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

30 April 1951

A Summary

of the

History of Collaboration Among French Cryptologic Agencies 1909 - 1939

as revealed in a file of

Ministry of War Correspondence

ARMED FORCES SECURITY AGENCY

Summary of a file of French Ministry of War Correspondence, 1909 to 1939

Summary:

A collection of documents from the files of the Cryptologic Section, Deuxième Bureau, Army General Staff, Ministry of War has been rapidly examined. The documents deal mostly with organization of the cryptologic services and efforts at collaboration among the services of the several Ministries engaged in cryptologic activities.

Three facts emerge from a study of these papers:

1. The Army Cryptologic Service, from 1909 at least until 1939, understood the need for close collaboration among the several cryptologic Agencies, both for cryptanalytic and crypto-security activities.

2. The other Ministries shared the Army's views and actually joined in fruitful common efforts -- all but the Ministry of Foreign Affairs.

3. Apart from the war years 1914-18, the Ministry of Foreign Affairs steadfastly refused to co-operate with the other services, except in certain limited fields. It was constantly indicted by the Army for its failure to collaborate, and it stands guilty by its own statements of a complete lack of understanding of the way in which the national interest can be served by a unified cryptologic command.

Discussion:

On 11 January 1909, the French Minister of War (G. Picquart) addressed to the President of the Republic a letter in which he made the following points:

(a) Certain Ministries and "Grands Services" each have a cryptographic service whose first purpose is to ensure the security of that organization's communications.

(b) Although their problems are analogous, these bureaus work completely alone.

(c) It would be desirable for them to establish such relations as would permit them to exchange views and study certain matters of general interest in common.

(d) To this end, an Interministerial Cryptographic Commission should be established, including representatives of each of the separate bureaus.

This letter was accompanied by a draft of a decree setting up such a Commission, whose president would be the President of the Military Cryptographic Commission. The draft decree was signed by the Ministers of War, Interior, Navy, Colonies and Public Works (Post, Telephone and Telegraph).

No further documents bearing on the Commission are available, until a report of a meeting, apparently the first, on 14 May 1912. From this report it appears that the President of the Commission had been trying to organize for readiness in case of war a "Comité de déchiffrement" (presumably a cryptanalytic organization) and had invited the

Foreign Ministry to participate. Immediately, the non-cooperative attitude of that Ministry, an attitude which was to persist for thirty years, was made manifest. The Foreign Ministry, while it had decided on its representatives, refused to divulge their names or order them to join the committee until "the moment of need". The Commission decided that it could not wait for 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 cryptologic organization in the event of war was, therefore, given instruction in cryptanalysis.

The Interministerial Commission met periodically from May 1912 to June 1914. (Its next, and probably last meeting took place in April 1922).

By the middle of 1916, two years after the beginning of the war, on the evidence of an unidentified member of the staff of the French General Headquarters, there were five separate cryptanalytic agencies functioning: in the Foreign Ministry, in the War Ministry, at GHQ, in the Sûreté Générale and in the Naval Ministry. Some degree of collaboration existed among certain of these bureaus, but for the most part they operated independently in spite of continuing efforts by the War Ministry to bring about closer relations.

Although there is evidence only of an imperfect kind of collaboration between the Army and the Foreign Ministry during the war in the documents, a letter on 20 December 1918 on War Ministry letter head indicates that the writer and the head of the Foreign Ministry Cryptographic Service, M. Hermitte, had worked closely together during the war. The writer, however, feared that isolationist sentiment, strong in the

Quai d'Orsay, would lead to a rupture in this relationship, so important during the period of peace negotiations.

Again in December 1919, the War Ministry proposed a centralization of effort, which the Foreign Ministry rejected completely on 4 January 1920, saying that "the arguments of war-time can not ... 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".

The history of the twenty years following is a continuous story of efforts to create an organization for cryptologic collaboration, with each attempt being balked by the refusal of the Ministry of Foreign Affairs to participate in any real pooling of resources other than exchange of some traffic and, for a time, of certain decryptions.

It may be useful in this place to quote from a letter on this subject, dated 4 February 1922, from M. Maginot, then Minister of War, to the Premier, M. Poincaré, who was then also the Foreign Minister. (M. Poincaré, as one of his first acts on assuming office, had ordered the Foreign Ministry to cease sending any decryptions to the Army.) The note cites the Foreign Ministry's dispatch of 4 January 1920 referred to above, and goes on to say,

> "I will ask you to be kind enough to inquire into whether, without speaking of 'concentration' of the Cryptologic Services, there might not be reason to strengthen collaboration among them in a practical way, instead of re-establishing watertight compartments.... The question of specialization of efforts according to the nature of the content can not, indeed, be with utility set forth when what is at issue is not the exploitation of the content of foreign telegrams, but the discovery of their keys: in reality the addressees 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 interests. Now at present, as before the war, for lack of an

over-all direction or of 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".

In a note "meant to be read to the Interministerial Cryptographic Commission," of 4 August 1922, the author (presumably Colonel Givierge) cites this letter and states that the Foreign Ministry did not reply to it. He goes on to say,

"We have, at War and Navy, important information concerning certain foreign cryptographic systems. We have frequently communicated this information to the Foreign Ministry without having been able to go on with its exploitation -- furthermore, it seems that the Department in question, for lack of personnel, allows a large part of the material communicated to it to be lost....."

In response to such pleas for community of effort, the perennial attitude of the Foreign Ministry on the subject of collaboration is clearly set forth in the following unsigned note of 8 June 1939.

"Note on the subject of a plan for Centralization of cryptanalytic efforts in time of war.

" During a recent session of the bi-monthly meeting of the Heads of the Cryptanalytic service, the question of the creation for wartime of a higher central bureau of cryptanalysis was brought up.

" This bureau would be charged with proceeding to studies for the discovery of the encrypting methods used abroad and with furnishing to the special cryptanalytic bureaus general information susceptible of facilitating their work for them.

" The body envisaged seems to answer a need for the Ministries of National Defense proper: War, Navy and Air. From the close relationship of the objects of the activity of these departments, as well as from the similarity of the methods employed by the Military Administrations, it follows in fact that a pooling of studies and results is undeniably useful.

" The same is not true for the Ministry of Foreign Affairs, whose domain is differentiated by definition from that of the aforementioned Departments, while at the same time remaining linked by the common goal pursued. Because the encrypting methods used by the diplomatic and the military authorities are most dissimilar, and also because the Foreign Affairs cryptanalytic bureau has never concerned itself with military systems, the centralization cannot, in principle, procure the same benefit for it.

"

It is nonetheless true, incidentally, that the liaison, then the collaboration, already established between the cryptanalytic bureaus have given results for certain consular codes. These codes in fact cover texts which sometimes contain intelligence useful to the Ministries of National Defense.

" It is worth noting, moreover, that when it is a question of complicated methods, the most capable specialists succeed generally in learning how they work only at the cost of long researches.

" However that may be, the cryptanalytic bureau of the Ministry of Foreign Affairs is functioning at the moment, as a result of various circumstances, only with an extremely reduced personnel. Efforts are being made to reinforce it but at present that bureau would find it absolutely impossible to detach a useful member to the Central Bureau without paralyzing its own activities -- a result which is obviously contrary to the goal sought.

" The Ministry of Foreign Affairs could therefore envisage, at the beginning of hostilities, only as frequent a liaison as will appear useful.

" If later on the number of personnel in its cryptanalytic bureau should permit, the detachment of a specialist to the Central Bureau might then be contemplated."

Conclusion:

We have no direct documentary evidence of the situation since 1939 with respect to cryptologic cooperation between the Ministries. From such indirect evidence as the construction of codebooks, methods of encipherment, etc., however, it appears that the pre-World War II situation has not changed. 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 reestablishment of the Government in Paris. This history of the French cryptographic practice in recent years points to the conclusions that (a) there is probably no single cryptologic agency in France; (b) there may be, as before, some loose collaboration among the Army, Navy, Colonies and Interior; (c) the Foreign Ministry still prefers to go its own way.