inadequacy of this procedure: During the War (1914 - 18) the Germans addressed to the Spanish Ministry of Foreign Affairs telegrams intended for their Ambassador and encoded with the Military Attaché's code. The Germans constantly mingled diplomatic, military, and sometimes private addressees to send a single series of telegrams encrypted with the same process. Such tricks were quickly discovered during the war, it was reported, "because, by force of circumstances, the greater part of the intercepted material was concentrated in a single office"[a] (at the War Department). In peacetime, however, for lack of the necessary coordination, there was confusion once more. For example, the 1938 proposal[b] reports that "messages encoded with the German diplomatic code are picked up by the Naval intercept services without being transmitted to the Quai d'Orsay; one part of a correspondence encoded with the aid of the Spanish code was sent to the Navy, the other to the Quai d'Orsay, without its being possible

a. Minutes of 20 April 1922 meeting of Interministerial Cryptographic Commission, P. 3

b. Appendix P. 54

to compare these two texts." a

b. Liaison on technical cryptanalytic questions

The establishing of liaison on technical questions, enabling cryptanalysts of the various Ministries to pool their knowledge and share their discoveries, was recognized to be of prime importance for achieving maximum cryptanalytic progress and avoiding much wasted effort.

As one report of 1922 put it, "We have very few good cryptanalysts, and that is true for all the cryptanalytic services. Now, in some Departments time was spent during the war and before in discovering keys and codebooks which were held by the Ministry next door, and during that time useful tasks were not done." b Another declares "....the capacities or previous studies of one cryptanalyst can be useful to his colleagues. Very recently, in a conversation, a Service Chief spoke of 'recovery work' on a code used by some diplomats, whereas in the nearby Department, where they are accustomed to codes sold commercially, the identity of the code in question had been determined in five minutes. By limiting oneself to certain series of documents, one becomes a specialist in a form of cryptograms that one solves to perfection, but it is useful to get in contact with specialists of the neighboring branch." c

---

a. Before leaving the subject of intercept, it might be interesting to note that in 1922 the War Department was protesting against the restrictions, prescribed by the law of 1852, relating to the communication of foreign diplomatic telegrams by PTT to Sûreté Générale (in the Ministry of the Interior). It seems that these restrictions had allowed the continued communication of Italian diplomatic telegrams to Sûreté for the purpose of training personnel. Sûreté was passing these on to the War Department "for necessary collateral study" until the source was stopped by order of the Premier to PTT. "Because of a convention whose legality does not seem defensible," declares Givierge, "these documents cannot be acquired gratis in a complete series and at the time they would be useful, as they could often be if this convention did not exist." The restrictions, he points out, are not only harmful to cryptanalytic studies but useless and costly since, as a result of the use of the radio, similar messages to those denied Sûreté are picked up (as they can be by any private individual) either by a special intercept station which could be more usefully employed or by still other procedures. He comments, moreover, that cryptographic works claim that "everywhere telegraphic administrations communicate to their governments the encrypted texts which they have transmitted."

b. "Note sur le Chiffre" 12 April 1922 P. 9

c. "Note sur le Service du Chiffre" 13 April 1922 P. 5

Exchanges on cryptanalytic problems among specialists in the various Departments had had other useful results, according to a 1931 summary: [a] (1) Before 1914 discoveries made in the War Department on military radiograms led to the decrypting of an entire police dossier regarding a sovereign's trip. (2) Diplomatic documents translated at the Sûreté gave a code the principle of which, applied to more recent documents, led to the complete reconstitution of very important military documents. (3) It was the decoding of Emperor Charles' letter on a peace proposal, done in the War Department with a code recovered with the aid of military documents, that enabled the Foreign Affairs Ministry to find the first words of the Austrian diplomatic code in French language.

Mention has already been made of the wasteful practice of duplication of effort when two or more sections work on the same code without exchanging results. For these reasons, it was urged that there should be frequent contacts, at least of the heads of the cryptanalytic sections, and perhaps of the cryptanalysts themselves. One proposal was even made (in 1922) for temporary exchanges of cryptanalysts. The intercommunication of dossiers and studies was likewise advocated.

c. Regular transmission of communications intelligence to all interested parties

The keyword here is "all", for there were many complaints during the periods of non-cooperation that, for lack of inter-Departmental communication of certain decryptions, much valuable help was denied cryptanalysts. Much military attaché subject matter was transmitted in diplomatic codes, for example, and it was well known that messages from both military and diplomatic authorities might discuss the same subject, the text of each throwing useful light on the other.

d. Preservation of the secrecy of cryptanalytic achievements

Concern for this point was presumably one of the chief reasons for the continued intransigency of the Foreign Affairs Ministry in the matter of cryptanalytic cooperation. The War Department pointed out the folly, in view of the post-war revelations of cryptologic work, of trying to conceal the existence of cryptanalytic agencies. The important thing was to keep secret the degree of success achieved. As for that, a War Department spokesman pointed out in April 1922,

> "Considering that the personnel employed in these services must be considered as equally secure, that moreover most of the communications (i.e. inter-departmental communication of information) concern especially the service chiefs, who know how to take precautions often neglected by the personnel of all kinds using communications intelligence, it is impossible to see what

a. "Note au sujet de la Collaboration Interministerielle" October 1931, P. 3

the ministerial Departments would have to look in breaking down the barriers raised between their cryptanalytic services." a

In 1917 some security leaks did occur as a result of a rather loose and uncontrolled type of distribution of both the intercepted traffic and the eventual decryptions. When closer coordination was established with centralized control in the War Department, the problem appears to have been solved.

e. Central archives and collateral information service

As early as 1912 at the time of the first meetings of the Inter-ministerial Cryptographic Commission, the value of building up a common library of cryptographic documents of all kinds was recognized. It was considered the most economical method of making available to all the cryptographic services standard works on cryptography, training material, samples of codes, etc. With funds from the Interior and War Ministries a nucleus of such documents was assembled by 1914 and remained in the custody of the Interior Department (Sûreté Générale) during the war. There is no evidence as to its eventual fate.

After the war there were occasional protests at inability to secure certain items of information known to other Departments and necessary for code recovery (e.g. movements of Italian officers in Occupied Germany). In 1922 it was urged that there should be a pooling of outside information, both general and specific (e.g. compromised codebooks). This already was being done between Sûreté, War, and Navy, but much was lost on both sides by the failure to bring the Foreign Affairs Ministry into the collaboration.

f. Research on complicated cryptographic methods (especially machines)

This first was mentioned as a problem -- and a strong argument for a centralized direction -- in 1938. The tendency toward more secure systems and elaborate machines had revolutionized the requirements of a cryptanalytic section. The work could no longer be done by cryptanalysts working individually but required teamwork, with staffs of clerical personnel attached to the analysts for the mechanical tasks. Long-term research projects had to be set up, and this required more extensive personnel than the individual services could afford. As a result the tendency was for these services to concentrate on the easy problems, setting aside the more difficult ones. Yet it was pointed out that in time of war or international stress it was solving of the difficult ones that would be most vital.

a. "Note sur le Service du Chiffre" 13 April 1922 P. 6

g. Research in a larger range of languages

This problem too was first mentioned in 1938. Here again, as in the case of machine research, lack of personnel prevented the extension of research efforts necessary to keep abreast of world problems. During World War I the cryptanalytic services decrypted German, Austrian, Bulgarian, Greek, and Turkish messages "to speak only of enemies", it was reported. In 1938 cryptanalytic research was presumably being done in English, German, Spanish, Italian, Russian, and French,[a] but such important languages as the other Slavic languages and Japanese were being completely ignored.

2. Preparation for Wartime Cryptanalysis

The value of COMINT in wartime depends on speedy decryption. Experience in World War I showed the vital necessity of having, at the very outbreak of war, cryptanalytic specialists methodically trained in peacetime in the encrypting procedures being used abroad. "This preparation is possible," it was declared, "for experience proves that the encrypting processes used during critical periods preceding the declaration of war and the opening of hostilities are similar, if not identical, to those of peacetime."[b]

During World War I, although about thirty officers were recruited for work in the War Department's Cryptanalytic Bureau, "most of them were never able to do more than decrypt a message when given the key; a few were able to recover the key when it changed or to reestablish in order the scrambled pages of a codebook".[c] Those who did the primary cryptanalytic work -- discovery of keys and systems -- were, with but one exception, those who had received pre-war cryptanalytic training, chiefly under the auspices of the Interministerial Cryptographic Commission. The one exception, brilliantly gifted and working under the best conditions for gaining rapid experience, required 18 months before he was able to make significant contributions. Even the trained cryptanalysts were unable to produce results until October 1914, thus losing much valuable intelligence, because most had received theoretical training only, with no opportunity to become acquainted with the particular systems actually in use or with garbled text.

---

a. Appendix P. 54
b. Letter from Minister of War to Director of the Services of the Permanent General Secretariat of the Higher Council for National Defense - 16 Dec. 1924.
c. "Note sur le Service du Chiffre" 13 April 1922 P. 9

One of the strongest arguments presented against lack of coordination in the distributing of intercepts and in cryptanalytic research was the great danger to national defense in preventing the proper training of cryptanalysts for wartime.

3. Crypto-Security

The problem of crypto-security, though less often mentioned in the arguments for cryptanalytic collaboration, was one of the principal reasons for the creation of the Interministerial Cryptographic Commission in 1909. At that time it was pointed out that for lack of liaison one cryptographic section was unable to take advantage of progress made in another, and that less advanced sections were unwittingly using insecure systems.

In 1922 when the Commission held its one and only post-war meeting the situation seems hardly to have improved. It is noted in the minutes:

> "He (the secretary) brought out the fact that in the present service it is to be observed that certain Ministries have codes and ciphers which are entirely inadequate to safeguard their security against cryptanalysts ....For lack of surveillance exercised by qualified people over cryptographers, certain telegrams are drafted by uninstructed personnel, so that the security of the codebook is gravely imperiled. A telegram from a Prefect addressed to the War Department, containing a mixture of plain language and code groups, was placed before the eyes of the Commission, with the remark that the document used for encrypting gives none of the rules to be observed for cryptographic security, and that it seems, from the frequency of such acts during the war, that no organization is provided to call the attention of code clerks to errors capable of imperiling not only their own cryptographic system but also those of the other Ministries. Examples were cited on the latter subject."

This may be compared with the following paragraphs from a "Note on Cryptography", presumably written by Givierge, dated 12 April 1922:

> "In many Ministries the officials responsible for this service have no idea of the successes achieved by the cryptanalytic services, that is, those that work on solving keys and recovering codebooks. The codebooks they prepare are consequently rather simple in the eyes of a cryptanalyst. Moreover, most of them do not know how to use the books and no one teaches them nor watches out for the proper use of the documents.
>
> "Thus during the war prefects used code to report bombing

results, interesting for the enemy to know, leaving almost all the telegram in clear, which is strictly forbidden, and encoding only a few words which were easy to recover. Not only did that endanger the codebook used, but it could have given indications as to the words of the telegram sent at the same time by the military governor, and facilitated progress in the recovery of his code if the enemy by spying or other means had been able to procure the copy of a few pages of this document.

"These bad cryptographing procedures still persist today...."

This matter of the inseparability of cryptographic security was recognized by the War Department's cryptanalysts, as is evidenced by the foregoing statements. It formed the basis of another protest and plea for collaboration in a letter drafted on 1 October 1922 by Givierge, suggesting that a commission be called together to study ways of achieving inter-ministerial cryptanalytic collaboration, especially between the Foreign Affairs and War Ministries. It adds:

"This commission might at the same time examine certain measures relative to the current encoding procedure which were taken without my service's understanding the reason for them; for example, the refusal to use one and the same codebook for the telegrams of the Commissioner General in Morocco addressed both to the War Department and to DIPLOMATIE, which can force the High Commissariat's services to make two encodings of the same telegram, a most dangerous measure for code security."

Actual collaboration in the use of codes and ciphers was otherwise not stressed, however, and in general the right of each Department to have its own secret systems was freely recognized.

There was thus a dual need:

a. to adopt secure cryptographic systems, and

b. to train and supervise personnel in the proper use of these systems.

In 1909 concern centered about the first point, and there followed a pooling of ideas and materials (commercial codebooks, works on cryptography, etc.) among all the Ministries concerned except Foreign Affairs. In 1922 both needs were considered, and a formal resolution was passed by the short-lived Cryptographic Commission, under the inspiration of Lt. Col. Givierge, recommending that the cryptographic bureaus be placed under the supervision of an experienced cryptanalyst.[a]

---

a. See Appendix P. 52

In a note prepared for reading at this meeting of the Commission, Givierge urged that all ministerial Departments transmitting and intercepting messages have a cryptanalytic service "not only to read intercepted traffic but also to provide surveillance over the codes and their use...".[a] This was particularly aimed at the Ministry of Colonies and the PTT, which had cryptographic bureaus only. (An interesting special case, brought out during the Commission's discussion was that of the Sûreté, which had a cryptanalytic but no cryptographic service. All of its telegrams were sent to the "Telegraphic Service" which was managed by PTT employees under the CABINET DU MINISTRE. This service created codes, encoded, and decoded for the Sûreté without supervision and without liaison with the latter's cryptanalytic service. The insecurity of such a procedure was to be called to the attention of the Ministry of the Interior, of which the Sûreté is a part).

Givierge himself evidently favored the combining of the cryptographic and cryptanalytic bureaus under one head, for in a "Note on cryptography" written at this same period (i.e. in 1922) he says:

> "There is no cryptanalytic service (responsible for decrypting the messages of others) except at Foreign Affairs, the Sûreté, and the Navy, (where they are distinct from the cryptographic service proper) and the War Department, where the two services are joined, which seems indispensable for the training of the personnel, the enlightened surveillance of the service, and the maintenance of the codes on a level with cryptanalytic progress."[b]

By 1938 the complications of cryptographic processes, and particularly the use of machines, had led to "frequent and completely cordial contacts"[c] between the head of the Foreign Affairs Cryptographic Service (separate from its cryptanalytic service) and the heads of the War, Navy, and Air cryptologic sections, "especially for the joint study of inventions which might improve cryptographing methods".[c] This seems to have been the extent of the collaboration; existing non-mechanical codes and ciphers were apparently not subjected to tests for security, nor is there evidence of any joint endeavors to check on the security of practices of cryptographic personnel.

---

a. "Note destinée à être lue à la Commission Interministérielle de Cryptographie" 4 April 1922 P. 7
b. "Note sur le Chiffre" 12 April 1922 P. 2
c. "Note au sujet de la collaboration interministérielle en matière de décryptements" -- May 1938

B. Proposals

1. Regular liaison among cryptologic service heads

The simplest method of achieving coordination in cryptanalytic matters was through regular liaison among the heads of the various cryptanalytic services. This had the virtue of achieving some of the objectives, at least in part, without making any changes in organization, which would be likely to be resisted.

Under such an arrangement certain exchanges could be made of intercept material which had been sent to a section unable to use it, of technical information, such as codebook recoveries or encipherment methods, and of collateral information considered of interest to another section. This could be done while retaining the independence of the Departments and localizing responsibility and security leaks.

Its principal disadvantages were that in practice it was rarely possible to achieve liaison among all the cryptanalytic chiefs, and even when achieved such liaison partially solved only a few of the problems to be met. Experience showed that greater compulsion than an appeal to good will, to national interest or even to self interest was required to persuade the Foreign Affairs Ministry to join in the liaison plan; yet without that Department's participation almost none of the major evils in the cryptanalytic situation could be coped with. When, through the persistence of the Premier, that Department was finally brought into a liaison project in 1938, some useful exchanges were made,[a] but it was recognized that such a loose relationship was still too inefficient, uncertain and incomplete for the stern requirements of national security in wartime. The coordination of cryptanalytic effort required the support of some extra-ministerial authority to win acceptance for recommendations and to maintain itself above the whim or convenience of the individual Ministry. Furthermore a tighter organization was essential to make any adequate reforms in the distribution of traffic. To give cryptanalysts a genuine opportunity to interchange technical information, they themselves needed to meet and work together, not only their chiefs. Without a central directing organization, the transmission of collateral information was bound to be irregular and spotty. The use of personnel remained uneconomical: the few cryptanalysts in each Department had to be spread over the same types of problems -- cipher, code, machine problems -- at the expense of extended work on the more complicated of any of these problems.

Thus the voluntary liaison plan, even when it succeeded, was considered, at least by the National Defense Ministries, as only a stepping stone to a more closely knit organization: either a single cryptanalytic bureau,

a. See Part II, page 40

centralizing all the functions of the various ministerial cryptanalytic services and completely supplanting the latter, or a central inter-ministerial cryptanalytic service, formally handling the necessary coordination and engaging in "speculative research", leaving the specific research and exploitation to the various ministerial services.

2. Single cryptanalytic bureau

The concept of the single cryptanalytic bureau, in direct contrast to the liaison idea which sought to preserve the autonomy of the various departmental services, would supplant these services completely, centralizing all cryptanalytic activity in one bureau separate from all the Ministries. When this idea was analyzed,[a] presumably by Giviergo, in 1916, he laid down certain conditions which he considered essential to the success of such an organization: it must be "created outside of all ministries, above the ministries, with a chief who has indisputable authority with the 'grands services' (the PTT and the public prosecutor's department as well as the ministries concerned) a competence as great as his authority in all general questions, military, political, etc.... and who has funds at his disposal."[b] Since he considered it unlikely that these conditions could be fulfilled, he was opposed to such a plan.

a. Organization

It was generally considered that such an organization must be placed under an existing interministerial body or the Office of the Premier. In the plan[b] of February 1938, it was proposed to concentrate all personnel and budgetary resources of the various departmental cryptanalytic services into a single service administratively under National Defense "or under the Office of the Premier (Higher Council of Defense) if the Foreign Affairs Ministry consents to join in the plan."

The organization was to be composed of a section head, "preferably a civilian to ensure continuity", and four or five sections. Each section would include officials, either civilian or military, detached by the Administration to which they belonged (Navy, War, Air, Colonies, Foreign

---

a. See Appendix P. 45 - 57

b. See Appendix P. 46

Affairs).[a] In addition there would be auxiliary personnel, possibly common to all sections, for purely mechanical tasks.

b. Functions

The functions of this organization would be:

(a) to maintain the current service,

(b) to prepare for the functioning of the services in wartime, and

(c) to verify the security of the national cryptographic systems used.

In maintaining the current service a section would be responsible for receiving and distributing all intercepts. (In 1916 Givierge had written that the single bureau would have to direct the intercept services; in the 1938 proposal this is not suggested). There would be an orderly distribution of COMINT to the interested Departments. A central documentation service would assemble all the documents now in the various Departments: dictionaries, reference books, etc. A press service would be organized. A study group would do research in new systems, inventions, machines, etc. Cryptanalytic work of all types from initial study to final exploitation would be carried on in this organization; cryptanalytic results (code recovery, observations on encipherment systems, etc.) would be communicated to the various sections. The individual Ministries would be allowed to do cryptanalytic work only for special well-defined missions, and the Central Service would be kept informed of the results.

---

a. There is some confusion in the plan at this point. These sections, according to the proposed table of organization, Appendix P 57, would be divided on a linguistic basis: English, German, Italian and Spanish, Russian, French, etc. This idea is also borne out in the advantage noted: "By having knowledge of all the systems used in the same country, one will more easily be able to ascertain the habits and enciphering systems of that country's services and reconstitute the principle which is being established on the other side."

On the other hand, as one of the assurances to the various Departments that their secrets would not be divulged to other services, it was stated that "In principle, each section, composed of agents responsible to a given Ministry, will work only on messages of interest to that Ministry and will have no knowledge of texts of interest to the other sections." This implies a primary division into sections for Army, Navy, colonial, diplomatic traffic etc. A possible interpretation is that the primary division would be by language, and a secondary division within the language sections would be by Ministry, but the evidence is conflicting.

As for maintaining security, Givierge had argued in 1916 that "security consists not in concealing the existence of services to which all the dime novels allude, but in concealing the exact nature of the work being done and the list of projects under study there". In 1938 three security measures were incorporated into the plan in an effort to reassure the various Departments that their secrets would not be divulged to other sections: (a) decryptions would be communicated exclusively to the ministries concerned: (b) agents from a given Ministry would work, in principle, only on messages of interest to that Ministry and would not be given knowledge of texts of interest to other sections; and (c) only the cryptanalytic results would be communicated to the various sections.

The organization would prepare for the functioning of the service in wartime by training reserve personnel and developing a thorough knowledge of the systems and encrypting habits of countries with whose traffic it was advantageous to be familiar.

c. Advantages

The advantages of the single cryptanalytic bureau were numerous:

(a) All traffic would be sent to a single service which would distribute it on a cryptanalytic basis, i.e. on the basis of type of system used and not exclusively on the basis of address and signature. This guaranteed the exploiting of all traffic. By having more traffic and, especially, complete series of messages from the same sender, cryptanalysts would have better chances of success.

(b) By pooling personnel it would be possible to make more economical use of them and thus to extend work to new languages and to engage in long-term research projects on the more complicated problems.

(c) By working in close proximity it would be possible for the cryptanalysts to interchange special knowledge and experience to mutual advantage.

(d) A centralization of all documents and collateral information would result in a much more complete and efficient reference service with less expenditure.

(e) A more uniform and rational training of personnel would be achieved.

d. Disadvantages

Many disadvantages to such a drastic proposal were presented, however. In his "Note on Cryptography"[a] written in April 1922 Givierge, speaking of a single cryptanalytic service, says:

> "Efforts have been made toward it several times and plans for it were even made during the war. These never succeeded because the Ministries want to be sure of obtaining detachments of personnel for special positions if they need them (e.g. the War Department for the armies in wartime), and to be able to have documents which interest them studied at once. Too great a specialization in military or diplomatic questions, for example, has always been feared. Now, the Foreign Affairs Ministry has never accepted even the idea of a control over the tasks which would establish a priority order."

Other elements pointing to the undesirability of complete unification were noted by him as follows:

(1) Diversity of problems: the profound differences between systems for correspondence of individuals, banks, etc. on the one hand and official systems (Diplomatic, War, and Navy) on the other hand;

(2) Value of specialization: the value, if one wishes to be able to make cryptanalysts into specialists and to obtain a good output, of assigning the various categories of cryptograms to separate study groups;[b]

(3) Need for departmental autonomy: the necessity for a ministerial Department not to be allowed to have recourse to another when a question of secret correspondence is involved in an affair in which it is concerned;

(4) Crypto-security: the need of having in the Administration qualified personnel to draw up cryptographic documents and to oversee their use;

(5) Administrative difficulties: the difficulties for various reasons, arising for example from the status of the officials, of having the rare cryptanalysts leave their present Administration;

(6) Size of task: the enormous quantity of documents susceptible of study and the material task of classification and of setting up archives.

---

a. "Note sur le Chiffre", 12 April 1922, P. 9-10
b. This argument seems hardly valid here, since such specialization is not incompatible with the idea of a single central bureau.

In 1938 a War Ministry note comments that:

> "The fusion of the existing cryptanalytic services seems difficult to achieve for reasons of command, recruitment, instruction and mobilization, and for material reasons (buildings, credits)."

The most valid fears with respect to a single cryptanalytic bureau seem to have been that:

(1) It might be dominated by one Department to the disadvantage of another;

(2) Special interests might be ignored or given low priority;

(3) The Departments would have no control over the topics studied and would be unable to assign analysts to special jobs; and

(4) Cryptographic sections would be deprived of the necessary criticism and guidance of cryptanalysts (unless the single bureau were made responsible for all cryptographic functions as well).

Although verifying the security of the national cryptographic systems was named as one of the functions of the single cryptanalytic organization in 1938, no expansion of the idea is given in the plan advanced. This would presumably involve studying the systems to test whether they would be highly resistant to cryptanalytic attack (it is not clear whether this includes checking their actual use for violations of crypto-security), but it does not imply a centralization of the individual services nor even direction by a cryptanalyst. In 1916, however, when Col. Cartier had proposed a centralization of cryptanalytic services only, Major Givierge had pointed out that the cryptographic services must, in that case, be centralized as well since they "must be directed by cryptanalysts" who will "instruct the operating personnel and prepare the documents." a

This point was, in fact, used as a strong argument against a single cryptanalytic bureau. In a "Note on the Cryptanalytic Service" in 1922 it was stated:

> "One can fail to be in favor of a plan of this nature if one does not wish to make this central agency responsible for the surveillance of the application of the French codes and ciphers in the various ministries. It is necessary, in fact, in our opinion to prevent the agents who use our codes and ciphers from using them carelessly. The qualified authority seems the Ministry to which they are responsible. Now to

---

a. See Appendix P. 45

watch over a cryptographic service properly, it is necessary, we think, to have cryptanalysts who, using the mistakes of others, know which ones must be avoided. The necessity of a separate service in each Ministry, as we have today, is therefore very readily justified." [a]

For these reasons the tendency was to favor the third possibility --- a central interministerial cryptanalytic service --- which would combine many of the advantages of a single bureau with fewer disadvantages.

3. Central interministerial cryptanalytic service

The central interministerial cryptanalytic service, originally envisaged as a purely coordinating agency, would have, as finally evolved, two major responsibilities: coordinating the work of the various ministerial cryptanalytic services, and engaging in "speculative research", leaving the specific research and exploitation to those services. This proposal avoids at the same time the Scylla of loose collaboration, where the heads of the various cryptologic sections meet under some persuasion to patch up here and there a few of the deficiencies of an uncoordinated system, and the Charybdis of complete unification of cryptanalytic activities, depriving the Departments of any cryptanalytic personnel. Such a central office was presented chiefly as a wartime measure, however, proposals for it being most numerous and urgent before and during World War I and again in 1938 -39 when World War II was threatening. The most specific of these proposals, reproduced in the Appendix, were Col. Cartier's 1917 plan for reorganization of the cryptanalytic services (presumably adopted for the last year of the war) and the Army, Navy, and Air Force plans of 1938 -39.

a. It was originally planned to place this coordinating group under one of the Ministries: in 1914 the cryptanalysts were intended to be under Interior, in 1917[b] the service was to be handled by the War Department, and at the end of 1918 it was proposed that all cryptanalytic work on peace negotiations be done under the aegis of the Foreign Affairs Ministry. From 1925 on, however, it was generally recognized that such a coordinating organization must be under interministerial control -- possibly the Office

---

a. "Note sur le Service du Chiffre" 13 April 1922 P- 2

b. Cartier had proposed that the cryptanalytic service, rightfully an organ of intelligence, should be attached to a General Intelligence Office, then non-existent. (This notion was immediately rejected by his superiors "because of the special nature of the intelligence utilized by the Department of War"). He suggested that under present conditions it be attached to the War Ministry at least for the duration of the war, but added that it could be under the Foreign Affairs Ministry or even the Office of the Premier.

of the Premier or, more usually, the Higher Council of National Defense. In the Army's 1938 note[a] it was proposed to place it under one of the Ministries of National Defense or the Higher Council of National Defense. The Navy proposal[b] later, however, insisted that it must be placed under an authority superior to the Ministries, giving as reasons:

(1) The easier participation of the Foreign Affairs Ministry;

(2) The possibility of using qualified civilians as research workers(e.g. former military cryptanalysts of real competence whom it would be difficult to employ in a subordinate position in a military agency).

b. Personnel was to be obtained from the ministerial cryptanalytic sections. (In 1917 a delegate from the Office of the Premier was to be included). The Navy suggested that each Ministry might contribute two or three persons of officer rank and if possible an equal number of secretaries; the entire Navy plan was more limited, however, making general cryptanalytic studies the only function of the service (excluding coordination).

c. The major proposals (except Navy's) involved a two-fold role for the central cryptanalytic service: research on all cryptanalytic questions of general interest, and coordination of the work of the various ministerial services.

The research aspect of the work would involve:

(1) Preliminary study of new systems intercepted to determine their general nature. When a system had reached a point where it could be handled by the proper ministerial service, it would be turned over to the latter with all necessary information for continuing the study (e.g. recovery of particular keys or bookbreaking) or for exploitation.

(2) General study of new cryptographing processes (machines, electromechanical or electromagnetic processes, etc.) with attempts to establish decrypting methods. This includes critical study of all inventions and systems proposed for adoption by the various Departments.

The coordination of the work of the various cryptanalytic services would involve:

(1) centralizing the receipt of all intercepted traffic;

(2) distributing it by system and category, not solely by address;

(3) establishing liaison among the various groups to get the best results while limiting and localizing responsibilities;

---

a. Appendix P. 58-59
b. Appendix P. 60

(4) setting up and maintaing a repository of documents and technical information regarding enemy encrypting systems and their use;

(5) setting up and maintaining a card file of each country studied and giving each group information to help its work;

(6) establishing direct relations with intercept and intelligence services as well as with the exploiting services in the various Ministries;

(7) setting up a press service for information purposes (and the Air Force suggests working with the Press to censor any publications likely to imperil crypto-security);

(8) making the necessary communications in the proper form to the services concerned.

d. To achieve these purposes, the Army and Air Force made generally similar proposals for organization:

(a) A director and assistant

(b) An archives or classifying section responsible for:

(1) receipt, classification and distributing of intercepts

(2) distribution of decryptions

(3) centralization of information and documents of any nature

(4) setting up and maintaining of card files of cryptanalytic information

(c) A liaison section, maintaining close relations with the departmental services and with the Information, Intelligence and Press Services

(d) A technical or study section responsible for:

(1) preliminary research after traffic classification

(2) study of systems, machines, cryptographic inventions

(3) checking on the security of national cryptographic systems.

(e) A translation service of plain text intercepts

The departmental cryptanalytic services would retain their autonomy to a considerable extent, handling their own recruitment and training of personnel. Since close and constant liaison was necessary among all the groups, however,

it was frequently urged that they should work in the same spot or at least in close proximity to each other. Another argument for proximity was the ease of establishing and using the central archives and information section. On the other hand, many advocated physical separation for the sake of localizing responsibility and reducing the chances of security leaks. Furthermore, as long as the various cryptanalytic services remained under control of the separate Ministries, there were bound to be administrative objections to detaching them physically.

e. The advantages of the central interministerial cryptanalytic service are many. It gives form and authority to the long-desired interservice liaison, and at the same time permits centralization in the important field of general research on new systems and machines.

f. One disadvantage of the proposal lies in a certain amount of duplication of documents and information services, and the necessity of separate archives, where there is physical separation of the various decrypting groups. More important is the undesirability of separating preliminary cryptanalytic work from its later stages. It was presumably Cartier who in 1916 presented that view:

> "It would be a grave error if one were to think that the cryptanalysts must be satisfied in finding the elements of a codebook or of a system without codebook, and that they can then leave to others who are less expert the task of decrypting by means of the elements discovered by them.
>
> "It is on the contrary indispensable that they themselves carry out the decrypting , or at least remain in close liaison with those who do so, in order to familiarize themselves with the special phraseology of the enemies and with their cryptographic mentality so that they may be able to find as speedily as possible the new codes or the new cryptographic system that are placed successively in service.
>
> "Our enemies in fact use many codes and various systems, each of them complicated by frequent transformations.
>
> "Certain texts, encrypted with a known system, often give very useful indications for finding those encrypted with other unknown systems, especially considering that the same subjects are sometimes in texts encrypted with different systems, sometimes in the same words."

Later, however, the same writer adds,

> "It should not be thought that it is essential to bring together in the same building all the sections which are charged with different categories of decrypting. There can even be an advantage in separating them in order to localize responsibilities and to reduce the chances of indiscretion."

Another disadvantage, corrected by the single bureau plan, lies in the failure to bring together all the systems -- military, naval, colonial, diplomatic, etc. -- of a given country into one section. Not only does a military message sometimes throw light on a diplomatic one, as they well knew, but the duplication of linguistic personnel is in no way reduced without such unification. Opportunities for extension of study to other important languages without increasing the total personnel would be therefore eliminated.

In a War Ministry note of 7 March 1938[a] it was observed further: "The creation of a centralizing body under the form of an Interministerial Office of Cryptanalytic Services, leaving to each Department its autonomy, would require supplementary personnel difficult to recruit and rather large credits."

In spite of some disadvantages, however, this solution, a compromise between maximum independence and maximum efficiency, found more favor than any other.

---

a." Note pour le Cabinet Militaire du Ministre", 7 March 1938, P. 2

PART II

The Struggle for Closer Collaboration among the Cryptanalytic services of the Various Ministries 1909 - 1939

The advantages of interministerial collaboration of the cryptanalytic services were early recognized by specialists in the War Ministry, and their efforts to achieve this goal over a 30-year period are revealed in a collection of documents from the files of the Cryptologic Section, Deuxième Bureau, Army General Staff, Ministry of War.

A. Pre-World War I Efforts

Around 1908-09, when the first suggestions were made for interministerial cryptographic consultation, this was the situation: Two centers of cryptographic study were functioning regularly and in a practical manner in Paris -- within the Foreign Affairs Ministry and at the Sûreté Générale in the Interior Ministry. In the War Ministry there was a Cryptographic Commission which, presumably for lack of documents, worked chiefly on theoretical problems. One of its missions was that of making codebooks.

In 1908 General Berthaut, President of this Military Cryptographic Commission, deploring the complete isolation of the various cryptographic services in the Government, proposed to the Minister of War the creation of an Interministerial Cryptographic Commission. He stressed its utility in time of peace for guarding French cryptographic security, pointing out that progress in encrypting methods remains localized for want of proper liaison, and less advanced sections are unwittingly using insecure cryptographic procedures. A pooling of ideas and materials, including commercial codes and books on cryptography, would be not only in the general interest but also in the particular interest of each section (whose independence in matters of organization and procedures would not be affected). General Berthaut emphasized, in addition, the need of preparing for readiness in time of war a "reading and supervising committee" to watch over encrypted correspondence. This was later expanded to the idea of a "cryptanalytic committee".

The proposal was submitted by the War Ministry to the other Ministries concerned: Foreign Affairs, Navy, Interior, Colonies, and Public Works (Post, Telephone and Telegraph). Agreement was easy with all but the first. Finally all agreed on a draft decree, which ultimately the Minister of Foreign Affairs refused to sign. This was the first manifestation of the non-cooperative attitude of that Ministry which was to run like a recurring theme through the next thirty years. The draft decree was then modified to exclude the Ministry of Foreign Affairs, and was signed on 9 January 1909 by the Ministers of War, Navy, Interior, Colonies, and Public Works.

This decree, submitted on 11 January 1909 by the Minister of War (G. Picquart) for the approval of the President of the Republic, set up an Interministerial Cryptographic Commission under the chairmanship of the President of the Military Cryptographic Commission, with membership consisting of representatives from the Cryptographic Services of the five Ministries concerned. The purpose of the Commission was "to study under what conditions the cooperation of the various cryptographic bureaus can be organized either in peacetime or in wartime".

Between 1909 and 1912 the role of this Commission seems to have been limited to personal contacts and the exchange of technical notes among some of its members. In 1912, when Millerand was first Minister of War, the War Ministry's Cryptographic Section was created, probably under the inspiration of Captain Givierge, then a member of the Minister's personal staff, who was particularly interested in cryptanalysis and who for many years figures prominently in the struggle for interministerial collaboration in the field.

Under the new impetus the first formal meeting of the Interministerial Cryptographic Commission took place on 14 May 1912. The prime objective now became the organization of the Cryptanalytic Committee (Comité de déchiffrement), in which the Foreign Affairs Ministry had been invited to participate. Again that Ministry was not ready to cooperate. Although it had appointed its representatives, it refused to divulge their names or order them to participate in the committee's work until the "moment of need". The Commission decided that it could not await that moment to begin to create so complex an organization, and proceeded to take steps in that direction without the cooperation of the Quai d'Orsay. A small group of men intended to form the nucleus of a cryptanalytic organization in the event of war was, therefore, given instruction, and a library of technical books and other reference material was developed.

Seven meetings of the Commission were held at intervals between 14 May 1912 and 16 June 1914. A practice exercise held in April - May 1914 showed gratifying results for the training which had been given over the past year to the budding cryptanalysts, but there was a recognized need for recruiting more trainees.

During this time, according to one somewhat embittered account, the Foreign Affairs Ministry had succeeded, following various incidents, in cutting off from the Sûreté Générale (Interior Ministry) the principal source of its material for study. The Navy Department, whose radio service was supplying the War Department with precious documents for study, was urged to have a special section, but lack of personnel prevented this step. At this point the outbreak of war altered the picture.

B. Extent of Wartime Collaboration (1914 - 1918)

1. The first months of the war

Upon mobilization the control and cryptanalytic service was supposed to begin functioning. When specific physical questions had arisen, however, with respect to the setting up of the Cryptanalytic Committee, a curious spirit had been encountered: there would be no war; besides, in case of war no encrypted telegrams would be sent. Thus the existence of the Cryptanalytic Committee remained in the realm of the vague. There was scarcely even an awareness of its existence, and, in any case, of its degree of preparation. When war broke out, the role of the various groups was to be as follows:

a. The Sûreté (in the Interior Department) would direct especially the interministerial telegraphic control service. (It was to this agency that the cryptanalytic group was first assigned.)

b. The War Department would concern itself particularly with radiograms from the front and would give GHQ the means of translating them.

c. The Foreign Affairs Department, which promised to furnish personnel for service (a), would continue its peacetime work.

The telegraphic control service, however, was improvised under the direction of personnel knowing nothing about the special service of cryptanalysis and its potential value. Discontent over mismanagement of the service and poor utilization of their skills led to the disappearance in a few days of the cryptanalysts trained for the cryptanalytic committee. Some went to join Captain Givierge at GHQ; others to the cryptanalytic section of the Navy, War, Interior, and Foreign Affairs Departments. All the Ministries set to work and achieved considerable results, but lack of adequate preparation led to annoying delays in the receipt of documents by the cryptanalytic sections and prevented the reading of encrypted traffic in the vital first months of the war.

2. The situation in 1916

In July 1916 the multiplicity of separate cryptanalytic agencies, with the attendant evils of duplicated effort and inadequate liaison among them, became the subject of a note[a] presumably emanating from Major Givierge at GHQ.

---

a. "Note au Sujet du Service de Déchiffrement" - 26 July 1916

He listed the following cryptanalytic services then existing:

a. at Foreign Affairs;

b. at the War Department under Colonel Cartier;

c. at GHQ, where in theory the task of the section was to make rapidly available to the Intelligence Bureau decryptions made with systems and keys found by the War Department's cryptanalytic section, but where, in practice, under Major Givierge joint studies were being made with that section;

d. in Interior (Sûreté Générale), where, under M. Haverna, study particularly concerned documents collected through the postal control; documents collected through the postal control particularly were being studied;

e. at the Navy, where work was done chiefly on the discoveries of the War Department's cryptanalytic section.

This he considered an abnormal situation, to be explained only if the documents could be strictly classified according to the service. Since, he claimed, practice shows such a classification to be far from possible, there was a duplication of work.

The following liaisons existed:

a. Colonel Cartier (War) and M. de Courcel (Foreign Affairs) collaborated.

b. Major Givierge (GHQ), ignored by Foreign Affairs, collaborated with Colonel Cartier, but without being able to obtain through him the useful information withheld by Foreign Affairs.

c. M. Haverna at Sûreté Générale worked absolutely apart, lending to Colonel Cartier or Major Givierge certain codebooks in his keeping, and scarcely seeing them except on those occasions to exchange some exceptional information. His abilities were therefore poorly utilized.

Close liaison between the War and Navy departments goes without saying since the former provided keys and probably reconstructed codebooks for the latter.

A division of labor had been made between the War and Foreign Affairs cryptanalytic sections on the basis of the destination and call signs of intercepted messages, a basis soon found to be highly fallible. In 1915 the GHQ cryptanalytic group, finding it impossible to secure from Foreign Affairs the contents of certain telegrams, known to be military, which were vital to their research, determined to ignore the agreement and undertake the study of all telegrams received when their diplomatic nature was

not immediately apparent. These were communicated to the War Department. Thus, in July 1916, it was pointed out that a single radiogram might be decrypted three times: once at GHQ, once at the War Department, and once at the Foreign Affairs Ministry. It was admitted, however, that such an occurrence was fairly rare in fact.

There was overlapping also between the Army and Navy. The latter had created a service, apparently to avoid depending upon the overworked Army section, for the decryption of documents of interest only to it, yet the Army in its search for daily keys was obliged to continue the decryption of Navy radiograms. Moreover, GHQ was decrypting some of those relating to meteorology and zeppelins and was examining them all.

3. The collaboration proposal and failures 1916-17.

Dissatisfied with this state of affairs, the Army spokesman proposed collaboration "to avoid having the same telegram decrypted three times, having the same study made in several places without the discoveries of one benefiting the other, having documents which might facilitate the recovery of an unknown code or encipherment remaining unused in another section". [a]

After first examining the alternative of creating a single central[b] cryptologic bureau, which he feared might become the monopoly of one ministerial Department to the detriment of the others, he recommended "the physical separation of the different services with genuine, complete collaboration without reservations". This collaboration would take the form of regular meetings of the heads of the cryptanalytic services, and if need be, of the cryptanalysts themselves, to divide up the tasks and to exchange remarks. Such contacts would acquaint each service with the problems, needs, and activities of the others, and would enable them to share documents and information of value to each other.

Some time later, presumably in late 1916 or early 1917, a meeting called by the Navy Minister took place at the Foreign Affairs Ministry, under the chairmanship of M. de Margerie, its director of Political Affairs -- a diplomatic gesture intended, doubtless, to give the Foreign Affairs Department a greater sense of responsibility in the matter of cryptanalytic cooperation. This move fell wide of its mark, however, for although it was unanimously recognized that it would be advisable to bring about effective cooperation of the cryptanalytic services of the Army, Navy, and Foreign Affairs Department, M. de Margerie promptly made reservations with respect to the study of foreign diplomatic systems which he considered should be exclusively handled by the Ministry of Foreign Affairs. No suggestion was made at the meeting as to the manner of achieving the desired cooperation. It was merely decided that the crypteralytic service heads of the three

a. "Note au sujet du Service de Déchiffrement" - 26 July 1916 P. 10-11
b. Appendix P. 45-47

Ministerial Departments would meet periodically when convened by M. de Courcel, head of the Cryptanalytic Service at Foreign Affairs.

Two such meetings took place at which, in the opinion of the War Department's representative (presumably Colonel Cartier), no useful results were obtained. Even his offer to collaborate by communicating all decryptions to the Foreign Affairs and Navy sections was turned down. He complained that at the second meeting M. de Courcel rarely asked some information concerning the radiotelegraphic service, thus interrupting the work of three officers, one of whom (probably Major Givierge) had come from GHQ, on a matter which was not in their province. He went on:

> "At this same session, the naval representative, Commander Friocourt, proposed bringing to the following meeting an American enciphered code to show it to the commission. There is reason to marvel at seeing, in time of war, the postponement to an indeterminate date of the examination of a question of this nature. This 'following' meeting has not yet taken place."

4. The centralization proposal and the security crisis - 1917.

Colonel Cartier, calling such meetings useless and a waste of time, outlined the basis of what he considered a really effective collaboration of the cryptanalytic services and the manner of achieving it. He protested that there is not a military cryptanalysis and a diplomatic cryptanalysis but that cryptanalytic problems are generally the same whatever may be their subject matter. Without considering it necessary to bring together all the different sections to one working place, he nevertheless emphasized that "a single administration is absolutely necessary to centralize the receipt of all encrypted documents for study, to handle the division among the different sections, to follow the work of each group and to enable each of these to benefit from the results obtained elsewhere".

These ideas, although informally approved by Admiral Lacaze, Navy Minister, lay fallow until an incident of a leak to the press in October 1917 aroused concern in higher echelons and elicited proposals from the Army's General Staff to tighten cryptanalytic security:

(1) To reduce to three the number of copies of decrypted secret radiograms distributed -- all within the War Department;

(2) To paraphrase messages being communicated for information;

(3) To communicate encrypted texts coming from the War

Department's intercept services to no cryptanalytic service of the other Ministerial Departments.

Colonel Cartier, commenting on these proposals, which were for the most part a retreat from even the small degree of collaboration that had been so painfully won, throws light on the degree of cooperation realized by the War Department at that time:

(1) Five copies of the radiograms in question were being regularly distributed within the War Department and in addition those of special interest to them were being communicated respectively to the Premier's office, to Foreign Affairs, and to the Navy. Colonel Cartier suggested that these recipients should be consulted before being dropped from the distribution list.

(2) He agreed to the proposal that originals be replaced by paraphrases but felt that the work must be done within the cryptanalytic section.

(3) Since the War Department's intercept service was regularly furnishing the Navy and Foreign Affairs cryptanalytic services with intercepts of special interest to them, Colonel Cartier protested that they could not be cut off without a previous understanding.

This crisis afforded Colonel Cartier the opportunity to gain a hearing for his own theory of an interministerial office of the cryptanalytic services, and he lost no time in presenting its advantages, with emphasis on gaining the maximum efficiency from the various cryptanalytic services with a minimum danger of security leaks. He sent his proposed reorganization plan[a] to his own superiors (the Army General Staff), to Foreign Affairs, the Navy and the Office of the Premier.

5. The Triumph of Centralization - 1918

That he achieved his purpose during the last year of the war is fairly apparent from the following bits of evidence:

(1) A reply from the Army General Staff in November 1917 presents "no objections" to the proposed reorganization (with reservations, however, on the reference to a General Office of Intelligence Services).

(2) In answer to queries on 24 October 1917, 14 November 1917 and 8 January 1918, the head of the Army Deuxième Bureau's intercept services assures Colonel Cartier on 13 January 1918 that his section alone

a. See Appendix P. 48-51

will receive all encrypted documents intercepted, since that is "the only one qualified to handle the decrypting of them". This could signify a retreat from the spirit of collaboration, but it is more probably a move toward centralized control, with the Army as the centralizing agency. Colonel Cartier, in the 8 January 1918 letter, had declared to the intercept services:

> "It is obvious that it is indispensable to centralize in the Cryptanalytic Section the study of all the encrypted documents or to leave it up to this Section to seek whatever qualified help is necessary. This organization is in conformity with the understanding reached with the Ministry of Foreign Affairs and the Navy".

(3) That the Army Cryptanalytic Section received cryptograms intercepted by other agencies as well, and that it acted as a central cryptanalytic, coordinating, and distributing agency may be implied from later comments. In a speech before the post-war meeting of the Interministerial Cryptanalytic Commission in April 1922, Lt. Col. Giviergo reviewed the wartime triumphs of the Cryptanalytic Section of the War Department, noting that:

> "One of the reasons for the excellent output of the Service was the abundance of the study documents and the concentration by the very force of circumstances of the greater part of them in a single office. Thus false addresses (the sending of German military telegrams to the Ministry of Foreign Affairs of a neutral power, etc.) and ruses in the use of codebooks without regard to content or addressee of the telegrams did not prevent recognition of the true addressees, the language of the correspondents, and the codes they were using; and the distribution of the telegrams (military, naval, diplomatic) among the Departments which had to use the intelligence in them was handled under the best conditions to ensure both the collaboration and the independance of the Ministries concerned. (The latter, as they knew how to do it, decrypted the documents, the key of which had often been found thanks to reciprocal help)."

In a letter of October 1922, reference is made to the preponderant share of the cryptanalytic work which was done by the Army Cryptanalytic Service during the war and "the help that it furnished particularly to Foreign Affairs in the discovery of systems and the communication of codebooks reconstructed at the War Department".

(4) Whereas in October 1917 Colonel Cartier had stated, "No intimate liaison has been established among the cryptanalytic services of

the various Ministries possessing them: Foreign Affairs, War, Navy, Interior (Sûreté Générale)," on 20 December 1918 he speaks of M. Hermitte, current head of the Cryptanalytic Service of the Foreign Affairs Ministry as a man "with whom I have collaborated intimately."

The 1918 period came therefore to be regarded in the post-war years of frustration as the Golden Age of cryptanalytic cooperation. At the post-war meeting of the Interministerial Cryptographic Commission in 1922 Lt. Col. Givierge reported that the War Department's Cryptanalytic Bureau in the month of July 1918, for example, decrypted nearly 1000 political or highly informative telegrams, not to mention hundreds of radiograms from the Command at the front, communications from submarines and from planes.

C. Post-war Decline in Collaboration (1918-1935)

After the war the Sûreté, and the Navy and War Departments continued to collaborate as before, but the Foreign Affairs section, after collecting from the other departments all the documents that it considered "diplomatic", refused any kind of collaboration. Repeated but vain attempts were made by the perennially optimistic heads of the War Department's Cryptanalytic Section, first Colonel Cartier and later Lieut-Colonel Givierge.

In December 1918, seeing the recent war-time collaboration in danger of falling apart with the transfer of M. Hermitte, who had been head of the Foreign Affairs Cryptanalytic Section, Colonel Cartier proposed a closely knit organization, attached to the Premier or to the Foreign Affairs Ministry, to handle the cryptanalytic work during the period of peace negotiations.

On 27 December 1919 a "Note from the Cryptographic Section of the War Ministry relative to the Centralization of the Cryptanalytic Services" was submitted to the Minister of Foreign Affairs for his opinion by the Premier, who was also Minister of War.

On 4 January 1920 the Minister of Foreign Affairs, while protesting that "my Department has, especially during the last few years, given its attention to establishing increasingly close contact between its cryptanalytic service and that of the War Ministry" announces that

> "Major insurmountable reasons of an internal nature and of principle, however, stand in the way of the adoption of the conclusions presented for a concentration of the cryptanalytic services, and the arguments of wartime cannot, in my opinion, be invoked in time of peace for the joining of similar services which henceforth have to occupy themselves with texts of quite different character which are of interest to our respective Departments".

As long as the Premier was also Minister of War, the Quai d'Orsay communicated some decryptions made by its Services ("green documents") to the War Department's Cryptanalytic Service. In January 1922, however, when Poincaré became Premier and Minister of Foreign Affairs, he ordered these communications to cease, but on the other hand he insisted that the War Department and the Sûreté Générale communicate all decryptions to the Foreign Affairs Service. (According to Lieutenant-Colonel Givierge, the War Ministry's Cryptanalytic Service was decrypting nothing at the time. The only light thrown on the reason for this state of affairs is:

(1) His complaint that intercept stations were still busy picking up German or Russian diplomatic correspondence for Foreign Affairs -- decryptions of which were never communicated to the War Department -- instead of working on the interception of other European stations which would be of more interest to his Service.

(2) The comment that the cryptanalysts require texts encrypted with sufficiently simple systems so that they can be studied fruitfully under the peacetime conditions of light traffic, good encrypters and few garbled telegrams.)

On 4 February 1922 the Minister of War, M. Maginot, wrote to M. Poincaré, pointing out the importance of continuing the communication of certain decryptions, and asking that the decision to halt them be reconsidered. (This request was ignored). He also brought up once again the need for more intimate collaboration among the cryptanalytic services of the two Departments, and invited the Foreign Affairs Ministry to participate in the work of the Interministerial Cryptanalytic Commission, now being revived for the first time since 1914. He even offered to study with Foreign Affairs a reorganization of the body and the attaching of it to the Office of Services of the Higher Council for National Defense (Direction des Services du Conseil Supérieur de la Défense Nationale) under the Office of the Premier. Citing the Foreign Affairs Minister's note of two years previously, 4 January 1920, M. Maginot goes on to say:

> "I will ask you to be kind enough to inquire into whether, without speaking of concentration of the cryptanalytic services, there might not be reason to strengthen collaboration among them in a practical way, instead of re-establishing watertight compartments, the disadvantages of which you yourself indicated in the above-mentioned dispatch. The question of texts 'of very different classes' cannot in fact be usefully set forth when what is at issue is not the exploitation of the content of foreign telegrams but the discovery of their keys: in fact the addresses do not mean very much with respect to the real addressee (the war clearly showed this) and until it has been possible to read a telegram, its content is not known for the purpose of

determining which Department it concerns. Now at present, as before the war, for lack of an over-all direction or an understanding among the chiefs of the Cryptologic Services, it is easy to prove that certain materials which reach a Ministry, through the Intelligence Service, for example, remain unused, without a serious effort's being made to get out of them all they can yield, since the existence of the needed texts or of complementary information is not always well known to the service that holds these materials."

When no reply was received to this note, Lieutenant-Colonel Givierge, under pretext of recovering a loaned codebook, sent an officer in March 1922 to see M. Berteaux, head of the Foreign Affairs Cryptanalytic Section, to learn the reaction. He learned that the letter had not been well received at the Foreign Affairs Ministry. M. Poincaré had formally ordered that there be no communication of decryptions from Foreign Affairs, and agreed only to the consideration of reciprocal communication of certain information concerning the radiograms.

At this juncture it was decided to revive the Interministerial Cryptanalytic Commission without the Foreign Affairs Ministry, as in pre-war days, and the first (and last) post-war meeting was held on 20 April 1922 under the chairmanship of General Bergault, Assistant Chief of the Army General Staff. It included representatives of the War, Navy, and Interior Ministries, which were already collaborating in cryptanalytic work, and of Colonies and the P.T.T., whose interest and cooperation were desired. The chief purposes of the meeting were:

(1) To achieve collaboration among the cryptanalytic services;

(2) To exert a common action over the assembling and classifying of materials for work and the training of new cryptanalysts;

(3) To study the possible use of radio stations in the colonies and in France to seek information, some of which would be of immediate importance;

(4) To call the attention of the Ministry of Colonies to the importance of information that it might obtain from a cryptanalytic service. (Both Colonies and P.T.T. were urged to develop such a service in the general interest, for themselves as well as the National defense).

The meeting led to resolutions to call the attention of the Ministries concerned to

(1) the importance of the cryptanalytic service and the collaboration necessary for the proper functioning of that service, and

(2) the necessity of safeguarding cryptographic security through strict skilled supervision over the construction and use of codes and encipherments.[a]

It was therefore requested that the various Ministries establish an inter-ministerial understanding with respect to cryptanalytic collaboration, and it was further recommended that everything to do with cryptographing of messages, and the construction of the documents and studies connected with those procedures, be taken care of within each Ministry by a cryptographic bureau in charge of a competent cryptanalyst. (Only at the War Department at this time were the cryptographic and cryptanalytic services combined under one head in the "Service du chiffre").

These resolutions after a slight flurry of interest were once more allowed to gather dust, and nothing more was heard of the Interministerial Cryptanalytic Commission.

In October 1922 Lt. Col. Givierge, exasperated by the exclusive behavior of the Foreign Affairs Ministry, which by depriving his section of useful intercepts and information was greatly hampering any effective work or training program, went so far as to suggest that Foreign Affairs take over military and naval studies itself and in time of war turn over its trained personnel to the War Department.

On 16 December 1924 the Minister of War made another attempt, which proved fruitless, to resume the collaboration plan under the auspices of the Permanent General Secretariat of the Higher Council of National Defense.

On 27 May 1925 M. Painlevé, Premier and Minister of War, sent a letter to the Minister of Foreign Affairs asking for exchanges of views among the heads of the cryptanalytic services of the Departments of War, the Navy, the Interior and Foreign Affairs to seek means of collaboration. There was no reply to this letter.

On 21 October 1925 the proposal made by Colonel Givierge to centralize the communications intelligence services under the Office of the Premier was called an "interesting suggestion" but it came to nothing.

In October 1931 it was revealed that although War-Navy collaboration was still close and fruitful, liaison with Sûreté Générale at the Interior Ministry had ceased with the retirement of M. Haverna. Since 30 October 1930 all encrypted texts of all origins had become centralized through the Intelligence Section, Deuxième Bureau, and the War Department's Cryptanalytic Section was receiving only messages bearing "Military Attaché" or "War" in their headings. Marshalling all the old arguments against this superficial and inaccurate method of determining the Department interested in a given cryptogram, the Cryptanalytic Section proposed a new attempt to achieve regular contacts among the heads of the various cryptanalytic services.

---

a. See appendix P. 52

On 16 February 1935 the Minister of Posts, Telegraph, and Telephone had a new decree signed by the President of the Republic, creating in that Ministry an Interministerial Commission with purpose of "studying all questions dealing with the security of the transmission of correspondence". (This rather vaguely worded purpose was explained in a covering letter by the Minister of PTT to mean the coordinating of the efforts of all the various ministerial cryptologic services, similar to the purpose of the defunct Interministerial Cryptographic Commission). This Commission, with representatives from the Ministries of Foreign Affairs, War, the Navy, Air, the Interior, Colonies, and PTT, held on 18 March 1935 a purely formal meeting which was never followed up. It was noteworthy as the first case, however, of any peacetime cooperation in this field on the part of the Foreign Affairs Ministry.

D. Collaboration Achieved

In 1938 the situation was as follows:

(1) Only the Ministries of War and of Foreign Affairs possessed organized cryptanalytic bureaus, and the one in the latter Ministry (Service des Travaux Réservés) had continued to resist all invitations to collaborate. (It might be noted here, however, that the head of the Foreign Affairs Cryptographic Service, a separate unit, had frequent and friendly contacts with the heads of the cryptologic sections in the War, Navy, and Air Ministries, especially for the joint study of inventions which might improve cryptographing methods).

(2) The Departments of War, Air and the Navy were working in close liaison. The Air Ministry was just beginning the organization of its service. It possessed trained personnel furnished by the War Department and had perfect liaison with the latter, but it did not yet have documents for study. The Navy Ministry, whose reserve cryptographic officers and some of whose active men were trained by the War Department's Cryptanalytic Section, possessed intercepts but lacked personnel capable of studying them continuously and fruitfully.

(3) The Ministry of Colonies did not appear to be interested in cryptanalysis, and the Ministry of PTT lacked the necessary means for providing continuous fruitful work.

(4) The Ministry of the Interior had, in its Photographic Service, an official who classified the intercepts, but lacked the means of carrying on sustained studies.

In February 1938 the Army General Staff was presented with a "Plan for regrouping the cryptanalytic services",[a] which consisted in grouping administratively all the existing services either under National Defense or under the Office of the Premier. It was very lucidly pointed out that the peacetime role of the cryptanalytic services was three-fold:

(1) to attempt to read current encrypted traffic,

(2) to prepare for the functioning of the services in wartime (by training reserve personnel and developing a thorough acquaintance with the cryptographic practices of the countries of interest) and

(3) to check on the security of the national cryptographic systems.

It was noted that the more complicated modern cryptographic techniques, especially the use of machines, require long-term research projects, no longer by individual cryptanalysts, but by teams including clerical personnel for mechanical tasks. Some disadvantages of the present uncoordinated system were:

(1) failure to exploit all intercepted traffic,

(2) duplication of efforts,

(3) lack of coordinated training of reserve personnel, and

(4) for lack of personnel in the various departments, neglect of difficult problems (especially machine problems) and of important languages, such as the Slavic languages and Japanese.

By concentrating all personnel and budgetary resources of the various departmental cryptanalytic services into a single service, it was argued, better results could be achieved without increasing the budgetary grants, and at the outbreak of war it would be possible to get intelligence immediately from cryptanalytic sources.

The General Staff, feeling that the time was not yet ripe for such centralization, nevertheless recommended on 7 March 1938 that a first step be the establishing of periodic liaison among the heads of the cryptanalytic services. A letter was accordingly sent on 31 March 1938 by M. Daladier, Minister of War, to the Minister of Foreign Affairs, proposing that the head of the latter's cryptanalytic section participate in monthly or bi-monthly exchanges of views with his colleagues in the Department of National Defense

a. See Appendix P. 53-57

and War. When this letter remained unanswered, a second was sent in July by M. Daladier, this time with the added prestige of his new position as Premier. A response was therefore finally elicited on 27 May 1938, displaying the Foreign Affairs Ministry's one-way conception of cryptanalytic cooperation and its customary myopia with respect to the basic reasons for such collaboration:

".....I have the honor of informing you that the Official Service of the P.T.T. communicates automatically to the Ministries of War, the Navy and Foreign Affairs the encrypted texts of foreign origin which appear to concern each of them. Besides, for more than ten years now contacts have been established between the service concerned at the Ministry of Foreign Affairs and the Army General Staff, Deuxième Bureau (Intelligence Service), which forwards to my Department the texts decrypted by the competent service in the War Department which has received them for cryptanalysis. Moreover, the same agency sends to my Department any encrypted text susceptible of interesting it, coming from its own intercepts.

"The actual liaison which thus results seems to me, therefore, at first glance, to answer your concern. However, I see no objection to a meeting of the heads of the sections concerned, during which your representative's proposals would be examined. He might get in touch with M. de Bobion, Minister Plenipotentiary, who is in charge of the section concerned in my Department."

This grudging consent to one meeting was skillfully misinterpreted by the Premier as an acceptance of the principle of establishing contacts. On 6 July 1938 the Premier instructed the Chief of the General Staff to agree to the organization of bi-monthly meetings of the heads of the cryptanalytic services of the three military Departments (War, Navy, and Air), with an invitation for participation also by the Ministries of Foreign Affairs, Interior, Colonies, and PTT "especially the Ministry of Foreign Affairs, since that Department has accepted the principle of making contacts (Letter of 27 May 1938)". He added an important note: "The heads of the cryptologic service will, moreover, receive the mission of preparing, for wartime, a centralized organization of the intercept and cryptanalytic services."

On 9 September 1938, spurred by the growing international tension, M. Daladier reminded the Chief of the Army General Staff of his previous instructions and asked that they be acted upon by 15 October 1938. Accordingly the first meeting took place on 27 October 1938 at the Ministry of War. It had a two-fold purpose:

"1. To establish collaboration on the technical level among the different cryptanalytic services existing in the seven Departments

-- Communication of technical procedures used with the foreign documents studied;

-- Delivery of radio and postal intercepts to the departments which would need them to facilitate their cryptanalytic work;

"2. To prepare a directive setting up for time of war a centralized organization of the services of radio and postal interception and of cryptanalysis. This directive would be submitted for the signature of the Ministries concerned."

In the course of the twelve bi-monthly meetings of the heads of the cryptologic services between 27 October 1938 and 8 June 1939 the first objective -- that of technical collaboration -- was fairly well realized. Among the War, Foreign Affairs, and Navy representatives there were exchanges of code recoveries and progress information on Italian diplomatic codes; the War Department's cryptanalytic section decrypted some Spanish consul telegrams for Foreign Affairs and furnished information on an enciphered code used by Argentina; a machine cipher employe in the Foreign Affairs cryptographic section was authorized to join a training course given by the Air Ministry; and it was agreed that the small and inexperienced cryptographic section in the Ministry of Colonies, urged to use more secure systems, might submit them for the approval of the War Department's experienced analysts. The Ministry of the Interior, which was interested in certain private code and cipher traffic reaching it by postal intercept from the PTT, was encouraged to create its own cryptanalytic section, with help promised from the War Department (which had previously done these decryptions). Efforts were likewise made, though with no perceptible success, to achieve collaboration between the two principal radio intercept agencies: in the Interior Ministry and in the Deuxième Bureau of the War Department (under the Intelligence Service, not the Cryptanalytic Bureau), with the dual purpose of avoiding duplication and of preparing for centralization of these agencies in time of war.

On 27 April 1939 steps were taken toward the second objective with the proposal of the creation, for wartime, of a central agency for cryptanalytic research under the Office of the Premier or the Chairman of the Higher Council for National Defense. (No mention was made of the centralization of radio and postal intercepts.) This agency, composed of the best cryptanalysts from the various Ministries, would have the task of centralizing cryptanalytic research and coordinating cryptanalytic activities. It would devote itself exclusively to "speculative research", discovering the systems, documents, and cipher machines used by the enemy and relaying all useful information to the cryptanalytic services of the various Ministries, which would be responsible for the actual recovery of specific keys, the reconstruction of codebooks, and the exploitation of the messages. Thus the advantages of a centralized control would be combined with those of independence of action within each Ministerial service.

The three National Defense Departments were in immediate agreement on

the principle, with the Air Ministry offering eleven cryptanalysts and the Navy two. The representative of the Foreign Affairs Ministry, although apparently personally favorable to the plan, was obliged to consult his superiors, and on 8 June 1939 he returned with a negative answer. Foreign Affairs gave the following reasons for its non-collaboration:

(1) The cryptographing methods of diplomats and the military are "most dissimilar". Since Foreign Affairs has never concerned itself with military codes and ciphers, centralization cannot, in principle, have the same advantage for it as for the Ministries of National Defense. (It admitted, however, that the collaboration already established among the cryptanalytic services had given results for certain consular codes, which sometimes contained intelligence useful for the Ministries of National Defense.)

(2) The very small staff of its Cryptanalytic Service makes it absolutely impossible for Foreign Affairs to detach a useful member to the Central Office.

At the beginning of hostilities, Foreign Affairs said it could therefore envisage only "as frequent liaison as appears useful". If later an enlarged staff permitted such a step, "the detachment of a specialist to the Central Office might then be envisaged".

In spite of this setback, which was probably not unexpected, the three National Defense Ministries agreed to centralize their cryptanalytic activities.[a]

This was the last recorded meeting of the heads of the cryptanalytic services. The next three were canceled for various reasons and then it was announced that the bi-monthly meetings would resume in October upon notification by the War Ministry's representative.

The fate of the centralization plan upon the outbreak of war in September 1939 is only a matter of speculation, for lack of specific information. There can be little doubt that the War, Navy, and Air Ministries carried out their plan; it is equally probable that the Foreign Affairs Ministry was recalcitrant. It is interesting to note, however, that on 13 September 1939 Daladier reshuffled his cabinet and assumed the portfolio of Foreign Affairs in addition to that of War. With a common head for the two ministries it may be presumed that the struggle for close cryptanalytic collaboration between them was finally won for the period up to the fall of France in June 1940.

---

a. See the three proposals, Appendix P. 58-63

Clues to the Situation since 1940

We have no direct documentary evidence of the situation since the fall of France in 1940 with respect to cryptologic cooperation among the Ministries. From various bits of indirect evidence, however, certain guesses can be made as to the degree of (a) cryptographic and (b) cryptanalytic collaboration.

A. Cryptographic Collaboration

From such evidence as the construction of codebooks, methods of encipherment, external appearance of traffic, etc., it appears that the pre-World War II situation has not greatly changed, cryptographically speaking. Although there was apparently some forced collaboration during the war, when for lack of codebooks of their own the Diplomatic and Colonial Departments of the Free French Government were obliged to borrow Army and Navy Codes, this practice came to an end shortly after the re-establishment of the government in Paris. The principal post-war Interior codebook bears strong points of similarity to the traditional Navy codes, suggesting some influence from that quarter. The Army, Navy, and Air Force appear to be continuing, within the National Defense Ministry, their close collaboration of pre-World War II days. With these exceptions, however, each ministry retains its distinctive ways of constructing codes, encrypting telegrams, and composing the plain-text portion of the message to be transmitted.[a] The Foreign Affairs Ministry, for example, continues to use unenciphered codes, a practice long forbidden by the Army.

As long ago as October 1922 Lt. Col. Givierge, aware of the dangers of such a practice to code security, protested the lack of collaboration which forced the High Commissariat in Morocco to have the same telegram encrypted in two different codes when it was to be sent both to the War and Foreign Affairs Ministries. Although it is not uncommon now for a telegram addressed to DIPLOMATIE to bear in its encrypted text the request "Communicate to DEFENSE NATIONALE", there are still many instances of the dangerous practice of enciphering a message in two systems. On 16 May 1951, for example, a message was sent from Tunis to DIPLOMATIE in a diplomatic code and then repeated to FRANCE OUTRE MER in a colonial cipher.

a. In this connection it may be of some interest to note that during the war some Free French diplomatic traffic bore external part indications (unpds, depds, etc) in conformity with Army and Navy practice. With the return to Paris, however, this procedure was soon abandoned for the distinctive practice of internal part indicators.

It is true that the new post-war Naval and Diplomatic codes in particular show enough of a change from the stereotypes[a] of the past to suggest that new blood came into the cryptographic sections of those Departments. There is no evidence, however, to imply any real increase in interministerial cryptographic collaboration nor the existence of any centralized agency watching over French cryptographic security.

B. Cryptanalytic Coordination

As for the cryptanalytic coordination for which the War Ministry had so consistently worked from 1909-1939, there are some grounds for surmising that it may have been realized since the war. The GCR (Groupement des Contrôles Radio-Electriques) and the SDECE (Service de Documentation Extérieure et de Contre-Espionnage), operating under the Office of the Premier, may be the centralizing agencies.

The GCR is a French Agency responsible for foreign intercept and radiogoniometry services. (There is no evidence that the former intercept service within the Ministry of the Interior is still in operation). It is not certain when the GCR first came under the Office of the Premier, but it was already under that authority in April 1947. On 28 May 1947 by decree of Premier Ramadier, M. Paul Béchard, Secretary of State to the Office of the Premier, was made responsible for National Defense (under the Office of the Premier) and for "all its services and agencies except the SDECE". He was also put in charge of radio broadcasting and the GCR. Thus the GCR was brought under the same head as National Defense but was administratively separate from the SDECE.

In October 1947 M. Eugène Thomas, former Minister of Posts, Telephone, and Telegraph, was made a Secretary of State to the Office of the Premier, and a decree assigned to him the responsibilities for PTT, radio broadcasting, and the GCR. This time the GCR, removed from its immediate relation to National Defense, was perhaps more logically joined with the other communications services. Under this arrangement, there appears to be complete centralization under the Office of the Premier of all intercept facilities.

---

a. The post-war Naval code, FRNAD, has only about 16,000 groups as compared to the usual 24,000-group codes. The Foreign Affairs Ministry introduced a series of 3-letter 1-part codes with fewer variants and a larger vocabulary than the traditional 4-figure 2-part codes. The post-war 4-figure 2-part codes also follow the new vocabulary pattern in great measure, using a new system of "doublets" (two meanings for certain code groups) to expand the vocabulary.

Moreover, although French intelligence activities still remain scattered in several different ministries, some coordination of them appears to have been achieved,[a] with reports from military intelligence (from the National Defense Ministry), political and economic intelligence (from the Foreign Affairs Ministry), industrial intelligence, and the SDECE, all being channeled to the Premier through the Second Section of the National Defense Staff.

Since the intercept and intelligence activities bear a close relation to the cryptanalytic activities, it is not unreasonable to assume that moves toward coordination in the former areas are accompanied by similar moves in the latter. Although there is no definite COMINT proof that the SDECE is the coordinating agency, there is some evidence[b] leading to the belief that cryptanalytic activities are at least among its functions. The general tendency to place the GCR, PTT and the SDECE under the Office of the Premier is interesting in the light of the argument advanced that any central coordinating cryptanalytic agency would have to be directly responsible to the Premier in order to enlist the cooperation of the Foreign Affairs Ministry.

---

a. See R-461-48

b. See for example FK 745 and FRM 409 (A)

From "Note on the Cryptanalytic Service" (? by Major Civierge ?)

G.H.Q. 26 July 1916 P. 7-10

III. The Single Bureau

It would seem advantageous to reach an understanding among the existing cryptologic bureaus to avoid the duplication of work. But before examing the conditions of an understanding, let us make a clean sweep of what now exists and examine the role of a single bureau of cryptography.

This bureau, responsible in a country for everything to do with codes and ciphers, would have to fulfill the functions devolving upon the various cryptographic services now in existence.

Now, aside from the decrypting of cryptograms, there exists a practical task of cryptographing and decryptographing telegrams which must, in order not to lay them open too readily to study by the enemy, be directed by cryptanalysts. These cryptanalysts must instruct the operating personnel and prepare the documents. It is not possible to accept the idea of a single service if the latter is to ignore completely the practical service of the various ministries. This is perhaps a new conception -- the construction of codebooks and the habits of certain Departments prove it -- but it is in our opinion an absolute necessity for crypto-security.

As for decryption the bureau will have to:

(a) be responsible for directing the service of gathering the documents to be studied (radiograms and other means).

(b) be responsible for gathering together and keeping numerous archives (documents studied, documents throwing light upon them, working tools). Letters obtained from perquisitions or from censorship may cast light on cryptograms and give names or keys.

(c) be responsible for recruiting personnel and using employes according to their aptitudes.

(d) be responsible for communicating to all the services the results that concern those services. In order to do this, one must be perfectly acquainted with the different services in order not only to keep at their disposal what may interest them, but to go and propose it to them, and at times to oblige them to work on it for the general interest.

(e) function under satisfactory conditions of security. This security consists not in concealing the existence of services to which all the dime novels allude, but in concealing the exact nature of the work being done and the list of projects under study there.

(f) finally, think of preparing for war.

Are these conditions compatible with a new organization?

Yes, if that organization can be created outside of all ministries, above the ministries, with a chief who has indisputable authority with the "grands services" -- with the P.T.T. and the public prosecutor's department (for perquisitions and correspondence of malefactors) as well as the ministries concerned -- a competence as great as his authority in all general questions, military, political, etc... and who has credits at his disposal.

Why these conditions? Chapter II shows that they are necessary, by showing the consequences of the spirit of compartmentalization* concealed under different labels, including that of the security to be maintained.

This spirit has perhaps not entirely disappeared: the GHQ has no knowledge of telegrams on certain military operations emanating from Military Attachés except through the decryptions made at GHQ. Another Department has the elements for decrypting those telegrams. Either it wishes no one to know that it has them, or it does not understand the interest of the documents for GHQ.

If a central bureau is established in a Ministry:

--who, if not that Minister or his representative, will decide on the documents to be communicated to the other Departments?

--how will discipline be ensured among the cryptanalysts, now scarce and therefore a precious commodity, who, both officers and civil servants, have a status and a position?

It is not a question of placing them in a hierarchy; but their work cannot be carried out on a piece-work basis, they must take to it; the slightest hurt feelings give rise to bad results. For the moment no use is being made of M. Haverna, whose competence is beyond question.

--how will the recruiting of personnel for the services of the other ministries be taken care of for the future? As far as we are concerned, we have to teach cryptographing practice to the officers of the General Staff. We need codebooks. The experience of the War has proved that an officer accustomed to military habits, thoroughly acquainted with the military nomenclature and hierarchy, renders quite different services in the military cryptographic service from a young reserve officer or a young interpreter. Who will train this personnel; who, at the time of another campaign, will make this service function?

*ESPRIT DE BOUTON

Will the end not be a monopoly which will result in preventing cryptanalytic vocations, for civil servants or officers not belonging to the Department in charge of the central bureau, from being revealed? And once this monopoly is assured in fact, will there not be a preference in the order of studies in favor of that Ministry? Is Foreign Affairs interested, as we are, in the gossip* of the German posts in the trenches at Verdun, which concern only a sector of the Second Army? And will it not leave this sector uneasy as to the contents of the radiograms intercepted by its posts? We receive from an Allied Army requests for intelligence which prove that a cryptanalytic service organized in a Ministry leaves the Armies in complete ignorance of some of its work and has for more than 18 months permitted officers to seek laboriously results which it has had for a long time.

For these reasons, considering the tendencies revealed up to now, particularly by the Department of Foreign Affairs, considering human nature and the difficulty of finding the one competent man in all the ministerial departments, we are not at present in favor of the installation of a single bureau --- either for the period of the war alone, because we fear that the distribution of the documents will be made in even worse fashion than now; or in the future after the return of peace, because we fear that the service requirements of the various ministries, particularly the preparation for war, will be sacrificed.

* Or possibly "chatter": BAVARDAGE

Paris — October 1917

NOTE
on a plan to reorganize the
cryptanalytic services

- -

A

1. At the present time there does not exist in France any cryptanalytic organization created for the purpose of obtaining the most efficient results while reducing as much as possible the chances of indiscretions.

2. It has not yet been possible to bring about any centralization, in spite of the obvious advantages which would have resulted in every respect.

3. No intimate liaison has been established among the cryptanalytic services of the various ministries which have such services: Foreign Affairs, War, Navy, Interior (Sûreté Générale).

4. Cases of duplication of research resulting from this lack of agreement are relatively numerous:

German naval codes are naturally studies by the Navy, but they also are by War because they are used by military zeppelins:

Certain diplomatic codes, used by the Military and Naval Attachés, as well as by the Ambassadors or Ministers, are studied by War and Foreign Affairs.

5. The first disadvantage of this duplication is that it demands, uselessly, an increase in personnel and consequently of quarters.

6. Furthermore, encrypted documents must be drawn up in several copies, to be distributed among the various groups studying them simultaneously; hence the need for additional staffs to copy and send them on.

7. The results obtained by one group are not communicated to those who are making the same studies or similar ones; hence, wasted effort.

8. The services that intercept encrypted documents do not always know to what Ministry they are to send them: either they send them to several, whence multiple copies and correspondence; or they take the risk, by sending them to only one, of not directing them to the one which should properly receive them.

9. This multiplicity of confidential documents and of people employed to copy them, transmit them, and study them increases the chances of negligence

or indiscretion in an unfortunate way.

10. The same disadvantage comes also from parallel communications made by the services studying the same documents.

11. Moreover, documents or intelligence coming to one cryptanalytic service might be very useful to another which does not know of their existence.

12. To sum up, there is no administration which centralizes everything to do with cryptanalysis and does the necessary coordination of the various groups assigned to the same type of work.

B

The time seems to have come to institute a reorganization which is all the more indispensable as recent incidents may unfortunately have seriously compromised a service which has proved its effectiveness since the beginning of the war, both from the diplomatic and from the military and naval point of view.

Without laboring the point of the services rendered to the armies and navies by the immediate decryption of field and naval radiograms, it seems appropriate to recall in particular the intelligence having to do with German actions in Greece, Spain, Morocco, America, and even Asia, which has been furnished by cryptanalysis, and the results of which have been so extensive from the point of view of the development of the World War.

C

In order to establish the bases of a rational organization of the cryptanalytic service, we must not lose sight of the fact that this service is above all an organ of intelligence and that it should logically be attached to a General Office of the Intelligence Service, which does not yet exist in France, and which it would doubtless be advisable to set up.

D

1. As for the cryptanalytic service, an Interministerial Office of this service should be created, including representatives of the principal Ministries of National Defense, to whom would be added a delegate from the Office of the Premier.

2. This Office would be charged with all cryptanalytic questions of general interest.

3. To this Office would be transmitted all encrypted documents intercepted, from whatever source: radiotelegraphic, telegraphic, postal, etc.

4. It would ensure their being studied by setting up as many groups as would be necessary according to the category of the documents.

5. It would ensure the necessary liaisons among the various groups in such a way as to obtain the most efficient results while limiting and localizing responsibilities.

6. It would communicate whatever was necessary in appropriate form to the services concerned in the various ministries through the qualified representatives indicated above, who would see each day all the work decrypted.

7. It would be in direct relations, through the same representatives, with the intercept and intelligence services, as well as with the exploiting services of the various Administrations which have them.

8. It would not be indispensable to bring together in the same quarters nor to attach to the same Ministry the various cryptanalytic groups, since the proposed Office would ensure the necessary liaisons among them.

9. Such an organization seems the proper kind to eliminate or to reduce appreciably the disadvantages noted above (in A).

E

1. The Office of the Cryptanalytic Services, it seems, should be attached, <u>at least for the duration of the war</u>, to the War Ministry; but it might, if that were judged preferable, be attached to the Ministry of Foreign Affairs or even to the Office of the Premier.

2. It would direct and coordinate the work of the various sections set up by the qualified ministries.

3. The War section would study the field radiograms of the various fronts.

4. The Navy section would study naval radiograms.

5. At the Sûreté Générale the encrypted documents relative to internal policy would be studied.

6. To Foreign Affairs would be reserved the study of the diplomatic documents; however, War would cooperate, at least until further notice, in the study of certain diplomatic codes and of the correspondence of the Military and Naval Attachés.

Chief of the Section du Chiffre

Resolution of the Interministerial Cryptographic Commission on the Subject of Crypto-Security (20 April 1922) P. 11

"Whereas it is important that in each ministerial Department the cryptographic systems be kept at a level with the advances in cryptanalysis and especially that the use of these documents not endanger security,

"Recalling that cases have often arisen in which, as a result of grave events, the representatives of various administrations have transmitted approximately analogous telegrams on the same subject, so that the discovery of the meaning of the one endangered the security of the text of the other and of the document which had served to encrypt it,

"That there thus results a certain solidarity in the cryptographic security of the ministerial departments, and that it is important, consequently, that this security be strictly safeguarded, by the drawing up of secure documents as well as by strict supervision over their use,

"That this supervision can, it seems, be exercised only by thoroughly trained persons who, versed in decrypting procedures, are acquainted with the weak points of codes and ciphers and with their use,

"The Commission expresses the desire:

"That the attention of the various ministries represented be called to the advantage of instituting serious and active supervision over the drawing up of cryptographic documents and especially over their use. It (the Commission) takes the liberty of suggesting in this respect the establishment of a cryptographic bureau, having at its head a person qualified in decrypting, having in its responsibilities everything that has to do with cryptographing and decryptographing of messages, the drawing up of documents and the related research."

(Annex to the report on the 100th session of the League of Nations)-

19 February 1938

Plan for Regrouping the Cryptanalytic Services

[Attached herewith is a plan drawn up by a reserve officer in the Navy, an official of the Secretariat of the League of Nations.

[It appeared that the proposals presented deserved to be examined from a higher point of view than the level of "Ministry". They seem to permit the coordination and centralization of research beginning in peacetime, especially with respect to the decrypting of machine systems destined to be generalized in wartime].

1. Role of the cryptanalytic services in peactime

The cryptanalytic sections, which rendered most valuable services during the last war, have an equally important role to play in time of peace. They must:

(1) maintain the current service, that is, seek to decrypt the encrypted telegrams which are furnished them by the P.T.T. services (for ordinary transmissions), by the intercept services organized by the various Ministries (for radiotelegraphic transmissions), or by other means (Intelligence Service, police, etc.)

(2) prepare for the functioning of the service in time of war:

-by ensuring the training of reserve personnel

-by possessing a thorough familiarity with the systems and encrypting habits of the countries with whose transmissions it is advantageous to be familiar.

(3) verify the impenetrability of the national cryptographic systems

2. Evolution of the technique of encrypting and decrypting

Since the war progress in cryptanalysis has obliged the services to look for code and cipher systems that are more and more secure, and has led several countries to begin introducing the use of machines. The problem, for the cryptanalyst, has become singularly complicated, and instead of being a work of individual analysts, decrypting in many cases today requires

recourse to team work; it has become indispensable to proceed to long-term research and to give the cryptanalysts auxiliary personnel responsible for the clerical tasks of simple stripping and tabulating of groups.

Unfortunately, the administrative organization of these services has not taken this evolution sufficiently into account. Each Ministry (War, Navy, Air, Colonies, Foreign Affairs) possesses a separate service and though, by the very force of circumstances, personal contacts have been established among the National Defense services, the present system does not permit the ensuring of the efficiency in these services that could be expected from them if there were a pooling of the various means according to a rational organization.

3. Some disadvantages of the present system

Without wishing to go into detail, it is interesting to note that:

(a) as a result of the lack of coordination among the services, part of the messages intercepted are not exploited (e.g. messages encoded with the German diplomatic code are picked up by the Navy's intercept services without being transmitted to the Quai d'Orsay; one part of a correspondence encoded with the aid of the Spanish code was sent to the Navy, the other to the Quai d'Orsay, without its being possible to compare these two texts);

(b) different services work on the same code without communicating their results or their hypotheses to each other (e.g. the diplomatic codes on which Foreign Affairs works for diplomatic messages, Navy for Naval Attaché messages and War for Military Attaché messages);

(c) for lack of personnel the services attack only relatively easy problems and neglect the difficult problems (such as the decrypting of machine encipherments) whereas this work is probably the most important for the preparation for wartime;

(d) as a result of the small number of cryptanalysts in each service, it is not possible to have the necessary range of linguistic knowledge, so that important languages (Slavic languages, Japanese, etc.) are almost entirely neglected;

(e) the training of reserve personnel is not sufficiently coordinated for there to be a unity of doctrine in the various services and it is scarcely possible to benefit from the experience of the other services in order to direct this instruction properly.

4. General outline of the organization that might be envisaged

It it is desired to obtain greater efficiency from the cryptanalytic services without increasing the budgetary grants, and if it is considered essential that these services, from the first day of mobilization, be able to be armed in order to enable them to take immediate advantage of the imperfections or blunders of the enemy code clerks, it seems absolutely necessary to concentrate efforts by grouping administratively the elements that are now distinct, either at the level of National Defense or at that of the Office of the Premier (Conseil Supérieur de la Défense), if Foreign Affairs agrees to join in the plan.

This grouping will have the following advantages:

(a) all the encrypted messages will come to the same service, which will be responsible for the distribution among the cryptanalysts, according to their knowledge and their technical specialization (army, navy, air, foreign affairs). This centralization will make it possible to rationalize the organization of the intercept services and to guarantee that all the texts intercepted will be usefully exploited;

(b) with more texts available, and especially, series emanating from the same sending authority, there will be more frequent hypotheses available and thus greater chances of success in the decrypting;

(c) with a larger number of agents in the same service, it will be possible to enlarge the range of linguistic knowledge and to enrich the field of decryptions;

(d) for the same reason it will be possible to reserve the services of one or more cryptanalysts for long-term research projects, such as the thorough study of the decrypting of telegrams encrypted with the help of machines;

(e) with knowledge of all the systems used in the same country, it will be more readily possible to ascertain the habits and cryptographic systems of the enemy services and to reconstitute the doctrine which is being established on the other side;

(f) it will be possible for the training of personnel to be more uniform and more rational.

Conclusions:

(1) It would be up to the Ministry of War, which possesses the largest cryptanalytic service and has the most experience, to take the initiative toward reorganizing these services and to present a concrete and detailed plan.

(2) This plan should provide for the concentration of all the present means (personnel and budgetary resources) into a single service which would be administratively attached to an existing interministerial body or to the Office of the Premier.

(3) This service would consist of a service chief, preferably a civilian to ensure continuity, and four or five sections. Each section would consist of agents, either civilian or military, detached by the Administration to which they belong (Navy, War, Air, Colonies, Foreign Affairs). Besides the cryptanalysts proper, it would be advisable to add auxiliary personnel for purely clerical work. This auxiliary personnel might be common to the various sections.

(4) The ministries would no longer be able to take up cryptanalytic projects except for particular well-defined missions. In this case it would be understood that the central service will be kept informed of the results of those projects which would have interest from the cryptanalytic point of view.

(5) All the encrypted messages will arrive at the central service and will be distributed among the sections. The decryptions will be communicated exclusively to the Ministry concerned, according to the instructions it has given. In principle each section, composed of agents belonging to a given Ministry, will work only on messages of interest to that Ministry and will have no knowledge of the texts of interest to the other sections. Only the cryptanalytic results (recovery of a code, decrypted groups, observations on the cryptographic systems) will be brought together in the office of the director of the service and communicated to the various sections. These precautions will make it possible to assure the various departments that their secrets will not be divulged to other services.

- - - - - - - - - - - - - - - - - - - -

Plan for Organization of the Cryptanalytic Services by Fusion of the Present Services Belonging to Different Departments

A. Organization

(a) Service chief

Assistant archivist responsible for:

(1) the receipt and distribution of intercepts

(2) the dissemination of decryptions to the departments concerned

(3) the documentation service (see below)

(b) Cryptanalytic groups

English
German
Italian and Spanish
Russian
French (private telegrams) and miscellaneous

(c) Translation group (plain text telegrams)

(d) Research group: new systems, inventions, machines, etc.

B. Intercepts

Furnished by the assembling of intercepts which may be gathered by the following services:

War
P.T.T.
SÛRETÉ NATIONALE
Colonies
Navy

C. Documentation

Formed by bringing together the documents now existing in the different departments (dictionaries, telephone books, etc.). Press service (to be organized).

D. Installation

The assembling of the documents would require installation of the entire service in quarters close together.

From "Note on the Subject of Interministerial Collaboration in the Matter of Cryptanalysis" * Page 4-5

-- May (?) 1938

.....

In case the idea of the coordination of the various cryptanalytic services should take shape, it seems that the most expedient procedure would be to create an Interministerial Directorate for those services.

This directorate, composed of representatives of the principal ministries, would be responsible for all cryptanalytic questions of general interest and for coordinating the work of the various sections set up by the qualified ministries.

It would receive all the encrypted documents intercepted, regardless of origin and destination.

It would ensure their distribution among the various special groups, no longer solely by address, but by systems and categories.

It would ensure the liaisons among the various working groups in such a way as to obtain the most efficient results while at the same time limiting and localizing responsibilities.

It would set up and keep up to date the card file for each country studied and would give each group all information susceptible of facilitating its work.

It would establish a press service or would receive from the various departments all press information susceptible of directing the efforts of the cryptanalysts.

It would entertain direct relations with the intercept and intelligence services as well as with the exploiting services in the various Administrations susceptible of giving it bases for orientation.

Through the qualified representatives of the various departments, it would see to it that the work of the groups was circulated in the appropriate form to those concerned.

Moreover, it should centralize all the inventions and all the systems proposed for adoption by the various departments, and have them studied by a technical section.

---

* Army proposal

The working groups would be allowed to keep their autonomy and to do their own recruiting and the instruction of their personnel individually.

The Directorate might be attached to one of the ministries of National Defense or the Permanent General Secretariat of the Higher Council of National Defense.

The Agency envisaged might therefore consist of:

1. a director, aided by an assistant;

2. an archives service for:

   (a) the receipt and distribution of the intercepts,

   (b) the dissemination of the translations,

   (c) the maintenance of the cryptanalytic files,

   (d) the centralization of the press information;

3. a liaison service composed of a qualified representative from each department responsible for seeing periodically all the work accomplished in his department and daily all the texts decrypted;

4. a translation service for plain text intercepts;

5. a technical service responsible for studying inventions etc. and for watching over the security of the national codes and ciphers.

"Central Interministerial Cryptanalytic Bureau" *

- 9 May 1939

At the bi-monthly meeting of the heads of the cryptographic services on 27 April 1939, the creation of a central agency for cryptanalytic research was contemplated.

The Navy proposes the creation of a central cryptanalytic bureau, an interministerial agency not directly under any Ministry and responsible solely for general studies:

(a) centralizing cryptanalytic research in order to discover the new cryptographic methods being employed and to establish theoretical rules for decrypting;

(b) studying enemy cipher machines, diagrams or descriptions of which we might possess, and seeking the weak points of these machines;

(c) centralizing all documents relative to the methods in reserve which might be used by the enemy.

This Central Bureau would not have to reconstruct the text of the intercepted messages nor to look for the specific keys; this role would be reserved for the cryptanalytic bureaus belonging to each Ministry, which, applying the general methods furnished by the Central Bureau, might utilize various bits of information that they possessed on the meaning of a message, probable words, encrypting errors, etc....

The Central Bureau would be placed under an authority higher than that of the three ministries of War, Air and the Navy. It might be under the Office of the Premier or under the President of the Higher Council of National Defense.

The advantages in having this Bureau under a very high authority would be:

1. The easier participation of Foreign Affairs.

2. The possibility of securing either the permanent or occasional participation of qualified civilians in the research; for example, former military cryptanalysts having real competence in the work whom it would be difficult to employ in a subordinate position in a military agency.

The contribution of each Ministry to this Central Bureau might be two or three persons of officer rank, and, if possible, an equal number of secretaries.

---

* Navy proposal

Central Cryptanalytic Service *

- 24 June 1939

Nature: an interministerial agency, functioning in time of war within the framework of the Higher Council of National Defense (Secretariat General).

Role: agency for general studies and coordination

General studies: the Central Cryptanalytic Service:

(a) centralizes:

-all materials for cryptanalytic study coming from the armies or Interior;

-all documents and information of a technical nature coming from the various Intelligence Services relative to the cryptographic systems used by the enemy as well as the principles of their use;

(b) does the sorting, by origin and by the cryptogram's form, of the various study materials received by the service;

(c) investigates in each individual case the nature of the system used, possibly with the help of the information and documents of a technical nature which are in its possession;

(d) studies new encrypting procedures (machines, electromechanical or electromagnetic processes, etc...) and tries to set up methods making it possible to ensure the decrypting of those systems.

Coordination:

(a) transmits to each of the cryptanalytic services of the different ministerial departments the materials for cryptanalytic study of interest to that Department, attaching to them all information already gathered by the Central Service and all results obtained in its research, with a view either to continuing the cryptanalytic study proper or, if the results already obtained permit, to undertaking the immediate exploitation of the materials;

---

*Air Force proposal. This plan, presented after Foreign Affairs had refused to participate in such a central agency, envisages collaboration among the three National Defense ministries only.

(b) maintains constant liaison for this purpose with each of the cryptanalytic services of the aforesaid ministries and proceeds, whenever the need arises, to all exchanges of views necessary for ensuring the greatest efficiency of the various services;

(c) maintains liaison with the Central Service and the Press Information Services, the Central Intercept Service, and various Intelligence Services with a view to assembling all necessary information and materials;

(d) participates in "censorship", in liaison with the Press Service, for everything concerning publications of any nature susceptible of imperiling crypto-security.

Organization:

A service chief (an officer - specialist from War's crypt section) aided by an assistant.

Classification Section:

(1) receipt and classification of study materials,

(2) centralization of information and documents of every nature,

(3) setting up and keeping current card files of cryptanalytic information.

(Personnel: officers -- crypt specialists, sous officiers -- specialists, possibly later civilian personnel).

Study Section

(1) preliminary research on study materials transmitted after classification by the Classification Section;

(2) dissemination to the cryptanalytic services of each Department of the materials of interest to them, as well as of the results obtained at the time of the preliminary research;

(3) dissemination to these same services of the translation of plain-text messages coming from various intercept or intelligence sources;

(4) studies of systems, machines or cryptographs.

(Personnel: officers -- crypt specialist, sous officiers-specialists; possibly civilian personnel for the translation of plain-text messages only).

Liaison Section: liaison with the various departments, the Information Services, the Intelligence Services, the Press Service.

(Personnel: officers--crypt specialists).

Observation:

Such an organization, as it emerges from the above outline, seems calculated to ensure the maximum efficiency of the various groups of specialists working both in the Central Service and in the various crypt-analytic services.

It divides the work by leaving to the Central Service the "speculative research" part and reserving for the cryptanalytic services the "cryptanalytic study" and "exploitation" part. Thus, while managing to bring together the means, it ensures for each ministerial Department the independence of action which is desirable.

On the other hand, its proper functioning implies close and constant liaison among the various groups, conditions which presuppose the assembling of these groups in the same building, or in immediate proximity to each other.