For Official Use Only Register No. 303

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

THE CONTRIBUTION OF THE CRYPTOGRAPHIC BUREAUS IN THE WORLD WAR

TITLE - THE CONTRIBUTION OF THE CRYPTOGRAPHIC BUREAUS IN THE WORLD WAR.

SERIAL No. 303

1. This pamphlet is a RESTRICTED document and is the property of the Office of Chief of Naval Operations (Communication Security Group).

2. This pamphlet is not a Navy Registered Publication and will not be reported as such. The Register Number, on the cover is used, for library records as a Serial number.

3. This pamphlet is loaned to:

Commanding Officer, U.S.S. ASTORIA

for a period of (6) months from the date of receipt. Upon the expiration of the loan period this pamphlet will be returned to the Office of Chief of Naval Operations (Communication Security Group) Navy Department, Washington, D.C.

For Official Use Only

WAR DEPARTMENT
WASHINGTON

303

THE CONTRIBUTION OF THE CRYPTOGRAPHIC BUREAUS IN THE WORLD WAR

By
YVES GYLDÉN

▼

Reprinted from
SIGNAL CORPS BULLETINS Nos. 75–81
November 1933 – November 1934

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1935

Foreword.—In 1931 there was published at Stockholm by Mr. Yves Gyldén, a well-known Swedish code and cipher expert, an important brochure on cryptography under the title "Chifferbyråernas Insatser I Världskriget Till Lands." The instructive and informative nature of Mr. Gyldén's work was at once recognized by the editor of the Revue Militaire Française, at whose request Mr. Gyldén prepared a condensed version, which was published in the above-mentioned journal in August 1931 (no. 122) and no doubt attracted the notice of official cryptographers all over the world. When Maj. William F. Friedman, Signal Reserve, Chief of the Signal Intelligence Section in the Office of the Chief Signal Officer, brought Mr. Gyldén's work to my notice and indicated the value the publication of a translation of the complete book would have for Signal Corps personnel, steps were immediately taken to obtain the author's permission to publish the translation in serial form in the Signal Corps Bulletin. Mr. Gyldén very kindly granted the permission sought and the translation appeared in seven successive installments in the Bulletin, beginning with the November–December 1933 issue and continuing until completed in the November–December 1934 issue. This pamphlet is merely a reprint of the translation as it appeared in the Bulletin, save for changes in the numbering of the footnotes. The translation was made by the Military Intelligence Division of the War Department General Staff. Major Friedman, who edited the translation, has added some comments, which are invariably enclosed within brackets and are signed by the initials W. F. F.—*Editor of the Signal Corps Bulletin.*

CONTENTS

THE CONTRIBUTION OF THE CRYPTOGRAPHIC BUREAUS IN THE WORLD WAR[1]

By Yves Gyldén

Motto: For in truth decrypted letters are very useful.—*A Venetian cryptanalyst of the sixteenth century.*

INTRODUCTION

To write a review of the contribution of the cryptographic bureaus to the World War is no light task. The material available is very meager and difficult of access, because all official cryptographic and cryptanalytic activities of a diplomatic, political, or military nature have, as a rule, until very recently been enshrouded by a secrecy difficult to penetrate.

However, some information has gradually leaked out in various ways, chiefly through the literature on cryptography published since the World War and also, to a considerable extent, through the numerous reports, articles, and memoirs recently published on the war or on events connected with the war. The more remote the war becomes, the easier it is for the cryptographic and cryptanalytic experts who took part in it to loosen their tongues, and that not without important reason.

That is, the secrecy which enshrouded almost all cryptographic activities before the war has proved itself to be a two-edged sword. The experiences of the World War proved conclusively that such secrecy most frequently does more harm than good. It prevents the spreading, among soldiers and civilians alike, of the general training in cryptography absolutely necessary for the conduct of modern warfare. It restricts the horizon of the cryptographer and lulls him into a fallacious self-conceit. A knowledge of the means, methods, and aims of military cryptography is a necessary prerequisite, especially for all commissioned officers, if effective protection is to be obtained by the use of one's own codes and ciphers and if the blunders and errors on the part of the enemy are to be exploited in the most effective manner by one's own cryptanalysts and utilized to the advantage of one's own leaders.

A general ignorance of questions pertaining hereto brought about results of very decisive importance on several occasions during the World War. We need merely cite the instance of the indiscretion on the part of the Russians in the use of radio and cryptography which contributed greatly to the German military successes on the eastern front during the fall and winter of 1914. General Hoffmann, in his renowned work, "Der Krieg der versäumten Gelegenheiten", says of these indiscretions: "This carelessness facilitated the conduct of warfare in the east for us; in many situations it alone really made it possible for us to carry on war."[2] The Russians were by no means the only warring nation guilty of such carelessness. The armies of all the warring nations were guilty, some to a greater extent, such as those of Italy and Germany, and others to a lesser extent, such as those of France, England, and Austria.

A great responsibility rests upon the cryptographic services in all countries. Surrounded by a strict secrecy, the chiefs of these services may very easily develop disastrous misconceptions with regard to the resistance their own codes and ciphers afford against the efforts of the enemy's cryptanalysts to solve them. The said chiefs perhaps do not realize that the enemy may possess other methods and other means of cryptanalysis than those possessed by themselves. If, besides this, they are ignorant of the technic of cryptanalysis, which so frequently was and in some places still is the case, the results can only be disastrous. The absence of criticism and of general testing which accompanies secrecy—a criticism and a testing which are all the more

[1] Original Swedish edition copyrighted by Yves Gyldén.

[2] Carlswärd, Operationerna på tyska ostfronten, p. 39.

necessary because cryptography, on the whole, is still an "unexplored field"—often prevents grave errors from being discovered at all. Much can be said about the all-too-common condition that too strict a secrecy serves rather to protect inefficiency and lack of knowledge from criticism than to protect one's own code and cipher system from being solved by the enemy.

Most dangerous of all is the prevalent misconception concerning the "degree of safety" of a code or cipher system. A person unacquainted with the methods and means used by the cryptanalyst judges the degree of safety of a system by the length of the periods or by the number of possible variations permitted by that system. He does not suspect that there are systems possessing permutative possibilities that can be expressed in millions and billions, which nevertheless can be solved in a few hours—often less—in a purely mechanical way. A person versed somewhat, but not sufficiently, in the methods of cryptanalysis often makes a still more dangerous error by seeking increased safety for the cryptographic system in involved complications. He fails to consider that these very complications most frequently render the cryptographing more difficult and thus give rise to blunders and errors which *facilitate* the solution of the system.

The degree of safety possessed by any code or cipher system is not dependent upon any theoretical calculations nor upon its complications.[3] It depends, in the first place, upon *the manner in which the system is employed.* It depends, in the last analysis, upon the technic applied by the cryptanalyst in trying to solve it. Only one who has a thorough knowledge of the modern technic of cryptanalysis is capable of judging the degree to which unavoidable errors on the part of his own cryptographers are increased or decreased by a certain system or by a certain complication, and is capable of judging with adequate approximation the highly complex question of the "degree of safety" possessed by a system. Innumerable were the instances in which an increased "theoretic" safety helped the enemy to solve a system.

In the hands of personnel inexperienced in cryptography the safest possible system is so handled that it can be solved in a manner entirely unsuspected by the said personnel. Little do rules and regulations help as long as the personnel does not *understand* their real import; they are blithely broken in the heat of combat, especially during the first part of a war. Devotion to duty and discipline are good foundations to build on, but they are insufficient for a cryptographic service. Knowledge and intelligence form a far more dependable and secure foundation. A devoted and conscientious personnel, if ignorant of the principles of cryptography, makes numerous errors, for it does not actually understand what an error in cryptography is. An apparently precautionary measure frequently constitutes an error. The experiences of the World War have shown that the diffusion of knowledge concerning the methods of cryptanalysis among the cryptographic personnel reduces errors to a practically insignificant minimum. They cannot, however, be entirely eliminated.

In brief, all unnecessary secrecy is to a high degree obstructive to knowledge of and efficiency in cryptography, both as far as the officers and the personnel of lower rank are concerned. To the cryptographic personnel, which is quite extensive in a modern war and which will rather be increased than decreased by the development of radio, most obviously the old saying that a chain is only as strong (strength here meaning knowledge of the subject) as its weakest link, is applicable.

Therefore we cannot marvel at the fact that at least in the countries which took part in the World War the experiences of that war have weakened the opinion regarding the necessity for secrecy. Significant enough is the fact that advocates of the elimination of all unnecessary secrecy are to be found among the foremost chiefs of the military cryptographic bureaus that were in operation during the World War.

[3] [An appreciation of the truth of this simple, clear statement would save much time and useless effort on the part of would-be cipher inventors. We are however inclined to modify the statement to the extent of saying that the degree of safety is not directly correlated with calculations or complications of a purely theoretical nature.—*W. F. F.*]

For example, General Givierge, who during the war was chief of the cryptographic bureau of the French General Staff, without doubt the most authoritative of all such chiefs, says on this subject:

> Too much secrecy is sometimes harmful; too greatly enshrouding the science of cryptography with secrecy and preventing anyone from learning it results in a lack of expert trained personnel, while diffused general knowledge in other fields such as, for example, that of transportation, by no means prevents the staffs from keeping secret the details which might be of interest to the enemy.[4]

The same author maintains that national safety demands that cryptographic and cryptanalytic talent be discovered and developed in time of peace so that in the event of mobilization the nation need not be solely dependent upon locating talent of that type in an instant, to be used for increasing the personnel in the cryptographic bureaus that have already been functioning in time of peace.[5] The Swedish writer, Capt. T. Carlswärd, expresses himself in a similar vein: "The officers who are to handle this phase (cryptography) in the field must gain an opportunity in time of peace for learning the art of cryptography, as well as the still more difficult art of cryptanalysis."[6]

These ideas and concepts are of still more importance for our country when we consider the fact that the long period of peace we have been enjoying has prevented practically all worries about the safety of our own code and cipher systems, or the contingency that those systems may be solved by a possible enemy. Exercises help little, no matter how nearly the conditions surrounding them are made to simulate actual war conditions. We can never reconstruct the mental tension under which many a cryptographic clerk in war neglects all elementary precautionary measures because the methods of enciphering and deciphering are too involved or too tedious.

The conditions surrounding cryptanalysis are analogous. This science easily tends to become restricted to chamber analysis, that is, analysis by one individual of one single message. This type of cryptanalysis is to the work done in a modern cryptanalytic bureau as a leather-cased gun is to a modern, long-range, railroad gun. Furthermore, this type of work is very treacherous, because it tempts the analyst to consider cryptanalysis in general as a linguistic-statistical and analytic work, individualistically performed on one or a few communications. Nothing is further from the truth. Modern cryptanalytic technic involves the cooperation of several persons in a combined analysis and synthesis, for which much material is required from *outside* the special domain of cryptography. Chamber analysis is merely a fraction of the work. Here, as in many other fields, the World War brought about an almost revolutionary development in technic, a development which was foreseen only by a few French writers on cryptography of the eighteen eighties.

Acquiring a knowledge of cryptography and cryptanalysis is rendered much more difficult in Sweden by the fact that there is no Swedish literature on the subject, with the exception of an essay by Torpadie which is very restricted in scope and shows an entire lack of familiarity with modern technic.[7] As belonging to this type of literature we can scarcely count the few academic dissertations from the eighteenth century by Ekerman and Forelius [8] or Hugo Grotius' various projected codes. Foreign literature on this subject is available in a striking minimum in

---

[4] Givierge, Cours de Cryptographie, Introduction, p. VII. [NOTE.—This book, undoubtedly the best and most important work on cryptanalysis thus far published, has already gone through three editions, the first two appearing in 1925, the third in 1931. It can be obtained at a very reasonable cost from the publishers, Berger-Levrault, 136 Boulevard Saint-Germain (VIe), Paris.—*W. F. F.*]

[5] Givierge, Cours de Cryptographie, Introduction, p. VII.

[6] Carlswärd, Den trädlosa telegrafien under världskriget, p. 105.

[7] Torpadie, Några ord om chifferskrift, Hist. Tidskrift VIII, 1888, pp. 376 and following. [NOTE.—The paucity of literature on cryptography in the English language is more striking than that in the Swedish language.—*W. F. F.*]

[8] Forelius, Dissertatio de modis occulte scribendi et praecipue de Scytala Laconica, Stockholm, 1697.
Forelius, Dissertatio de Hieroglyphicis et sacris veterum literis, Upsala, 1701.
Ekerman, Ratio scribendi hieroglyphitica, Upsala, 1755.

the Swedish civilian and military libraries. The basic French works written in the eighteen eighties on cryptography are not, as a rule, included. But it must be admitted that the procurement of such literature published some time ago has become very much more difficult, particularly since the World War.

Interest in military cryptography has, however, been very great in certain countries. For example, in France, which without doubt may be said unquestionably to have held the leading place in the field of crytography for several decades, not less than 15 works on cryptographic subjects were published by military authors in the period from 1880 to 1905 alone. Five of these works can even yet be classified as standard on their respective phases of cryptography.

The present work is written for the purpose of pointing out the extraordinarily great part played by cryptography during the World War and of giving an account of the cryptographic activities at that time, within the scope permitted by the information available to the author. On the other hand, its aim is also, so far as possible, to increase interest in cryptography among extensive circles from which experts may be recruited.

Reports on cryptographic activities during the World War, published after the close of that conflict, are of varying value. In them also the excessive secrecy has tended to create confusion, for it has tended to favor obvious exaggerations and distortion of facts which can only with difficulty be evaluated by an outsider. However, the exaggerations, as a rule, are of such a nature that they have transferred to the credit of espionage the result of many cleverly effected cipher solutions, and this has often been done with the consent of the cryptographic bureaus concerned, as we shall point out farther on. We have therefore found it necessary to make a careful expurgation and collation of the material collected in the warring countries and elsewhere. Consequently, this book is submitted to the reader as an attempt at synthesis which has as far as possible been compiled from reliable sources written by experienced cryptographers.

For the purpose of making clear the widely differing conditions under which the great powers introduced and developed their cryptographic operations, the author has deemed it necessary to preface his actual report by a discussion on the development of cryptography in the countries concerned during the period just preceding the late war.

CHAPTER I

THE PRE-WAR PERIOD

The period in the history of cryptography immediately preceding the World War is usually designated by the majority of authors on that subject as the "period from 1880 to 1914." The dates of demarcation are without doubt correctly selected, because a marked turning point occurred in the history of cryptography in 1880, and an entirely new era began with the World War.

After a long period of decadence, about the year 1880, cryptography began to be affected by the extensive technical development which had set its impression on so many other fields of human endeavor. A flourishing, although very irregular, literature on cryptography demonstrates the regular development of that science until 1914; it deserves great attention because it forms an excellent criterion whereby to judge the technical skill and knowledge of the experts concerned in the various countries. That is to say, all this literature deserves great attention except the works published by amateurs, which usually are worthless.

Cryptographic literature in general is not, however, distinguished by any profuse richness. Yet, comparatively complete bibliographies contain a list of about 200 works exclusively devoted to cryptography which were published during this period, and a list of more than 100 works dealing partly with cryptography. That cryptographic literature still is difficult to procure is chiefly due to the fact that practically whole editions, at least of the first-class works, are taken for military instruction purposes in the countries of the various authors, and also due to the fact that it is difficult to obtain such literature at public libraries, both inside and outside of Sweden. It is worthy of mention that in the Royal Library of Stockholm this literature is classified under the rather misleading category of "paleography" and that in the libraries in foreign countries it is sometimes classified under such divergent categories as "military science" and "stenography."

If to this we add the fact that until recently no dependable or entirely complete bibliography was ever compiled on the said literature, it is obvious that such obstacles have greatly restricted the development of cryptography and that cryptography has developed very differently in the different countries. We need not, therefore, be surprised that in those countries in which there is no tradition and in which no combined and coordinating cryptographic bureaus have been in existence for a long time, a stagnating level of knowledge is found to exist among a number of consecutive authors, while in other countries there is evident a marked and perceptible increase in knowledge resulting from the increased experience gained in permanently organized cryptographic bureaus.

Two tendencies, separated as to end and means, are to be distinguished in the pre-war literature, all the more easily as they represent different national "schools." These schools, the German and the French, together dominate all of the cryptographic literature. The latter school, however, still is greatly superior, both as to quality and quantity of its achievements, for reasons which I shall try to point out later on.

The German school, the forerunner of which was Colonel Fleissner von Wostrowitz [9] of the Austrian Army, obviously restricted its activities to simple cryptography, entirely neglecting

[9] Fleissner von Wostrowitz, Handbuch der Kryptographie, Vienna, 1881.

cryptanalysis. All its authors, among whom are to be noted the well-known German criminologist Schneickert [10] and in our day Colonel Figl [11] of the Austrian Army and the criminologist Türkel,[12] were absorbed in a hopeless system of cipher complications, without prior explanation of the cipher theory, and they placed a minimum of importance on cryptanalysis, which was chiefly restricted to a repetition of the methods of solving elementary ciphers given by the older German authors Klüber [13] and Kasiski,[14] and the corresponding method of the latter for the so-called "multiple-alphabet substitution cipher", both systems of the very simplest type. All these works except a few restricted special treatises, may be said to constitute catalogs of simple systems, mostly old-fashioned. These systems are repeated by every author, with the addition of numerous complications, which always make the work of the cryptographic personnel more difficult and frequently prove no obstacle to the enemy's cryptanalytic experts. The lack of cryptographic theory often led the above-mentioned authors, for example, Fleissner, Schneickert, and Figl, to describe under different names systems which are identical in structure and which may sometimes be solved in identically the same way.

It is exceedingly easy to find the main sources of the German school. They include the above-mentioned authors, Klüber and Kasiski, so far as the description of the systems and the primitive cryptanalytic regulations are concerned. Again, so far as the classification of the systems is concerned, it may without difficulty be traced to an author as early as Selenus.[15] Without being guilty of underestimation, we can state that the authors of the German school after Kasiski did not make any real progress. He was meritorious enough for his time, but his work was absolutely antiquated by the end of the nineteenth century. As far as Fleissner's work is concerned we must, on the whole, join in the warning against inaccuracies and mistakes which is issued by the French authors Lange and Soudart.[16] Schneickert's work is characterized by an unlimited overestimation of the safety of the system described in it, and as for Figl, we cannot forego expressing our surprise that so modern an author can display, on the ordinary plea of a "strictly scientific system", such numerous misconceptions concerning code and cipher theory and the effectiveness of the protection afforded by proposed complications.

With the exception of certain other purely historical works by other authors, works which moreover are highly interesting, we are naturally impressed by the obviously slight knowledge possessed by the German school concerning the progress shown in the literature of other countries, especially France. This ignorance may possibly be attributed to the striking lack of bibliographic material which we have already mentioned, but must to a far greater extent be due to the lack of a permanent center of study in the form of organized cryptanalytic bureaus.

If we attempt to analyze the reasons for the false estimate of systems in the various works, we find that it appears to be due to a faulty theoretic basis for the analysis. In such an uncertain subject, one so difficult to survey as is cryptography, explicit theoretic bases are indispensable; without them every analysis risks becoming not only one-sided and incomplete, but even to the highest degree misleading if used for judging the real resistance of the system to efforts of the enemy to solve it (providing that it is carefully used).

The analysis in the above-mentioned works, which has been made with the usual German thoroughness and accuracy, is entirely directed at the complications. The actual or substantial

[10] Schneickert, Moderne Geheimschriften, Berlin, 1900.
Schneickert, Geheimschriften im Geschäfts-und Verkehrsleben, Leipzig, 1905.
Schneickert, Die Graphologie als Hilfsmittel zur Entdeckung von Geheimschriften, Munich, 1899.
[11] Figl, A., System des Chiffrierens, Graz, 1926.
[12] Türkel, Morse u. Morseähnliche Zeichen, Graz, 1926.
Türkel, Chiffrieren mit Geräten u. Maschinen, Graz, 1927.
Türkel, Kryptographische Parerga, Graz, 1929.
[13] Klüber, Kryptographik, Tübingen, 1809.
[14] Kasiski, Die Geheimschriften und die Dechiffrierkunst, Berlin, 1863.
[15] Selenus, Systema integrum Cryptographiae, Lüneburg, 1624.
[16] Lange et Soudart, Traité de Cryptographie, Paris, 1925, p. 67.

structure of the system has been overlooked entirely. If we find little to say concerning the relation of the conclusions to the premises, the premises themselves are, on the contrary, not only faulty but even in certain cases entirely false, which explains the inability to find a utilizable standard for estimating the value of the system. For similar reasons the classification is entirely wrong. It is based everywhere, except in the work of Figl, on the *aspect* of the cipher signs. Anyone who is, in the slightest, familiar with the art of cryptanalysis knows that this detail is of no importance and can never mislead anyone except the cryptographic clerk himself. Again, speaking of Figl, his "new" classification was only relatively new because it was known by the authors of the French school 40 years before.

The faults enumerated above illustrate that the technic of cryptanalysis was neglected. The latter is based on purely theoretical grounds, starting with the 2- or 3-dimensional structure of a system. A knowledge of the structure of any system enables us readily to discover its weaknesses and its strong points. Such a knowledge enables us to locate several negative complications in the examples given by Figl—that is to say, complications which instead of rendering the solution of the cipher more difficult directly facilitate that process.

It may seem peculiar to a layman that such misconceptions should be found in the works of authors from whom we have every reason to expect a logical analysis. This is none the less extremely common when the investigations are not based on a knowledge of the science of cryptanalysis. A locksmith may in the same way be mistaken about the dependability of a lock if he has no idea of what a lock pick looks like or how it is used.[17]

Now, to take up a consideration of the French school, we find that it also is represented by a comparatively great number of authors, a few of whom may be designated as very eminent. A number of works, beginning with those of the remarkable cryptanalyst and philologist Kerckhoffs, display a very plain indication of a tendency toward a synthetic cipher theory and of a frequently astonishing insight into the technic of cryptanalysis. Several works by the military authors Viaris, Kerckhoffs, Valerio, and Bazeries, and some by the mathematician Delastelle, deserve to be designated as standard so far as certain subjects are concerned. These works, which followed each other at very short intervals, are characterized by a continuity of aim that may certainly be attributed to the influence of a permanently organized, effective cryptographic bureau, so that the primeval forest of cryptography was cleared according to a clearly drawn-up and consistently executed plan. To the authors we have already mentioned there may be added a great number of less important ones who for the most part merely copied the work of their predecessors, but at times also advanced some original views. Such were Myskowski, Simonet, Dallet, Angammare, etc. Others again, such as Josse, published works purely historical in character or catalogs of known systems of ciphers.

The French school based its work to a great extent on purely theoretical grounds. It analyzed the real structure of the different systems and deduced therefrom, correctly enough, the various methods used in cryptanalysis. In this way these highly theoretical works have led to extremely practical results as far as the technic of cryptanalysis is concerned, which in turn have affected the choice of suitable systems for the use of the French and of complications really effective in rendering those systems safer.

If we attempt to compare the two above-mentioned schools, we find that the theoretical bases of the French ciphers and the great interest of the French school in cryptanalysis led to much more valuable, practical results, both in the application of cryptography and cryptanalysis, than the systematized analysis of the German school which was executed without any previous knowledge of the underlying principles necessary for the correct evaluation of a system. The

[17] [The author is, in my opinion, somewhat severe if he intimates that Colonel Figl is lacking in knowledge of cryptanalysis. General Ronge (p. 57) says: "So I managed, in November 1911, to have an officer assigned to the cipher service, to relieve me of the burden. It was Captain Andreas Figl, who developed into a brilliant helper, and headed the cipher group, with few interruptions, up to the end of the World War."—*W. F. F.*]

German school, with surprising consistency, committed the common error of assuming that an increased complication of the code or cipher necessarily meant an increased security. Experience has shown, singularly enough, that real security in a code or cipher is often in inverse proportion to the complication of that code or cipher, for reasons which we need not discuss any further here.

Just as the German school entirely ignored the French school, so the French school apparently also failed to take any notice of the German school. Each school went its own way unconcerned about its competitor. What is said here applies to the authors on cryptography and not to the French cryptanalytic bureau. Farther on we shall show how the latter followed the development of the German school very closely.

The cryptographic bureaus in some countries date very far back; in others again they were founded very recently. These differences in age apply to the cryptanalytic bureaus to a still higher degree.

The lack of a clear line of demarcation between the activities of the bureaus mentioned above often leads to a misunderstanding. Permit us to explain here that by the expression "cryptographic bureau" we generally mean a government establishment, usually under one of the Ministries of Defense, the Ministry of Interior, or the Ministry of Foreign Affairs, which is responsible for the compilation and application of the codes and ciphers. But by a "cryptanalytic bureau" we mean a corresponding establishment performing the following missions: In time of peace examining and solving the code and cipher systems of any possible adversaries; drawing up the necessary instructions for the mobilized personnel; and also assuming responsibility for the execution of the measures through which in time of war the necessary material for solving the codes and ciphers of the enemy is transmitted to the bureau. As a rule, the cryptographic and the cryptanalytic bureaus are organized as one bureau; only when the activities are extensive, such as is true in time of war and even in time of peace in the government departments of the countries of the great powers, they may be organized as entirely independent bureaus, although very intimate contact always has been found to be absolutely necessary between them.

Hence, in what follows, the expression "cryptanalytic bureau" will be used to indicate an *organization composed of cryptanalysts, the main mission of which is to solve the enemy's codes and ciphers*, irrespective of the said organization's relation to or cooperation with the corresponding cryptographic bureau.

The oldest known cryptographic bureaus were located at Venice under the Doges and at the papal curia in Rome. From 1300 to 1400 these centers were so very well organized that they may in some respects be considered as models even today. Their work included both cryptography and cryptanalysis to an equal degree, and with a logic which even today has no equal in many places, cryptanalysis was placed first for the very logical reason that the person who is best able to solve a cryptogram is able to grasp the weaknesses of his own systems and work out means for eliminating them. The requirement for admission to the said Italian bureaus, especially that in Venice, for this reason consisted of the passing of a very difficult examination in the science of cryptanalysis, which was given once a year for applicants satisfactory in other respects. The technical literature on cryptography of that period also shows a most surprising insight into the problems of cryptography, and we must call attention to the fact that the dissertation on cryptanalysis written at Milan by Sicco Simonetta, a cipher clerk, and dated 1474, is even today considered greatly superior to all reports prepared by the German school on the solution of the same cipher system.[18]

During the period of decadence of cryptography—that is to say, the eighteenth century and the first half of the nineteenth century—the remarkable insight of the Italians into the importance of cryptanalysis gave way to the primitive conception that entirely safe ciphers may be compiled and employed by a personnel not versed in cryptanalysis. The said idea,

[18] Sicco Simonetta, Regulae ad extrahendum litteras zifferatas sine exemplo, Milan, 1474.

which is based on a widespread, deep ignorance of the nature of cryptography, certainly resulted in a corresponding decline in the skill of the cryptanalysts during the above-mentioned period. In several places the same idea still persists today.

Thus, in many countries during this period of decadence, the science of cryptanalysis was entirely neglected; while in others, those which previously had maintained permanent cryptographic bureaus, it appears to have been at a standstill. The latter was the case, for instance, in France, among other countries. There the cryptographic and cryptanalytic bureau established by Richelieu had been extraordinarily well organized by the well-known cryptanalyst Rossignol,[19] who laid the foundations for the traditions of the modern French school. In Austria also there was in existence during the reign of Maria Theresa a particularly well organized and effective cryptanalytic bureau directly under the Minister, Prince v. Kaunitz.[20] Its traditions also have been lost, however, at least as far as cryptanalysis is concerned.

In England and Prussia, during the same period, cryptographic activities were to a great extent restricted to the compilation of the British and Prussian code and cipher systems. No cryptanalysis was done in these countries, or if there was any it was only very unimportant. All that is known about conditions in Russia is that Czar Alexander I had a corps of cryptanalysts who succeeded in solving a number of the ciphers used by Napoleon I. These were probably of great importance for Russian strategy.[21]

We must, of course, remember that successful cryptanalytic operations were not always made public, even long after they had been accomplished, and that the work achieved along this line certainly was greater than documents so far available have shown. We may also with certainty assume that such work was restricted to a very few centers in the period under discussion, due to the lack of qualified experts.

At the beginning of the eighteen eighties conditions were as described in the following chapter in the places where military cryptography was chiefly employed.

A. FRANCE

In France all official cryptographic work was placed under the Government ministries. The sharp delimitation which the republican regime brought into the executive ministries is reflected in the division of the cryptographic bureaus among five ministries, namely, the Ministries of War and Navy, the Ministry of Foreign Affairs, the Ministry of Interior, and the Ministry of Posts and Telegraphs.[22] In addition to this, the special police, known as the "Sûreté Générale", operated a cryptographic bureau, which became widely known for its clever cryptanalysts.[23] Despite unavoidable rivalry, cooperation between these various bureaus was comparatively good, a circumstance which was to a great extent promoted by the fact that the military experts received their training and instruction from specially trained civilian experts in the Ministry of Interior and the Ministry of Foreign Affairs.[24]

The work in all these bureaus included both cryptography and cryptanalysis. The latter, that is to say, cryptanalysis, as far as the Ministries of Defense were concerned, was chiefly a matter of theory and organization, while the experts at the Ministry of Foreign Affairs were wholly engaged in solving diplomatic codes, and the Ministry of Interior, or the Sûreté Générale, was engaged in solving the codes and ciphers used by criminals and anarchists, the cipher of the

[19] Lange et Soudart, Traité de Cryptographie, p. 44.

[20] de Broglie, Le secret du roi, Paris, 1879, II, p. 514 and following.
Boutaric, Correspond. secrète inédite de Louis XV, Paris, 1866, p. 162 and following; II, p. 379, 384, and following.

[21] Bazeries, Les chiffres secrets dévoilés, Paris, 1901, pp. 214 and 215.

[22] Lange et Soudart, Traité de cryptographie, Paris, 1925, p. 11.

[23] The Sûreté Générale comes under the Ministry of Interior.

[24] Givierge, Cours de Cryptographie, including p. IX. (Ancel and Haverna were the experts in the Ministry of Foreign Affairs and the Sûreté Générale, respectively.)

royalist conspirators, and after the Dreyfus case, the ciphers and codes used by spies, as the counterespionage service was transferred from the G–2 Section of the General Staff to the Sûreté Générale.

Work was never lacking; on the contrary, there was too much work, because the analysis of the most important codes and ciphers was assigned simultaneously to the experts in the various ministerial departments, competition then spurring them on to do their best.

The material came pouring in from various sources. The most important of these sources was formed by the copies of telegrams which the "Black Chamber" of the Ministry of Posts and Telegraphs constantly brought to the cryptanalytic bureaus.[25] Other sources were the military radiograms sent by the neighboring countries during peace maneuvers and intercepted by the special intercepting sections, which we shall discuss later on, also spies and deserters.

A very good instance of the above-mentioned cooperation was to be found in the handling of the material available in the Dreyfus case, all the operations involved in which have by this time been made public. During the whole time required for solving the famous so-called Panizzardi telegram, Colonel Sandherr, chief of the Statistical Section, G–2 of the General Staff (counterespionage service), who in that capacity kept in direct contact with the cryptanalytic bureau in the Ministry of War, was daily kept informed of the progress made in the solution by the bureau in the Ministry of Foreign Affairs.[26]

As we have already mentioned, the military cryptographic bureaus did not restrict themselves solely to cryptography. This work, at least in the Ministry of War, was organized and divided into two services, the cryptographic service and the cryptanalytic service, until 1912,[27] at which time a general merger of the two services was effected.[28]

On that occasion the cryptographic bureau was placed directly under the Minister of War for several reasons, one of which was the great urgency for immediately encoding and decoding the current correspondence of the Ministry of War. In time of peace there were only two cryptanalysts in the service of the cryptographic bureau, Majors Cartier and Givierge, now both holding the rank of general. However, the bureau cooperated intimately with the "Commission de cryptographie militaire" (Military Cryptographic Commission) which had been organized at the beginning of the twentieth century and is still in existence. This commission, of which Major Cartier was secretary up to and including 1903, consisted of about 10 cryptanalysts selected from among the officers of all ranks and arms who had shown a special aptitude for and knowledge of cryptography and cryptanalysis. The members of the commission were not removed from their normal duties in their regiments, staffs, or corps, but were to devote themselves to cryptographic studies and work in their spare time, as a reward for which they were given certain fixed compensation. Special leave was also granted those who participated in the meetings of the commission, but contact between the various members was maintained chiefly by correspondence.

The work of the commission, which attained an extraordinary importance during the World War, included both cryptography and cryptanalysis. The cryptographic work consisted of theoretical and practical tests of the systems which were proposed to the commission by its own members, by other military personnel, or by civilian personnel. The latter used to apply directly to the commission, submitting all kinds of systems, ideas, and proposals for consideration, many of them valueless, but some, however, of exceedingly great value. The author was

[25] Reinach, Histoire de l'Aff. Dreyfus, Paris, 1901, I, p. 245. Viaris, L'art de chiffrer et déchiffrer, Paris, 1893, p. 78. Myskowski, Cryptographie indéchiffrable, Paris, 1902, p. 4.

[26] Cassation du procès Dreyfus, Paris, 1906, III, p. 175. Dreyfusprocessen in Rennes, Stockholm, 1899, I, pp. 51, 55, 57, and 58.

[27] Givierge: Questions de chiffre, in Revue Militaire Française, Paris, 1924, p. 409. [NOTE.—A translation of this very important article was published in the March and May 1926 issues of the Signal Corps Bulletin.—*W. F. F.*]

[28] Idem, p. 399.

informed by two of the former members of the commission that some of the systems adopted were proposed by civilians.

The cryptanalysis consisted partly of general theoretic studies and the compilation of the so very important statistics on the linguistic and the professional-terminology frequencies used by a possible enemy, partly of a special cryptanalysis of the material sent by a service specially organized at some of the forts on the eastern boundary for intercepting German radio messages sent during peace-time maneuvers. Considerable work was devoted to the detailed analysis of cipher systems, information about the application of which in time of peace and the possible use of which in time of war was obtained through spies, deserters, members of the Foreign Legion, or from German military manuals. A series of confidential memoranda was drawn up containing a description of the said systems, statistical data, instructions for cryptanalysis, and other necessary instructions to be distributed directly among the mobilized cryptanalysts, both military and civilian, in the event of war.

In addition, in cooperation with the officers of the cryptographic bureau, the commission organized certain training courses, including among the subjects given an analysis of the German system described in German works on cryptography. These courses were intended partly for staff officers, partly for the military and civilian personnel to be used as a kind of reserve in the event of war. An examination was given at the end of these courses.

The cryptographic bureau in the Ministry of War, the chief of which, for administrative reasons, was also chief of the Central Bureau for Wireless Telegraphy, in turn drew up detailed instructions for the application of their own cipher systems, in the form of regulations, and systematized in detail the highly important connections to be established in time of war with the "special radio stations" charged with listening in, identifying and, if necessary, interfering with the radio communications of the enemy. The regulations governing this matter, "Instruction sur l'emploi des postes radiotélégraphiques spéciaux" (Instructions on the Employment of Special Radiotelegraphic Posts), placed these stations in time of war directly under the cryptographic or cryptanalytic officer at General Headquarters. It should be mentioned that only one officer was to perform cryptanalysis at General Headquarters, but that only a few days after the outbreak of the war there were no less than seven cryptanalysts, which cannot be considered too much in the case of a service that was to be in operation both night and day. Although coming under the minister and attached to his office, the cryptographic bureau in the Ministry of War worked in intimate cooperation with the General Staff.

An experiment was performed particularly for testing the control and supervision of the cryptographic and cryptanalytic work in the field during the General Staff maneuvers held under the direction of General Joffre shortly before the outbreak of the World War, or to be more exact, from April 28 to May 2, 1914. Another maneuver of a similar type, held from May 25 to May 29, 1914, experimented on the supervision of the cryptographic service under similar conditions, especially with regard to liaison between it and the field radio service.

The above facts which for the most part have been taken from "Questions de chiffre", by General Givierge, which appeared in the Revue Militaire Française for June and July 1924, have been complemented by information given by a former chief of the War Ministry's cryptographic bureau and by the chief of the Criminal Technical Laboratory at Lyons, Dr. Locard, who served as cryptanalyst during the World War.

A review of the measures taken shows a very well-organized cryptographic and cryptanalytic service, superior to any that has ever been organized in any other country. It greatly reminds one of such services in the days of affluence of Venice. Both based their efficiency on the technic of cryptanalysis and both obtained extraordinarily good results. The results obtained by the

French will be discussed in this work, but readers interested in the achievements of the Venetian bureau are referred to the singularly detailed and extensive literature on that subject.[29]

Certain phases of the activities of the French bureaus were kept strictly secret; others again were made fully public. These latter included the measures taken by the Military Cryptographic Commission with the view to creating a reserve of civilian cryptanalysts and its work in connection with testing the code and cipher systems offered to it.

Very little information has leaked out concerning the cryptanalytic work done before the World War except concerning the activities of the bureau in the Ministry of Interior which led to public court proceedings, for instance, the trials of the anarchist Ravachol in the year 1892 and the royalist conspirators in the year 1899.[30]

According to a Swedish source, the French Ministry of Foreign Affairs, even long before the World War, was in possession of the key to the German diplomatic code,[31] probably obtained by a successful solution of that code. We also learn from the correspondence of Isvolsky, which has been published by the Bolsheviki, that "This (the French) Ministry of Foreign Affairs, which has the key to the Italian telegraphic code, is thus in a position to secure information not only from telegrams sent to the Italian Ambassador at Paris, but also from those exchanged between Rome and its Ambassadors at Berlin and Vienna." [32] Very interesting and illuminating are also the revelations concerning the codes solved by civilian and military experts during the Dreyfus trial mentioned above, which were made public during later trials (Rennes and Court of Cassation trials).

A study of absolutely dependable sources has induced the author to give here the details of the most important events connected with the solving of those codes.[33] These seem to be of sufficient importance to deserve repeating here.

It is known that the first Dreyfus trial was surrounded by an impenetrable veil of secrecy. When later on it was found that some of the "evidence" submitted before the courtmartial had been falsified, the conclusion was drawn that the secrecy was caused by the fear that the said "evidence" might become generally known and might cause an appeal for a new trial. However, that could not have been the case, for the secrecy was based not so much on any preconceived purpose of unjustly and illegally injuring Captain Dreyfus but was rather due to the anxiety to conceal two very important facts, namely: that the code used by the Italian military attaché Panizzardi in the exchange of telegrams with the Italian General Staff was unsafe, could be broken, and that there were spies belonging to the counterespionage section of the French General Staff at the German embassy in Paris, which spies were particularly to keep informed concerning the correspondence of the German military attaché, von Schwartzkoppen.

It is also known at present that the famous so-called Panizzardi telegram of November 2, 1894, the real tenor of which wholly exonerated Captain Dreyfus, was later purposely altered

[29] Cecchetti, Le scritture occulte nella diplomazia veneziana, Venice, 1868.
Pasini, Delle scritture in cifra usate dalla rep. Veneta, Venice, 1873.
Pasini, Cifra e studii del. cav. L. Pasini, Archives of Venice.
Perret, Les règles de Sicco Simonetta, etc., Paris, 1890.
Meister, Die Anfänge der modernen dipl. Geheimschriften, Paderborn, 1902.
Baschet, Les Archives de Venise, Paris, 1870.
Wagner, Studien zu einer Lehre von der Geheimschrift, Arch. Zeitschrift, XII, Munich, 1887.
[30] Lange et Soudart, Traité de cryptographie, pp. 75 and 79.
[31] E. Anderberg, Maritim förbindelsetjänst under världskriget, Stockholm, 1926, p. 30.
[32] Nic Blaedel, Storpolitik i Mars, in the Nya Dagligt Allehanda of Apr. 1, 1931.
[33] Bazeries, Les chiffres secrets dévoilés, Paris, 1901, p. 146 and following.
Reinach, Histoire de l'Affaire Dreyfus, Paris, 1901, I, p. 245 and following; p. 592 and following.
Dreyfusprocessen i Rennes, Stockholm, 1899, II, p. 177 and following.
Clemenceau, Des Juges, Paris, 1901, p. 175 and following; p. 357 and following.
Lange et Soudart, Traité de cryptographie, Paris, 1925, p. 80.
Locard, Le crime et les criminels, Paris, 1925, p. 207 and following.
Locard, L'enquête criminelle, Paris, 1925, p. 234.
Givierge, Cours de Cryptographie, Paris, 1925, p. 240.

so as to prove the guilt of the captain. As we all know, it required several years for Parliament and for public opinion to break down the stubborn resistance of the General Staff and to obtain knowledge of the actual contents of that telegram.

Dreyfus was suspected of having engaged in traitorous transactions with the Italian and German military attachés just before his arrest. As so often is true of the military attachés of the various countries, these two attachés were cooperating in the purchase of documents from spies and traitors.

It was likewise known that Panizzardi's code correspondence with his superiors in Rome was carried on with an ordinary commercial code known as the Baravelli code. That this code nevertheless could be used for such important correspondence was due to the fact that its page numbering, which involved every cipher group, was entirely arbitrary and could be agreed upon by any two correspondents using it. For example, one code group 4711 could mean page 47 agreed upon, expression no. 11 (the expressions on each page were numbered serially). The code contained both 4-figure and 3-figure groups.

The day after Captain Dreyfus' arrest had been generally made known through an indiscretion on the part of the press (La Libre Parole, Nov. 1, 1894) and caused a great sensation, Panizzardi sent a telegram in the above-mentioned code to the Italian General Staff. As usual, a copy of this telegram was turned over by the Black Chamber of the Ministry of Posts and Telegraphs to the cryptographic bureau of the Ministry of Foreign Affairs. It was natural to connect the supposed contents of the telegram with Dreyfus' arrest, so much the more so as the report constantly spread to the effect that he had acted as a spy for Italy.

Consequently, the experts calculated that Panizzardi probably had used the expression "capitano" and "arrestato", found in the code, together with the letters and syllables which permit the composition of the name Dreyfus. The page numbering was certainly as a whole unknown, but some earlier attempts at solving the code had permitted the identification of a few page numbers, and in the present case the fixed numbered expressions for the words or letters as surmised were known. The last-mentioned expressions were found correctly in the relative order, which fully confirmed the accuracy of the hypothesis, but the page numbering which had partly been learned during the previous efforts at the solution of the code had been changed and therefore its identification had to be begun from the beginning again.

Therefore, although it was possible to identify the numbering on the pages from which the words or letters contained in the telegram "arrestato capitano Dreyfus" could be found, there still remained the task of finding the numbering of the other pages containing clear-text expressions. This could not be done, because there was no apparent connection in the page numbering, and therefore the efforts at solving the code had to be directed toward identifying the words or sentences (a code contains text units of greatly varying lengths), a task which chiefly was based on successively testing the possible text expressions, one per page of the code, which corresponded to the fixed parts of the cipher groups.

There were great difficulties connected with such work, but it was successfully accomplished except for a couple of expressions the correct interpretation of which was of decisive importance. It was found that a cipher group with a fixed part 88 could mean either "relazione" (relations) on regular page 75 or "provi" (evidence) on regular page number 71. The following alternatives were also found to exist: "Prevenuto emissario" (emissary warned) and "commentare stampa" (press commentaries) in lines 91 and 65 of regular pages 69 and 20 in the first case and 17 and 88 in the latter case.

An absolutely definite knowledge of the arbitrary page numbering consequently was necessary. In order to obtain this the cryptanalytic experts in intimate cooperation with Colonel Sandherr conceived the singularly clever plan of having Panizzardi himself betray his arbitrary

page numbering. For this purpose a number of expressions which were found on the very pages whose numbering it was desired to ascertain were selected from the code. A fictitious message was composed of the expressions thus selected. The idea was to cause Panizzardi to transmit this message in code to the Italian General Staff. That would give the French bureau both a code telegram and its corresponding text in clear language; from such evidence the page numbering could, of course, be deduced.

In order to cause Panizzardi to transmit the message it was very cleverly drawn up in the form of an exposé concerning the activities of an alleged French spy in Italy. This was verbally transmitted to Panizzardi through one of his own spies, who unknown to him was working for the French counterespionage service. The message read as follows:

A certain Y, who at present is at X, will go to Paris in a few days. He is taking a mobilization document which he has procured from the bureaus of the General Staff. He lives at Z street.[34]

Not suspecting the trick the Italian military attaché sent the fictitious message very accurately, after having properly encoded it. He considered that he had every reason to inform his superiors immediately concerning such important activities.

With the copy of this telegram the work of solving the code was easily accomplished. The trick of the experts was successful beyond all their hopes, and there was almost no doubt any longer concerning the exact meaning of Panizzardi's first telegram. That the correct meaning of this telegram was later changed at the General Staff to another detrimental to the interests of Dreyfus (embracing the very interpretation alternatives which proved to be *false* when tested, among others, "evidence" and "emissary warned") is another story which does not concern the subject of cryptography.

It is therefore quite evident that even as early as that day cryptanalysts were extraordinarily clever, aside from the strategy of the fictitious message. It may also be said that similar guile was displayed on several other occasions by the French cryptanalytic bureaus, often with good results, especially in solving diplomatic codes. The surprising success of such tricks is due to the usual ignorance of the technic of cryptanalysis and of the manner of using codes on the part of both military and diplomatic code clerks. A direct allusion to the employment of such tricks in warfare is contained in the French regulations for the Communications Service drawn up after the end of the war. In those regulations it is stated that radiotelegraphy is especially well suited for "offensive camouflage" with the application of "fictitious messages." Paragraph 313 when translated contains the following statement on the subject: "Difficult to execute properly, they must not be used except upon orders issued by General Headquarters."

Such methods do, however, assume as an absolutely necessary prerequisite that there be the very closest possible cooperation between the cryptanalytic bureau and the corresponding military and diplomatic leaders, a type of cooperation which could exist in no other countries than France and England.

After this rather extensive digression from the subject, we shall now take up a consideration of the activities of the German cryptographic bureaus during the pre-war period.

B. GERMANY

Little is known about the work of the German cryptographic bureaus for the very simple reason that they did very little. No favorable conditions existed in Germany. There were no traditions and no fruitful modern literature on cryptography.

Still less importance was attributed to the science of cryptanalysis because no really competent cryptanalysts were available for consultation or had received the necessary training.

[34] The name is omitted both in the record given by the historian Reinach (I, p. 250) and in the version of Premier Clemenceau (Des Juges, p. 253).

Cooperation between the civilian and the military authorities was not noteworthy for its intimacy, and there was still less cooperation between the Army and the Navy. And as far as cooperation between military cryptanalysts and civilian experts in that line was concerned, it was made impossible from the beginning by the existence in the Army of regulations governing secrecy in military affairs. Nor was anything like an adequate importance attributed to cryptanalysis by the leading military authorities.

Three cryptographic bureaus or details were in existence before the outbreak of the war. There was one attached to the General Staff of the Army, another to the General Staff of the Navy, and a third to the Ministry of Foreign Affairs. On the other hand, due to the fact that the German Empire was divided into several administratively autonomous states, there was no centralized imperial police service or corresponding organization of such importance as to justify the organization of a special cryptographic bureau.

Of the three bureaus mentioned above, only one, that in the Ministry of Foreign Affairs, engaged in cryptanalytic work, and that to a very restricted extent, presumably on account of the lack of trained experts in that line. The information which was gathered about the code and cipher systems of the leading powers, and the texts in clear for them came, in the great majority of cases, through the well-organized Intelligence Service under the General Staff. This service had practically nothing to do with the cryptanalysis as such.

A very certain index of the nonexistence or extreme limitation of the cryptanalytic work is provided by the weaknesses of the German code and cipher systems. They were such, as is now generally known because of the numerous successful efforts of the Entente at their solution, that an adequate knowledge of cryptanalysis evidently was not required of the compilers or of those whose duty it was to employ them.[35]

The personnel of the General Staff cryptographic bureau was simply assigned to that bureau without any prerequisities as to a knowledge of cryptanalysis. It was the mission of the personnel thus assigned to compile dependable codes and ciphers, safe against solution by the enemy.

It is obvious that this was demanding too much of personnel unacquainted with the rules of cryptanalysis, even though it might have been actuated by the most honest and the most conscientious zeal for the work. The results were such as were to be expected, as we shall show further on.

The assignment of the bureau to the General Staff indicates an entirely different concept of the nature of the cryptographic bureau from that held in France. While in France the cryptographic service was entirely divorced from the General Staff and directly subordinated to the Minister of War, thus possessing a much greater freedom of action and greater possibilities of contact both with other ministerial cryptographic bureaus and with civilian experts in that line, the German organization, in which the cryptographic bureau was placed under the General Staff, excluded all such independence and the possibility of such outside contacts. The heads of the General Staff in Germany, ignorant in all matters pertaining to cryptanalysis, by ordering absolute secrecy made it absolutely impossible to check up on the competence of the cryptographic personnel and on the safety of the code and cipher systems proposed by that personnel. Germany had to entrust itself to a safety that was purely dependent upon chance. The unreliability of code and cipher systems compiled by a service thus organized may very clearly be understood from a statement made by Colonel Nicolai, Chief of the Intelligence Service of the German General Staff during the World War, to the effect that there was need for the organization of a "section to compile safe code and cipher systems and constantly to test the systems in use" (Abteilung zur Sicherung und dauernden Prüfung der verwendeten Chiffriersysteme) during the war under the General Staff.[36]

[35] [For a good picture of the situation as viewed by a German naval officer, see the Dark Invader, by Capt. F. von Rintelen, published by Macmillan, 1933.—*W. F. F.*]

[36] Nicolai, Geheime Mächte, Leipzig, 1925, p. 143.

Inasmuch as the basic difference between the conditions and methods of work which prevailed in France and Germany consisted in the entirely different opinions concerning the importance of cryptanalysis for the cryptographic service, the subject deserves more detailed consideration here.

The safety of a code or cipher system is based upon its resistance to the efforts made to solve it. Therefore, in order to judge the degree of safety possessed by any code or cipher system, provided that system is used according to practical regulations and instructions, a complete knowledge of the means or methods used in cryptanalysis is required, just as a full knowledge of the power of penetration and of the explosive effect of the projectiles which will be fired against it is required in order to judge the resistance of an armor plating.

However, the analogy is applicable only to a certain degree; for the calculations of the effects of the projectile are much easier to make than an estimate of the methods used in cryptanalysis. The latter are particularly complex and little known, vary from case to case, and use the most varied types of aids. For a person who is not a specialist they are exceedingly difficult, if not impossible, to judge.

It has therefore always been true that a personnel ignorant of the technic of cryptanalysis is misled into judging the safety of a code or cipher by standards which are entirely worthless, such as the length of the periods or the number of variations in key. The degree of safety possessed, for instance, by a substitution cipher has long been judged according to both of these factors; that is, a key of 10 units is calculated as giving more than 130,000 billion different combinations for the cipher or letter keys. The solution of such ciphers is very simply accomplished in a purely mechanical way with adequate material and is not disturbed in the least by a "degree of safety" expressed in exceedingly large figures. This estimate does not have anything at all to do with the real safety but is to be considered as a mathematical game. We can best compare such estimates of the safety of a code or cipher system to the estimates of a villa owner with regard to the resistance of his main entrance which has been bolted and locked with ingenious locks, while his kitchen window remains open.

Many authors who have had practical experience in cryptanalysis have pointed out the above-mentioned misconception. Even Lord Bacon warned of the cryptographic personnel's mistaken idea of the safety of a cipher, as follows: "Inexperience and ignorance are so great among the clerks and amanuenses at the royal courts that they very frequently entrust most important messages to unsafe and treacherous cipher systems." [37]

General Cartier, who stresses the common misconception of those code compilers who know nothing about the methods of cryptanalysis and believe that, by complicating the codes and ciphers, efforts at solving them are made more difficult, writes as follows on that subject: "In cryptography there is no positive correlation between the complexity of the cipher operations and the difficulties connected with solving the cipher." [38]

General Givierge is still more categorical: "There are abundant examples of theoretically admirable complications which have proved to be especially advantageous for cryptanalysts. The second system of the German campaign is one of them: They substituted a method which could be solved by means of a single telegram for the preceding system, for the solution of which we needed to find at least two telegrams fulfilling certain conditions." [39]

[37] Lord Bacon, De dignitate et augmentis scientiarum, London, 1623, Liber VI, ch. 1. [NOTE.—The following is the exact wording of Bacon's statement as contained in his London (1605) English edition of his well-known work, The Advancement of Learning: "For suppose that *Cyphars* were well mannaged, there bee Multitudes of them which exclude the *Discypherer*. But in regarde of the rawness and unskillfulnesse of the handes, through which they passe, the greatest Matters, are many times carryed in the weakest *Cyphars*."—*W. F. F.*].

[38] Cartier, Décryptement du Système Schneider, Paris, 1921, p. 7.

[39] Givierge, Questions de chiffre, Paris, 1924, p. 409.

Similar ideas were expressed by Major Bazeries,[40] by the British cryptanalytic expert Hooker [41] and by Lieutenant Colonel Myskowski [42] and others. It is characteristic that, so far as the author has been able to ascertain, no such warnings are found in any work written by the members of the German school.

These almost incredible misconceptions, which as a matter of fact cannot be separated from the ignorance of the technic of cryptanalysis, further accentuate the absolute necessity for making a knowledge of cryptanalysis a basic prerequisite for all cryptographic work. It is a prerequisite for the work of compiling dependable code and cipher systems. It is a basis for the knowledge and the solution of the cipher and code systems used by the enemy. It was, strikingly enough, the basis on which were established the most excellent cryptographic centers in the history of cryptography: that of Venice in the fifteenth century and that of the British and French during the World War.

The general misconceptions concerning the problems involved in cryptography, mentioned above, placed their imprint on the German preparations before 1914. No special measures were taken for mobilizing reserve personnel versed in cryptography nor for cooperation between the various branches of the service and also between the various fronts. Thus it came about that during the first few months of the World War, the code and cipher regulations, the code and cipher systems, and the changes in keys differed on the eastern and western fronts, and that the cryptanalytic service, which was not in existence before the war, was laboriously organized, bit by bit, without any common leadership and without the centralization of experiences or results.

Coordination of the work is of the greatest importance. The medium in which the cryptographer has found himself until recently has been like a forest primeval in the clearing of which the efforts of the individual have availed little. Cooperation and constant contact between as many individuals as possible, individuals having as varied ideas as possible—the more cooks, the better the broth, is a rule which applies to cryptanalysis—and a constant exchange of observations and experiences are necessary for an effective development of cryptanalytic studies. No matter how clever a cryptanalyst may be, he can always learn something from another, and important observations may escape him which may very readily be made by others but not properly utilized. Cryptanalysis requires such a great number of different qualifications that only in the rarest of cases are they combined in one and the same person.

The excessive love of complications, so common among those who know nothing about cryptanalysis, as we have mentioned above, frequently affected the German code and cipher systems, and that all the more so because the same tendency prevailed all through the German literature on cryptography. The result was, as we shall demonstrate further on, that laborious and complicated cryptographic regulations were compiled, regulations which proved to be extraordinarily impractical and time-consuming under field conditions. These complications, the safety of which was frequently illusory, resulted in innumerable violations of the cipher regulations during the first few months of the war (such as mixed messages, partly in clear and partly enciphered, and messages entirely in the clear), constant complaints concerning the difficulties of deciphering, with consequent repetitions of telegrams in the clear text, etc., all circumstances which to a maximum extent assisted the French cryptanalysts and very greatly facilitated their work. We can even assert, with a probability which may be accepted as a certainty, that the first solution of the German ciphers by the French, which was accomplished before the cryptanalysts had yet become well accustomed to the German technic of issuing orders and reports, was to be

[40] Bazeries, Les chiffres secrets dévoilés, Paris, 1901, p. 38.
[41] Hooker, The deciphering of cryptograms, The Police Journal, No. 4, London 1928, p. 623.
[42] Myskowski, Cryptographie indéchiffrable, Paris, 1902, p. 35.

attributed to mistakes on the part of the Germans, particularly those caused by illusory complications in encipherment, rather than to cleverness on the part of the cryptanalysts.[43]

Some of the errors referred to in the foregoing are clearly demonstrated in two special works, written by Swedish authors, on the signal corps and the naval communication service. These are Capts. T. Carlswärd and E. Anderberg.[44]

In a carefully documented work, which, however, unfortunately is far too limited in its discussion of the cryptographic service, for the said service is treated only as an unimportant part of the author's main subject, Captain Carlswärd gives a report of the activities of the German Signal Corps during the World War, up to the Battle of the Marne in 1914.

From this study we infer, among other things, that several of the German radio stations went into the field without any code and cipher regulations,[45] which is still more remarkable because the cryptographic work was entrusted to the German telegraph troops.[46] Furthermore, numerous complaints registered by the Germans concerning extensive loss of time are mentioned. This loss of time was occasioned by the far too complicated cryptographic methods in use [47] and the consequent necessity for telegraphing in clear text.[48] Concerning the latter, we must emphasize the fact that it played a much greater part than Captain Carlswärd assumed in the counteraction of the French troops, especially in the case of General v. d. Marwitz' Cavalry Corps, as we shall point out further on. Furthermore, the fact that telegrams had been sent in clear text later was of great practical importance for the solution of subsequent German ciphers by the French, for they accustomed the French cryptanalysts to the German telegraphic style, to the ordinary abbreviations used by them, to their terminology and style, all details which are of extraordinary importance for cryptanalysis.

Captain Carlswärd also contends, and that quite justly, as may be seen from the great number of errors made, that the necessary routine training of officers in cryptographing and decryptographing must be given before mobilization takes place.[49]

As far as the German naval communication service during the war was concerned, it is to be inferred from Captain Anderberg's study that, at least at the beginning of the war it was not much better than that of the German Army. The German naval cipher systems were so inferior that the captain of a German collier, which had been ordered to supply the German Pacific Fleet with coal, succeeded in a relatively short time in decrypting the cipher in a cipher radiogram sent him by Admiral von Spee, although he did not have the key to that cipher.[50] The British very soon obtained the German commercial maritime cipher and code books,[51] which fact we do not doubt at all, at least not as far as ciphers are concerned, in view of the case of cipher solution cited above. Captain Anderberg also stresses, and that quite justly, the false opinion prevalent among those who are unacquainted with methods of cryptanalysis that messages in cipher cannot be read by outsiders.[52]

It is further explained that the German ciphers were "relatively easily solved, at least during the first years of the war." [53] A singular statement, attributed to Langie, to the effect that

[43] [It is difficult to see how such a situation can be avoided, in view of the rapid and enormous expansion of forces upon mobilization. At the same time, this points to the vital necessity of having a completely organized and efficient signal intelligence service, ready to function on M-day, in order to take advantage of the mistakes and blunders committed by enemy forces as well as to reduce to a minimum those committed by our own forces.—*W. F. F.*]

[44] T. Carlswärd, Den strategiska signaltjänsten, etc.; E. Anderberg, Maritim förbindelsetjänst under världskriget.

[45] Carlswärd, Den strategiska signaltjänsten, p. 28, and Den trådlösa telegrafien under världskriget, p. 73.

[46] Givierge, Questions de chiffre, p. 402.

[47] Carlswärd, Den strategiska signaltjänsten, etc., pp. 65, 104, 122, 158, 166, and 173.

[48] Carlswärd, Den strategiska signaltjänsten, pp. 123 and 173.

[49] Carlswärd, Den strategiska signaltjänsten, etc., p. 173.

[50] Anderberg, Maritim förbindelsetjänst under världskriget, p. 59.

[51] Anderberg, op. cit. p. 59.

[52] Anderberg, op. cit. p. 88.

[53] Anderberg, op. cit. p. 90.

cryptanalysis was a German science is dismissed by Anderberg with the observation that "up to the present it is not based upon the results of experience." [54]

If we compare the foregoing statements made by the Swedish authors quoted above with the detailed reports of General Givierge in "Questions de chiffre" concerning the solution of the German cryptographic systems during the World War—with emphasis on the weaknesses of those systems—and also with Colonel Nicolai's acknowledgement that the French and British cryptographic services possessed a "superior training and carefully handled their cryptographic systems",[55] we get quite a clear picture of the inferiority of the German military and naval cryptographic services, so often pointed out in the literature as existing before the World War and during the first half of that conflict. We have attempted to outline the reasons for this circumstance in the foregoing.

Before we leave this discussion of the qualifications and tendencies of the German cryptographic service, one characteristic may be emphasized again. At the time during the World War when the Germans began to organize a cryptographic bureau under the General Staff, mathematical scholars were summoned to serve in it.[56] Such scholars were supposed to possess the special qualifications necessary for that work. In reality, there is no science or profession which is particularly suitable as a recruiting field for cryptanalytic experts. Such persons are found in widely different occupations. For instance, in France the four most expert civilian cryptanalysts were a paleontologist, an archives research worker, a criminologist, and a philologist,[57] and in Germany, on the eastern front, the civilian scientist who by mere chance came to play so extremely important a part in the development of events was a philologist. Others again were not engaged in any scientific professions. If we attempt to determine whether there are any traits common to these experts, they perforce consist of logic, method, and ingenuity, more than anything else. These qualities are inborn rather than acquired.

C. ENGLAND

If we now take up a discussion of the cryptographic activities of the British before the World War, we must state that exceedingly little information is available on the subject. For that reason we are forced to have recourse to deductions based upon our knowledge of such activities during the first months of the war and of the cryptographic systems and regulations during that same period.

We also know with certainty that that well-known institution, Scotland Yard, as well as the intelligence department of the Foreign Office, each had regularly employed, especially expert, cryptanalysts. These men worked with the extremely varied material which the well-organized British intelligence service procured from all corners of the world. The speed with which these civilian experts were organized at the outbreak of the war into a well-organized military cryptanalytic bureau indicates that mobilization plans had been drawn up providing for the immediate summoning to the colors of available civilian forces.

British literature on the subject of cryptography before the war was practically nonexistent. The influence of the French school is, however, clearly distinguishable in the British cipher system used at the beginning of the war. A further indication of this influence is given by the fact that the Parisian book dealer who always has specialized and still does specialize in cryptographic literature, declares that Englishmen have always been his best and most numerous foreign customers.

[54] Anderberg, op. cit. p. 89. [NOTE:—See p. 18 of English version of Langie, Cryptography, E. P. Dutton & Co., New York, 1922.—*W. F. F.*]
[55] Nicolai, Geheime Mächte, p 145.
[56] Nicolai, Geheime Mächte, Leipzig, 1925, pp. 143-145. The information, however, is doubtful.
[57] Aside from experts regularly employed in civilian cryptographic bureaus.

The British military and naval cryptographic bureaus were closely connected to the Intelligence Departments of the Army and Navy, respectively. The latter, which had been wonderfully well organized for a long time, were distinguished by a very great centralization of work. We can with certainty presume that this centralization was of great importance for the cryptanalytic work organized at the beginning of the war; for in this way it was possible to obtain for that work exceedingly important information within the shortest possible time. A quick collection, a careful examination and selection, and a skillful collation of information have at all times characterized the British Intelligence Service.

It is probable that the cryptographic work done by the British Navy was more extensive than that done by the Army, at least before the World War. During that war, on the other hand, cryptanalytic activities came to play the dominating role. Of the greatest importance in this connection was a close cooperation with the signal corps, which very early resulted in the establishment of special stations for intercepting German radio messages, so-called "intercept stations", supplemented later on by radio-goniometric stations. Both types were for the purpose of obtaining material to be used for cryptanalysis. By a combined analysis of the location of the stations sending the radiograms, the call signals, the amount of traffic, and partial and complete cryptographic solutions, the cooperating radio and cryptanalytic services succeeded in very greatly facilitating each other's work and were able to bring the commander of the British Fleet extremely valuable strategic and tactical information, as may very clearly be understood by reading Captain Anderberg's account.

Lord Fisher's memoirs contain information concerning the interest of the British Fleet in ciphers before the World War. According to this work a bureau for collecting foreign code telegrams was established in Switzerland.[58]

D. RUSSIA

In Russia we find a particularly uneven development. The military cryptographic service was very faultily organized, without any effective central head. The systems recommended at the outbreak of the war, but practically never used on account of lack of organization, were far too complicated and tedious for poorly instructed and untrained personnel to use. The result was that the majority of the Russian radio stations either telegraphed in clear text or used a cipher system which was adequate in time of peace or a system of the simplest type which had arbitrarily been agreed upon beforehand by telegrams sent in clear text. It is no exaggeration to state that the cryptographic service was a complete failure at the outbreak of the war, a circumstance which was of decisive importance for the Austro-German operations. Cryptanalysis, about which the author has no information available, presumably was not performed at all in Russia before the war.

The diplomatic cryptographic service, on the contrary, was particularly well organized and capable of fulfilling its missions after the cryptographic bureau had been reorganized by Savinsky, formerly Russian minister to Stockholm. He had all ciphers and codes in use up until then improved, introduced strict regulations for enciphering code, and organized the service in an extraordinarily meritorious manner. A special cryptanalytic bureau was placed directly under the Minister and employed several capable experts. Among its accomplishments we can mention the solution of the Turkish, British, and Austrian codes and also of the Swedish diplomatic code.

The cryptographic bureau mentioned above used from six to seven different codes for different purposes, codes possessing theoretically different degrees of safety. Superencipherment was strictly performed on the most important codes, the addressee of the telegram being

[58] Nicolai, Geheime Mächte, Leipzig, 1925, p. 13.

informed by one of the first cipher groups, likewise enciphered, as to which code was in use, and in certain cases, as to the nature of the superencipherment.[59] Prohibition of the use of repetitions in clear text or code text or of special division of the clear texts into a few parts, the normal order of which was made up according to rules agreed upon, indicates without any doubt a very good knowledge of the technic of cryptanalysis. We must mention as specially worthy of note the fact that the Russian Ministry of Foreign Affairs even used a compromised code, which it knew had been solved by one of the leading powers. The said code was used continuously for the purpose of lulling the enemy into a feeling of safety, but only for comparatively unimportant telegrams. On a very important occasion later on, some fictitious information was encoded with the use of the said code for the purpose of deceiving the cryptanalysts of the enemy. It is quite obvious that such a method could only be used for a short time but may have have been of importance. After that the code was compromised to a double degree.

Changes of code were made regularly. In order to effect savings, however, the same code was sometimes used several times. It was transferred from one embassy or legation to another, but always in such a way that the country where the code was first used never did exchange, or never was supposed to have to exchange, telegrams with the other country. We can see, in all the instructions reported, an unmistakable influence of very highly experienced cryptanalysts.

Cryptographic work of internal political character also was very great, probably actuated by the peculiar war waged by the Ochrana against the Russian Nihilists. In the numerous prosecutions of the Nihilists a solved cipher often was the basis for the indictments, and the Nihilists in turn very actively used ciphers and codes. An interesting report concerning such codes and ciphers is found in an article by Schooling.[60]

The notorious successors of the Russian Ochrana, the G.P.U., continuously used a number of different cipher systems for their foreign affairs, most frequently consisting of so-called pseudograms, that is to say, messages concealed by apparently wholly innocent texts. This organization, which constantly carries on a regular war against the French and British cryptanalytic bureaus, may perhaps also have extended its operations to Sweden. It may be added that after the World War Russian spies were discovered in the French air defense plants at St. Cyr and in certain British naval centers, as the result of the successful solution of Russian codes.

E. AUSTRIA

There seems to be very little information available on the activities of the Austrian cryptanalytic and cryptographic services before the World War. The most important of this information is supplied by General Ronge, Chief of the Austrian Military Intelligence Service during the World War.

The cryptographic and cryptanalytic service came under the Evidenzbureau of the Austrian General Staff. Very rudimentary at the beginning, this service was developed from the beginning of the twentieth century by Ronge, according to his own statement. Up until then cryptanalysis was entirely unknown, although on the contrary, good practice in code and cipher work was obtained by a very extensive correspondence with the military attachés and spies, etc.[61]

Interest in the cryptographic systems of neighboring countries was restricted to the acquisition of keys through spies, an activity which furthermore, must have been reciprocal, at least so far as Russia was concerned.[62] Beginning with the year 1908 real cryptanalytic work is to be recorded, in that the service began to work with enciphered radiograms from the Antivari station, intercepted by the Austrian Navy.[63]. This very interesting cryptanalysis is charac-

[59] [NOTE.—"Superencipherment", enciphering the code groups of a message.—*W.F.F.*]
[60] Schooling, The Pall Mall Magazine, vol. VIII, nos. 33 to 36. London, 1896.
[61] Ronge, Kriegs- und Industrie-Spionage, p. 55.
[62] Ronge, op. cit., pp. 21, 22, and 55.
[63] Ronge, op. cit., p. 55.

terized by Ronge as a Sisyphean task, a comparison which must chiefly be based upon the difficulties encountered by personnel which had not been especially trained beforehand to deal with the complicated and not precisely approachable technic of cryptanalysis.

From the outbreak of the Italian-Turkish War it actually rained intercepted telegrams. Thrown upon his own resources, Ronge very soon was swamped with work, which circumstance later produced one advantage, important for the subsequent activities of the service during the World War; namely, that Ronge succeeded in having an officer assigned as his assistant. One of the achievements of this service was the solution of a spy cipher used by the German noncommissioned officer, the traitor Schreiber.

At the beginning of the year 1914, the Evidenzbureau of the General Staff was partly reorganized and Ronge states concerning the cryptanalytic work of that bureau that up until then it had attained only unimportant results. The solution of the more difficult systems of codes and ciphers was not accomplished, which circumstance, however, spurred the personnel on to renewed efforts and also led to the necessity, so clearly seen by Ronge, for further increasing both the force and the means available for the service. The material was collected by the various intelligence offices. Thus, among other results was the fact that the solution of the Serbian cipher telegrams no longer presented any difficulty.[64] Nevertheless, we can with great probability of accuracy assume that the said results were attained because the Serbian cipher keys had been obtained through the intelligence service; hence, this was an ordinary decipherment and not in any sense of the word an actual solution of the cipher.

Almost simultaneously the service began work on Russian ciphers—peace-time ciphers, as were the Serbian—which proved to be very difficult to solve. At the outbreak of the war, which occurred later, work on the solution of these ciphers had only advanced very little.

Several remarks may be added here. The cipher system in use in the Russian Army in time of peace was really particularly simple to solve with the use of the cryptanalytic technic which had been developed long before the war by the French military authors, Kerckhoffs, Valerio, Viaris, and Bazeries, and which was improved to an unprecedented extent during the World War.

It is very probable that the Austrian cryptanalytic service before the World War based its work chiefly on very primitive methods, as reported in the well-known work by Colonel Fleissner von Wostrowitz of the Austrian Army, "Handbuch der Kryptographie." However, the establishment of a regular, permanent cryptanalytic service, which was organized by Ronge, resulted in having a number of Austrian officers learn to analyze the Russian cipher system, and therefore these officers were comparatively well prepared for the extremely important and momentous work which the war against Russia brought with it. Thanks to the innumerable indiscretions on the part of the Russians, including a repeated use of the systems of peace time, which we shall discuss later on, the Austrian cryptanalytic experts succeeded, as the result of their superior preparation, in solving the Russian ciphers in a considerably shorter time than was required by the Germans.

The Italian ciphers were also of great interest. The cryptanalytic bureau succeeded in obtaining keys to several different Italian ciphers. It was found later on that this knowledge, which Ronge intimates was obtained through espionage, to a great degree helped the Austrians in solving the Italian cipher systems during the World War.

The Austrian cryptanalytic service was developed very quickly during the World War, thanks to the fact that its importance was clearly understood in advance by Ronge. According to a French source, the archives research worker, G. Lenôtre, not less than 26 cryptanalysts were employed in February 1916 in the cryptanalytic office at Vienna alone.[65]

[64] Ronge, Kriegs- und Industrie-Spionage, p. 80.
[65] Lenôtre, Le Chiffre, Le Temps, Sept. 29, 1917.

F. ITALY

Lastly, we must say a few words about the cryptanalytic and cryptographic activities of the Italians, although the general level of that work, before 1914, probably was as low as that of the Russians and the Germans.

This circumstance is remarkable when we consider that in the 1880's the Italians possessed a very clever cryptanalytic expert in the historian L. Pasini, but it may partly be explained by the fact that the General Staff presumably did not attempt to make any contact with the said expert, partly by the fact that modern Italian literature on the subject of cryptography was extremely meager and practically limited to a rather simple work, "La crittografia diplomatica, militare e commerciale", by Gioppi. Much more was to be derived, from the viewpoint of the technic of cryptanalysis, from the extraordinary Italian literature on the subject written in the fifteenth and sixteenth centuries, paradoxical as that may seem. The latter works probably slept undisturbed in some dusty archive.

There was certainly a cryptographic service connected with the Italian General Staff beginning with the year 1901. Its chief and force consisted of one man, Col. Felice de Chaurand de Saint-Eustache, who became known because the year before he had compiled a cipher system known as the "cifrario militare tascabile", which the Austrians later solved with extreme ease. The colonel also succeeded in solving a cipher correspondence carried on alternately in French (Sittler) and Italian (Mengarini) codes, which, according to his own account, required 2 months' work of several hours a day. Both of these codes, which were of the same type, were encoded by regularly shifting the normal pagination in the code a certain number of places in one direction or the other, positive or negative.[66] A glance at the special work of cryptanalysis published 6 years prior to that by the French military expert Valerio would have made it possible for him, in a purely mechanical way and in only a few hours, to solve the code in which the correspondence was written, again demonstrating the importance of careful documentation, against which most countries sin constantly and equally seriously.

It is more than probable that the colonel cited above, aside from being responsible for the said "cifrario tascabile", also was responsible for the other cipher systems used by the Italian Army. Their low value as ciphers may readily be understood from the number that were solved during the World War by the Austrians, and a new system of ciphers, publicly announced as absolutely indecipherable and introduced in 1927 by the said officer, still further demonstrates the astonishing lack of comprehension of modern cryptanalytic methods on his part.[67]

* * * * * * * * *

In the foregoing we have several times mentioned diplomatic telegraphic communication by means of codes. A brief report on the various methods of application of these codes may be in point at this time.

As we know, such a code usually consists of a list of textual elements consisting of a considerable number of letters, syllables, words and whole sentences and a corresponding list of code groups ordinarily consisting of four- or five-place numbers, sometimes even of groups of letters. One code unit corresponds to each textual unit.

The code is ordinarily divided into two parts, the first being intended for use in encoding and consisting of the textual list arranged alphabetically, the second being intended for use in decoding and consisting of the code list arranged in systematic order. In each part we find the corresponding units of the other list, so that we can best compare the arrangement with

[66] La crittografia di fronte alle esigenze dei tempi moderni, in the Rivista Marittima, October 1923. Also see the reports on the solution of the code in the Panizzardi telegram and the principle of the Sittler code.

[67] Per un cifrario universale, Rivista Marittima, October 1927.

that in an ordinary dictionary, for example, that in a Swedish-English and an English-Swedish dictionary.[68]

The secrecy attained by the use of such a code consists partly in the selection and the order of the textual units, partly in the arbitrary selection of the corresponding code units (aside from superencipherment).

Such a code, when used without the application of any precautionary measures, such as superencipherment, changing the order of the clear text, avoiding all repetitions, balancing the frequency by the use of several different code units for textual units having a high frequency, etc., is not at all safe, especially if the cryptanalysis is done by a fully equipped cryptanalytic bureau cooperating with government authorities. Codes have been solved in this way in great numbers, and that work has been based chiefly upon the analysis of frequencies and sentence structure, and of certain easily identifiable group units, such as telegram numbers, signatures, introductory phrases of a stereotyped nature, words guessed by the context, etc.[69]

Much is also based upon comparison of the probable contents of different telegrams, because they may be, and also frequently are, deduced from connecting them with other external, known circumstances. Thus, for instance, the reports issued to the press by the Ministry of Foreign Affairs or by an embassy or legation, explanations given by parliament, and the so-called white, blue, yellow books, or books of other colors issued during periods of political stress, form valuable and quickly referred-to sources of comparison with definite telegraphic correspondence. Still simpler are the ordinary methods used in countries where a knowledge of cryptanalysis is on a high level. They are somewhat as follows: The Minister of Foreign Affairs, after having conferred with a minister or ambassador from a foreign country on any important subject, immediately sends the cryptanalytic bureau a résumé of the conversation, so that the bureau may compare it with a copy of the telegram which the embassy or legation concerned usually sends to its government on such an occasion. It has even happened that the note from the Ministry of Foreign Affairs to a foreign embassy or legation has been prepared specifically with a view to use in connection with solving the foreign code.

It is self-evident that such methods presuppose a great confidence in the experts and an absolute discretion on the part of the latter, likewise the most intimate cooperation between the cryptanalytic bureau and high government officials. Under such conditions the work of solving the code becomes much less difficult than is usually supposed to be the case by those who are unacquainted with the technic of cryptanalysis. An example has already been given of the way in which such comparisons are made. This example was given during the discussion of the method used in solving the Panizzardi code telegram. This, to be sure, was an inferior type of code, but the skill of professional cryptanalysts is often such that they can in a very short time reconstruct important parts of an unfamiliar code of the diplomatic type, as we have described in the introduction to this part.

Several nations have used simple codes of this type for diplomatic correspondence, entirely secure in the conviction that they could not be solved. Furthermore, such codes were used without any change, at least until the outbreak of the war, for long periods of time, often many years, without the application of any of the precautionary measures mentioned above.

[68] [As regards the arrangement of their contents, codes are of two types, called "one-part" and "two-part" codes. In the former, one book serves to encode as well as to decode messages because the textual units in the code are arranged alphabetically and are accompanied by code groups *also* arranged *alphabetically* (or numerically in the case of figure codes). In the two-part code, however, the textual units are accompanied by code units in an entirely *random*, unsystematic order so that two books are necessary; one to encode messages, and another, in which the code groups are arranged systematically (with their meanings as given in the encoding section) to decode messages.—*W. F. F.*]

[69] [It is believed that the author might well have qualified his statement concerning the ease in solving a two-part code by adding that the resistance which such a code offers to solution also depends partly upon the size of the code, that is, the extent of its vocabulary but mostly upon the amount of traffic available for analysis. A small two-part code of only 5,000 groups may resist solution entirely if only a few messages are available. It is for this reason that small two-part codes, such as field codes used in military operations, are changed frequently in active service by the issue of successive editions in which the same textual and code units are maintained but their equivalence is entirely changed from edition to edition.—*W. F. F.*]

"Change of code" is often effected by the very primitive method of merely replacing the code units by others, by pasting loose strips of figures over the old code lists. In this way only one of the unknown factors in the code is changed, which greatly facilitates the work of solving it, for a knowledge of one text list, or merely of part of it, is sufficient, in the majority of cases, to identify a changed code list very quickly. The general structure of the telegram remains unchanged in such cases.[70]

That the successful solution of codes and ciphers was kept strictly secret is self-evident. That cryptographic work and even cryptanalysis was going on could certainly not be kept secret, but as a rule, the impression was probably generally spread, even in diplomatic circles, that the results were more imaginary than real. This plan was partly based on the general ignorance of the technic of cryptanalysis already discussed in this work, but perhaps even more on the circumstance that cryptanalysts always have been interested in using spies as dummies. If a code was suspected of having been compromised through espionage activities, photography, etc., the government concerned merely changed the code list, which, as we have already explained, did not cause any difficulty worthy of mention to the cryptanalytic experts. If it was discovered that the code actually had been solved, then not only was the code list changed, but also the textual list,[71] the methods of enciphering and deciphering, etc., and usually regulations covering special precautionary measures were issued, which rendered the work of solving the new code or cipher much more difficult.

It does not come within the province of this work to give a detailed report concerning the technic used in cryptanalysis. It may be considered adequate to state here that cryptanalysis often is performed along lines similar to those used by archeologists and philologists in reconstructing an unknown language. That the latter often have succeeded in their tasks, despite the fact that they knew absolutely nothing about the said language to begin with, must give us food for reflection, for to these scientists certain factors were unknown which are fully known to the cryptanalytic expert, such as the construction of the language, its spelling and sentence structure.

Experience in cryptanalysis sometimes made it possible for cryptanalysts to read telegrams which somehow or other had become garbled and to do that more easily than the real addressees. Thus, for instance, on one occasion the cryptanalysts of the Russian Foreign Office had the unusual satisfaction of being able to solve a code telegram from Constantinople and at the same time of reading the reply from the Turkish minister, worded somewhat as follows: "I cannot read your telegram; be so good as to repeat." A similar occurrence took place in 1916 in a French cryptanalytic bureau on the western front.

Aside from the codes of the above-mentioned types, which were used extensively by nations which were ignorant of the technic of cryptanalysis, other types of codes were used in which the tendency was developed of increasing the number of different text units to a maximum. Some of the German codes belonged to this category.[72] They had been selected because of the supposedly greater difficulties involved in solving them.

These precautionary measures, which may be very effective in the hands of experienced personnel, in actual practice, however, led to practically no increase in the degree of safety of the code, due to the ordinary tendency found among cryptographers of restricting their selection of the different text units to a minimum. This led to a recurrence in the telegram, constantly and regularly, of sentences and words of a stereotyped nature.[73] The result was that in actual prac-

[70] [The author has failed to state that what he says of this type of "change of code" applies only to one-part codes. Obviously, to paste a new list of code words over the old list in a two-part code would necessitate a complete change in the decoding section; but where the code groups and the textual units progress in parallelism, as in a one-part code, it is obvious that a simple change can be made by pasting a new list of code groups over the old—but such a change brings no security at all.—*W. F. F.*]

[71] [The author must also mean to apply this specifically to the case of one-part codes.—*W. F. F.*]

[72] [This did not apply to the German field codes used during 1916–18, but as may be noted in Mr. Gyldén's next paragraph, to the German diplomatic codes of the World War period.—*W. F. F.*]

[73] Givierge, Questions de chiffre, pp. 61 and 67.

tice a few hundred units were used out of the many thousands contained in the code and the identification of the said, ordinarily used, units was one of the most important tasks to be undertaken preparatory to the solution of a code. Therefore, we cannot be surprised that such codes were solved with comparative ease, for instance, the code of the Zimmermann telegram, the publication of which was one of the decisive factors in bringing about the entry of the United States into the World War, and that of the so-called "Luxburg telegrams", the publication of which, as we all know, resulted in a situation which was not entirely pleasant for the Swedish Ministry of Foreign Affairs and for the then Swedish minister to Argentina, and which was not without influence upon the attitude later assumed by the Entente Powers toward Sweden.

A great number of sensational reports concerning the immediate causes of the solution of these codes, for instance, that a young Austrian by the name of Czek had stolen the German code in Belgium during the World War, may be ascribed to the phantasy of far too clever authors, unless, as often was the case, they were purposely spread with a view to deceiving the Germans about the actual conditions surrounding the solution of the code telegram in question. The English particularly are past masters of camouflage of that type.

The English and French diplomatic codes form a third category. These codes were singularly well compiled, although a personnel not well versed in cryptography could be exceedingly indiscreet in their use. The most unimportant chargés d'affaires in the remote corners of the world were, however, provided with very detailed instructions regarding the use of these codes, among other things, regarding the avoidance of repetitions and the use of superencipherment. Superencipherment was performed ordinarily by the use of so-called transposition encipherment, consisting of a rearrangement, according to varying rules, of the groups composing the code telegram. Such superencipherment, if undertaken without any knowledge of the technic of cryptanalysis, often leads to a purely illusory complication, such as that produced in the German submarine code, which, before the superencipherment was introduced, was the first of the German codes solved by the Allies during the World War.[74] The instructions with regard to the French and English codes, however, give undeniable proof that they were compiled by personnel versed in the science of cryptanalysis.

The superencipherment varied with every tenth or every twelfth telegram; in times of political tension, with every other or every third. In case of change of codes, not only was the code list changed but also the textual list.[75]

In the application of the above-mentioned precautionary measures, which, without doubt, must be designated as of the very highest type, sometimes peculiar blunders were made because of the ignorance of the personnel which performed the cryptographing. For instance, sometimes the text of telegrams in clear text, which were considered unimportant and were encoded merely because the regulations so prescribed, were handed to the press in foreign countries by ignorant subordinate personnel in the diplomatic service.

Leaving the diplomatic codes now, and taking up the military cipher systems in use before the war, we find that the German school and the French school each went its own way.

The French school, which for very good reasons mistrusted the so-called "regular" transposition cipher [76] as being unsafe and easily solved and had very carefully studied the theoretic structure of this system,[77] shortly before the outbreak of the war used the so-called "arbitrary substitution" cipher, together with an irregular transposition cipher.

The German school, on the contrary, obviously inspired by the tendencies of the German literature on cryptography, apparently believed that regular transposition systems were very safe, if further reinforced by the complication that the key was made double. Before the war

[74] Givierge, Questions de chiffre, pp. 61 and 67.

[75] [Obviously, these were two-part codes.—*W. F. F.*[

[76] Bazeries, Les chiffres secrets dévoilés, Paris, 1901, p. 33 ff. Delastelle, Traité élémentaire de cryptographie, Paris, 1902, p. 27

[77] Viaris, L'Art de chiffrer et déchiffrer, Paris, 1893. Delastelle, op. cit.

two such systems were used, one of which was a double transposition cipher. The simple system was abandoned at the outbreak of the World War, while the other was in use on the Western Front until the 18th of November 1914.[78]

An interesting and illuminating statement contained in Lt. Gen. v. Alten's military reference book,[79] strengthens and supplements the above information. It reads as follows:

> Now a simple system has been introduced into the German Army, of which only those handling the cryptographing and decryptographing must know the key text, that is to say, a few easily remembered words. The system is characterized by an ingenious combination of groups of figures with superenciphered letters,[80] and is learned through secret instruction, chiefly by general staff officers and adjutants. In order to prevent the solution of this system by unauthorized persons, an operation which in and of itself is very difficult, the text key can be changed at any time as soon as it is feared that the cipher has been learned by some person not authorized to know it.

The foregoing quotation, which is reproduced here because it shows the ideas concerning cipher problems prevalent in military circles, is further corroborated by the information that the German system at the beginning of the war was a double transposition cipher with two key words.[81]

After that, the system, as may be inferred from the following discussion, was extensively solved by the French military cryptanalytic bureaus, and consequently, the harsh but just criticism made of such systems by the cryptanalytic expert Major Bazeries seems justified. Major Bazeries said that "to change a substitution cipher for a transposition cipher is the same as changing a one-eyed horse for a blind one." [82]

In writing the report concerning the various periods and phases of cryptanalytic and cryptographic work done during the World War, which is contained in the following chapters, we have endeavored to bear in mind the great handicap in the form of incomplete and misdirected preparations under which the Germans began this work. The achievements in this field were, as we can clearly see, at least as much due to the skill of the Allies as to the blunders committed by the Germans.

---

[78] Givierge, Questions de chiffre, Paris, 1924, pp. 401, 402, 404. [NOTE.—However, use of the double transposition cipher was later resumed by the Germans and continued to the very end of the war, but only between high commands, on the Western Front as well as between Berlin and Constantinople and Tiflis.—*W. F. F.*]

[79] v. Alten, Handbuch für Heer und Flotte, Berlin, 1912, vol. IV, p. 105, article on "Geheimschrift."

[80] Applies equally to the procedure of encipherment and the product.

[81] According to information furnished by Dr. Locard, of Lyons.

[82] Bazeries, Les chiffres secrets dévoilés, p. 34. [NOTE.—This very general statement should be taken with some discretion. Obviously, much depends upon the specific systems involved in such an interchange. In this connection see also footnote 120.—*W. F. F.*]

Chapter II

THE PERIOD FROM 1914–18——THE WORLD WAR

Much more information is available concerning the cryptographic and cryptanalytic activities during the World War than concerning the same activities before that conflict. The unprecedented increase in the personnel of all the cryptographic bureaus made impossible the maintenance of secrecy and the warring powers often published information concerning the cryptographic activities of the enemy, and since the war have published information concerning their own activities in this field.

A report concerning this cryptographic and cryptanalytic work can be classified either by time or place. For several reasons, one of which is the very great difference between the cryptographic and cryptanalytic work on the two fronts, we have classified the subject according to fronts, and our report is, so far as possible, made to follow the chronological development on each of these fronts. As the development on the Western Front is perhaps the better known of the two and is extraordinarily characteristic in its various stages, it is the first one discussed here, and hence, the reports following it concerning this type of work on the other fronts can be fitted without any great difficulty into a common chronological whole, which in this case seems desirable.

Remarks, explanations, and comments for each period and place studied might be assembled into a résumé or included in the report itself. Because of the frequent necessity of analyzing the causes of certain events or making comments on them, the author has deemed it best to follow the latter plan.

A. The Western Front

1. THE PERIOD FROM 1914–16

In Captain Carlswärd's analysis of the German Signal Corps on the Western Front up to the time of the Battle of the Marne, which we have cited in the last chapter, the faults of that service and the resulting effects upon the outcome of the Battle of the Marne have been fully explained.

In the main, we infer from it that the Signal Corps was not equal to its mission, that of establishing and maintaining strategical communication, particularly on the right wing of the German Army. The rapidity of the advance, the difficulties connected with the employment of the telegraph lines in the occupied territory, together with the lack of preparation, are cited as the main reasons for this failure. It is evident, among other things, that the failure of the systems of communication constituted the immediate cause for the disastrous misunderstanding on the part of the German High Command concerning the relative positions of the First and Second German Armies directly before the decisive phase of the Battle of the Marne.

Due to the collapse of the means of wire communication, a very great burden was placed upon the German radio stations,[83] and this brings us to a discussion of real cryptographic work. In using radio communication, it necessarily had to be assumed that there was danger of interception of the messages by the enemy and, consequently, a safe system of codes and ciphers had to be used.

[83] Carlswärd, Den strategiska signaltjänsten, p. 54.

The first direct experiences with cryptographing in the field demonstrated that the systems were very time-consuming.[84] Before the war no difficulties had been encountered in establishing communication between two radio stations and in corresponding in cipher—although the cipher parts, probably, were frequently marked off, if not by red brackets, at least by telegraphing in clear text. Conditions in the field were entirely different. The overworked stations found it difficult to form a distinct separation among themselves between transmission and reception; a sort of line of messages, so to speak, was formed in the air and the enemy purposely interfered with the communications. The messages became so jammed that many telegrams had to be repeated from three to four times before their whole import could be clearly understood, and the time required for cryptographing was so great that sometimes at critical moments the transmission of an important message by radio required at least 24 hours.[85]

That the enciphering or encoding alone caused the greatest loss of time is to be inferred from the fact that telegraphing in clear text was recommended for use in certain critical situations.[86]

This brings us to a subject connected with cryptography to which far too little attention has been paid, that is to say, the relation between safety and speed. With the conception regarding the nature of safety and the means for securing it prevailing among the Germans, the need for speed was entirely overlooked, for safety was sought through the employment of complicated encipherment, and thus safety and speed were placed in inverse proportions to each other. The plan adopted proved to be wrong and false at all times, partly because the safety based on complications proved to be illusory, partly because its practical application under adverse conditions was never given adequate consideration. It would have been best in any case to have followed the example of the French, to have compiled different cipher systems for different purposes, strategic ciphers for use in cases where safety was of prime importance, and tactical ciphers for use in cases when speed in enciphering was most important. Experience has also shown that adequate safety may be secured by a very simple and easily used cipher system, one which furthermore possesses the altogether neglected, but most important advantage of reducing to a great degree, the number of very common errors in enciphering and the consequent numerous blunders in the form of inquiries and explanations in clear text or in a "mixed" text, that is, in mixed cipher and clear text.

The experiences of the World War also demonstrated a third point which was disregarded before that conflict both by the Germans and the French, namely, the need for a system which, in the event that a cipher or code telegram arrives in an incomplete or garbled condition, would permit decryptographing the greater part of it. Such considerations, which perhaps merely apply to messages of tactical importance, after that made it imperative to have systems in which the sequence of the clear text was preserved.

The German systems employed during the first few months of the World War were particularly impractical from the viewpoint we have just mentioned. The double transposition cipher, which produced an apparently entirely arbitrary mixture of the letters of the clear text, required that before the clear text could be deciphered the whole telegram should reach the addressee without any errors in it. This explains the uncommonly great proportion of repeated telegrams and the unnaturally long delays mentioned above.[87]

---

[84] Ibid., pp. 65, 104, 122, etc.

[85] Carlswärd, Den strategiska signaltjänsten, p. 166.

[86] Ibid., p. 123.

[87] [It may be well to emphasize here the two principal objections to the use, in practical military cryptography, of the double transposition cipher. The first is that the accidental addition or omission of a single letter makes the decryptographing of the message very difficult, if not impossible for the average cryptographic clerk because it prevents the speedy and correct reassembling of the successive letters of the original plain text. The second and even more serious objection is the fact that inexperienced or careless cryptographic clerks are very prone to omit the second of the two operations involved, with the result that if a single message in which only one of the transpositions has been carried out has been intercepted, its easy and rapidly accomplished solution leads directly to the decryptographing, by the enemy, of all other messages in the same key, even if the latter have been correctly enciphered.—*W. F. F.*]

70313—35——3

From the above it may be understood that the cryptographic instructions were not always obeyed and also that the numerous difficulties which were based upon errors in cryptographing and interference during transmission produced an extensive extra correspondence which to a great degree facilitated the work of the French cryptanalytic experts.

The real origin of the deficiencies is known and has been explained in the preceding chapter. They were caused by the fact that the personnel assigned to the cryptographic service of the General Staff was not equal to its mission, due to its inadequate knowledge of cryptography. The systems were far too difficult to handle by radio personnel not especially trained in that line; they were likewise far too time-consuming for practical purposes and useless when there was interference. Farther on we wish to point out that these real disadvantages were not offset by any corresponding increase in the safety of the codes and ciphers.

The foregoing misconceptions concerning cipher systems are in no sense specifically German; they are exceedingly general in all places where a knowledge of cryptanalysis is not a basis of their preparation, and once more we must point out the fact that the consequence was an unwieldy and, in practice, an undependable system. "It is better not to employ any ciphers at all than to employ them poorly." [88] General Givierge's emphatic concluding words in "Questions de Chiffre", are based on an extensive experience with regard to the dangers inherent in the use of poor cipher systems. This brings us to a discussion of the measures taken by the French.

At mobilization an order was issued by the commander in chief providing for the establishment of an important cryptographic service, "Service du Chiffre", at General Headquarters. This service, which was composed exclusively of trained experts, in less than a week had seven such experts enlisted and was removed to Vitry-le-François,[89] with Major Givierge as chief.

The chief function of this service was to handle the code and cipher correspondence of General Headquarters, and its secondary function was to solve the code telegrams of the enemy, although the main part of the cryptanalytic work was performed in the cryptanalytic bureau at Paris. The bureau at Vitry-le-François in the meantime was developed to form the base for the cryptanalytic bureaus established in the field, which were gradually organized on the staff of every army group and, later, on the staff of every army.

At the same time, in accordance with preparations made before the war, special intercepting stations were established and were assigned the mission of providing the necessary material for the cryptanalytic bureau at Paris. These stations, which, as we have already stated, were established in a great number of fortresses in eastern France (as the French mobilization plans had not at the beginning at all foreseen the German advance over Belgium) had even before the war provided the cryptanalytic bureau with a number of German radio ciphers which had been intercepted and which, as mentioned already, formed a subject of very extensive studies by the Military Cryptographic Commission. Information was sometimes furnished about the said systems also through the Intelligence Service.

Consequently, the intercepting stations located in eastern France did not, during the first few weeks of the war, pick up a great number of radio messages which were expected from a German offensive on the eastern boundary of France. To this was added the fact, which we shall discuss farther on, that a number of the telegrams intercepted by these stations did not reach the cryptanalytic bureaus until after too long a time had elapsed.

The permanent radio stations located in the interior of the country, which were quickly adapted for the intercepting service, on the contrary, came to play an ever-increasingly important role as the days went by. Although radiograms were rare during the very first days of the war, so long as the Germans still had their own telegraph lines at their disposal, their numbers

[88] Givierge, Questions de chiffre, p. 78.
[89] Ibid., p. 400

increased very quickly the moment the frontier was crossed, assuming an unprecedented and entirely unexpected scope.

Identification of the transmitting German field radio stations began immediately. Because of the lack of radio goniometers, which had been demanded in vain before the war by the then Major Cartier, an attempt was made to identify the different German sending stations by the strength with which the messages sent by them were heard. Thus, it was accurately recorded whether the message could be heard very loudly, loudly, medium loudly, weakly or very weakly. The call signals were also recorded. Starting with the assumption that the intensity of the signal was to a great extent inversely proportional to the distance from the sending station, as early as in the middle of August 1914, a diagram was drawn up showing the probable grouping of the German stations. This diagram later on proved to have been in a great measure correct.[90]

From the numerous telegrams which reached the cryptanalytic bureaus on an average from one-half hour to 1 hour after they had been intercepted, the German stations were classified into the following categories:

(*a*) Stations with a series of correspondents who were always the same. These were identified as stations assigned for the use of the higher commands. The remaining stations were identified as subordinate.

(*b*) Subordinate stations sending messages thick and fast. These were considered as belonging to the German cavalry divisions.

(*c*) Subordinate stations transmitting a limited number of messages. These were presumed to belong to units moving more slowly than the cavalry divisions, such as army corps or infantry divisions.

A comparison of the intercepted radiograms on the basis of call signals, strength of sending station, and category of sending station, soon led the French to identify the call signals for the different German Army commands, cavalry divisions, and army corps or infantry divisions.

In addition to this the grouping of the cavalry divisions into cavalry corps was easily identified, because all the call signals for the divisions belonging to one and the same corps began with the same letter. The corps command station also was identified by the fact that it was the only station to correspond with all other stations belonging in the same group of call signals.

In this way the French very quickly identified four main combat groups, each one having one cavalry corps with divisions whose call signals began with S, G, L, and D, respectively. Their location was determined according to the cited original standard of the strength of the station, into the group S in Belgium; the group G in Luxemburg; the group L in the Woevre district, except at Verdun; and the group D in Lorraine. This disposition was also verified quickly enough by certain parts in clear text in several radiograms. It was also found that the radio station at Cologne had retained its peace-time call signal, CL, unchanged, and those of Metz and Strassburg were quickly recognized.

As a rule, the correspondence was in cipher. However, frequently names in clear text occurred, as well as words and even whole sentences which had not been understood by the person for whom the message was intended. There were even whole telegrams, with the signature of the sender, sent in clear text. In this way in only a few days it was learned that v. Marwitz was in command of the Cavalry Corps which used the call signal beginning with the letter S and that v. Richthofen was in command of the corps with the call signal beginning with the letter G.

In the same way other telegrams sent in clear text by a station belonging to the group L informed the French that two German cavalry divisions had entered the valley of the Woevre, probably via Audun-le-Roman, and were advancing toward Verdun via Malavillers and Xivry-

[90] Cartier, Le service d'écoute pendant la guerre, Radioélétricité, no. 16, 1923, p. 454.

Circourt, where one of the divisions had established headquarters.[91] The said advance had been entirely unknown to the French High Command up to that time, and later on we shall point out the exceedingly important role which the name of Circourt came to play in the solution of the German cipher system.

The ever-increasing number of intercepted telegrams gave rise to certain difficulties. It was found that it was more difficult to intercept messages through the field radio stations than was expected, if the telegrams were written in cipher. The result was that one and the same German cipher telegram, intercepted by several different stations, sometimes reached the cryptanalytic bureau in Paris in different versions. While waiting for the necessary increase in the number of permanent intercept stations, orders were issued to several more French field radio stations to assist in the work of interception, so as to improve in that way the possibilities for determining the exact text of the German cipher telegrams by collation. As no preparations had been made for this last-mentioned type of intercept service before hostilities broke out, the desired results were never fully attained. Conditions regarding command particularly led to obstacles, as always happens in cases when appropriate preparations have not been made before a war breaks out. It took considerable time before the subordination of the field radio stations mentioned above to the cryptanalytic bureau had actually been accomplished, in contrast to the "special intercept stations" established along the eastern frontier which we have already mentioned.

However, the cryptanalytic bureau very quickly was able to determine that of the two systems which the Germans used before the war, one had been entirely given up, while the other, it was true, still seemed to be in use; nevertheless, it caused unexpected difficulties due to complications which were not explained until later. They were based, as we shall discuss farther on, upon certain stereotyped military abbreviations and interpolated nulls.

Therefore, although the extraordinarily well-equipped and well-prepared cryptanalytic service was immediately ready to start work, the intercept service did not come up fully to expectations during the first few weeks. For this reason the work of solving the ciphers would have been rendered very much more difficult, if, as General Givierge states, the numerous blunders on the part of the Germans had not quickly come to the assistance of the cryptanalysts.

As we have already inferred from the report given by Captain Carlswärd, many of the telegrams were full of mistakes caused by the difficulties inherent in employing the cryptographic system, as well as because of interference. The constant repetitions and the resulting delays, perhaps also the confidence inspired by their great successes, caused the Germans even to telegraph instructions regarding ciphers at times extensively in clear text, especially on the right wing, where the radio stations assigned to the Cavalry Corps were in operation.[92] This phase, which came to be of extraordinary importance in furnishing the French with knowledge of the methods employed by the Germans, is mentioned in French technical cryptographic literature as "The Period of the Marwitz Telegrams." [93]

The example set by Marwitz's Cavalry Corps was quickly followed by other German radio units. Stations which, up to that time, had conscientiously enciphered all their correspondence, adopted the habit of requesting in clear text explanations of incomprehensible parts of telegrams and received these explanations also in clear text. This correspondence permitted the French cryptanalytic experts to make very important comparisons between the clear text and the corresponding cryptographic text, and also gave them a knowledge of part of the contents of a telegram, which led to interesting conclusions concerning the remainder.

Still more important was this telegraphing in clear text because of the fact that it accustomed the French cryptanalytic experts to the ordinary telegraphic style used by the Germans and

[91] Cartier, Le service d'écoute, etc., p. 456.
[92] Carlswärd, Den trädlosa telegrafien under världskriget, p. 73.
[93] Givierge, Questions de chiffre, p. 402.

to their ordinary abbreviations, as well as to the nulls which they interpolated in their messages.

This cleared up doubts which had formerly existed with regard to the German cipher system known before hostilities broke out, which was employed very correctly. It also permitted a direct attack on the German system. For this attack the methods of cryptanalysis worked out before the war by the Military Cryptographic Commission for this system proved to be particularly good. The cryptanalytic bureau in the Ministry of War, which was in the meantime moved to Bordeaux, was every day able to send a few solved telegrams to General Headquarters; the reading of these telegrams, however, merely consisted of a textual analysis, that is to say, the gist of the telegram could be obtained with adequate certainty, but the original contents could not be reconstructed letter for letter, as for that purpose the keys used had to be solved.[94] Therefore, the work had to be begun over again on and for each telegram from the beginning. This resulted in the need for more personnel. By summoning civilian experts in very great numbers and by recalling from the front several military experts who had passed the examination, the task of completing the personnel in the cryptanalytic bureaus was quite easily accomplished. Special preparations for solving the system in use had also already been made in time of peace by the Military Cryptographic Commission and had been distributed in the form of printed instructions.

Several comments are in place here. The factor which was of decisive importance for the solution of the ciphers, as we have already stated, consisted in the constantly increasing knowledge on the part of the French experts of the subject of the general aspect of the German radio telegrams, such as the style of the telegrams, the terminology and structure of ordinary reports and orders, ordinary abbreviations, introductory and closing service expressions, etc., all of a highly standardized and stereotyped nature. During the whole war, as we shall later point out, this stereotyped style formed one of the most valuable sources for the French experts in the work of cryptanalysis, especially in the solution of the code books later used by the Germans. It was quite a common occurrence that only one or two such service expressions, or a few introductory words, proved sufficient to permit the drawing of conclusions with regard to the general contents of the telegram, meaning hereby the nature of the different cipher units and not their exact wording. However, this was as a rule enough to permit bringing the cryptanalysis to a successful conclusion.

This brings us to a phase of the subject to which far too little attention has been paid and which apparently has not been adequately studied, namely, the great danger inherent in too great a standardization in the technic of military orders and reports. Without attempting to discuss fully the indisputable service rendered by such standardization both to the technic of mnemonics and in other respects, we must most emphatically point out the dangers to the safety of a code and cipher system caused by a stereotyped structure of sentences or other forms and by a too strict use of abbreviations and other special military terminology. Because we know the excessive accuracy and care with which such details are drilled into the students at the different Swedish military schools, we feel that it is to be likened to firing a shot over the target when, with a view to introducing order and clarity into military correspondence, there has come to be observed too strict an adherence to a type of fixed military style, a knowledge of which is easily acquired by the enemy and the value of which for cryptanalysis is greater than suspected by those uninitiated in cryptography. The Swedish people are inherently well disciplined and used to order and clarity, and it seems to me that it would be sufficient to learn thoroughly what is to be said but to allow a great latitude in the manner of saying it. We can to a certain

[94] [The method then employed in solving double transposition ciphers was based upon the fortunate finding of two or more messages of exactly the same number of letters and anagramming the superimposed texts. In such a method of solution it will often happen that success will be obtained only with *portions* of the text, resulting in the reconstruction of more or less *isolated words*, thus giving only a general idea of the contents of the messages.—*W. F. F.*]

degree compare the effects of excessive and pedantic love of order to the well-known pattern followed by the German artillery in firing, according to which during a certain period there was prescribed and strictly followed a series of precise intervals between shots (for example, in the bombardment of Paris in 1918). This very quickly led to the adaptation of the adversary to the tempo. He always sought shelter at the hour at which another shot was to be expected. The greater individuality inherent in the French military psychology, besides its undeniable disadvantages, perforce possesses corresponding advantages, among which are the variations in style and manner of expression which are particularly important for the maintenance of the safety of a cipher, free from all too stereotyped rules except those necessary for securing the necessary order and clarity.

The fact that the said stereotyped military terminology greatly facilitated the work of the enemy's cryptanalytic experts was stressed by many experienced cryptanalysts, among whom was Givierge. He mentions this fact in several places.[95] The importance which was placed upon that detail by the French Command may indirectly be seen, and that with the desired clarity, from section 165 of the new French regulations for service of the staffs in the field (Instruction sur l'organisation, etc., des Etats-majors en campagne, Paris, 1924).

Now leaving the subject of the work performed by the French in the field of cryptanalysis and taking up that done in the field of cryptography, we learn that during the first few months of the war this work was greatly assisted by the circumstance that the war was fought on French territory. This resulted in having the French system of telephones and telegraphs used to a maximum extent for strategic communication, without any possible interference by the enemy. This circumstance also, to a great extent, permitted the use of radio stations for intercepting purposes. Their use for these purposes was much more important because of the fact that the German signal service, as already stated, used radio very extensively for the very important strategic messages interchanged between General Headquarters and the armies fighting on the right wing. As is known, the German General Headquarters was located at Coblenz until August 30, after which date it was moved to Luxemburg.

Furthermore, the French command was fully conscious of the perils inherent in using radio for communication purposes. During general staff maneuvers which were held in May 1914 (mentioned in ch. I) serious blunders and deficiencies had come to light. They were made because of the ignorance of personnel, which was not specially trained. Certain orders containing a statement with regard to the grouping of forces had been sent unenciphered. This blunder resulted in the issuance of a special report to the chief of staff, and a renewed emphasis on the conclusions drawn in the said report certainly had an effect on the circular sent out by the assistant chief of staff as early as August 6, 1914, governing the strict application of cipher regulations. The same circular stressed the fact that wireless telegraphy was to be considered as an exceptional means of communication, one to be used only when regular telegraphic and telephonic connections could no longer be maintained.[96]

The great importance which nevertheless was placed by the French command upon dependable and quick communications is to be deduced from the fact that the telautograph was in use for some time between the office of the Minister of War and General Headquarters. This instrument was considered as perfectly safe, for at the time mentioned it was the only instrument of its kind in use.[97]

A similar method was tried by the Germans in August 1914, when the radio station at Metz used the Hughes system for transmission purposes. The French experts, however, succeeded within a few days in setting up for reception, instruments located in the Eiffel Tower,

[95] Givierge, Questions de chiffre, pp. 60, 67-68, and 402.
[96] Givierge, Questions de chiffre, p. 407.
[97] Cartier. Le Secret en Radiotélégraphie, Radioélectricité, no. 97, 1925, p. 445.

which were synchronized with this instrument. This easily permitted them to identify the German texts despite difficulties in catching the first letters in such communications.[98] The system, however, apparently was too difficult for the German radio operators to use or it was not considered safe enough, for the transmission of messages ceased in a few days.

It is evident from the foregoing statement that the cryptanalytic service in France was, for one thing, able to undertake the interception of German radiograms, etc., without any great loss of time. This work was greatly facilitated by the circumstance mentioned in the preceding chapter, namely, that in time of war the intercepting service was placed under the cryptanalytic officer at General Headquarters, in contrast to the principle adopted in Germany, where the cryptanalytic service was placed under the telegraph troops. Since in innumerable spheres of action during the war it was found that the effects of erroneous and improper organization had extended especially far, the above-mentioned detail deserves attention.

The first solution of a German cipher key was made on October 1, 1914, by the group of cryptanalysts which, under command of Major Cartier, included Captain Olivari and the civilian cryptanalytic experts and interpreters Freyss and Schwab.[99] This exposed the German cipher messages fully to the scrutiny of the French, for a knowledge of the key (or keys) permitted the French to decipher the German telegrams at every intercepting station as quickly as the legitimate addressees could.[100] As already mentioned, the double transposition system had two keys (or the same key applied twice) in the form of keywords, which, according to a very simple rule, were changed into a corresponding numerical key. The keywords were of about the same nature as words of the solved text.

The work of solving the cipher was performed along two different lines, which led to the same result at about the same time. One was the well-known intuitive method known among cryptanalytic experts as the "Bazeries method", after its chief advocate. By this method, beginning with a logical (a priori) synthesis, the presence of words suspected of being in the text or in the keys was tested. The other again, known as the "analytic method", was in the case in question based on purely linguistic-statistical investigations of the phonetic combinations of letters. This work was based on the careless employment by the Germans of single transposition ciphers in which all the letters of the clear text retained unchanged values.[101]

According to detailed information furnished by the cryptanalyst, Dr. Locard, at present director of the police technical laboratory at Lyons, which confirmed and supplemented information given by General Givierge, the discovery of the German keys was facilitated to a great extent by the carelessness of the Germans.[102]

For instance, one of the intercepting radio stations picked up the following short telegram in clear text "Was ist Circourt?" Because all circumstances connected with intercepted telegrams were always carefully recorded (such as, place from which they were sent, in case it was known or could be guessed with sufficient probability of accuracy, time, call signals of the sending stations, and distinctive introductory features, etc.), it was easy, with the assistance of detailed classification of intercepted telegrams, to identify the previous telegram which gave rise to the above-cited question in clear text.

The previous telegram happened to be very short and, so far as could be determined from already identified stereotypic characteristics of German communications, it was an order for

[98] Cartier, Le Secret en Radiotélégraphie, Radioélectricité, no. 97, 1925, p. 445.

[99] Givierge, Questions de chiffre, p. 403.

[100] [See in this connection footnote 94.—*W. F. F.*]

[101] [The translation here seems to be correct, but I feel sure that the author does not use the term "unchanged values" with the meaning it commonly has in our terminology, in which the term "value" applies only to the case of substitution. The author is clearly here dealing with transposition, not substitution. What he undoubtedly means is that in the case of simple columnar transposition, the relative positions of letters of whole columns of the plain text remain undisturbed or unchanged; whereas in the case of true double transposition all the letters become very much shifted about, so that even letters originally in the same columns and rows become dissociated.—*W. F. F.*]

[102] In Policiers de Roman et de Laboratoire, Paris, 1924, p. 267, and in written reports.

the transfer of troops. When compared with the cited clear-text telegram, it permitted the drawing of the inference that the name of Circourt must be in it somewhere.

In order to check up on the validity of this inference and, if possible, to obtain an explanation, perhaps of an illuminating nature, with regard to the contents of the first telegram and the real nature of the question asked in the clear-text telegram, the geographic service (Service Géographique de l'Armée) was requested to furnish information with regard to any circumstances connected with the name of Circourt. It was found that the name Circourt occurred on certain French maps which were known to be used by the German staffs, while the maps with which the German troop units were equipped merely gave the location of the town by its initial C.

As the occasion for the clear-text telegram was thus clarified and the cryptanalysts were able to infer the probable meaning of the telegram from the German order style known to them, it became a comparatively easy matter to read the first telegram on the basis of the knowledge that the name Circourt must be found in it, especially because by good luck the message was found to be a short one.

With and by the complete reading of the telegram the numbers corresponding to the keywords became known—the wording equivalent to the key sequence made no difference whatsoever—and the cipher correspondence of the Germans was thus entirely exposed to their enemies.

At almost the same time the French succeeded in identifying the key-word "Kaiser" by the Bazeries method. The selection of such a keyword indicates an obvious lack of psychological insight on the part of the chiefs of the German cryptographic services, for the solution of keywords which were successively tested according to the Bazeries method consisted first and foremost of important names in the history of the country using the system. For very good psychological reasons it is assumed that these words are most prominent in the association of ideas of a personnel not acquainted with the methods of cryptanalysis. Such names as "Kaiser", "Vaterland", "Sedan", for the Germans; "Austerlitz", "Patrie", "République", for the French; "Cesare", "Dante", etc., for the Italians, are highly characteristic of the military mentality. The first names which an experienced cryptanalytic expert would test for reading Swedish telegrams under similar circumstances would be "Lützen", "Narva", "Svensksund", "Sveaborg", and others of a similar nature.

We must therefore stress the fact that even if the French cryptanalytic experts did wonderful work, the numerous blunders made by the Germans considerably facilitated it.

We must stress the fact that errors of some kind cannot always be avoided and that a just criticism consequently should not blame the individual for such errors. In order to avoid them, a complete knowledge of the technic of cryptanalysis on the part of all the personnel engaged in the cryptanalytic and cryptographic bureaus is necessary, an ideal which is practically unattainable. On the other hand, we must strictly condemn the commission of such errors by executive personnel responsible for the safety of the cipher or the recommendation of unsafe systems and systems not easily employed, without any regulations governing the prevention of the most ordinary errors which serve as a basis for enemy cryptanalysis.

The wide-spread ignorance of the means and aims of cryptanalysis on the part of the French, which has already been mentioned, gave rise to the circumstance that extremely important information about the activities of the German cryptographers was not utilized at all or was utilized too late. Thus Givierge quotes numerous instances in which French troops had intercepted German cipher messages, clear-text messages, records, and cipher keys, but these did not reach the cryptanalytic bureaus until much later. A notebook with information containing references to previously used keys, found at Fontenoy-la-Joute near Baccarat, did not reach the cryptanalytic bureau of the Ministry of War until September 22, and an important record found September 20 was not turned over until September 28. It was likewise discovered

by examination of the register of intercepted messages at the stations along the eastern frontier that several important telegrams had never reached the cryptanalytic bureau. In other cases, on the contrary, when by chance some former member of the Cryptographic Military Commission happened to be present, utilizable information was submitted immediately. Once again, the examples cited above give us an idea of the great importance of giving general training in cryptography to officers, preferably as early as possible in their training.

It is self-evident that the German keys found in connection with the incident of the Circourt telegram were transmitted directly to the armies, together with the strictest instructions regarding the maintenance of secrecy concerning the actual circumstances under which the solution was accomplished, this for reasons which have already been discussed in a previous chapter.[103] A hypernervous general opinion, affected by the war psychology prevailing in the warring countries, ascribed an enormously excessive importance to espionage, an opinion from which the corps of officers and higher command were not always entirely free. The members of the French cryptanalytic bureau, who realized that the fact that they knew the German cipher system must perforce leak out sooner or later, above everything else desired to guard against a dreaded change of system, which would occur if the real circumstances were discovered, and therefore by placing the blame on the broad shoulders of spies they hoped that merely a change of key would be made.[104] The same tactics were constantly applied both by the French and English cryptanalytic bureaus.

The secret that the German keys had been discovered was kept very poorly. As early as October 3, French General Headquarters was compelled to send out a confidential circular written with a view to suppressing the numerous telephone conversations on the subject which were intercepted by the operators of their own telephone lines.

However, it was not until October 17 that the German keys were changed. But the system remained unchanged and by October 21 the new keys had already been discovered.[105] The same day the high command wrote the following letter to the subordinate Army group commanders in turning over to them the German keys so that they might be used for reading German telegrams directly at the intercepting stations:

> It has come to my knowledge that during the period when the previous keys were in use, the most elementary precautionary measures were disregarded at certain headquarters. The deciphering of German ciphers then was a sort of game. The fact that the keys were known and the exact or suspected meaning of the German telegrams were the subjects of conversation even among privates.

Hence, a knowledge of the fact that the French were reading the German telegrams, but not of the manner in which they were enabled to accomplish this, was relatively early spread in German cryptographic circles. The much more numerous changes of key, following the change of key we have just discussed, apparently indicate this. In the beginning of November, the French cryptanalytic bureau solved such keys in 3 days, and again, several weeks later it solved the new key the same day it was introduced.[106]

So far as concerned the contents of solved German cipher telegrams, at least at the beginning, before regular telegraphic and telephonic communication had been completely established, they were of extraordinary importance. It must be remembered that communication between German General Headquarters and its subordinate Army headquarters was maintained for a comparatively long time through the radio stations assigned to the different armies and that the habit of using such easy and readily operated means of communication as that offered by the radio, at least after the initial difficulties had been overcome, often led to the continued use of that means even when wire communication was available.

---

[103] Givierge, Questions de chiffre, p. 403.
[104] Ibid., p. 411.
[105] Ibid., p. 404.
[106] Givierge, Questions de chiffre, p. 404.

The ciphers solved later on also were of great importance to the French. The keys which thus were solved, as well as the earlier keys, which, thanks to the greater training and experience of the personnel, were now more easily discovered if they had not already been deduced from the German documents found, permitted the reading of all German radio communications sent before October 1.[107]

In this way, among other things, full knowledge was gained of the radio correspondence exchanged by the Germans before the Battle of the Marne. This explained the reasons, until then unknown, for the change of direction taken by the German right wing east of Paris.

The last-mentioned cases of retrospective solution were especially of historical interest; they were also of very great direct interest. They were very highly valued by the French Army commanders, especially during the period known as the "race to the sea." [108] They gave the said commanders a very important insight into the divergent mentality and conduct of the various enemy Army commanders in different situations and into the manner in which the German High Command conducted operations. Full insight was gained through them into the great freedom of operation which was granted the German Army commanders by an almost entirely passive commander in chief, and there was found herein once more a worthwhile analogy to the traditions from the time of Moltke, which were very clearly explained before the war by the then Lieutenant Colonel Foch in his well-known lectures on the art of warfare.

It is therefore not to be wondered at that General Maunoury explained that through the said retrospectively solved German cipher correspondence he had gained a valuable mental composure and that the high command wrote as follows to the Ministry of War:

> I have, like all the Army commanders, during the last few days, learned to realize the value of the services which have been rendered by the cryptanalytic bureau of your department. Please transmit the thanks of all of us to Major Cartier and his group.[108]

On November 18, a radical technical change in the structure and appearance of the German cipher telegrams indicated that this time not only the key but also the whole system had been changed. This was the first time such a change had been made since the beginning of the war. Carelessness on the part of the French, certainly, was the real reason for this change. It probably was the cause for the establishment by the German General Staff of a section for testing their own cipher systems and for making them safer. This has been mentioned in this work.

It took the French experts about 3 weeks to solve the new system. No other information was found about the nature of the system than that obtained through an analysis of the text, this in contrast to the circumstances connected with the previous system, which was known even before the war broke out. The telegrams were also much less numerous. Hence, the work of solving the cipher consisted first of all in identifying the system and then in finding the keys used. All the cryptanalytic experts were assigned to the work of solving this problem and the members of the Cryptographic Military Commission who were still at the front were assigned the mission of helping in the work, each in the place where he happened to be, and of maintaining constant liaison with existing cryptanalytic centers. Among the members of that commission were Captains Paulier and Latreille and Lieutenant Colonel Thévenin; the last-mentioned gentleman succeeded in making the first solution, on December 10, by comparing results obtained in many different ways.

As usual, the cryptanalysis was assisted by blunders made by the Germans, which were very cleverly exploited. It was found that, despite external complications, the system was in reality relatively easily solved and that the structure of it permitted its solution by key on the basis of only one telegram, as already mentioned. Hence, the system contained a typical illusory

[107] Ibid., p. 405.

[108] Givierge, Questions de chiffre, p. 406. Also Reichsarchiv, Der Weltkrieg 1914–18, vol. V, p. 249, 260, and 376.

complication.[109] If we compare the said information with that given by Colonel Nicolai regarding the manner in which the new German testing division had been added and was recruited, it is fully demonstrated that safety measures, no matter how scientifically planned or carefully elaborated, are to be considered as worthless if the correct conception of the basic importance of the technic of cryptanalysis is not held and the technical knowledge necessary for such analysis is absent.

A review of the solutions which we have already reported shows the utmost importance which must be attached to the external and internal cooperation necessary for cryptanalytic work. The necessity for constantly comparing and supplementing results gained in different ways requires the most flexible liaison and fully dependable cooperation between the various cryptanalytic centers. The external contacts are, if possible, still more important. They may be divided into two main classes, that is to say: contacts with the services which obtain the material, such as the intercepting stations, the staff sections engaged in obtaining and translating enemy documents, etc., on one hand, and contact with the General Staff intelligence branch on the other hand. Absolutely constant cooperation must be established with the latter branch. The slightest bit of intelligence may be of value, intelligence about our own operations (perhaps reported in an enemy's cipher telegram) and about all measures known to have been taken by the enemy. Information that so many enemy airplanes of a certain type have been seen over a certain place, that they were flying toward a certain destination, and information concerning the time, etc., may help in the solution of some cipher telegram which may be connected with a subsequent aviation expedition because of the time, place from which it was sent, place to which it was addressed, and our knowledge of the enemy's order-writing technic. It also happened several times that their own operations, such as a certain bombardment, feigned preparations for attack, etc., were directly ordered for the purpose of comparing enemy cipher reports with them, all for the purpose of helping in the solution of cryptograms. We must also emphasize the fact that such measures were not taken until during the latter half of the war.

From the above we conclude that no definite rules can be laid down for such cooperation and that it places exceptionally great demands upon the general military training and intelligence of the experts, for which a certain limit cannot be exceeded. As a rule, this cooperation, at least so far as the efficient cryptanalytic bureaus on the French staffs were concerned, consisted in allowing the bureau chiefs free access to all other divisions and sections of the staff and allowing them to attend the daily conferences of the Chief of Staff with his section chiefs. It was the duty of the chief of the cryptanalytic bureau properly to instruct his subordinate personnel, but the said personnel as a rule also maintained intimate contact with the staff personnel.

Consequently, it is not strictly necessary to have the chief of the cryptanalytic bureau himself actually do the cryptanalytic work, but it is rather to be desired that he chiefly devote his energies to the mission of constantly collecting information and documents. On the other hand, it is absolutely necessary that he be sufficiently well informed concerning all the methods used in cryptanalysis to be able to judge directly whether a certain event may or may not be of interest and especially whether it may be of practical interest. He must be absolute master of the difficult art of selection.

It may seem that the requirements outlined above are too high and that they demand the services of so large a force as to be entirely out of proportion with the attainable results. There is no doubt that this danger exists, but the size of the force depends entirely upon the ability of the cryptanalytic experts, of whom very great demands must be made. The effort of an officer or civilian are practically wasted if that officer or civilian has been assigned to the cryptanalytic service without any consideration whatsoever of his qualifications for such work, or at least,

[109] Givierge, Questions de chiffre, p. 409.

without good prospects of his possessing the qualifications necessary for it. During the latter part of the war, the tendency therefore was to use civilian personnel for the cryptanalytic work proper; if possible, personnel which had obtained previous training for that work in the reserves or the like, and to appoint as bureau chiefs, officers who had received complete training as cryptanalysts, regardless of their service or rank.

It was also found that the cryptanalytic personnel constantly increased, and that, at least in France, a great number of competent officers, often of the higher ranks, served in those bureaus. From this fact we can deduce the importance assigned by the high command to the cryptanalytic service. Among other things, this was expressed by promotion to the rank of general of the two cryptanalytic officers who had served from the year 1914 in the cryptanalytic bureau of the Ministry of War, Majors Cartier and Givierge.

Now to return, after this long digression, to the development of the methods of cryptanalysis, we wish to mention the fact that the high command was compelled the day after the new German system had been solved, that is to say, December 11, to issue another circular with a view to eliminating the persistent carelessness on the part of the personnel in revealing the secrets connected with its work.

The experts had by this time become so skilled and the new system was, as we have stated, so inferior to the former system that the successive keys adopted by the Germans after that were practically all found the same day they were placed into effect, as were subsequent variants of the same system.

In the fall of 1914 the French command began making preparations for an expected, or at least a desired, general advance. Among these preparations was the organization of the radio service, the extensive use of which was considered necessary during the advance march. Due to the fact that the encipherment of telegrams transmitted by wire revealed that the clerks who performed this work had an excessively great ignorance of and a contempt for the application of the rules necessary for keeping the ciphers secret, it was decided to entrust this work only to trained specialists, who at the same time were ordered to instruct all officers with whom they came in contact officially. As early as September 17 an order to this effect was issued.

Every army headquarters was provided with such a specialist, either one who had been trained in the cryptographic bureau at General Headquarters, or preferably one recruited from among the officers who before the war had taken one or more of the many special courses given by the cryptographic bureau of the Ministry of War. The necessity for maintaining service both night and day led to the enforcement of regulations to the effect that this officer should be assisted by one of two army staff officers in turn or one of the assistants sent out from General Headquarters.

Some of the chiefs of staff caused certain difficulties, it is true, for they did not see the necessity for the prescribed regulations, but the discovery of the German keys and the necessity for restricting the number of persons handling cryptograms in order to maintain their secrecy, resulted in the definite order to attach the cryptographic service to the second bureau (Intelligence Bureau).

In this connection it must be emphasized that although the French cryptanalytic personnel and the personnel compiling the ciphers functioned particularly well, conditions were far from being as favorable so far as the extensive force of cipher clerks was concerned. It is true that good systems had been compiled before the war, one of which was used during the first 3 years

of that conflict without there being any indication of its possible solution by the enemy,[110] but it also very soon became evident that the cipher personnel, which was not especially trained for its work, was making numerous blunders. Fortunately for the French, the said blunders were made during the period when wire telegraphy was used, and therefore, they did not involve any direct risk of having the enemy solve the ciphers. But the situation was serious enough to attract attention. It was found that definite instructions were not followed when the personnel was totally ignorant of cryptanalysis and did not understand the real import of the regulations; for that reason the method of detailing specialists to army headquarters, which we have already discussed, was adopted.

The most ordinary and frequent blunders were the following: Telegraphing in clear text on purely official business from one station to another; telegraphing in "mixed text", although this was less usual with the French than with the Germans; having on one's possession, when in the vicinity of the enemy, documents which might be useful to that enemy (clear-text confirmation of cipher telegrams already transmitted, copies, records, etc.); confirming by telephone telegrams received or sent, etc. These blunders, even after the war, were the reason for the inclusion of carefully drawn up rules covering the necessary precautionary measures in a number of the French military regulations.[111]

The extremely great importance to be attributed to the manner in which a cipher system is used is illustrated by this. Simple and easily applied systems are therefore much more advantageous than systems that are difficult to use or systems that are complicated, for they save time, cause less errors in encipherment, and prevent the extra communication resulting therefrom. They are less likely to cause cipher clerks to use clear text under all kinds of conditions. Clear texts must not be used, no matter how safe such telegrams may appear to personnel unacquainted with methods used in cryptanalysis.

Both the French, and especially the British, used more easily handled systems than did the Germans, at least during the first half of the war, and experience has conclusively proved that such systems were much safer.

As we have already emphasized, the cryptographic service and the cryptanalytic service are very intimately connected. Experience has shown that they cannot successfully be separated. A cryptographic clerk must perforce have an adequate insight into the blunders and errors which are taken advantage of by the enemy in solving his cryptograms, and the cryptanalytic expert also requires practical experience in cryptographing and decryptographing in order that he may be able to comprehend the special "knack" and tricks of the routine cryptographic clerk and in order that he may be able to recognize them in making his cryptanalysis. Furthermore, the cryptanalytic expert who is responsible for the safety of a new cryptographic system must also be fully experienced in the practical application of the system by cryptographic clerks. It would therefore be best, as General Givierge rightly contends, to combine these two activities and to attach the bureaus in time of war to the intelligence division of the staff, leaving them, however, entirely independent of the latter as far as operation is concerned. An exception to this rule should be made of the central cryptanalytic bureaus. These have the most skillful and most

[110] Givierge, Questions de chiffre, pp. 407, 411, and 59. [Note: From the manner in which the author refers to the cipher system used by the French during the first 3 years of the war one might be led to infer that the system was practically, if not absolutely, indecipherable. But such an inference would, in my opinion, be wholly unwarranted, for the French system not only had most of the defects of the German double transposition cipher but also, theoretically at least, it was much more vulnerable to solution. The greatest weakness of German cryptography lay not in the cipher systems themselves but in their improper handling by untrained, unskilled personnel. On the other hand, if the Germans failed to solve the French cipher system here referred to, this was not only because the French cryptographic personnel were better trained, but also because the German intercept and cryptanalytic service was poorly organized and lacked properly trained cryptanalysts until 1916. It should be added, however, that the Germans claim to have had as much success with the cryptograms of the French and the British, after 1916, as the Allies had with theirs. Detailed reports are, however, not available, if they have ever been published. See, in this connection, Gyldén's remarks on p. 43 below.—*W.F.F.*]

[111] Instr. sur le fonct. et l'org. des Etats-majors en campagne, Paris, 1925, secs. 24, 47, 96, 106, 163, 164, and 165. Instr. prov. sur l'org. et le fonct. de la liaison et des transmissions, Paris, 1927, secs. 124, 139, 140, 147, 148, 149, 188, 198, 199, 200, 201, 202, 234. Instr. prov. sur le service en campagne, Paris, 1924, secs. 68 and 75.

reliable experts and are to the best advantage attached to the office of the Minister of War and also placed in very close liaison with the Ministry of Foreign Affairs.

Now, with respect to the measures mentioned above, which were adopted with a view to instructing the cryptographic personnel at army headquarters, the deficiencies already discussed proved to be great in scope. Later on, in January 1915, these errors and blunders caused the issuing of a special order requiring all officers who had anything to do with codes and ciphers on any part of the front to cryptograph 4 or 5 rather long messages every day for 1 month as necessary training in that work and as practice in the observance of the safety regulations.[112]

There is relatively little to be reported concerning the work of this kind done in the year 1915. The number of German radio messages decreased daily, as did also the importance of the messages sent, and in the spring of 1916 such communications were chiefly restricted to official reports of local nature transmitted between army corps or still smaller units. However, the systems were very interesting to solve, and although they were unlike the systems previously used, they still possessed inadequate theoretical safety. As General Givierge declares, they always indicated that although the men who had compiled them perhaps possessed some technical knowledge, nevertheless they did not have adequate practical experience in the problems presented by cryptography.[113] Painvin, professor of paleontology and lieutenant in the reserves, the cleverest of all cryptanalysts, also known as perhaps the greatest expert in this line at the present time, obtained splendid results because of his extraordinary keenness of mind. Cooperation between the various cryptanalytic centers was very close, and it often happened that General Headquarters within a few hours received from several different centers the identical solution of some new German telegram.[114] It must be emphasized that cooperation with the British cryptanalytic bureaus at that time was very well organized and that the personnel of those bureaus gradually developed a skill equal to that of the French.

The time made available for extra work by the decrease in the number of German radio communications was utilized chiefly for the solution of other German ciphers, especially diplomatic ciphers, and also for the analysis of the codes used by the German fleet and of weather reports sent by telegraph. Ciphers from distant fronts were also studied, especially those from the Balkans, where German units also were fighting and where they were still using systems long since abandoned on the Western Front and already solved by the French. This, therefore, indicates the faulty centralization of German cryptographic work.

There is an interesting incident to be reported concerning the weather reports mentioned above. As early as 1914 the German station at Norddeich sent out by telegraph regular weather reports in mixed text. In these the cipher clerks had not taken the trouble to encipher the letters and numbers ordinarily used for indicating the direction and strength of the wind, etc.[115]

The station at Brugge, on the contrary, committed the inexcusable stupidity of transmitting the same telegram after having enciphered the said figures and letters. A comparison of the two telegrams gave an exceedingly valuable clue to the code used, and, as ordinarily is the case in code solution, this permitted, by successive expansion of the "break" in the system thus obtained, a gradual reconstruction of great parts of it.

Very few details are available about the solution of the German diplomatic codes. This much is certain: work on them was begun very early and was based on radiograms sent out by the station at Nauen, together with other diplomatic cipher correspondence which was supplied, particularly by the English from numerous sources.

That which first of all helped to start the cryptanalytic work was the war propaganda and instructions which were telegraphed in cryptographic form from Germany, important parts of

[112] Givierge, Questions de chiffre, p. 410.
[113] Givierge, Questions de chiffre, p. 412.
[114] Ibid., p. 413.
[115] Ibid., p. 63.

which were given out to the press unchanged in phraseology. A comparison of the names, etc. occurring in them, permitted a comparison with corresponding telegrams. Later on, we shall also discuss this problem in connection with the discussion of the numerous code solutions successfully performed during the war.

During the period from 1914 to 1916 the Germans did practically no cryptanalytic work on the Western Front. The lack of a continuous tradition and the lack of the necessary textbooks on cryptanalysis certainly played a great part in producing these circumstances, as did the fact that contact with expert civilian cryptanalysts was made too late. The latter was, however, of slight importance for the same reason as was mentioned in connection with the military cryptanalytic experts, and, as on the Eastern Front, so here also it was probably chance which directed all the cryptanalytic work.

The French reports to the effect that the Germans did not succeed in decrypting the French cipher until during the winter of 1917–18 seem, to judge from all circumstances, to be correct. It takes years to train an expert cryptanalyst, and nothing is more difficult than self-training without the assistance of previous experience and practice, which fact has been stressed by all experts since the war; for instance, Givierge, Cartier, Lange, and Soudart. What we know about the faulty preparations on the part of the Germans for cryptanalytic work, and especially about the faulty course adopted by the German General Staff Cryptographic Section before 1914, confirms this idea. The absolutely safest indication, interpreted according to methods analogous to cryptanalysis, however, lies in the structure and nature of the German cryptographic systems. We can follow the development of the German cryptographic systems step by step. First we see an obvious ignorance of the elementary rules of cryptanalysis. This was followed by a period during which practical experience had not yet secured supremacy over a faulty estimate of safety. Then not until much later came a period in which experience and observation gradually were utilized in compiling new systems. The foundation for cryptanalysis, a knowledge of the theory of cryptography, apparently never was possessed by the Germans to the degree in which it was displayed in France by a number of clever experts and in perhaps to a still greater degree by the Cryptographic Military Commission, which was active before the war and whose share in the cryptanalytic work of the French was of decisive importance.

Centralization and cooperation were never taken into consideration to an adequate extent. For instance, from the information given by Captain Carlswärd in his account of the activities on the Eastern Front, we learn that change of system and of keys during the year 1914 was made independently on the Eastern and Western Front, and apparently there was no liaison in the cryptanalysis performed on the Russian cipher systems by the Germans, which we shall discuss farther on, with any central cryptanalytic official and much less with the cryptographic centers on the Western Front, at least during the year 1914.

Such a center or bureau was located at Neumünster, and it became famous because of the solution of some of the British naval ciphers,[116] the date of which unfortunately is unknown. Since the existence of this bureau was not reported until at the beginning of 1916, it is probable that these ciphers were not solved until after that year. It must also be conceded that the experts who by chance were available for this duty found their work much more difficult because of the fact that the radio communications of the Allies were purposely restricted from the very beginning, and still more because of the fact that cryptanalysis was begun altogether too late, as the British and French cipher regulations had already obviously been affected by experiences gained in observing the mistakes and blunders made by the Germans. The great start which the French particularly had in preparations for cryptographic work before the war, not only made it possible for them, step by step, to keep up with the work done in that line by the adversary,

[116] Commandant X, Les Grandes Heures de la T.S.F., in Q.S.T., April 1928, p. 24.

but also to a great extent to apply to their own cryptographic work important experiences concerning the ordinary risks involved in the application of cryptography.

Not until about 1917 may it be said that the Germans caught up with the Entente to a certain extent so far as cryptography was concerned. On the other hand, in the field of cryptanalysis the Germans apparently never acquired the same technical perfection as their enemies; conditions were far too unfavorable for this. The Germans, however, were certainly aware of their own faults, as is shown, among other things, by the extraordinarily lucid and instructive regulations for the use of ciphers, which were captured by the French during the war and which are reproduced in full by Lange and Soudart.[117]

Lastly, we must mention the following opinion expressed by Colonel Nicolai as markedly characterizing the period from 1914 to 1916:

> As far as cryptographic systems were concerned, the Russians were the most harmless and ignorant of all. The disadvantages resulting therefrom were of decisive importance to them in their conduct of warfare. On the contrary, most prominent and distinguished were the compilation and the careful application of their cryptographic systems by the other hostile powers. Systems and key-words were changed at very short intervals. It was obvious that the intelligence services of the enemies did careful work in solving the cipher systems of the Germans and through their achievements in that line became more careful in their own cryptographic work.[118]

Despite the fact that in this opinion the author confuses the work done by spies and that accomplished through cryptanalysis, as well as a misconception concerning some details, this opinion as a whole is, however, quite correct.

As far as the cipher systems used during the period from 1914 to 1916 are concerned, the Germans, as already stated, used regular transposition ciphers of several different kinds to a preponderant degree. As for the French, in addition to a code used for correspondence between army headquarters and General Headquarters, they used an irregular transposition cipher, which is given by Colonel Figl [119] and which is recognized immediately again from a passage in General Givierge's account,[120] and also a so-called substitution cipher with running key text and arbitrary alphabet. The British, on the other hand, besides the substitution cipher like that of the French, used a particularly practical and simple system based on digraphs, which possessed satisfactory security because of an exceedingly simple and convenient change of keys. This system also is given by Colonel Figl,[121] although he never mentions the methods of superencipherment used later by the British.

2. THE PERIOD FROM 1917–18

From the standpoint of cryptography and cryptanalysis, the latter half of the war on the Western Front may suitably be characterized as the "code-book period."

Code books had, it is true, been used by the higher French Staffs from the very outbreak of the war (4-figure codes), but elsewhere generally ciphers and not codes were used for military correspondence, in contrast to the rule applied to diplomatic correspondence, for which code books were generally used.

---

[117] Lange et Soudart, Traité de Cryptographie, p. 88.

[118] Nicolai, Geheime Mächte, p. 145.

[119] Figl, Systeme des Chiffrierens, p. 46.

[120] Givierge, Questions de chiffre, p. 410. [Note: The author contrasts what he calls the "regular transposition ciphers" with what he calls "irregular transposition ciphers", and in view of previous statements seems to have a much higher opinion of the latter than of the former. By regular transposition ciphers he apparently means the class in which the letters are inscribed in a regular manner within a geometric figure presenting definite symmetry, and are then taken out of the design in a regular or more or less fixed order; by irregular transposition ciphers he apparently means the class in which, while the letters may be inscribed within a similar geometric figure, they are taken out of the design in an irregular, more or less variable manner. In my opinion it is doubtful whether other experts will agree with the author's estimate of the relative merits, from a theoretical viewpoint, of the two specific systems he contrasts, i.e., the German (double) regular transposition cipher and the French irregular transposition cipher.—*W. F. F.*]

[121] Figl, Systeme des Chiffrierens, p. 89. [Note: The author refers here to the Playfair Cipher, which, it is true, is "particularly practical and simple"; but it is extremely easily solved, no matter how frequently the keys may be changed. It is no difficult matter to solve even a single message if it is not too short.—*W. F. F.*]

As early as 1916, however, minor beginnings were made in the use of codes by both sides on the Western Front. Short code or secret word lists, chiefly intended for use when telephoning in the vicinity of the enemy, were generally in use. The French code lists, to begin with, contained only about 50 expressions, encoded by groups of 3 letters. The corresponding German lists, known as "Befehlstafeln" or "Geheimtafeln" were composed either of concentric rotating disks with the text expressions on one disk and the code expressions on the other, or of small codes with arbitrary numbers at the side, of about the same type as the Baravelli code, which we have explained in connection with the discussion of the Dreyfus case.[122]

However, it soon became evident that the safety of such systems was very inadequate. The intercepting service, both for radio and telephone communications, called the "Abhorchdienst" by the Germans and the "Service d'écoute" by the French, which was far better organized, brought the cryptanalysts a great deal of material to work on. As usual, the blunders made by the cipher clerks formed the most dependable starting point for the decrypting, but even aside from them, the solution was made possible because of the far too inadequate safety of the system.

For instance, the variation factor, which the German concentric cipher seemed to possess, proved to be mostly illusory. From a knowledge of one position a knowledge of all other positions of the rotatable disks could very easily be deduced by the so-called "parallel test." That is, starting with the identification of some one stereotyped telegraphic or telephonic message, such as the message which was sent so often on quiet sectors of the front, "nichts zu melden", or some similar message—most frequently repeated at certain definite intervals—it was possible to determine the relative positions of the two rotatable disks. This meant that in reality first a few messages were successfully solved through a knowledge of the enemy's stereotyped habits, and then later, thanks to the change in key, the plain-text expression on the disks were reconstructed, an apparently paradoxical but by no means uncommon procedure in cryptanalysis. This was not the first time that changes in key to a very great degree assisted the cryptanalysts of the enemy, while the German code compilers blindly trusted in the so-called "increased safety" secured thereby. To this was added the fact that a regularity in the text and code lists greatly facilitated the analysis, even if this regularity applied merely to certain groups, such as for example, the code list having the following aspect: "AAA, AAB, AAC . . . AAZ; KAA, KAB, KAC . . . KAZ; PAA, PAB, etc." Such regularity is of the most dangerous kind but it recurs time and again in systems invented by personnel unversed in the science of cryptanalysis. The Italians and the Germans particularly sinned in this respect. "Regular" alphabetically arranged lists of this kind, known in France as "codes ordonnés", were condemned very early by the French and their use was expressly forbidden.[123] As far as the codes of the Baravelli type mentioned above were concerned, we have already discussed their analysis earlier in this work.

The use of "cover" words or equivalent expressions also proved to be very treacherous, because the great majority of officers, both commissioned and noncommissioned, who used such veiled language, did not possess the slightest knowledge of cryptography and very easily made the most serious blunders. It is indeed self-evident that a text of the following type, "Colonel seriously 6524 this morning", as Lange and Soudart justly maintain,[124] shows us by direct inference that 6524 means "wounded", and that the communication, "The herring attacked our foremost mackerels at 6:33 o'clock this morning, etc.", merely shows that the "herring" means the "enemy", and a comparison at the cryptanalytic bureau of the rest of the text with the

[122] Givierge, Questions de chiffre, p. 414.

[123] [The author here refers to what we call "1-part" codes.—*W. F. F.*]

[124] Lange et Soudart, Traité de Cryptographie, p. 87.

fact that an operation had been undertaken by our forces against a couple of enemy machine-gun nests in the front line at the time indicated in the message instantly permits us to infer that "mackerels" must mean "machine-gun nests" or corresponding words.

We must not think that such cryptograms are unusual; quite the contrary, they are the rule. Even in the heat and hurry of the battle, it does not require a great deal of intelligence to solve a "mixed text" of this kind. Failure to encipher the time, which was such an ordinary blunder on the part of the Germans, is one of the most dangerous mistakes, for it permits a direct important comparison of the intercepted message and events which, as a rule, are known equally well by both sides and are carefully recorded in war diaries.

The use of "mixed texts" of this kind was condemned long ago. For instance, Lange and Soudart very justly write: "Nothing is more dangerous than a partial encoding or enciphering." [125] General Ronge writes as follows in speaking of the solution by the Austrians of Russian ciphers: "What joy when radiogram after radiogram reached us in clear text! And what still greater joy when words in cipher were added now and again." [126] General Givierge is still more emphatic. He writes: "The habit of enciphering only a few words is deplorable as far as safety is concerned, and is forbidden in all cryptographic bureaus." [127]

In this way the warring powers gradually changed to the use of pure codes, and in June 1917 the use of such codes became general on the Western Fromt.[128]

The majority of such codes intended for use in the Army, so-called "troop or Army codes", were at first alphabetically arranged (1-part codes). The great volume of the material available and the great disadvantages of the system greatly facilitated the solution of such codes. The most usual division of the code was to have certain pages for numbers and figures, others for letters of the alphabet, others again for ordinary words and expressions and in certain cases for syllables. Because of ignorance of cryptanalytic methods on the part of the compilers of the code, such groups were usually easily identifiable, especially the numbers. There was no difficulty encountered in following the numbers of each telegram and directly identifying the corresponding code expressions, if the interception was good, for they usually occurred at the beginning of the telegram. The regularity in the sequence of code groups immediately gave proof of the correctness of the hypothesis. For instance, in four successive telegrams from the same transmitting station the groups KAA, KAB, KAC, and KAD, etc., were found. These indicated the principle on which the code was based, that is to say, regularity. Beginning with the identified numbers, which most frequently gave the best "start" into the solution of the code,[129] related words were obtained. For instance, the number 127, found in one telegram, could be identified with a known enemy regiment of the same number; then with great probability of being correct, the group following it could be identified as "infantry regiment" or "regiment", etc. The "break" in the code was gradually widened, as is always the case in code cryptanalysis. In the case of a regular, alphabetically arranged code (1-part), such a solution is simple to make, thanks to the very close approximation with which the corresponding clear text for a certain expression can be determined. For instance, if we have identified JAC with "regiment" and JAF with "regulation", we know that the code words JAD and JAE (if they both appear in the code) must mean some word or expression beginning with "reg", for instance, "regimental commander", "regimental order", etc. We do not need many such discoveries in order to solve the code, particularly if the solution may be based upon a knowledge of the enemy's stereotyped order and report technic, as well as of his normal grammatical construction. After having identified a certain text as meaning the "127th infantry regiment", we can justly

[125] Lange et Soudart, Traité de Cryptographie, p. 87.
[126] Ronge, Kriegs und Industrie-Spionage, p. 113.
[127] Givierge, Cours de Cryptographie, p. 256.
[128] Givierge, Questions de chiffre, p. 415.
[129] Givierge, Cours de Cryptographie, p. 260.

assume, with a high degree of probability of being right, that this is followed by a verb. The beginnings and endings of sentences are also particularly worth while subjects of investigation, and the numbered sections, such as paragraphs 1, 2, 3, etc., so frequently used in writing military orders, are easily identifiable in the telegrams.

To use letters to spell out a number or figure, as was done in the French codes, is sometimes of advantage, because it eliminates regularity, and, on the other hand, it restricts the number of times the figure is used. The repetition of the same figure is most treacherous, for no cryptanalyst, for example, would seek any other explanation of the repetition JAB JAB than that JAB either indicates one single letter or one number or possibly one syllable.

Punctuation is also a treacherous factor, due to the high frequency of the corresponding code group and its place in the telegram. It occurred with remarkable frequency during the World War that certain cryptographers always finished their telegrams with "period", which made the other periods occurring in the telegram available for purposes of reconstructing the general structure of the text.

It does not come within the province of this work to report on the highly interesting and technically highly improved science of cryptanalysis. It will merely suffice to point out that such analysis is made by very carefully prepared tables of statistics of all the assembled material, in which the frequency of each code group, its location in the various telegrams, and its combination with other groups are compared with what is known about the stereotyped style used by the enemy, the probable nature of the telegram (order, report, etc.) and its probable contents (made by comparison with certain events, and the time, if identified, etc.). For 1-part codes, also, the particularly original and effective intersection methods are used, some of which are reported by Hooker,[130] and Givierge.[131] These employ a sort of goniometric intersection of each code group.

The alphabetically arranged codes were quickly given up by the French and later also by the Germans. The French troop codes at the close of the war were of exactly the same type as the staff codes,[132] although not as extensive, and therefore included entirely *arbitrary* code lists for the alphabetically arranged text lists and a necessary double list with the code list in "normal" sequence, to be used for decoding.

Cryptanalysis by the French of the German codes was in charge of Captain Painvin,[133] whom we have already mentioned. He developed a remarkably detailed and exceedingly ingenious technic of cryptanalysis, which may be designated as a masterpiece produced by a logical and analytic mind.

The most intimate cooperation was established between the cryptanalytic bureau under the Ministry of War and the various bureaus operating in the field, the chiefs of which were allowed to serve in the office of the Minister of War for certain periods, during which they took certain courses of instruction. In the cryptanalytic service in the summer of 1917 there was the following military personnel: 15 officers assigned to the cryptanalytic bureau at General Headquarters, 3 at each of the headquarters of the Army group and the Army.[133]

There were also about 35 experts in the cryptanalytic bureau in the office of the Minister of War, which was composed both of civilians and soldiers. Of these, about 10 experts were permitted to concentrate on the solution of the German codes, using the method of Painvin mentioned above. A special network of dependable communications made it possible to report the results obtained at any one cryptanalytic bureau to any other.

The bureaus were supplied with a regular stream of intercepted messages. The majority of the purely military messages intercepted were from the smaller German radio stations

[130] Hooker, The deciphering of cryptograms, The Police Journal, No. 4, London, 1928, p. 629.
[131] Givierge, Cours de Cryptographie, p. 259.
[132] Givierge, Questions de chiffre, p. 414.
[133] Ibid., p. 415.

assigned to comparatively small units, and the necessity for comparing the contents of the radiograms with events occurring upon the corresponding sector of the front entailed so great a decentralization that the various bureaus were moved up as near the front as possible and assigned to Army or corps headquarters.

General Cartier has written an exceedingly interesting and complete account [134] of the extraordinarily extensive activities and organization of the intercept service, from which we learn that the country as a whole was divided into three intercepting zones, with centers at Paris, Lyons, and Bordeaux, and that the Paris center included intercept groups at the Eiffel Tower, El Trocadero, Issyles-Moulineaux, Mont-Valerien, Palaiseau (all in Paris or its immediate vicinity), and at Chartres, Orléans, Neufchâtel, and Poitiers. A corresponding radio goniometric network extended from Le Havre to Salins, with stations at Gisors, Chartrainvilliers, Melun, Toucy, and Saussy.

At the beginning of the war, general interception of messages was begun at the stations located in the fortresses of Maubeuge, Verdun, Toul, Epinal, and Belfort (where messages were intercepted even before the war, as we have already stated), and at the three special stations, that at Lille, that at Rheims, and that at Bésançon, all under the general staff. Later on they concentrated upon intercepting messages sent over the enemy's field radio net. The special wire system which was to provide communication with the cryptanalytic bureaus was extended inward so as to provide communication between the cryptanalytic bureau in the Ministry of War and the three most important intercepting stations, Orléans, Neufchâtel, and Poitiers, and outward, with a view to the immediate utilization of the code solutions effected, with the various higher Army staffs. We get a good picture of the extent of the work done in these radio intercepting stations from the statement made by Cartier that more than 100,000,000 words were intercepted during the World War by the French intercepting stations.

Exceedingly important results were obtained [135] in the solution of German codes, and up to the end of the war a total of more than 30 German military codes were successfully solved.[136] The solution which had the most important consequences was without doubt that of a German staff code of the Satzbuch type which was used for radio traffic by a station near Roye as the result of the fact that wire communications had been broken off during the summer offensives of 1918. A German radiogram, sent on June 1 and encoded in the said code, was decrypted on June 3. It read as follows: "Expedite supplies of ammunition; if not under observation, even in the daytime." [136] It is worthy of mention that the said code solution, accomplished by the group of cryptanalysts working under the direction of Captain Painvin, was also facilitated by the blunders made by the Germans in the employment of the code.

The fact that the radiogram already cited was sent from a certain station to a certain other station, as well as other circumstances connected with it, led the French to assign extraordinarily great importance to it as the forerunner in time and place of a German offensive against the Humbert Army, and directly led to the countermeasures which were started June 11 at Méry-Courcelles by General Mangin in the form of a counterattack against the German offensive which was started during the night of June 9 east of Montdidier. The results of that counterattack were of very great importance, a fact which is too well known to be mentioned here, for, as a matter of fact, they turned the tide of the war.[137]

---

[134] Cartier, Le service d'écoute pendant la guerre, in Radio-électricté, nos. 16 and 17, November 1923.

[135] Givierge, Questions de chiffre, p. 415.

[136] Givierge, Questions de chiffre, p. 417.

[137] [The reader, who is assumed to have at least some slight familiarity with the difficulties and especially of the *time* required in solving code, will no doubt wonder how it was possible for the French to solve within the short space of 2 days a message encoded in a code of the 2-part type, such as the German "Satzbuch." His astonishment would be justified if that were really the case, but the fact of the matter is that the message was *not* in code. I have in my possession a copy of the message in question, as officially deciphered by the French cryptanalytic service. It is plainly marked as having been transmitted in the "ADFGVX Cipher", which puts a wholly different light on the matter. Mr. Gyldén can hardly be blamed for the error, because General Givierge, whom he cites as authority for the incident, fails to make the matter clear. See, in this connection, footnote 9 to the translation of Givierge's article as printed in Signal Corps Bulletin No. 33, March 1926.—*W. F. F.*]

The code solutions were of great importance in showing the grouping of the enemy's forces and in giving information about the measures he was taking and his preparations. By this means, in the period between December 5 and December 15, 1917, alone, the location of 4 German divisions, 32 regiments, and 1 "Angriffsdivision" was identified. In this way also, within that same period, the presence of General von Erp, chief of the Three Hundred and Forty-second Division, at a certain point on the front was learned. Another telegram, sent on December 15, betrayed a localized German attack, which was repulsed, thanks to countermeasures that were taken in time. Another telegram, sent on December 5, disclosed the new call signals for the German radio stations.[138]

As a rule, the telegrams were short. It is self-evident that every word, expression, or whole phrase in the code which could possibly be solved had to be solved by cryptanalysis, unless the enemy's code had been captured on the field of battle or had been learned in some other way. The main objective was to learn the chief contents of the communication and to determine the figures, dates, numbers, and time. This was so much the easier because these very factors were the most favorable points of attack. General Givierge gives a few examples of incomplete solution of telegrams of this kind: "May 13, 1918 . . . infantry regiments 97, 137, and 265. Gas attack will be made the 14th day of May from 6 a.m. to 8 a.m." Also, "R.C. to the brigade—contact made with 9/122 and 4/128. Losses: One dead, five wounded . . . 479th regiment." As may be seen, all important data are identified. It was sometimes an advantage when the whole code was captured, but the advantage was somewhat limited because of the fact that the code was changed as soon as it was discovered that any copies had fallen into the hands of the enemy.[139] In this connection, we must point out the fact that in the relatively numerous instances in which codes were lost their loss was not always reported immediately to the cryptographic officers and sometimes it was not reported at all. The reasons for this were either carelessness or fear of punishment. The responsibility assumed by persons who were guilty of causing delays in reporting the loss of code or of failing to report such loss is so great that the value of the ordinary form of direct or indirect penalties imposed for this misdemeanor may rightly be doubted. It is better to have the loss reported in time.

About the end of 1917 and the beginning of 1918 the German codes were improved by increasing the number of the text expressions. For example, the codes used by the armies and army detachments, the so-called "Satzbücher", were enlarged so as to include about 4,000 expressions, and the so-called "Schlüsselhefte", used by the divisions and smaller units, were enlarged so as to include about 1,000 expressions. Corresponding French codes were called "codes" or "dictionnaires", for the higher units or staff, and "carnets reduits" for the smaller units.

The necessity for being able to cryptograph with facility all kinds of clear texts was the reason for this expansion. The dangers connected with the use of "a mixed text" had become far too well known by that time. What was not definitely known, at least not by the Germans, was that the safety of a code is not in any way proportionate to the number of different text expressions in it,[140] for it is a fact well known to cryptanalysts that every cipher clerk has his own habits and practices and as a rule merely uses a few of the code expressions available, and those always the same ones, which are consequently quickly recognized when adequate study material is available.

The great disadvantages of the "regular" alphabetically arranged codes, especially from the viewpoint of safety, resulted in a change to purely arbitrary codes, which was made in France about 6 months before the same measure was taken by the Germans. Such arbitrary codes

[138] Givierge, Questions de chiffre, p. 416.

[139] [It is true that a code was changed as soon as it was discovered that a copy had fallen into the hands of the enemy. But, in addition to this, a new edition of the German "Satzbuch" was distributed about every 18 to 20 days, on the assumption that after this length of time the codes had been broken down sufficiently to compromise them.—*W. F. F.*]

[140] [To say, without any qualification whatever, that "the safety of a code is not in any way proportionate to the number of text expressions in it," is, I fear, quite unwarranted. If this were true a code of 1,000 items would be sufficient for all purposes, which is obviously not the case.—*W. F. F.*]

contain arbitrary code lists, as we have already mentioned, and have the following appearance, for instance:

Armored	5878
Army	4879
Army commander	0875
Army group	6612
Army will	6894

Such arbitrary codes require double code lists, one like that from which the above extract is taken, having the text expressions arranged in regular sequence (in this case, arranged alphabetically) with their corresponding code groups, the other having the code groups in regular sequence (arranged serially) with their corresponding text expressions. The lists are used for encoding and decoding respectively.

The lack of a clear, explicit cryptographic terminology, as well as the ordinary confusion of the various meanings of the different terms, leads the author to maintain that cryptographing is an operation whereby a clear text is transformed into a message incomprehensible to a third person, while decryptographing is the opposite operation, the one whereby a message which is incomprehensible to a third person is changed into a clear text on the basis of a complete and legitimate knowledge of the procedure whereby it was encoded or enciphered. Hence, decryptographing has nothing in common with decrypting, which is the successful reconstruction of the clear text by a third person, accomplished by other methods. The expression decrypting, used in France as a synonym for code solution and in Sweden as a synonym for decoding or deciphering,[141] etymologically is the discovery of something that has been kept secret (from the Latin "de" and the Greek "kryptos", which means secret) and consequently is applicable to decrypting but not to decryptographing.

In the above-mentioned arbitrary codes there are used as code groups either figures or letters, usually of 4 or 5 units in the larger codes. Practical experience has shown that pronounceable 5-letter groups, compiled according to definite technical rules, which are found among other places in Bentley's commercial codes, apparently are to be preferred for military purposes. By their use the correct readings for errors in cryptographing [142] and also for the ordinary transmission errors, which occur so frequently in the field, are very easily found, because in such codes at least two of the letters are always different in two different code groups. Codes of the older type that were used on the Western Front, with trigraphs having only one letter or figure varying in the different groups, often led to great difficulties due to the errors in encoding or transmission. A code expression HAM, for example, which during the decoding process seemed to have been erroneously encoded or transmitted, required the testing of not less than $3n$ different code expressions, if n was the number of letters or figures in the alphabet or cipher used; hence, 78 different expressions have to be tested for the French alphabet of 26 letters. This is on the assumption that only one letter was wrong. The successive testing of AAM, BAM, . . . ZAM; HAM, HEM . . . HZM, HAA, HAB, . . . HAZ, easily may lead to, and has led to, very unfortunate errors in the interpretation, especially of numbers and hours.

During the period in the development of cryptography here under consideration, different codes were generally used by both sides for the different armies. This plan was adopted with a

[141] Radioinstruktion för Armen, p. 48.d.

[142] Lange et Soudart, Traité de Cryptographie, p. 206. [Note: The pronounceability requirement for code words transmitted over international telegraph circuits was modified by the International Telegraph Conference of Brussels, 1928, and was completely eliminated by the International Telegraph Conference of Madrid, 1932. The principal, self-imposed requirement that now remains is that code words of the same code should show a minimum 2-letter difference.—*W. F. F.*]

view to decreasing the risks involved should the enemy succeed in solving any one code, and also with a view to restricting the great volume of material available when one and the same code was used. The successful solution of a code depends to a great extent upon the volume of the material available for study.

The use of different codes, however, involved an important danger, one which, as a rule, is entirely overlooked by persons who are not specialists in the use of codes, namely, that involved in sending cryptograms containing the same orders to different units in different codes. The resulting possible comparison of such material is of invaluable help in cryptanalysis, especially if one of the codes has already been solved, and extremely valuable results were obtained by the identification of such messages.[143] Once again we must emphasize the fact that the manner of using a code determines its real safety.

The same statements applied during the whole World War to the ineradicable habit of code clerks of using the same stereotyped idioms and phrases. "Only with the greatest difficulty", writes General Givierge, "was it possible to make the originator of telegrams realize the danger involved in the use of such expressions and it was difficult to make them desist from making involved references to date and number." [144]

Hence, one of the very important problems connected with safety was that of eliminating, or at least of masking, such stereotyped forms. Several means were used for accomplishing this.

The first consisted of giving instruction to code and cipher clerks, or better still, to the persons who drew up the telegrams, in the manner of using codes and cipher with strict adherence to regulations, and the establishment of certain courses with a view to giving to the persons concerned as good instruction in the avoidance of the most important errors and the underlying reasons therefor as possible. It must be emphasized that they were not effective unless the students were given a clear picture of the manner in which codes are solved on the basis of their own errors.

Another method consisted of setting up in the code text lists of individual expressions for longer typical sentence or phrase structures which occurred very frequently. Instead of dividing a sentence such as "a barrage will be laid tomorrow at 7:30 a.m.", for example, into three groups, such as "a barrage will be laid", "tomorrow", and "at 7:30 a.m.", they are combined into one code group by means of the so-called "coordinate system", for example, as follows:

	7:00	7:30	8:00	8:30
A barrage will be laid today	BABAC	SEBUL	NIRAL	TOJEK etc.
A barrage will be laid tomorrow	XYLOF	VIDAR	POKOK	SATIR
A bombardment will be executed today	VEDIM	MALIS	PUTAV	WOKIS
A bombardment will be executed tomorrow	LAJOK	XIMAD	LOLOB	VICIC
A gas bombardment will be executed today	NYGOG	MOJYT	MOHAF	SALEM

If properly composed, such composite expressions may be of very great value because of the fact that they prevent too high frequencies of repeated expressions, such as, for example, the time of day or "today." On the other hand, they may burden the code with a great number of new expressions and they require that the code clerks have full knowledge of and make proper use of the different expressions to the greatest possible extent.

A third expedient consisted in neutralizing the too frequent text expressions by assigning to such expressions a number of different code groups based upon carefully compiled statistics. These could be used alternately at the discretion of the code clerks.

The fourth expedient consisted of superencipherment, which we shall discuss again later on.

[143] Givierge, Cours de Cryptographie, p. 264.

[144] Givierge, Questions de chiffre, p. 61.

Of the various methods mentioned above, there were in use at the close of the World War only the instruction of code clerks and superencipherment. The other two had in practice not given the desired results, due to repeated errors and violations of the instructions. Numerous points of attack, however, remained. For instance, place names formed the most profitable objects of attack when they, as often was the case, were not represented in the code by one code group. Such names were repeated very often in the radiograms from several stations and were, as a rule, encoded differently by each code clerk by the use of code groups for individual letters and syllables. Thus, for example, one might divide the name "Armentieres" letter by letter, another might divide it into Ar-men-ti-e-re-s, a third into Ar-men-t-ie-res, etc., and from such an encipherment the cryptanalyst could very easily become accustomed to recognizing the more or less similar groupings and to obtaining from them, by comparative analysis, the code groups for the letters and syllables. It was quite important in the solution of a code to be able to reconstruct all names of persons and places occurring in a radiogram.

Superencipherment of codes was introduced in France as early as 1915, for the special code used by the higher staffs, which, as we have already stated, had been in use since the outbreak of the war.[145] Later on the use of superencipherment was extended to all troop codes, but as is pointed out by General Givierge, it, however, often happened that these later regulations were not obeyed. The regulations for superencipherment were printed on separate loose sheets of paper, so that they could be changed easily, independently of the codes.

In the German Army, on the contrary, superencipherment was introduced much later, and then merely for communication between larger units,[145] and therein lies, without doubt, the reason for the fact that so many German troop codes were solved by the enemy during the World War.

The same general rule applies to superencipherment and to complications in a cipher system. If compiled by personnel ignorant of the science of cryptanalysis and not sufficiently experienced in cryptography, the superencipherment may be entirely worthless and may facilitate the solution of the cipher, for the cryptographers as a rule believe that they are fully protected by superencipherment and therefore neglect all elementary precautionary measures in drawing up the messages. Its value therefore is entirely dependent upon the technical knowledge of its compilers. Even superenciphered codes have been solved in many cases. This was accomplished, among other cases, in the case of the German submarine code, which is a good example of the manner of superencipherment which should not be recommended.

This code, like so many others, was a three-letter code, and it also was solved. In one case it was discovered from certain changes in the appearance of the cryptogram that a new system was in use, consisting either of a new code or of a superencipherment of the old one. Analysis of the frequency factors particularly revealed the fact that the structure of the radiogram had been left unchanged. After sufficient material for statistical analysis had been collected, the highest frequencies in the older and the new codes were compared, and it was found that all groups which could be identified as being similar with the same frequencies and places in the respective codes were entirely unlike in appearance—that is to say, that all three letters were unlike in the new code when compared with corresponding expressions in the old. This indicated that superencipherment had been used, for in the case of change of code at least some of the letters must have remained alike in similar places in the expressions in the different code equivalents of the same text groups.

A comparison of the groups having the highest frequency in each of the radiograms directly confirmed this hypothesis. If, for example, the groups occurring with the highest frequency in the former code were KAB, and in the new series MPA, there was obtained, by testing the relations, M=K and P=A and A=B in other groups, a number of groups from the former series

[145] Givierge, Questions de chiffre, p. 66.

which were immediately recognizable. From other groups in which only two of the new letters were found, the third was easily discovered, and gradually all the relations were identified. In this way codes, or, more correctly speaking, superencipherments, were solved.[146]

Superenciphered German military codes of the Satzbuch type were solved according to similar principles.[147] This was facilitated, however, by the fact that the German Army's regulations were even worse than those used by the German fleet, because in several cases merely one of the letters in the code group was changed, and thus unchanged letters, easily discovered through statistical studies, formed good guides for successive tests.

In both cases we marvel at the grave ignorance on the part of the compilers of the superencipherment. It once more illustrates the dangers connected with permitting personnel ignorant of the science of cryptanalysis to be responsible for military or naval cryptography.[148] Another type of superencipherment, consisting of adding a certain number to the cipher groups or subtracting it from them, group for group, also proved to be treacherous. It justified the opinion of the renowned expert Hooker (in speaking of the German submarine codes):

> Changes of key were carelessly made and the whole system formed an interesting commentary on that German "thoroughness" of which we hear so much. In one official document, issued later during the World War, the Germans warned against the careless application of codes and ciphers and highly praised the efficiency of the British cryptanalytic bureau. However, it was the Germans themselves who gave the British such excellent chances.[149]

That the Germans in time, however, became clearly conscious of their own errors and blunders is without any doubt true. However, it was at a far too late stage of the World War that this occurred. This is to be inferred not only from the information given by the Germans, but to a still more marked degree from the explicit and well-planned measures against code solution which were adopted by the Germans during the very last stages of the World War. In contrast to practically all previous measures, they were well planned and were well suited for the purpose in the best sense. Provided the knowledge of the cryptographers was adequate, they ought to have been adequate to assure that the German codes and ciphers would be secure.

For instance, there were introduced into the codes last used during the war frequency-equalizing auxiliary expressions for the time of day, figures, numbers, and syllables;[150] hence, for all the expressions which are chiefly used as points of attack by cryptanalysts and which most quickly serve that purpose. Nulls were also used. These greatly puzzled the experts.

At the same time conventional names (Decknamen) were extensively used. These were changed frequently, sometimes many times the same day.[151] We wish to call attention here to the fact that the use of unencoded conventional names in code text is as inadvisable a procedure as the use of such names in connection with clear text, and is absolutely to be condemned. The coded conventional names in the code text eliminate the possibility of the very ordinary

---

[146] Givierge, Questions de chiffre, p. 67.

[147] Givierge, loc. cit., p. 68. [Note: The German "Satzbuch" (literally, "Sentence book") was *not* used with superencipherment, except in very rare instances. Mr. Gyldén has again been led astray by an error in the source to which he refers. General Givierge meant to refer to the German "Schlüsselheft" (literally, "Key book") as the one which was superenciphered by means of a cipher key called the "Geheimklappe" (literally, "secret flyleaf"), but what he actually mentioned was the "Satzbuch."—*W. F. F.*]

[148] [In this connection I think it advisable to point out that the "Satzbuch" was a two-part code of approximately 4,000 groups; it was distributed only down to and including regiments, and was changed approximately every 18-20 days. It required no superencipherment. The "Schlüsselheft" introduced into service in March 1918, was a one-part code of only 1,000 groups; it was distributed to front-line units, was the only authorized method of secret communication within the danger zone, and was always employed with superencipherment by means of a small enciphering table ("Geheimklappe") which was changed by each division at frequent intervals (toward the close of the war *daily*). It is true that the Allies solved most of the messages in the "Schlüsselheft" as well as a great many in the "Satzbuch", but this was not done as quickly and as easily as one might infer from this discussion by Mr. Gyldén. Messages in the "Satzbuch" were often solved much too late to be of any value. Considering their handicaps, the German code and cipher compilers performed their work in a fairly efficient manner; it was the blunders and errors on the part of the personnel using the codes and ciphers which rendered the work of the compilers less effective than it might have been. In the next paragraph it will be noted that Mr. Gyldén admits that the Germans improved quite markedly in regard to their secret communication toward the end of the war. But, as Mr. Gyldén points out, the improvement came too late to do much good.—*W. F. F.*]

[149] Hooker, The Deciphering of Cryptograms, The Police Journal, No. 4, London, 1928, p. 623.

[150] Givierge, Questions de chiffre, p. 68.

[151] Givierge, Questions de chiffre, p. 68.

and fruitful comparison between place names of the type of Armentieres, which occur very frequently and prove treacherous to a high degree.

The number of German radiograms intercepted by the French varied with war conditions. During periods of calm the messages were mostly of local importance and were comparatively carefully enciphered. On the other hand, such periods were always characterized by a stereotyped form of telegraphing, and as a rule only a few days were necessary for recognizing the habits of the cryptographers concerned. Despite quick and numerous changes of call signals, even the telegraph operators of the various stations were identified by their individual peculiarities in operating, a circumstance which is well known by every experienced intercepting operator. During periods of great activity, on the contrary, for instance, during the great spring and summer offensives of 1918, numerous larger units and staff radio stations added to the traffic, and it frequently occurred that about 60 radiograms concerning the operations of the larger units were intercepted during one and the same 24 hours, not including the innumerable telegrams from smaller units.[152] It was during such periods that the most ordinary errors and blunders were made and that the regulations were disregarded.

Now if we try to sum up the work of the German cryptographers on the Western Front, we find that it was on the whole characterized by a purely empirical development. A uniform cryptographic doctrine, based upon purely theoretical bases, was always lacking. It does not exist even yet, to judge by the work which up to the time of writing has been published since the war by the foremost representatives of the German cryptographic school. But, on the other hand, the Germans have displayed an indisputable cleverness in gradually devising and prescribing protective and preventive measures as soon as they became aware in some way of their own mistakes. This procedure is, however, very uncertain from the general standpoint, for the measures taken most frequently involve other entirely unsuspected weaknesses and points of attack. We can most properly compare such a method with the plugging of successively appearing holes using one and the same plug, during which process older holes again come to light. The various systems used since August 1914, and the innumerable regulations and measures taken, produce a kaleidoscopic picture of a cryptographic experimentation without any cohesion. Not until the last few months of the war can we see in the system the beginnings of a simplified and rational opinion concerning the correlation of the different parts of the cryptographic problem. Compare with these constant changes the uniform doctrine of the French cryptographic service, which made it possible to use one and the same cipher system for 3½ years without its being solved by the enemy, and a few different types of codes and ciphers. The exceedingly important advantage which is gained by having definite and uniform principles on which to base the handling of the systems by the great mass of officers who are ignorant of cryptography can never be sufficiently stressed. A complication or improvement, real or apparent, is easily ordered but is unendingly difficult to apply in practice by such a large personnel which thinks it has all reason to call down curses and maledictions upon the inventions of the cryptanalyst.

In the same way the work of the German cryptanalysts was at first empirical. The experts in this line had to train themselves, with the assistance of successive experiences, and this explains the great unevenness in the development, as well as the fact that while on the Eastern Front in a very early stage of the World War there were very good forces available, mostly thanks to good fortune, on the Western Front much later evidence of German blunders in the use of codes and ciphers was to be found. Similar blunders on the part of the Russians formed the most worthwhile objects of attack for the German cryptanalysts on the Eastern Front.

[152] Givierge, Questions de chiffre, p. 60.

Not until the very last part of the war did the cryptanalytic service become someward efficient. The central cryptanalytic bureau was moved to Spa [153] and there several of the French troop codes were successfully solved, according to the account of General Givierge.[154] These examples of code solutions happened to a high degree to have been assisted by the capture of copies of French codes, but various now well-known German instructions and regulations, however, give plain evidence of an improved conception, at least, of important aspects of the technic of code solution. The same may be inferred from the German regulations issued at the end of the war governing the compilation and employment of their own codes.

The technic of cryptanalysis attained an almost incredible perfection during the last years of the war. To treat this subject adequately we would have to write a thick volume. It was developed into a regular science, based upon extensive statistical analysis, grammatical investigations, and probability calculations. In the countries which were behind in the development of cryptography there was attributed to codes a high degree of safety merely on account of their existence. No idea can be more inaccurate. For of no other form of cryptography is it more true than of codes that their value is dependent upon the knowledge of cryptanalysis on the part of their compilers and to a still higher degree upon the manner in which they are employed.

The cryptanalysis of codes is not anything new, despite the prevailing general misconception on that subject. As early as the period from 1588 to 1594, the renowned mathematician Viète solved a Spanish code, with all its successive variations.[155] This code was not greatly inferior to those which are still used in many places for military and diplomatic purposes in the countries where nothing is known about cryptanalysis. The Englishman Wallis was also very clever in the artof cryptanalysis and his biographer Davys in the year 1737 published a discussion of cryptanalysis which contains an account of the technic of the analysis of codes.[156] Later on, the French military authors Bazeries and Valerio published in detail reports concerning successful code solutions, and several other authors intimated how such solutions were made.[157]

Many also were the codes solved during the World War. We know that several Italian and Russian codes were solved by the Austrians [158] and several French troop codes were solved by the Germans, as has already been mentioned.

The French solved more than 30 German, purely military, codes,[159] as we have already stated, besides a great number of diplomatic codes.[160] We also know that many of the German submarine codes [161] and the codes used by Zeppelins were solved,[162] and we know that the French and British solved the Zimmerman Code.[163] Other cases, such as that of the solution of the Baravelli code before the war, and the solution of the Swedish and other codes by the Russians, have been mentioned several times during the course of this work. It is therefore not without good reason that a review of current opinion concerning the safety of codes has had to be given. It may be added, with regard to some of the sources cited, that Gen. Max Ronge during the World War was the last chief of the "Nachrichtenabteilung des Österr. ung. Armeeoberkommandos und des Evidenzbureaus des Generalstabes", that General Givierge was chief of the cryptographic and cryptanalytic bureau of French General Headquarters, and that Sir

[153] Ronge, Kriegs und Industrie-Spionage, p. 316.
[154] Givierge, loc. at., p. 59.
[155] Bazeries, Les chiffres secrets dévoilés, p. 40.
[156] Davys, An Essay on the Art of Deciphering, London, 1737.
[157] Bazeries, Les chiffres secrets dévoilés, Paris, 1893. Bazeries et Burgaud, Le Masque de Fer, Paris, 1893. Valerio, De la Cryptographie, Paris, 1895, part II.
[158] Ronge, Kriegs und Industrie-Spionage, pp. 238, 298, 318, etc.
[159] Givierge, Questions de chiffre, p. 417.
[160] Cartier, Le service d'écoute pendant la guerre, p. 495. Givierge, Questions de chiffre, p. 61.
[161] Sir Alfred Ewing, War Work at the Admiralty, Times, Dec. 14, 1927. Givierge, Questions de chiffre, pp. 61 and 67.
[162] Cartier, Le service d'écoute pendant la guerre, pp. 459 and 491. Sir Alfred Ewing, War Work at the Admiralty, see above.
[163] Sir Alfred Ewing, War Work at the Admiralty, see above. Cartier, Le Service d'écoute pendant la guerre, p. 495.

Alfred Ewing was chief of the cryptanalytic bureau of the British Admiralty during the first half of the World War.

Aside from the "direct" material used for solving codes, that is to say, the material derived from the telegrams themselves, sometimes all the indirect material available was utilized for the cryptanalysis. The latter type of material is exceedingly rich and varied in nature, and we can without exaggeration assert that a great majority of the people who did cryptanalysis during the World War were experienced merely in comparing intercepted enemy radiograms or telegrams with material for indirect comparison. The number of real cryptanalytic experts, capable of doing direct cryptanalysis, was very limited. Their work was all the more important because by far the most important code and cipher solutions were performed chiefly on the basis of direct material. It may be deduced from the above that it is very difficult to obtain a correct estimate of any piece of cryptanalysis unless we have access to the material which was available at the time it was performed. For the same reason it may be deduced that much of the code and cipher solution work boasted of was nothing more than a mere reading of the code on the basis of captured code or cipher instructions or tables. However, it is evident that marvelously clever solutions were accomplished on the basis of very restricted direct material. Never in the history of cryptography have experts been afforded a better opportunity to develop the technic of cryptanalysis than during the late World War, and we can with good reason maintain that the stage of development existing in the majority of places before 1914, and not yet surpassed in many places, is to be considered as greatly antiquated and primitive as compared with the latest advances of the technic of cryptanalysis.

B. The Eastern Front

1. THE PERIOD OF 1914

Of the three great powers which fought on the Eastern Front at the outbreak of the World War, only one, Austria-Hungary, possessed an organized military cryptanalytic bureau before the declaration of war.

We have already discussed the general state of the cryptographic service in Germany before 1914. Just as on the Western Front, so on the Eastern Front, no provisions whatever had been made for cryptanalytic work, much less had any preparations been made for it.[164] The cipher systems compiled by the General Staff were used in practically the same way both on the Eastern and on the Western Fronts, but change of keys was made at different times, depending upon the general situation at the respective fronts.[165] The systems used by the enemies apparently were not known, or if such was the case, they certainly were not the subject of cryptanalytic studies.

The conditions existing in Russia before the World War have also been discussed above. The personnel provided for handling the radio messages apparently had no preparation whatever in cryptography under field conditions, and cryptanalysis apparently entirely escaped the attention of the Russian General Staff. We have reason to be surprised at this in view of the fact that we know of the high degree of technical skill which had been attained even long before the war by the Russian cryptanalysts in the Ministry of Foreign Affairs. Apparently this state of affairs is to be attributed to the isolation which had become a policy governing the work of the general staffs in the majority of countries. The lack of contact with civilian authorities and individuals in this respect, as well as in many other fields, proved to be disastrous.

Austria-Hungary on the contrary, seems to have been comparatively well prepared for extensive cryptographic work, as we have already intimated in the foregoing. The credit for

[164] Carlswärd, Operationerna på tyska ostfronten 1914, p. 74.
[165] Ibid., p. 121.

this is to be given to Gen. Max Ronge, according to his own statement. During the World War he was chief of the "Intelligence Department"[166] of the Austrian Army. There apparently is nothing to contradict his statement. One of the important missions of the Austrian espionage system, even long before the World War, was the stealing or purchasing of Russian cipher keys[167] and very good studies must have been made beforehand of the Russian systems. It must, however, justly be emphasized that cryptanalysis, at least before the war, merely consisted in solving comparatively simple cryptographic problems, because of the markedly primitive nature of the Russian cipher system. The most important fact, however, is that Austria-Hungary was considerably better equipped than its opponents or confederates for undertaking cryptographic work in the field. The results attained due to this circumstance were of decisive importance, which we shall attempt to prove in the following.

The earliest report of cryptographic activity on the Eastern Front which the author has been able to find dates from August 16, 1914. That day a Russian radiogram, in clear text, was brought to the German Command upon the Eastern Front. This radiogram reported the removal of Russian wounded belonging to the Thirtieth Infantry Division to Wilkowischki.[168] A clear-text telegram of this kind apparently has nothing to do with cryptography, but the circumstances connected herewith require some comments.

For this telegram was the first radio message of Russian origin which the extensive and detailed work on the World War, Der Weltkrieg, 1914–18, published from the official records in the German archives, reported as having been intercepted on the Eastern Front.

It is certain that Russian radiograms in clear text had been sent before that date. The very faulty communication between the Russian Niemen and Narev Armies, as well as between the various parts of the Russian Army as a whole, are far too well known to be discussed any further here. Details about this are to be found in the Ny Militär Tidskrift for 1930, and Capt. T. Carlswärd also devotes an extensive study to the quesion.[169] It is more than probable that, not many days after mobilization operations were started, at least the Russian units which were nearest the frontier were forced to consider radio in order to try to get into communication with other units and staffs.

The fact that the radiogram was drawn up in clear text was also very illuminating. As we shall point out in the following, many of the radiograms sent by the Russians during the period just following this were sent in clear text, which circumstance was directly due to the poor quality of the cryptographic systems. The cipher systems introduced by the Russians at the outbreak of the war were very badly designed, and, like the German systems used on the Western Front in the year 1914, were far too complicated and too slow to use. The personnel of the radio stations, which was obviously unprepared to perform its duties, was unable to encipher the messages correctly, and still less able to decipher the radiograms received. The Russian system was composed of a so-called "Sprungchiffer", which consisted in enciphering letter for letter by means of uniquely corresponding 2-figure groups,[170] and a periodic change to other corresponding alphabets.[171] Colonel Figl writes about them: "The messages were often wrongly enciphered, for which reason after a short time this system was abandoned, even before the end of 1914. Reports from the commanding officers in charge of the Russian radio stations designated the

[166] Ronge, Kriegs- und Industrie-Spionage, p. 53.

[167] Ibid., p., 22.

[168] Reichsarchiv, Der Weltkrieg, 1914–18, vol. II, p. 62.

[169] Carlswärd, Operationerna på tyska ostfronten 1914.

[170] Later increased to include 3-figure groups or groups of greater length.

[171] Figl, Systeme des Chiffrierens, p. 84 and appendix 19. [NOTE. The very important role played in the military situation on the Eastern Front as a result of the solution of the Russian cipher system, as will become apparent from Mr. Gyldén's remarks on the subject, warrants a discussion of the nature of this cipher system. A brief description of the method, followed by the discussion, will be found at the end of this translation.—*W. F. F.*]

system as far too difficult to employ; the *simple Caesar cipher*, which had been used up to that time in all its forms (*during the World War!*), obviously was preferred by them.[172]

About this same system General Ronge writes as follows: "It disappeared quickly, for it was far too complicated and they (the Russians) returned to the letter-substitution ciphers, the so-called 'Caesar ciphers', which were the very simplest type to solve by the enemy." [173] We must add to both the above citations that the "Sprungchiffer", as a matter of fact, was recommended at the beginning of the war, but due to failure in organization in many cases never reached the front. The Russian radio operators most frequently were left to use their own initiative, and the majority of them telegraphed in clear text; others again used an exceedingly primitive substitution cipher, which was utilizable in time of peace and is erroneously called the "Caesar cipher" both by Figl and Ronge. The failure in organization went further than merely to cover the lack of cipher instructions. Der Weltkrieg, the German official history of the World War, which we have mentioned above, mentions the fact that the Russian Thirteenth Army Corps sent radiograms in clear text during the Battle of Tannenberg because it went into the field without receiving the proper cipher keys.[174]

In conclusion, it must be stated that the interception of messages by the Germans, at least in the beginning, was based more upon good luck than upon any really organized intercepting service. It is probable, because of the importance attributed before the war to interference in radio, that the German radio operators devoted themselves at first more to that sport than to any careful interception of radiograms which were unintelligible anyway. No Russian interpreters were apparently assigned to the intercepting service until a relatively late date. The opinion expressed by German cryptanalysts after the war that excessively important material was unfortunately lost because of the neglect to intercept it seems to have been fully justified.

During the days immediately following the interception of the telegram mentioned above, other Russian telegrams of extreme importance were intercepted, always in clear text. Such great importance came to be attached to them that, because some of the information contained in them was confirmed by reports brought in by German aviators and spies, they greatly contributed in inducing General von Prittwitz to decide to withdraw behind the Vistula. It is a very well-known fact that von Prittwitz's decision resulted in his removal from his command in favor of von Hindenburg. The Russian radiograms contained important details about their grouping which informed the German command that the First, Sixth, Thirteenth, Fifteenth, and Twenty-third Army Corps, together with the Fifteenth Cavalry Division, belonged to the Narev Army.[175]

Then gradually Russian telegrams in clear text followed, which gave the new commander of the Eighth German Army, von Hindenburg, exceedingly valuable information about the grouping of the Russian armies. Thus, for example, it was established on August 23, hence, simultaneously with the beginning of the German regrouping before the Battle of Tannenberg, that the Second Russian Army Corps was marching toward Lötzen [176] on the lakes, although it was not yet known whether the said unit intended to advance toward the north.

Another telegram also indicated General Rennenkampf's intention of crossing the Angerapp River with the Fourth Russian Army Corps, and advancing west of it,[177] at a time when the Eighth German Army's eastern group was retreating.

After the battles at Lahna and Orlau on August 23, about which Russian radiograms once more gave valuable information,[178] the carelessness of the Russians attracted still greater attention during the advance to the Battle of Tannenberg. With the crossing of the German frontier

[172] Figl, Systeme des Chiffrierens, p. 85. (Italic by Figl.)
[173] Ronge, Kriegs- und Industrie-Spionage, p. 54.
[174] Reichsarchiv, Der Weltkrieg, 1914–18, vol. II, p. 351.
[175] Ibid., p. 97.
[176] Ibid., p. 116.
[177] Ibid., p. 117.
[178] Reichsarchiv, Der Weltkrieg, 1914–18, vol. II, p. 128.

southeast of Deutsch Eylau-Allenstein still greater demands were placed upon the Russian radio stations, for other means of communication were very faulty and uncertain. At the same time the German command must certainly have realized the importance of a permanent interception of the Russian radiograms, for the messages formerly intercepted apparently proved to be both correct and very valuable. Furthermore, German scouting activities, at least with the eastern groups, were made much more difficult because of the combats and hardships undergone by the small force of cavalry.

The report published by the Germans of the operations immediately preceding the Battle of Tannenberg (Der Weltkrieg, 1914–18, vol. II, pp. 111–135) does not happen to mention all the Russian radiograms read by the Germans. We can ask, among other things, whether the very bold measures taken on August 24 in ordering the First Reserve Corps and the Seventeenth Army Corps south, with the Russian Niemen Army threatening its rear, were not to a greater extent than stated in the report based on statements in intercepted Russian radiograms, not published until now. We must, in this connection, remember that the Russians had telegraphed in clear text even earlier and that the information contained in the telegrams proved to be correct. That carelessness on the part of the Russians and the ignorance prevalent among the Russian radio units, both of the technic of radio transmission and cryptography, were not chance circumstances, but were general throughout the service, is to be deduced very clearly from the account of General Ronge, of the Austrian Army, with regard to conditions prevailing beginning the middle of the month of August 1914: "An effective unsurpassed source of information was, however, opened to us by the Russian radio messages, which were transmitted with a carelessness similar to that of which the Germans were guilty when opposite the French troops at the beginning of the war",[179] and "The Russians acted just as if we were not in possession of similar devices and were not able to tune them to their wave lengths. We used our radio stations much more sparingly and more carefully in transmitting orders, but, on the contrary, we used them very extensively for intercepting purposes." [180]

It is not improbable that the legendary aura which surrounds the modern Cannae is only unwillingly removed by German historians, both military and civil, by publishing details which may in any way tend to detract from the high opinion prevailing concerning the originality of the ingenious plans made by the active German High Command. To act otherwise would not be human, and the history of other countries shows similar limitations. Furthermore, it must be borne in mind that a large part of the material which might serve as a basis for comparison, especially the Russian documents of that time, fell into the hands of the Germans.

The clear-text telegram mentioned above, which was reported as having been intercepted early on the morning of August 25, is a good example to demonstrate the unprecedented responsibility placed upon the Russian cryptographic service. Two Russian radiograms, each one containing a comparatively complete army order, one from General Rennenkampf, the other from General Samsonov, gave the groupings, direction of march, and objectives of the Niemen and Narev Armies, respectively.[181] Concerning the importance of these radiograms, the official German history, Der Weltkrieg, states: "In this way the German High Command learned the immediate objectives and aims of both enemy armies during the hours in which the decisions and orders for the battle (Battle of Tannenberg) were reached." [182] Aside from this information, the importance of which is readily understood, it was also learned from the radiograms that both Russian armies were not planning to attack the Germans on August 25 but on August 26.

It never had happened before in the history of the science of cryptography that so exceedingly important and complete information about the measures and grouping of the armies

[179] Ronge, Kriegs- und Industrie-Spionage, p. 113.
[180] Ibid., p. 113.
[181] Carlswärd, Operationerna på tyska ostfronten 1914, pp. 36 and 37.
[182] Reichsarchiv, Der Weltkrieg, 1914–18, vol. II, p. 137.

command; at least we infer that to be true from the German official history of the war so frequently quoted here. Just as happened on the Western Front in the case of German radiograms in mixed text, the Russian mixed text radiograms permitted the Austrians gradually to identify parts of the cipher tables, and therefore the change to texts entirely in cipher did not offer any difficulties worthy of mention to the Austrian experts. They had taken very good advantage of the blunders of the Russians.

The Germans first succeeded in solving a cipher at the permanent radio station of the Fortress of Königsberg at the end of September 1914. This was not accomplished as the result of any organized activity, but was rather due to mere chance. Professor Deubner, the philologist, had voluntarily enlisted as a member of the Landsturm, claiming to be well versed in Russian. At first his work consisted of translating intercepted Russian radiograms in clear text. When the Russian messages gradually took on the form of cipher, Professor Deubner, on his own initiative, began to try to analyze and solve them, although he had never studied cryptography. Nevertheless, the fact must be stressed that training in philology is an excellent preparation for cryptanalysis, for the methods of investigation in both sciences often follow along the same line of reasoning, and the same analytic technic is, on the whole, used in both. However, it probably took Deubner some time to complete the working out of a suitable technic of cryptanalysis for use on the Russian cipher system, despite the simple nature of that system. Despite the best qualifications, a self-taught man cannot in one instant teach himself the science of cryptanalysis. This explains why Deubner, and consequently also the German command, lost valuable time while the Austrians were reading the Russian cipher radiograms with great ease.

Nevertheless, the place taken by Professor Deubner in the course of events was of the very greatest importance later on, and he no doubt more than deserved the following honorable mention in the official history of the World War written in Germany:

> We were extraordinarily well informed concerning the actions of the Russians. The Russians, to be sure, sent only cipher radiograms after the Batte of Tannenberg; [197] nevertheless, the archeologist (?) Professor Deubner on the Eastern Front, and the Austro-Hungarian General Staff, thanks to persistent work, had succeeded in finding the keys for the Russian cipher system. Because of this fact the Russian radiograms, if they could be intercepted, no longer remained a secret to the German and Austrian commands. Only when the Russians changed keys was there an interlude, usually brief, until the new keys were again successfully solved.[198]

Professor Deubner's work was highly valued by the German command on the Eastern Front. The professor was called to the headquarters of the Eighth Army at the end of September, where he was in direct contact with Generals von Hindenburg and von Ludendorff. He was placed in charge of a number of interpreters, to whom was assigned the task of cryptanalyzing, each in his place, the radiograms which were intercepted at the permanent radio stations at Königsberg, Thorn, Posen, and Breslau. [199] This work they were to do upon the basis of their experience in this line. According to information given by General Dupont in the Révue Militaire Française—obtained, it is claimed, from one of the staff officers at German General Headquarters on the Eastern Front, whom the general met in Berlin in 1919—it is claimed that General von Ludendorff waited every evening for the latest results from the cryptanalytic bureau before drawing up his orders for the morrow.[200]

The first solution of Russian ciphers mentioned in the German official history of the World War was that of a report about their own grouping and about the supposed grouping of the Germans, sent by the Russian General Novikov on the 25th of September.[201] The said analysis was not accomplished by Professor Deubner, as might be supposed from the text in the official

[197] Due to his ignorance of cryptography, the author obviously considered "mixed" text as cipher.
[198] Reichsarchiv, Der Weltkrieg, 1914-18, vol. V, p. 422.
[199] Carlswärd, Operationerna på tyska ostfronten 1914, chap. IV.
[200] Dupont, Le haut commandement allemand en 1914, in Révue Mil. Française of July 1, 1921.
[201] Reichsarchiv, Der Weltkrieg, 1914-18, vol. V, p. 423.

history—although no direct statement is made to that effect—but was performed by the Austrian cryptanalytic expert, Captain Pokorny, mentioned above, who required from 6 to 7 hours to decrypt the telegram.[202] Obviously, cooperation with the Germans had been established by this time.

A new, very important cryptanalysis was successfully accomplished, also by the Austrians, on September 27, the message being an order to retreat, and as this retreat was actually carried out, the correctness of the analysis was thereby confirmed.

It would take far too much space to report in detail the numerous cases of successful cryptanalysis, which were frequently of the utmost importance for the command of the Central Powers and which were accomplished during the following campaign against Russia. The scope of this work was entirely unprecedented and never in the history of the world was there any comparable case, one in which an army command was so exceedingly well informed concerning the plans, orders, and reports of the enemy as was the command of the Central Powers during the Russian campaign. The last part of the present section contains information about the data available in the volumes so far published by the Reichsarchiv, and for that reason only a few of the most important events will be repeated here.

During the advance of the main body of the Austrian Army, which was begun October 4, the command was able day by day to follow the changes of position of the Russian Ninth, Fourth, and Fifth Armies from the San to the middle part of the Vistula, thanks to ciphers which had been successfully solved. As many as 30 radiograms were decrypted daily under the direction of Captain Pokorny, and he followed the offensive as closely as possible in order to obtain the best opportunities for interception.[203] It may be added here that it is of the very greatest importance from the purely cryptographic standpoint that a few cryptanalytic experts be sent to far-advanced staffs, for they thus more easily obtain access to material that is important from the viewpoint of comparison, such as that composed of the orders and reports issued by their own units. In addition to this, they thus get a great opportunity for directly comparing documents captured on the field of battle, statements of prisoners, etc., all of which information may be of very great importance. As we have already stated in our discussion of operations on the Western Front, for the benefit of both parties concerned there must be the most intimate liaison between the cryptanalytic experts and the staff personnel, and the experts in question must have especially good wire communications with the central cryptanalytic bureaus, both at General Headquarters and in the office of the Minister of War. In connection with this we wish to state that the above-mentioned cryptanalytic services stationed at the permanent radio stations on the German Eastern Front in time developed a particularly good system of communication between the stations, to the great advantage of the work of cryptanalysis.

The great importance of good and quick communication may be understood indirectly from the recital of the following event: A radiogram, sent by the commander of the Russian Tenth Cavalry Division at Sanok, Colonel Engalichev, and intercepted by the Austrians, was decrypted in a very short time. It betrayed the fact that a powerful Russian attack was to be started against the southeastern fort of the Fortress of Przemysl.[204] The commandant of the fortress was immediately notified by radio and we can readily comprehend what disastrous results the delay of a few hours might have had.

The radiograms sent by the Russians, announcing the measures which were to be taken in the First Guard Reserve Division for the purposes of preventing the attempt of the Germans to cross the Vistula to the west of Ivangorod, were also decrypted, this time by German experts.[205]

[202] Ronge, Kriegs- und Industrie-Spionage, pp. 117–118.
[203] Ronge, Kriegs- und Industrie-Spionage, p. 118.
[204] Ronge, Kriegs- und Industrie-Spionage, p. 118.
[205] Reichsarchiv, Der Weltkrieg, 1914–18, vol. V, p. 442.

The important effect of these successful cipher solutions upon the operations of the Germans may be seen, among other things, from the accounts of the attack on Warsaw. On October 8 General von Mackensen received a certain directive from German Army Headquarters, but, immediately after the said directive had been sent, there came from the cryptanalytic bureau a Russian radiogram which had been decrypted and which changed the estimate of the situation at that time held by the German command.[206]

In the middle of October the Russians themselves changed their cipher system. They had probably learned something about its great weaknesses. The new system was somewhat better, although it was far from being able to fulfill the qualifications to be demanded of a military-staff cipher. However, the Russians gained nothing by the change, for renewed instances of carelessness betrayed the whole system to the Austrian cryptanalytic bureau. The most significant of these blunders was made by a Russian station which repeated in the old cipher a radiogram which had previously been sent in the new cipher but had not been understood by the addressee, for the latter did not know of the change of cipher.[207] The very same blunder has already been discussed in our account of events on the Western Front, and once more gives proof of the so very important, but unfortunately far too unappreciated, principle that the manner of encipherment is much more important for safety than the type of the system itself, whether it is a code or cipher, or whether it is produced by mechanical or electrical apparatus. Only a person who is unversed in the modern technic of cryptanalysis can assume that the safety will be based upon the properties or characteristics of the system itself as such, or can base the safety upon calculations of the infinite number of different possible combinations or period lengths permitted by a system. However, fortunately for the cryptanalytic experts, the said opinion still generally prevails.

The retreat from Poland, in the end of October 1914, is expounded in the official German history through long discussions of strategy. However, there is a short passage which reads somewhat as follows:

> The manner in which the German high command obtained its estimate of the situation during the following days may be seen from an entry in the war diary of October 23: "According to reports issued by the corps and according to the numerous Russian radiograms intercepted, we can with approximate certainty assume that the Russian forces to the south of Warsaw are comparatively weak; but, on the contrary, that those at Ravka and Bsura are very strong." [208]

General Ronge, who, by virtue of his official post, was necessarily exceedingly well informed, is much more categorical in his statements concerning the real causes for the decision to retreat. After having mentioned the fact that Russian radiograms showed that there was a greatly superior Russian force close by, he writes: "This information led General von Hindenburg to decide to start the retreat toward Silesia with a view to gaining freedom of operation for a new offensive." [209]

Concerning the battles on the San during the Russian advance, General Ronge states that the Austrian command was able, day by day, to follow the Russian operations, thanks to the efficiency of its cryptanalytic service.[210]

The Austrian retreat in a southwesterly direction from about the Sandomierz-Kjelzy line,[211] during the first days of November 1914, very greatly worried the German high command on the Eastern Front. The advance of the Russians began to threaten the Silesian industrial district. The German Ninth Army, which adjoined the left wing of the Austrian Army, had everything to lose by a frontal battle; on the contrary, everything to gain if it could, with its main force, attack

[206] Reichsarchiv, Der Weltkrieg, 1914–18, vol. V, p. 442.
[207] Ronge, Kriegs- und Industrie-Spionage, p. 124.
[208] Reichsarchiv, Der Weltkrieg, 1914–18, vol. V, p. 485.
[209] Ronge, Kriegs- und Industrie-Spionage, p. 124.
[210] Ibid., p. 125.
[211] Map VI in Weltkrieg, 1914–18, vol. VI.

some vulnerable part of the Russian Front. The German Official History of the War states that General von Hindenburg, even as early as in the latter part of October, intended to attack the right flank of the advancing Russian Army with his main forces, after regrouping the Ninth Army in the vicinity of Gnesen-Thorn.[212] The operation was dangerous; for the Russians, in the event of a continued advance, could force their way into Silesia without meeting any great resistance or could smash the left wing of the Austrian Armies. However, further on in the text of the German history of the war there is the report of the solution by the Austrians of a radiogram from the Fourth Russian Army, from which it was learned that "the Russian Armies thus seemed to intend to stop their advance",[213] which seemed to a great degree to favor the bold German regrouping.

However, the account in the German Official History of the World War apparently departs somewhat from the chronological order. For instance, it first discusses the opinion prevailing among the members of the "High Command" of the Ninth Germany Army, after General von Ludendorff's return from Berlin *on October 31*, concerning the urgent necessity for the planned offensive.[214] Later on in the history the aforementioned instance of successful cryptanalysis is mentioned, however, as having been performed on a radiogram dated *October 30*.

No information is available about the date or the hour when the highly important telegram mentioned came to the knowledge of the German command. However, we must bear in mind that the telegram was enciphered according to tables which Captain Pokorny succeeded in reconstructing *in their entirety* even as early as in the middle of October, and that th time required for this type of cryptanalysis, which was from 6 to 7 hours in September, certa nly had been decreased by the end of October. Furthermore, the communications were much improved for the cryptanalytic services, as has already been stated, both in the German and Austrian Armies. The said radiogram must, therefore, certainly have been known before the estimate of the situation made clear the need for an offensive. This offensive was all the more advisable as it was known that the Russian Army, which formed the greatest danger on the right wing (before the regrouping), intended to remain passive for several days. It may be inferred from another passage in the German Official History of the World War that the German plans for the attack were still uncertain as late as *October 30*, when General von Ludendorff conferred with General von Falkenhayn in Berlin.[215]

The same reversal of the chronological order apparently occurs once again a little farther on. In the said history mention is made of a directive from General von Hindenburg to General von Mackensen sent *November 2*. This provided that, in the event that the said Russian advance should cease, German troops should be transported to the north.[216]

After a mention of the import of the said directive we find the following statement: "In the meantime it became evident that the Russians actually halted the forward march", which fact was learned through intercepted Russian radiograms, as well as in other ways. However, we find that one of the said radiograms, which had just mentioned that the Fourth Russian Army had intended to stop the advance until November 3, is dated *November 1*.

The order and the information to the effect that the "Russians had actually stopped the advance" apparently give the reader the idea that the events occurred in the following chronological order: (1) The high command clearly estimated the situation and drew up suitable, bold plans based on speculations as to the probable measures that would be taken by the enemy. (2) The intercepted radiograms of the enemy showed that the speculation as to the probable

[212] Reichsarchiv, Der Weltkrieg, 1914-18, vol. VI, p. 36.
[213] Carlswärd, Operationerna på tyska ostfronten 1914, p. 133.
[214] Reichsarchiv, op. cit., vol. VI, p. 41.
[215] Ibid., vol. VI, p. 36.
[216] Reichsarchiv, op. cit., vol. VI, p. 43.

measures that would be taken by the enemy was correct. (3) The plans were successfully carried out.

The above-mentioned sources concerning the order of these events seem to indicate that it must have been (2), (1), and (3), if we understand by (2) the information which had been obtained through intercepted radiograms.

It would be presumptuous to attempt here to explain all the factors which had an effect upon the decision reached. We can merely state that the example given shows identically the same tendency as has already been discussed in connection with the importance of intercepted radiograms to the decision in the Battle of Tannenberg, that is, to let the radiograms appear as being not determining, but merely confirmatory factors. The reports are, however, far too much alike to have been entirely correct, as far as the said details are concerned.

The foregoing discussion has been actuated by the desire on the part of the author to explain the real importance of the solutions of Russian telegrams successfully made by the Germans and Austrians, insofar as his knowledge and understanding have made this possible. Their importance can be seen later on in the account given in the German Official History of the World War, where the following statement is made concerning the same part of the operations:

> Seldom has a commander in open warfare had such definite information on which to base his decisions as the command of the Germany Army in the east had available November 3, 1914. The strength, composition, and momentary grouping of the enemy were discovered; only the time when the Russians intended to continue the advance was unknown, but it was possible, with considerable certainty, to assume that at least a few days would have to elapse until its resumption.[217]

If we extend the opinion also to apply to the days immediately preceding November 3 and if we add that one of the Russian radiograms intercepted November 3 betrayed an order from the Russian High Command to the Second and Fifth Armies (see map no. 6, Reichsarchiv, Der Weltkrieg, vol. VI) to remain in their position, a remarkable demonstration of the extraordinarily great importance of the cryptanalysis performed is here available.

Concerning the exceptionally favorable conditions under which the cryptanalytic work was performed during these and the following days (for, as is known, an important break occurred between the German and the Austrian commanders), Ronge makes the following statement:

"The Russian Fifth Army Command at Tomaszov requested General Oranovski at Siedlce, on the front itself, to send all communications by radio, for the wires were destroyed", and the conclusion following thereupon: "This made available for our use a still greater number of messages."[218] It should be noted that after it had opposed the German Ninth Army, the Fifth Russian Army formed the most serious danger to Austro-German operations, since the regrouping of the German troops had accidentally caused a break of considerable size in the front.

As a general opinion of the importance of the cryptanalytic work during the period concerned, aside from the chapter headed "Triumph of the intercepting service over the Russian steamroller", Ronge writes as follows:

> It was reassuring to our command that the radio-intercepting service played on the Russian grouping as on a piano, instantly was able to report the intent and purposes of the enemy's command, and so well helped in the determination of the enemy's forces that as early as the end of October [note the date] the diagram of the daily disposition of the Russian forces, even down to the divisions, could not have been much unlike the diagram which was found at Stavka or at the headquarters of the command on the southwestern front at Cholm. Consequently, we may be certain that a troop unit which disappeared from the front without any explanation as to what had become of it could be located within a short time in its new position.[219]

It would therefore, without doubt, be of very great interest for a more detailed knowledge of the operations of the said period if all the Russian radiograms which were intercepted and

[217] Reichsarchiv, Der Weltkrieg, 1914–18, vol. VI, p. 46.
[218] Ronge, Kriegs- und Industrie-Spionage, pp. 125 and 126.
[219] Ibid., p. 127.

solved by the German and the Austrian cryptanalytic bureaus were published, with information as to the time they were intercepted, solved, and sent, in translation, to the command concerned. The account in the German Official History of the World War states that, in addition to the radiograms mentioned, "radiograms of this kind intercepted daily"[220] were available, fully confirming the fact that the Russians were passive and that "good information concerning the situation was obtained through the intercepted radiograms." [221]

The preparations made by the Germans for the Battle of Kutno were also aided to a great degree by the successful solution of Russian cipher telegrams. Of special importance was one radiogram sent by the chief of staff of the Second Russian Army, General Chagin, the morning of November 13, and solved the afternoon of the same day.[222] There is no available information as to who solved it, but, according to General Ronge, the telegram in question was available, in solved form, both in the "Operations Division" of the Austrian Chief of Staff and at German General Headquarters at Posen.[223] The said telegram gave the very clearest possible picture of the Russian idea of the grouping of the German forces, of their own intentions and the consequently necessary grouping of their own forces, of the measures taken to provide protection on the flanks, etc. This permitted the German command to plan its operations as if in a war game. A study, in conjunction with map no. 9, accompanying volume VI of Der Weltkrieg, 1914–18, of the order which General von Mackensen issued November 13 to the troop units under him [224] gives the reader a better idea of the extent to which these telegrams were used as bases for the dispositions than any of the accounts can give him.

During the course of the battle more Russian radiograms were intercepted. In this way it was learned, among other things, on the afternoon of November 15, that the Russian troops at the Ner and Bsura Rivers were to be reinforced by the Twenty-third, Second Siberian, Fourth, and First Army Corps, and that the Sixth Corps was ordered to cross to the left bank of the Vistula at Plozk.[225] Numerous other radiograms contained information of less importance.[226]

At this time an improvement was made in the Russian cipher system. This is to say, the keys were changed every day. However, the Austrian experts had gained such an insight into the habits of the Russians—in which they had probably been aided by the constant blunders on the part of the Russian cryptographers—that the solution of the new keys kept pace with their appearance. The new keys could be solved every day.[227]

The battle around Lodz, from November 17 to November 19, once more demonstrated the importance of the many successful solutions.[228] A good example of the importance which was assigned by the German command to these solutions may be gained from the circumstance that General von Mackensen on November 19 delayed the transmission of the "army order" for November 20 until the arrival of information contained in some intercepted radiograms. The said information was received correctly both from Breslau and Posen,[229] and gave an exceedingly clear picture of the Russian estimate of the situation and the measures they were consequently planning to take.

Information about the great speed with which the cryptanalytic work was accomplished is given in the German Official History of the World War, in the account of the events of the subsequent days. For instance, there is discussed, among the instances of intercepted and solved Russian radiograms a knowledge of the contents of which reached headquarters of the Ninth

[220] Reichsarchiv, Der Weltkrieg, 1914–18, vol. VI, p. 58.
[221] Ibid., p. 63.
[222] Ibid., p. 71.
[223] Ronge, Kriegs- und Industrie-Spionage, p. 127.
[224] Reichsarchiv, Der Weltkrieg, 1914–18, vol. VI, p. 72.
[225] Ibid., p. 83.
[226] Ibid., pp. 84, 85, 88, 102.
[227] Ronge, Kriegs- und Industrie-Spionage, p. 127. [Note: See, in this connection, my note at the end of this translation.—*W. F. F.*]
[228] Reichsarchiv, op. cit., vol. VI, pp. 104, 107, 110, 114, 116, 122, 125, 126, 127.
[229] Ibid., pp. 126 and 127.

German Army during November 20, that of a telegram sent at 8:15 p.m. the same day by General Scheidemann, addressed to the Forty-third Russian Infantry Division.[230] Another radiogram, sent at 8 p.m., November 21, had already reached army headquarters at Hohensalza by 9:30 p.m.[231] Compared with a number of other facts from the same source,[232] these cases of quick solution show that the new keys of the Russians probably were not solved—as claimed above—but that the messages were read off day by day in a continuous correspondence. The Germans and Austrians must in this way have obtained the new keys at the same time as their rightful recipients. If such really was the case, we must point out the absolute futility of changing the key for a cipher that has already been solved. No matter how many changes of key may be made in that event, it matters nothing.[233] We must bear in mind the excellent rule applied by the French, never to change key by radio (or by any other means which involves danger of interception), a rule which the various armies on the different fronts broke frequently.

The continued fighting around Lodz, November 20 and 21, which is discussed in a special section of the German Official History of the World War, perhaps more than any other of the numerous operations of the war, gives proof of the important role which may be played during decisive periods by a well-organized cryptanalytic service. The Russian radio communications brought the German command a steady stream of exceedingly important information.[234] This information was of all the greater importance because the systems of communication of the Germans during the battle of Lodz were very faulty,[235] added to the fact that the German ciphers were very difficult and tedious to employ.[236] This latter fact we have already taken up in our discussion of conditions on the Western Front. To this was added the fact that the information which the army command at Hohensalza obtained from the subordinate German corps and group commanders' reports was far from being reliable, for these commanders assumed to a strikingly great degree that desires were reality. This excessive optimism was based on the almost limitless underestimation of the strength of the enemy and was to a certain extent justified by their own magnificent and boldly fought successes. A careful analysis of the information concerning this period contained in the German Official History of the World War shows that the grounds on which the decision of the German Army command was based were the remarkably matter-of-fact Russian orders and reports.

[230] Reichsarchiv, Der Weltkrieg, 1914–18, vol. VI, p. 140.

[231] Ibid., p. 152.

[232] Ibid., p. 156.

[233] [The author must have in mind the changing of a cipher key by sending the new key in a radiogram cryptographed by means of the old key. This is made clear by his subsequent sentence. However, in my opinion, Mr. Gyldén is not warranted in his assumption, based merely upon the *speed* with which certain of the intercepted messages were translated, that the daily change in key to the Russian cipher system must have been made by radio, using the old key. It is usual for a new key to go into effect in the early hours of the day (commonly at midnight), so that in the case of both radiograms cited above the cryptanalysts most probably had at least 12 hours in which to solve other traffic in the same key. Consequently, by the time these two radiograms were intercepted, there remained little analysis to be done in order to read them. [See my note at the end of this translation.] This point is, however, not so important as the one to which I deem it wise now to direct attention. In view of the masterly manner in which Mr. Gyldén has handled his subject, it is with some hesitancy that I approach the matter. But candor compels me to say that, in my opinion, he is entirely unwarranted in making his statement regarding "the absolute futility of changing the key for a cipher that has already been solved" and that "no matter how many changes of key may be made in that event, it matters nothing." I believe I am correct in stating that nobody has as yet devised a *practical* cipher system for *field* use which cannot *sooner or later*, be solved. The "sooner or later" in this case is not a matter of years or months; actual experience would indicate it to be a matter of only a *few days*. It takes a much longer time (say a month or two at the very least) to teach a widely scattered, numerous personnel how to use any cipher system, not to mention the time it would take to teach them how to use it *properly*. Therefore, it is impracticable, if not impossible, to change the basic cryptographic system every time a message or a set of messages has been solved by the enemy. From this it follows that cryptographic systems for field usage *must* be of such a nature that even with a complete knowledge of the general system, obtained as the result of actual solutions or otherwise, so long as the enemy lacks the specific key to messages in as yet *unsolved* keys, the latter will resist solution for a sufficient length of time to make the contents useless to him, except possibly for historical purposes. This fundamental principle is the generally accepted basis for the cryptographic systems of all properly indoctrinated military, naval, or diplomatic establishments. Mr. Gyldén has, I fear, been led astray on this point, because he has based his conclusions upon a system which, while conforming to the principle set forth herein, nevertheless affords a very low degree of cryptographic security.—*W. F. F.*]

[234] Reichsarchiv, Der Weltkrieg, 1914–18, vol. VI, pp. 129, 136, 139, 140, 149, 150, 152.

[235] Ibid., p. 124.

[236] Ibid., pp. 132 and 146.

The cryptanalytic work was rendered more difficult by the circumstance that the Russians used several different cipher tables simultaneously, [237] although these were all for one and the same system. However, the difficulties caused thereby must have been greater for the Russians themselves, because by using so many cipher tables they only increased the confusion and bewilderment. It is certain that the complications thus produced increased the errors and blunders many times and thus gave rise to many questions in clear text, repetitions, mixed text, etc.; in other words, the errors usual in such cases.

At that time an event occurred which clearly demonstrates the complete collapse of the Russian cipher service. A Russian radio officer stationed at the radio station at Novogeorgievsk sent a telegram November 20, which was intercepted by the Germans and solved. It read as follows: "The enemy has solved our cipher. Until a spare key is drawn up, the keys used heretofore at the stations should be employed." [238] The comments are obvious. The same radiogram is mentioned by General Ronge. He states that the officer in question was a liaison officer sent out from the Fourth Russian Army. A newly ordered key was, however, solved in a short time both by the Germans and the Austrians.[239]

The same conditions prevailed again in the beginning of December when a new Russian radiogram was intercepted, which read as follows: "The cipher keys, including the last ones issued during November, are known by the enemy." However, the Russians continued sending radiograms in the keys which had already been solved by the enemy, as if nothing had happened. They were obviously dependent upon radiotelegraphy as a means of communication and believed themselves to be protected by changing the station signals! The only remark which can be made about this information furnished by General Ronge is that, on the whole, a greater lack of comprehension of the proper functioning of a cryptographic service can hardly be imagined. The lesson to be drawn from this is useful. It proves with convincing clearness where ignorance of cryptography can lead.

It is very ironical that the Russians succeeded in solving the German cipher about November 20. The German cipher key had fallen into their hands,[240] a fact which was learned from a radiogram read by the Austrians. (How this was accomplished is not mentioned, but it is not impossible that the results of the work done by the French cryptanalysts were gradually communicated to their Russian allies.) The account in the German Official History of the World War mentions this fact as being uncertain,[241] but the strikingly good knowledge of the measures taken by the Germans, to be deduced in several places from the import of Russian radiograms decrypted after November 20, seems to verify the report that the Russians had successfully solved the German ciphers. We cannot help being astonished at the inability of the Russians to draw a lesson for their own use from the dangers connected with the careless employment of ciphers and radiotelegraphy.

During the course of the fighting around Lodz, during the part of the operations already mentioned, from November 22 to November 25, when the von Scheffer group performed its unparalleled feat of breaking through the circle of Russians surrounding them and joining the main body of the German troops again, still other Russian telegrams were solved by the Germans. The German Official History of the World War writes as follows on this subject:

> The mission of the Scheffer group now seemed to be impossible to accomplish. An indomitable will to conquer and intercepted Russian radiograms resulted in the circumstance that the German command failed to judge the situation thus.[242]

[237] Carlswärd, Operationerna på tyska ostfronten 1914, p. 151

[238] Ibid., p. 151. [Note: This undoubtedly was one of the few times when the change in key consisted in changing not only the sequence in which the cipher alphabets were to be employed in encipherment but also the composition of the cipher alphabets. See my note at the end of this translation.—*W. F. F.*]

[239] Ronge, Kriegs- und Industrie-Spionage, p. 128. [Note: According to Ronge's account it took two days.—*W. F. F.*]

[240] Ibid., p. 128.

[241] Reichsarchiv, Der Weltkrieg, 1914–18, vol. VI, p. 289.

[242] Ibid., p. 222.

The German command was equally well informed during the battle which led to the capture of Lodz.[243] The assault planned by the Russians was known in good time; the regrouping of forces was cleverly used; advantage was promptly taken of gaps, as was the case during the previous period. We can readily understand the peculiar situation quoted by Captain Carlswärd, namely, that the difficulties encountered by the Germans in telegraphing by radio were due to the fact that German Army headquarters did not wish to dispense with the Russian radiograms, the interception of which was interrupted and interfered with if they themselves sent messages by radio.[244] We can also well understand General Hoffman's opinion of the importance of cryptanalysis and General Ronge's frank and open recognition of it. The statement made at the time this book was written in an interview at Stockholm by von Glaise-Horstenau, chief of the war archives at Vienna, privy councilor, and former officer on the Austrian general staff, was as follows: "If we had not intercepted the Russian radiograms, we should most probably have lost the war as early as in the winter of 1914–15." [245]

In the "Observations", in the German Official History of the World War, on the part of the war beginning with November 1, which we have already mentioned in the foregoing, there is expressed the following general opinion concerning the operations around Lodz: "During those days the German command was reduced, on the strength of intercepted Russian radiograms, to underestimate the power of resistance of the enemy. They thought they were engaged in a Tannenberg." [246]

The information happens to be misleading. It is largely based upon a selection of "Calls for help sent out by the Russian Second Army", pessimistic in tone, which are assembled on page 149 of volume VI of the German Official History. If we place these extracts in their right setting—that is to say, if we read the Russian telegrams in as complete form as they appear in another place (p. 140)—the picture is different. "The army has placed all reserves in action", we read on page 149. "The behavior of the troops is heroic", we read on page 140. "Help!" we read on page 149. "An energetic, rapid advance of the First Army is necessary", we read on page 140. And yet the information given on page 140 consists merely of snatches, those even intended to show the desperate situation of the Russians at Lodz. The same meaning, or at least the same spirit, is without doubt found in the telegrams on pages 140 and 149, a spirit which clearly demonstrates the excessively hazardous risk, but also as clearly demonstrates a tenacious will of defense. There apparently can be no doubt of this.

In the discussion already mentioned concerning the importance of the intercepted Russian radiograms for the decisions reached by the German command at the Battle of Tannenberg, it is stated that these radiograms were not of any importance. In the discussion of the operations around Lodz, on the other hand, it is stated that they were of far too great, but misleading, importance. If we attempt to follow the course of events according to the information given by the German Official History of the World War, we find, however, that the underestimation of the strength of the Russian resistance was probably based on another reason. This lies in the far-too-great optimism of the German generals concerning their own reports. Let us compare these reports, for instance, those furnished by General von Pluskow,[247] General von Schaeffer,[248] and General von Morgen, [249] with the actual situation as it is described in the History of the World War published by the Reichsarchiv, and General von Mackensen's underestimation of the Russians, despite intimate knowledge of their measures and aims.[250] In several places in Von Kundt's

[243] Reichsarchiv, Der Weltkrieg, 1914–18, vol. VI, p. 267.
[244] Carlswärd, Operationerna på tyska ostfronten 1914, p. 154.
[245] Stockholm's Dagblad, Mar. 9, 1931.
[246] Reichsarchiv, Der Weltkrieg, 1914–18, vol. VI, p. 221.
[247] Reichsarchiv, Der Weltkrieg, 1914–18, vol, VI, p. 123.
[248] Ibid., vol. VI, pp. 125 and 126.
[249] Ibid., vol. VI, pp. 115, 138, 148, and 155.
[250] Ibid., vol. VI, pp. 139, 140, 150, and 151.

reports to the high command,[251] we can point out instances in which he quotes wishes as realities. No one can reproach the German command for having utilized to the utmost Russian telegrams which had been decrypted. Nor can anyone doubt the extraordinarily great power to act and bold desire for attack which the German command steadily displayed during the battles mentioned. On the other hand, the manner in which the German Official History of the World War connects the solution of the messages with the decisions reached by the German command does not seem to show the influence of a sufficient acknowledgment of the importance of the said solutions.

Concerning the organization of the radio-intercept service of the Germans during the operations on the Eastern Front in 1914, a detailed and very interesting account is found in Captain Carlswärd's Operationerna på tyska ostfronten 1914, pages 74 to 83. A good example of the decentralization of the cryptanalytic work is given on page 76. This work was done at several German stations located in fortresses, where the telegrams were sorted according to their importance.

The said decentralization is as necessary for the reading of telegrams written in ciphers that have already been solved, as a strict centralization is necessary for actual cryptanalysis. In both cases a particularly close liaison is necessary as well as a strict discipline among the cryptographic personnel. Combining intercept work with cryptanalysis is no sinecure under such conditions. These conditions are best illustrated by the statement made by General Cartier to the effect that the majority of the French radiotelegraphic operators who were called from the French front and assigned to the intercepting service in the interior in a short time earnestly requested to be permitted to return to the front, despite the danger involved in such a move; the discipline and isolation of the intercepting service were far too great and the work was too strenuous.[252] Special training was necessary for this service. Such training had to be obtained before hostilities broke out.

The report concerning a special dictionary of Russian words compiled by Professor Deubner is of special interest.[253] A modern cryptanalytic bureau, however, has a number of special dictionaries, tables, and frequency lists specially compiled for cryptanalytic purposes. Work on these is best done, or at least best planned, by a cryptographic military commission, such as the one the nature of which we already outlined in this book. These documents are compiled in the so-called "statistical section" of a cryptanalytic bureau, a section of which no other demands need be made than that it be orderly and discreet. This section often has quite a large personnel.

There is not much to tell about the last battles in December 1914. The Russians had changed keys on December 14. Inasmuch as this circumstance is especially mentioned both in the German Official History of the World War and in Ronge's report as being connected with delayed cryptanalysis,[254] it is probable that the keys this time were not given in the running radio correspondence read off by the Germans and Austrians, but were transmitted in some other way. This made the work connected with reading the telegrams actual cryptanalysis in contrast to much of the work that had been done before. The cryptanalysis was done by Lieutenant Colonel Zemanek, Captain Pokorny, and Lieutenant von Marchesetti of the Austrian Army, in a few days, and the intercepted telegrams gave a clear insight into the retreat planned by the Russians, as well as its scope.

[251] Reichsarchiv, op. cit., vol. VI, pp. 154 and 159.

[252] Cartier, Le service d'écoute pendant la guerre, p. 497.

[253] Carlswärd, Operationerna på tyska ostfronten 1914, p. 78.

[254] Ronge, Kriegs- und Industrie-Spionage, p. 130. Reichsarchiv, Der Weltkrieg, 1914-18, vol. VI, p. 306. [Note: See my remark in connection with footnotes 238 and 239. It is perhaps permissible to conclude that the Russians changed their cipher *alphabets* only two times, once about November 20, again on December 14. The system was entirely abandoned shortly thereafter.—*W. F. F.*]

The confusion between espionage and cryptanalysis, which has already been pointed out in several cases in this work as existing in the minds of many, becomes evident again in the Russian idea of the reasons for the circumstance that the German and Austrian commands knew their ciphers.

Thus Ronge, for instance, writes: "The Russians did not suspect that we could solve their ciphers and alphabet keys. As a matter of fact, it was an amazing achievement to solve all the 16 keys used. Even if the Russians did suspect that their radiograms were betraying them, they assumed that we had purchased their cipher keys."[255] Aside from the slight correction to the effect that some of the keys cited certainly were not solved by cryptanalysis but were merely read off from the Russian radio correspondence, once again we find an indication of the fact that the general ignorance concerning the means used by cryptanalysts and the possibilities of their application was the root of the misconception. If any of the higher commanding officers in the Russian Army had possessed an intimate knowledge, or merely a general knowledge, of the technic of cryptanalysis, the Russians would without doubt have changed systems, and not merely keys, much sooner. "Espionage", "treason", these are words which in time of war seem to deprive the wisest of men of their ordinary common sense. It can very readily be understood that the very thought of espionage or treason in one's own ranks will eliminate all thought that the ciphers might merely have been solved. Furthermore, how could such a thought enter the head of persons who shared the general opinion that their own ciphers, compiled by general-staff personnel assigned for that work, were indecipherable? Even since the war there are exceedingly few of the many generals who served in it who really understood what cryptanalysis is and how it is performed. There is an illuminating picture of the importance of cryptanalysis for the operations of the Austrian Army during the campaign fought in the fall of 1914. The chief of operations of the Austrian Army writes as follows about that subject in Der grosse Krieg.[256]

> In those days of breathless tension, there were available almost every evening decrypted radiograms of the enemy from which the whole scope of the dangerous situation could be inferred; these invaluable messages informed us that the command which had advanced to Teschen not only knew where the enemy was located yesterday and today but also where he expected to be located tomorrow and the next day. Quite unexpectedly the intercepted radiograms sometimes gave information concerning the location of the Russians, exposing the location of their armies and army commanders. Our weakness prevented us from utilizing this information; nothing could be done about it. The highly reliable information (observe!) which thus, unknown to the enemy, reached the armies of the Central Powers, was quite valuable to us in making our decisions (observe!). We merely wish to mention one case in which the information had an especially tranquilizing effect. This was on November 10, 1914, when the First Army had not yet prepared its position northwest of Krakow and was in great need of a short rest. The Russian attack, which seemed to be almost imminent, was awaited, not without some anxiety. From Russian marching orders intercepted by radio it was learned that the following day the Third Caucasian Corps, as the result of a misunderstanding, would without doubt enter the march zone of a neighboring corps, which belonged to another army. And sure enough, the next day, indignant radiograms were exchanged between Ninth and Fourth Russian Army headquarters. The misunderstanding caused congestion, delays, and loss of time, totaling 2 days, for the enemy's advance, and an invaluable gain for the armies of the Central Powers.

2. THE PERIOD FROM 1915–17

The operations on the Eastern Front beginning with 1915 have not been discussed in any of the volumes of the German Official History of the World War thus far published. Consequently, the chief information about that period is to be obtained from Ronge alone.

This information confirms what has been said in the foregoing section about the failure of the Russian cryptographic service. The blunders continued throughout the whole war; the

[255] Ronge, Kriegs- und Industrie-Spionage, p. 151.
[256] Carlswärd, Den trådlösa telegrafien under världskriget, p. 64.

forms in which they were made varied. Not until 1916 can we discern the beginning of an improvement in the employment of ciphers. However, routine was so ingrained in the habits of the Russian cryptographers that the Germans and Austrians all along were able to follow the development of the Russian cryptographic service step by step without any great difficulty.[257] Nevertheless, the results became less fertile for the Central Powers the nearer the war drew to a close.

Concerning the penetration on the Eastern Front in the spring of 1915 Ronge writes as follows: "Once again our radio service (here the intercepting service) triumphed. Especially good were the results which were obtained by the Eleventh Army's radio station under command of Captain Pokorny, even though very frequently it was interfered with by the German radio stations." [258]

Further information may be obtained from Captain Carlswärd's work on wireless telegraphy during the World War. For instance, in April 1915, a great many Russian radiograms were intercepted. These informed the Austro-German commands concerning the condition and the situation of the Russian troops and their grouping. In particular, it was learned that the Third Russian Army (Dmitriev) was in serious need of men and ammunition and that the said army had suffered great losses in the Battle of the Carpathians and had only very slowly been able to recover. Here was an opportunity for the Central Powers to obtain great results by combining their forces. On May 2, General v. Mackensen's attack via Gorlice against the Third Russian Army was made, with the results which are now known. During the battle many telegrams were intercepted.[259]

As an example of the scope of the cryptanalytic work during the battles which were fought in the following months, Ronge states that on August 23, 1915, not less than 52 radiograms were solved, and that during the critical days in the end of August very valuable results were obtained by interception of radio messages.[260]

Among other things, we can mention the fact that from a message later intercepted it was learned that the Thirtieth Russian Army Corps was to enter the battle on September 13.[261] A cleverly planned flank attack by the Russians also failed, thanks to messages which had been successfully solved by the Austrians.[262]

The Russian preparations for a general offensive against Eastern Galicia in the end of November 1915 were also betrayed through the messages decrypted by the Austrians. The most important of these was an extensive description by the Russians of their situation and aims, telegraphed by the Fourth Russian Army. This was exceedingly important for the armies of the Central Powers.[263]

Although the Russians were not able to grasp the correct reasons for the fact that the commanding officers of the enemy's forces were constantly so well informed concerning the intentions and undertakings of the Russian forces, they, however, came to understand, although late, that there were great dangers connected with the use of radio for telegraphing purposes. On December 2, 1915, the Russian officers in command on the southwestern front forbade all radio traffic. But it was already too late.[264] The Austrians already knew too much. On December 20 the use of the radio was permitted again, this time with a new key. However, the new key was solved even before it was placed in use on the said sector of front, for, through a blunder on the part of the Russians, it had already been used earlier on another sector of front.[265] This informa-

[257] [This is a usual and almost inevitable result of an initially faulty cryptographic technic.—*W.F.F.*]
[258] Ronge, Kriegs- und Industrie-Spionage, p. 157.
[259] Carlswärd, Den trådlösa telegrafien under världskriget, p. 65.
[260] Ronge, Kriegs- und Industrie-Spionage, p. 174.
[261] Ibid., p. 175.
[262] Ibid., p. 176.
[263] Ibid., p. 187.
[264] Ibid., p. 187.
[265] Ibid., p. 187.

tion once more confirms the remarkably good organization and methods used in the Austrian cryptanalytic service.

In the spring of 1916 a novelty was introduced, the radiogoniometer. These instruments were introduced by the Austrians in the month of March 1916 on the Russian front. By that time the Austrians had become fully accustomed to the use of the radio for telegraphing purposes, for Ronge reproaches the Germans for having used the radio for communications continuously, despite the fact that the Russians were intercepting such messages and were using the radiogoniometer at Nikolajev to locate the stations.[266] This reproach seems to have been both well grounded and not well grounded. The new German cipher systems in use at the time still were of rather limited value. On the other hand, the intercepting service of the Russians most probably was much worse. Due to prevailing conditions, the use by the Germans of the radio for telegraphing, which was perhaps very risky on other fronts, could not be very dangerous here. Sound judgment must solve a threefold problem of this kind, one in which the need for quick and convenient means of communication, the quality of the cipher system—and the discipline in the employment of ciphers—and the standard of the enemy's cryptanalytic work form the three different elements.

Sending "faked" radio communications for the express purpose of having the enemy read them or solve them was a ruse which even the Russians tried in the spring of 1916. The attempt, however, failed, partly because the ruse was discussed in a preliminary telegram which was decrypted by the Austrians, and partly because it was betrayed in the "faked" telegrams themselves. That is to say, at the end of these telegrams was a statement, in a cipher which had already been analyzed by the Austrians, to the following effect: "Do not be disturbed; this is merely intended to mislead the enemy".[267] This act is characteristic of the organization and knowledge of the Russian cryptographic service.

Another case of communication of this kind, which also proved to be a failure, is discussed by Captain Carlswärd.[268] This one, however, does not happen to involve "faked" cipher messages, purposely compiled for the enemy to decrypt.

The great offensive of General Brussilov in June 1916 was also betrayed beforehand by successful cipher solution. On June 3 the general's verbose order about the offensive which was started the following day was captured.[269] After the victory of the Russians, the Russian radio stations which were located in the zone of the advance were again very loquacious. As many as 70 radiograms, including operations orders, reports, information about troop movement, etc., were decrypted daily by the Austrians. The newly introduced radio regulations and cipher tables were far too difficult for the Russians, and for that reason some of the commanding officers and units continued using the old system. The command of the guard division of the Eighth Russian Army committed the serious error of telegraphing in clear text the latest cipher key ordered.[270]

With the entrance of Rumania into the war on the side of the Entente, much more work was placed upon the Austrian intercepting and cryptanalytic services. The service on the Eastern Front was divided into two groups, known as the "Austro-Nord" (Austro-North) for the Russian sector, and the "Austro-Süd" (Austro-South) for the Rumanian sector. The latter group was organized by Captain Pokorny and was placed under the command of Captain Jansa, with central office at Sofia. However, it was some time before any results were obtained, which was in a large measure to be attributed to the fact that the Rumanian ciphers were much superior to the Russian. The cryptanalysis was very difficult to perform, but that work was most profitable,

[266] Ronge, Kriegs-und Industrie-Spionage, p. 218.
[267] Ibid., p. 219.
[268] Carlswärd, Den trådlösa telegrafien under världskriget, p. 60.
[269] Ibid., p. 65.
[270] Ronge, Kriegs- und Industrie-Spionage, p. 227.

for the Rumanian telegrams, like the Russian during the "great" period, contained operations orders or reports of the greatest possible value for the Austro-German Command.[271]

In this way the Austrians gained full knowledge of the plans of the Rumanians for a counter-attack, the 14th of September 1916, with the Dobrudja Army, reinforced by troops from Transylvania.[272] On the Transylvanian front the first Rumanian radiogram was decrypted September 16.

During the following months the "Austro-Süd group lived through palmy days. Captain Jansa's clever assistant, the cryptanalyst, Captain Marosan, had the opportunity to work on and analyze very extensive material which was sent in by the many intercepting stations. It is true that carelessness on the part of the Rumanians to a great degree assisted in the cryptanalysis. Despite prohibition of telegraphing in clear text, with severe penalties for infringements, the Rumanian code clerks and telegraphers made the same blunders as some of their Russian colleagues. The work of the Austrian cryptanalytic service was so increased that a special cryptanalyst had to be assigned to the "Intelligence Department" (Kundschaftsstelle) at 1st Army Headquarters.[273]

The activity on the part of the Russians, who were working in order actually to assist in the victories expected through their new ally, was recognized in good time by the Austrians. The "Austro-North Group", under command of Captain Boldeskul, "always learned in good time the intention of the Russians to attack."[274] We get a clear picture of the extent and meaning of the counter-measures to be taken by the German and Austrian commands from the fact that the intention of the Russians to send reinforcements to the Rumanian north wing was known as early as 1 month before their arrival at the front.

However, the radio communications of the Russians ceased October 24, 1916. A radiogram forbade the use, for strategic purposes, of radio as a means of communication, the Russian Sixth Cavalry Corps having lost the cipher key, as well as for correspondence with the office of the Minister of War and with adjoining units. A new cipher key was introduced. At the same time the Rumanian stations stopped sending communications by radio, with the exception of those between the Navy and the Danube Divisions, and those between General Headquarters and the Dobrudja Army.[275] A little later the use of the Russian Communications Cipher No. 14 was also prohibited, for it was known by the enemy.

At the time when Rumania started her counter-attack with a view to attempting to rescue Bucharest, as well as during the Russian attack with the Carpathian Army, radio was used again. However, we get the idea, by a careful reading of Ronge's account, that to a great extent cryptanalytic work ceased at this time. A number of bits of information tell about changes in the cipher system of the enemy, or changes of key, etc., and, on the contrary, practically nowhere do we find reports of successful cryptanalysis. At the same time, there are reports in a couple of places about the use of codes. As this period practically coincides with the time when codes were coming into use on other fronts, we can, with all probability of being correct, infer that the cryptanalysis of codes involved such difficulties that the Austrian cryptanalysts were unable to overcome them. The solution of codes was an entirely different matter from the decrypting of the quite simple cipher systems which had been in use by the Russian Army up to that time. For 2 years the Russians had continued to rely upon systems the solution of which was really quite possible even by moderately well-trained experts. They were typical problems for so-called "chamber analysis." However, the use of codes placed an entirely new problem before the experts, a problem for which they apparently were not

[271] Ronge, Kriegs-und Industrie-Spionage, p. 236.
[272] Ibid., p. 236.
[273] Ibid., p. 236.
[274] Ibid., p. 236.
[275] Ibid., p. 237.

ready. For instance, Ronge mentions the use, but not the cryptanalysis, of Rumanian superenciphered codes.[276] As in this same connection French radiograms turned up, probably sent by the French military mission headed by General Berthelot, it is not impossible that the French taught the Rumanians both the manner of compiling good codes and the method of using them. Thus we find, also, on the Russo-Rumanian front, that the last part of the war was characterized by a great decrease in the efficiency of the cryptanalytic work in the purely military field (the solution of diplomatic codes, on the contrary, reached a high point of perfection during the years 1917–18 in the French and British cryptanalytic bureaus). Nothing else was to be expected. It is taken for granted that the experiences gained in a war covering several years would naturally lead to a gradual improvement in cryptographic systems and cryptographic discipline. This was aided to a great extent by the relative stabilization of the front and the great improvement in means of wire communication, which permitted a considerable restriction of radio communication, at least for strategical purposes. In the constant combat between cryptography and cryptanalysis, the latter had a decided advantage during the first few years of the war. It was quite natural that an equilibrium should gradually be established, even if the constant blunders and errors on the part of the cryptographers had not always given the advantage to the side of the cryptanalysts.

The very active analysis by the Austrians of the Russian ciphers, beginning with the start of the Russian Revolution in the year 1917, merely forms the exception which proves the rule. The confusion in the Russian Army was even greater than before. Garrulity by radio was unprecedented. All discipline gradually disappeared, for no common command was able to control the forces. From the fact that the Austrians succeeded in 1 day in decrypting not less than 333 radiograms [277] we cannot help inferring that the Russian cryptographic service, which was disorganized to an unparalleled degree, had finally fallen into a complete state of chaos by the end of the war.

A review of the cryptographic operations on the Eastern Front necessarily emphasizes the dangers connected with the use of radio for communications. A few words on this subject may be in place. The said dangers are very great; that fact cannot be denied. But it would be like throwing out the child with the bath water to give up such a valuable, rapid, and simple means of communication as radio for this reason alone. Its value as a means of communication is undeniable, and, strikingly enough, it has been assigned a much greater importance in the armies of the great powers on the continent since the war. Nor was it radio as a means of communication which so often failed, but the cryptographic service, a fact which can never be too greatly emphasized. But if used with a well-organized cryptographic service, fully experienced in cryptanalysis, radio becomes an invaluable means of communication. When used by a personnel ignorant of the principles of cryptanalysis and poorly prepared, it, on the other hand, becomes to the highest degree dangerous for the activities of the armies using it. Common sense alone tells us that the use of a means of communication which leads both to friend and foe must necessarily presuppose exceptionally great knowledge of cryptography and cryptanalysis on the part of the personnel responsible for the operation of that means. Such knowledge must be made compulsory.

However, it often occurs that certain radio personnel is given orders to send in cryptographic form certain information which in itself involves an element of risk. This is true, for instance, of certain reports on the situation, etc., which frequently are made public through the proceedings of parliament, through diplomatic documents, through the press, etc. This occurred more than once in the course of the World War. In this case the blame is not to be placed on the radio personnel, which merely obeyed orders. It is to be placed

[276] Ronge, Kriegs-und Industrie-Spionage, p. 238.
[277] Ibid., p. 298.

on the officer who, in making the decision to have the message sent in cryptographic form, did not consider that the clear text of the message might come to the attention of the enemy. For such officers also, therefore, a general training in cryptography is irrefutably necessary. Before deciding to transmit cryptographed material, the man who is versed in cryptanalysis first makes certain that measures have at the same time been taken to remove all material which might be used in making comparisons and which thus would aid the enemy in making the cryptanalysis. Otherwise, such messages should not be cryptographed, if the cryptograms may fall into the hands of the enemy, which is always possible in the case of radiograms. Other means must be sought. Those concerned, however, seldom consider all these details, any more than they consider that if just one message is decrypted all messages prepared with the same system are thereby exposed to the enemy, or at least, there is danger that they may be so exposed. Change of key helps only little. The solution of keys is one of the easiest tasks of the cryptanalyst, provided the bases for the system are known or have been betrayed.[278]

References to radiograms sent by the Russians on the Eastern Front and decrypted by the Central Powers, found in Reichsarchiv, "Der Weltkrieg, 1914–18":

Volume II, pages 62, 97, 116, 171, 128, 136, 137, 138, 155, 161, 165, 167, 168, 174, 177, 182, 191, 199, 203, 207, 209, 218, 219, 274, 279, 280, 281, 291, 315, 351, 352.
Volume V, pages 422, 423, 425, 426, 440, 442, 485, 487, 513.
Volume VI, pages 41, 43, 45, 48, 49, 58, 59, 63, 66, 71, 72, 83, 84, 85, 88, 99, 102, 104, 107, 110, 114, 116, 122, 125, 126, 127, 129, 136, 139, 140, 149, 150, 152, 154, 155, 156, 159, 166, 167, 191, 193, 205, 221, 233, 237, 259, 260, 261, 262, 272, 273, 276, 280, 288, 290, 292, 294, 298, 306, 311, 313.

C. The Italian Front

More scarce than the information available about the other fronts is that available about the cryptographic and cryptanalytic activities in the Italian theater of war. It is to be found, almost without exception, in the work by General Ronge, of the Austrian Army, which we have already cited so many times, "Kriegs- und Industrie-Spionage." It would have been of great interest if we had had access to some reliable Italian account which we might have used for purposes of comparison. Unfortunately, no such account of these activities has yet been published, as far as the author has been able to ascertain.

Pre-war conditions both in Austria and Italy have already been discussed. They cannot be directly connected with the activities carried on during the war, for by the time Italy declared war, in the year 1915, the Austrians had already been applying military cryptography for almost a year and had brought it to a very high degree of perfection, thanks to their experiences on the Russian Front. Consequently, the Italian cryptographic bureaus found, in the Austrian bureaus, adversaries much superior to them in their line of work. The outcome became evident soon enough. To this must be added the fact that even before the war the Austrian cryptanalytic bureau had studied the Italian cipher system carefully. This proved of very great value later on.

At the time of the outbreak of the war, the Italian Army was extensively using the "Cifrario tascabile", which we have mentioned in the foregoing as having been compiled by Colonel de Chaurand de Saint-Eustache of the General Staff. The system is described, among other places, in Colonel Figl's "Systeme des Chiffrierens,"[279] and possesses no real theoretic safety, regardless of the manner in which it is employed. Several copies of the tables necessary for its

[278] [It is true, of course, that the task of the cryptanalyst is usually simplified if he has full knowledge of the basic system employed. But to say that a "change of key helps only little" is, in my opinion, too broad a general statement to make. The underlying assumption for all practical military cryptography *must* be that the enemy *knows* exactly how the system operates. The system must be such that even with this knowledge of the general system, his ignorance of the specific, variable key prevents him from solving the cryptograms in time to yield information of practical value in the tactical situation.—*W. F. F.*]

[279] Figl, Systeme des Chiffrierens, pp. 77, 85, and pl. 20.

application probably fell into the hands of the Austrians, for the system was used, imprudently enough, even in the lines nearest the enemy. It was used merely for relatively subordinate purposes. "Cifrario tascabile" vanished comparatively quickly from use, after a period of about 1 year.

On June 5, 1915, four Italian telegrams were successfully decrypted. These were the first telegrams successfully solved, but they were of limited value. They consisted of official communications exchanged between the radio stations of Coltano and Massaua.[280]

Exactly a month later a telegram from General Cadorna to the commanding officer of the Second Italian Army, enciphered with the Italian staff cipher "Cifrario rosso", was read. But it must be emphasized that no analysis was required in this case, for the said system of ciphers had long been known to the Austrians. "I acquired it before the war", said Ronge on that subject.[281]

This circumstance explains a blunder very common in most countries, namely, that of using at the outbreak of a war ciphers or codes which had been compiled long before that. They might have been stolen or photographed; as a rule, nothing is known about such mishaps. Despite the great trouble generally involved in quickly compiling, and if necessary printing, new ciphers and codes, it is of great importance to be able to start with an almost entirely new set of systems which have never been used before. Therefore they must not always be exchanged for others, but must be entirely new, which is a different matter. Reaching a decision concerning the working methods and standardizing them may save a great deal of time and the main requirement is quick adaptation. Far too radical changes may even prove to be detrimental, for the great majority of the cryptographic personnel in a war are easily confused by absolutely new regulations and consequently may commit numerous blunders and errors in enciphering. In the last analysis, everything depends upon the preparation of the cryptographic bureau for the work.

On July 10 a change of the arbitrary alphabet of the "Cifrario tascabile" caused the Austrians considerable difficulties; they succeeded in solving the cipher only after a great deal of work.[282] From this fact we can judge the type of technic used in cryptanalysis by the Austrians at the time. It certainly was entirely based on intuition, for if the Austrians had been acquainted with modern statistical methods, they would, without any doubt, have been able to solve the new alphabet in a very short time on the basis of the available material.

During the month of June the Austrians succeeded in solving 20 radiograms sent by the Italians; in July, only 13. The knowledge of the new alphabet, gained with such great labor, however, helped the Austrians to solve a total of 63 telegrams up to August 12. As time went on the proportion rose with avalanche-like speed and in a few cases they succeeded in decrypting a total of 50 telegrams a day, and in exceptional cases, even as many as 70. This work was done at not less than three bureaus, those located at Adelsberg, Villach, and Bozen.[283]

The Italian ciphers were, however, not nearly as good as the Russian, for they, as a rule, merely were used for less important messages. The names of commanding officers, information about the grouping of troops, the movement and strength of troop units, etc., were, however, very valuable to know. Among other things, Ronge gives us the important information that a large-scale forward movement of Italian cavalry divisions was a very certain indication of the imminent commencement or conclusion of quite large operations.

Parallel with the "Cifrario tascabile" the Italians used a system which was known as the "Cifrario servizio." Unfortunately, there isno in formation available about its nature. Ronge, however, states that it was used to a great extent, with change of keys every sixth week. The

[280] Ronge, Kriegs- und Industrie-Spionage, p. 168.
[281] Ibid., p. 168.
[282] Ibid., p. 168.
[283] Ibid., p. 168.

last bit of information indicates a flagrant disproportion between the change of keys and their application, because for every system there is a certain optimum change of keys and tables which can be calculated theoretically with considerable accuracy, without consideration of carelessness in the application. A regularly employed system, which in addition is exposed to interception by the enemy, probably requires much more rapid change of keys than, for example, a staff cipher which is used only in exceptional cases for radio traffic. Here, as well as in all matters pertaining to cryptography, good judgment is necessary, for an unnecessarily great number of key changes may easily lead to errors and also irritate the cipher clerks.

In the spring of 1916 the Austrians started an offensive against Italy. With a view to misleading the enemy concerning the sector of front on which the attack was to be made, a "faked" radio traffic was started by the then Captain Figl on the eastern Carinthian front.[284] A very simple cipher system was used for this purpose, one which it was assumed that the Italians would be able to decrypt without any difficulty. According to other sources, which unfortunately cannot be checked except with difficulty, the preparations for this traffic, it is reported, were made with very great care, and this war stratagem was crowned with complete success. Analyses of the grouping should now be possible, and it is to be hoped that studies by experts will in the near future clear up the actual state of affairs. A similar "faked" traffic was also carried on in connection with the great offensive in 1917.

At the same time the Austrian cryptanalytic services were particularly active. Captain de Carlo and Lieutenants von Chiari and Scheuble, who were stationed at Bozen, in the Tyrol and Carinthia respectively, are given splendid testimonials in Ronge's work for their great contributions in this respect. More than 30 Italian radio stations were intercepted and each radiogram was utilized within the shortest possible time.[285]

The cryptanalysis was apparently made on all kinds of Italian cipher systems. It is also probable that here, as on so many other fronts of combat, carelessness helped the cryptanalysts in their work, for the Italian High Command on March 30, 1916, prohibited all further use of the staff cipher "Cifrario rosso" mentioned above. However, as a matter of fact, merely a change of key was made, for that was ordered the first of April. The new key was solved that same evening.[286] For lack of information, it is impossible to reconstruct the circumstances, but it is quite probable that the poor cryptographic knowledge of the Italian specialists may have led them to compile some illusory complication or, for example, some "congruent" key change, both of which are easily solved.

However, it is worthy of mention that, despite the prohibition, the "Cifrario rosso" continued to be used by the radio station at Valona, even for very important messages.[287] As that very same blunder was also made by the Germans and the Russians, it gives us a good idea of the dangers involved if the cryptographic service is not highly organized and centralized. It proved to be true that what might be called the "cryptographic discipline or training" was not present to a satisfactory degree in the very countries where enough importance was not placed on the cryptographic service and means for strictly controlling the cryptographers were not assigned to it.

Another illuminating example of the general confusion existing in the Italian cryptographic service is to be inferred indirectly from the statements made by Ronge. That is to say, Ronge mentions that the Italian expeditionary forces in Albania had used the "Cifrario mengarini" for their correspondence with Italy. This code was known by the Austrians before the war.[288]

[284] Ronge, Kriegs-und Industrie-Spionage, p. 129.
[285] Ibid., p. 129.
[286] Ibid., p. 129.
[287] Ibid., p. 220.
[288] Ibid., p. 220.

This knowledge is, however, not very much to boast of, for the code in question was simply composed of codes of the Sittler and Baravelli type, which are in general use in commerce. As in the above-mentioned codes, the arbitrary element in the Mengarini code merely consists of arbitrary page numbering. When we consider that the chief of the Cryptographic Service of the Italian General Staff had himself solved correspondence written in that same Mengarini code about 15 years before,[289] and that the public procedure in the Dreyfus case must indeed have shown the Italians what great weaknesses were peculiar to that type of code, not to mention the fact that Valerio in the year 1895 published a splendid general cryptanalytic technic for use in solving just such codes—the use of the said code during the World War is an incredible instance of lack of good judgment. It can hardly be explained otherwise than that the cryptographic service did not possess, or was not assigned, means for supervising and regulating the extensive traffic concerned.

During the great offensive on the plateau at Lavarone and Folgaria, in the late spring of 1916, the Italian counter-offensive was betrayed by decrypted radiograms. During the night of May 20 an Italian telegram was intercepted containing descriptions of the arrangements made for a large-scale counter-attack with the reserves. By 3:00 o'clock in the morning the telegram had been decrypted and 1 hour later counter-measures were ordered which successfully checked the counter-attack.[290]

The cryptanalytic experts were also, by that time, fully familiar with the Italian cipher. They had a thorough knowledge of the enemy's habits and the changes of key caused them less work than they did the Italian cryptographers themselves, a paradoxical but nevertheless often usual circumstance when cryptographic work has been carried on methodically for some time. "Daily change of key and adoption of a special key for aviation purposes did not prevent the decrypting of the messages", General Ronge [291] writes on this subject, and he is certainly right.

Hence, we cannot be surprised at the fact that the seventh, eighth, and ninth Isonzo offensives of the Italians in no way took the Austrians unawares.[292] Perhaps the Italian system had been improved in the meantime and, according to Ronge, the cryptanalysts had developed a very high degree of intelligence. It is true that the new Italian system, which was introduced August 20, 1916, had been solved within 38 hours, but later the Italians used several different keys simultaneously; they had special keys for divisions and brigades and in some cases, at times, also for individual regiments.

There may be a difference of opinion with regard to the suitability of the last-mentioned measures. They may render the cryptanalysis much more difficult. The technical aspect of the cryptanalysis remains unchanged, it is true, but the classification of the intercepted ciphers is made much more difficult and the statistical work is increased to a great extent. On the other hand, such a restriction of the "radius of action" of a system or key "makes it difficult to avoid blunders and errors in encipherment, and communication between the different units is on the whole rendered more difficult thereby." If effective communications are to be established by this means, the cryptographic personnel must be highly trained in its work and must be well experienced.

Although not directly applicable to the domain of cryptography, the following detail deserves mention. During the frequent changes of call signals made in the Italian Army, the great majority of the radio stations, tried, for purposes of control and check-up, to get in contact with the other radio stations, both those located near them and those located far away. This gave rise

[289] La crittografia di fronte alle esigenze dei tempi moderni, in the Rivista Marittima, October 1923, p. 45.
[290] Ronge, Kriegs- und Industrie-Spionage, p. 224.
[291] Ibid., p. 224.
[292] Ibid., p. 243.

to the circumstance that many stations which had been silent for some time betrayed their location. They were identified by radiogoniometry. We can readily understand the importance for the Austrian Command of being able in this way to check up periodically, at least in the main, on any changes that might have been made in the grouping of the Italians.

At times, even the higher Italian officers mentioned such blunders. For instance, on November 22, 1917, the chief of the Italian Radio Service, because of the confusion arising during the retreat, committed the blunder of asking all stations under his command to report their location and relation to other troops. This gave the Austrians information about the whole grouping of the Italian forces, including the reserves, and the distribution of the medium and heavy artillery.[293]

At about the same time the decrypting of certain Italian radiograms furnished very valuable information. The chief of the Italian Military Mission in Rumania, General Romei, telegraphed repeatedly to his superiors at home. The exceedingly important information which he sent in these messages concerning conditions in the Russian and Rumanian armies, was so much more welcome to the Austrians because the Russian radio stations happened to be silent at that time.[294] This information is also interesting from the standpoint of the inner organization of the Austrian cryptanalytic service. The interception must certainly have been performed by a combined intercepting and cryptanalytic service, which functioned under the name of the "Austro-Süd" Group, with main station at Sofia, under the command of Captain Jansas, and was responsible for the part of the front which included Rumania, among other places. Perhaps the telegrams of the Italian Military Mission were not decrypted in that group but were transmitted to the "Austro-West" Group, to which all specialists in Italian ciphers had been assigned. When we consider the great importance, for effective cryptanalytic work, of the classification and the determination of the origin and system and the practical difficulties connected with recognizing the right telegrams from among great quantities of intercepted material and of transmitting them to the right place, this fact shows that a very high degree of organization existed in the Austrian service. Certainly a great centralization, such as the German High Command never was able to attain, greatly contributed to this.

A radical change must have been made in the whole Italian cryptographic service with the arrival of the French and English troops in large numbers on the Italian theater of war.

The new system which was used by these troops, according to Ronge's account, "placed new missions upon our radio and cryptographic experts." [294]

Ronge, it is true, states that good experience was gained through the radio work of the French on the Salonika front, but he says practically nothing about successful solutions, which indicates that no such solutions were performed; on the contrary, Ronge previously gave many very precise details concerning the decrypting of Italian and Russian ciphers.

Remarkably enough, at the same time, reports concerning the solution of Italian ciphers stopped, except for a couple of doubtful cases which certainly are to be attributed to the activities of the espionage service rather than to those of the cryptanalytic service. The use of the word "reports" (Meldungen) instead of the word "decipherment" (Entzifferung), which had so frequently been used before that time, reports concerning information from "confidential" sources, reports concerning the fact that many Italian radiograms were "evaluated" instead of "deciphered" or "decrypted"; other information which, when critically considered, proved to be an analysis of the location and movement of Italian stations determined by radiogoniometry—all this is cleverly woven into Ronge's account as if it were to be credited to the cryptanalytic service. His purpose is clear enough. The greatly lowered efficiency of the cryptanalytic

[293] Ronge, Kriegs- und Industrie-Spionage, p. 315.
[294] Ibid., p. 316.

services of almost all the warring nations during the last year of the war, caused by the great advance in the technic of cryptography, also affected the Italian front. The change was all the greater because the highly experienced French and English experts effected a radical reorganization of the Italian cryptographic service. It is, however, pardonable for the man who succeeded in building up the splendid Austrian cryptographic and cryptanalytic services to be very unwilling to admit that the achievements of the last year of the war, at a time when the Austrians were opposing adversaries who were much cleverer than the Italians, were slight or nonexistent. The brilliance of the previous achievements is in no way lessened thereby.

CONCLUSION

In this work the author has endeavored to give a clear idea of the importance of cryptanalysis during the late war. Its importance was such that General Cartier wrote that it "was indisputably superior to all other means for securing intelligence",[295] not to mention numerous similar opinions expressed by high military authorities.

That cryptanalysis is little known in Sweden and that the technic used in that science is practically unknown here is not due to any lack of interest, but much rather to the actual difficulties connected with securing dependable and adequate literature on the subject. We have already discussed the reasons for this. Without doubt, it is possible that we in Sweden can train good cryptanalytic experts, provided only instructors with an adequate knowledge of the technic of cryptanalysis are obtainable. So far this has not been the case, for the simple reason that, there being no permanent cryptanalytic bureau, this science has not been developed here on the basis of tradition and theory, and there has been no suitable literature on the subject available for those who might have cared to study it by themslves. To be sure, there are foreign sources, but they have, as a rule, been overlooked, or, still more frequently, we have been unable to judge their real worth. To this may justly be added the fact that, although secrecy surrounding general cryptographic conditions has to a great extent become a thing of the past in the leading countries of the world, the latest and most perfect methods of cryptanalysis have very reluctantly been made public.

The sense of discipline and order which so greatly characterizes the Swedes as a nation augurs well for the development of a dependable cryptanalytic technic in Sweden also. Such work is based on the faculties of observation, method, and logic—all of which are found in the officers of the Swedish Army.

A good insight into psychology, a power of imagination, and a speculative mind are also required for doing cryptanalysis. Although uncommon, this brilliant combination of abilities is not at all unusual among the active and critical younger generation, which is placing on the corps of officers of today its stamp of an intelligent spirit of progress and a comprehension of modern development.

Under the force of circumstances, that is to say, during one or several years of a war, it is possible to develop an efficient cryptographic and cryptanalytic service in any and every trained, intelligent western army. It does, however, require considerable time, during which blunders on the part of one's own forces are unavoidable and the blunders of the enemy cannot be utilized. It is therefore an absolute necessity that preparations be carefully made for such an organization before the outbreak of hostilities, that properly trained personnel be assigned to it, as well as the necessary units for immediately handling and exploiting the errors and blunders of the enemy, and that this organization be ready to enter into action the first day of mobilization or, preferably, a few days before that.

For it has been found to be true that modern mass armies are not placed on a war footing without a certain, unavoidable disorder and confusion in the first few weeks. This period is

[295] Cartier, Le service d'écoute pendant la guerre, p. 457.

exceptionally favorable for all cryptanalytic work, and it is during this period that the basis is laid for habits and methods which will later be applied for a long time by the enemy and which will be changed only gradually; it is consequently of the greatest importance to learn to recognize these habits from the very beginning, for that will help in keeping check on the subsequent development.

In order to make the most effective preparations for an efficient cryptographic and cryptanalytic service, the work of many men is required. One person alone cannot cover the prodigious scope of cryptography, and important details might escape his attention. A permanent organization before the outbreak of a war, such as that which existed in France even before the World War, consisting of a permanent cryptographic and cryptanalytic bureau, as well as a cryptographic military commission, seems to be highly desirable. The work of the bureau should consist chiefly in the application, in concrete cases, of the regulations for cryptographing, and the utilization, with a view to cryptanalysis, of material obtained in other countries, and the preparation for the work of the service in the field. The duties of the military commission should consist of making theoretic studies, both of the Swedish cryptographic work and of that in foreign countries, making decisions with regard to the methods of cryptanalysis and instructions to be adopted, maintaining the necessary liaison with civilian work of a nature such as to interest it: cryptography, radio, linguistics, criminology, etc. The commission should outline the general principles; the bureau should apply them and arrange the details.

As far as the appointment of personnel for these two types of work is concerned, its qualifications for the work should be considered above everything else, regardless of rank. The cryptanalytic work, which requires a high degree of intellectuality and the constant application of the powers of concentration and deduction, requires young men, physically and mentally alert. Nevertheless it is to be noted that the principles of organization within this bureau are not different from those ordinarily applied in any office as far as the details of organization are concerned. In the military commission, on the other hand, rank and position must yield entirely to technical knowledge.

The importance of centralization and of allowing the greatest possible independence to the cryptographic and cryptanalytic services, which are to work in close cooperation with the intelligence service and the signal corps, can never be too greatly emphasized. Personnel placed under the higher staffs, more or less isolated from the central organization, is of very little value. Much better work is to be obtained if the men are allowed to work on the material, each independently and yet in a centralized organization.

The importance of having its own, rapid and dependable means of communication is also very great. A radiogram intercepted on some one part of the front may give the solution to a problem involving a very distant sector of front and should be cryptanalyzed there. It is also of great importance that all captured material, whether intercepted, captured on the field of battle, or obtained in other ways, should reach the hands of the central cryptanalytic officer as quickly as possible. To draw up instructions for that purpose, with indications as to what should be looked for, how it should be sought, where and how it should be sent, is one of the duties of the cryptographic military commission.

Finally, the following aims may be emphasized as desirable. They may be summarized from the works on cryptography which have been published since the war by eminent chiefs of military cryptanalytic bureaus:

(1) The technic of cryptanalysis and a good knowledge of it should be made the indispensable basis for all this work, both cryptography and cryptanalysis.

(2) Whenever possible, an examination in cryptanalysis should be required of all applicants for cryptographic positions of the higher grades.

(3) A maximum general knowledge of both cryptography and cryptanalysis, with the elimination of all unnecessary secrecy, should be given to the corps of officers.

(4) Training of and contact with civilians in the reserves who are to be called on, in the event of war, to serve either in the cryptographic or cryptanalytic service should be given the necessary attention.

(5) Attention should constantly be paid to the securing of cryptographic literature of all kinds.

(6) Plans should be made for cooperation with the directors of both our domestic and foreign policies, at least in time of war.

The expense of the maintenance of a permanent cryptographic bureau, both for cryptography and cryptanalysis, may be kept within very restricted limits. Aside from the problem of personnel, the only requirement is access to a suitable library containing only cryptographic literature and copies of the Swedish codes and dictionaries, as well as those of other countries which have been made public. Paper and pens are the only other type of equipment required; sound judgment and clear brains the only motive power.

As mentioned above, the selection of personnel should be based entirely upon personal qualifications. It would be as sensible to assign any person whatsoever to the cryptanalytic service as to assign such a person to become an artist. For cryptanalysis is an art, known as the "Art du decryptement" in France, "Dechiffrierkunst" in Germany, and the "Art of deciphering" in England. It has, however, been found that artillery officers are especially well qualified for this work. This may be merely a matter of chance or it may be attributed to their mathematical training, which is an important part of their schooling.

Pure theory has often been found to be more harmful than useful. Although inescapable, the theoretic aspects of cryptography must be constantly held in rein by the practical, or they may, as so frequently happened, lead the compilers of codes and ciphers straight into the treacherous waters of illusory complications. The most important qualification of the cryptanalyst may be summed up in two words: good judgment. To this must be added a mode of thinking which is at least to as high a degree synthetic as analytic.

The general advance in the knowledge of cryptography throughout the world seems to indicate a limitation in the future missions and possibilities of the cryptanalytic experts. This is not at all the case. The coefficient of error, which can never be entirely eliminated, is equally high in the majority of armies and becomes higher, the higher the degree of perfection attained by the cryptographic art. Much has been done; much more remains to be done. The unexplored field is very great.

If, despite its many faults, this work has succeeded in awakening a new interest in cryptography and the art of cryptanalysis, the author feels that he has been adequately rewarded. May the new disciples of this new entrancing work never forget that their highest duty to their country lies in spreading, not in concealing, the experiences they have gained. Only under those circumstances can fruitful cooperation exist, which is an indispensable essential for modern cryptanalytic work, in contrast to what was true of old-fashioned chamber analysis.

* * * * * * *

NOTE ON THE RUSSIAN CIPHER SYSTEM EMPLOYED ON THE EASTERN FRONT TOWARD THE END OF 1914

(See footnote 238)

[We may assume that Figl gives a correct description of the method, which I have condensed below. He also shows an example of one of the enciphering diagrams, which I give herewith:

Enciphering diagram

*	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ѣ	ю	я	ь	ъ	ы	й	і	*
3	31	61	81	79	57	35	12	56	46	74	37	41	89	43	45	47	97	65	32	59	24	39	38	86	13	84	23	85	62	17	54	58	14	3
1	31	21	81	79	42	56	72	26	83	27	37	61	89	43	28	23	97	13	29	59	36	32	38	73	63	24	64	85	41	17	25	51	46	1
4	15	37	21	64	31	17	67	25	49	69	18	23	35	93	59	86	52	13	46	89	74	98	28	47	72	42	45	24	48	87	34	65	39	4
5	86	92	52	23	18	97	36	13	46	67	54	71	19	14	65	27	93	85	16	79	12	58	76	48	83	34	26	74	62	38	37	29	81	5
6	25	31	17	42	38	13	41	61	23	45	89	15	84	75	48	54	34	73	14	53	37	24	64	18	28	12	95	57	93	78	82	76	27	6
7	41	64	84	43	92	53	85	34	67	71	27	26	46	49	24	58	31	75	18	23	98	29	62	39	42	51	95	65	17	96	13	91	94	7
8	12	56	82	74	13	38	96	54	61	37	83	26	49	68	39	65	57	16	23	95	48	31	78	17	59	73	14	72	98	52	41	53	69	8
2	73	86	31	93	42	56	21	62	19	47	75	61	32	59	28	84	14	71	35	91	87	69	16	13	25	76	89	38	64	94	95	83	29	2

In this diagram the letters of the Russian alphabet appear in the top line; the 2-figure groups within the 8 successive horizontal lines below it, are their cipher equivalents. The latter therefore constitute 8 cipher alphabets which are designated by the numbers 1 to 8 standing at the left in mixed order. This order is subject to change. Before enciphering a message the encipherer prefixes it with a single digit repeated 5 times, for example, 55555, 77777, etc., which indicates how many letters are *consecutively* enciphered in each alphabet. The encipherment is accomplished by enciphering the first set of letters (5, 7, etc., according to the indicator) by cipher alphabet 1, the next set of letters by cipher alphabet 2, and so on. After the 8th set of letters, which he enciphers by cipher alphabet 8, he returns to cipher alphabet 1, repeating in this manner until the entire message has been completed. If the encipherer in the course of his work decides to shift to a greater or lesser number of letters to be enciphered in each alphabet, he merely inserts the new indicator, repeated 5 times, just before the shift in grouping occurs, but enciphers the new grouping by the next alphabet in sequence, that is, without breaking the sequence in which the cipher alphabets are used. The cipher text is then sent in 5-figure groups. Gyldén, in footnote 170, says that later the cipher equivalents were increased in length, to include 3-figure groups or groups of greater length, but this is of no consequence. So much for the mechanics of the method.

Basically this system is but a minor variation of the ordinary multiple-alphabet substitution cipher with three serious weaknesses not inherent in the latter. First, whereas in the ordinary method one may vary the length of the key from message to message, that is, the number of alphabets may be varied from 2 to as many as one may conveniently handle, in the Russian system the number was apparently fixed, and was kept small, from practical considerations arising out of the nature of the enciphering diagram. Secondly, whereas in the ordinary method one may readily vary the sequence with which the different alphabets are brought into play in the encipherment of different messages, in the Russian system the sequence certainly remained the same for many messages until it was changed by what Figl, Ronge, and Gyldén term a "new key." Lastly, whereas in the ordinary method the encipherment proceeds monoliterally, that is, within the period or cycle a given cipher alphabet is used to encipher a single letter, so that the various alphabets are brought into play with successive letters of the plain text, in the Russian system the encipherment was polyliteral, that is, within the period or cycle several successive letters (up to 9) were enciphered by the same alphabet. For example, if the indicator is 8, it must often happen that a common word like "division", which has a "telltale formula", will be enciphered monoalphabetically, and such cases will afford easy places for the "entering wedge" in analysis.

The solution of traffic in such a system may be treated under two phases. First, when nothing is at hand except the traffic, consisting of, let us say, a dozen messages of fair length, all intercepted within a short time, and presumably in the same key as regards the particular cipher alphabets and the sequence in which they are employed. In such a case a straightforward detailed analysis based upon frequency tables will yield the solution. How long this will take will depend upon accidental or extraneous factors, which need not here be discussed; suffice it to indicate that in my opinion a solution should always be possible within 12 hours and might be accomplished within as little as 3 or 4 hours. This solution would yield the details of the enciphering and deciphering diagrams; that is, the arrangement of the cipher equivalents within the alphabets, as well, of course, as the sequence in which the alphabets are employed. If additional messages in the same key are intercepted they can now be read as rapidly as the legitimate recipients can read them.

Suppose that the key is changed. The change may consist in two things: (1) The alphabets themselves may be completely changed or (2) merely the numbers designating the alphabets may be changed. If we are confronted with only the second type of change, the solution is, of course, much easier than that discussed above. We are here concerned with the second of the two phases of solution referred to in the preceding paragraph. The alphabets are now *known* alphabets; only the *sequence* of their employment remains to be determined. This should take a cryptanalyst with a fair degree of skill only a few minutes to accomplish, even if he has only a small amount of traffic, and once more all messages can be read with ease.

A careful study of what data there are leads me to conclude that the second type of change in key was the one most frequently applied by the Russians, for example, when they changed keys daily. The first type of change, involving completely new alphabets, was applied quite infrequently. It is only two times that we encounter in the German Official History mention of "delays" in translating the intercepted traffic, and it seems certain that these cases represented times when the alphabets were changed. Also, by the same reasoning, we should be not at all astonished when we encounter cases in which the translation of intercepted messages by the Germans or the Austrians was accomplished with what appears to be a mystifying promptitude. These represent cases involving only a change of the sequence in which the alphabets were to be used.—*W. F. F.*]

○