THE INFANTRY SCHOOL
Fort Benning, Georgia

ADVANCED COMMUNICATION OFFICERS COURSE
1938-1939

MILITARY CODES AND CIPHERS--THEIR DEVELOPMENT AND USE

1st Lieutenant Thomas F. Wall, Infantry

TABLE OF CONTENTS

BIBLIOGRAPHY

Abbreviations	Text.
Glyden	"The Contribution of the Cryptographic Bureaus in the World War" by Yves Glyden. The work of an eminent Swedish cryptanalyst, translated by W. F. Friedman, Major, Signal Corps Reserve. This book represents scholarly considered judgment from a strictly cryptographic point of view. An invaluable source, and the only work of its kind in English. Footnotes excellent. A "must" book for military cryptographers.
Yardley	"American Black Chamber" by Herbert O. Yardley, war-time head of Military Intelligence Cryptographic Bureau, M.I.8; post war head of U. S. Central Cryptographic Bureau. Probably accurate but by no means an official publication. An excellent source for background and a study of methods. Captain Yardley didn't make a mistake for 375 pages. A now-it-can-be-told best seller mixed with history and cryptography. Excellent parallel reading.
Chief Sig. Off.	"Report of the Chief Signal Officer, 1919." An official source which unfortunately mentions codes and ciphers very infrequently.
Hart	"The Real War" by Liddell Hart. A standard and very worthwhile work by a fine historian. Tannenberg described to show, by inference, a command decision crystalized by military intelligence which was deduced from intercepted radio messages.
	"Signal Corps Bulletin, No. 101". Office of the Chief Signal Officer, September 1938. Excellent article on modern use of codes and ciphers, with several historical examples, written by Major W. F. Friedman, Signal Corps Reserve.
	"Cryptography and Cipher Writing" by Edward Koch, 1933. Useless.
	"A Manual of Signals". By Brigadier General Albert J. Myer. Useless
	"Manual for the Solution of Military Codes and Ciphers" by Colonel Parker Hitt, U.S.A. Published 1916, this book is very sound and a "must" book for military cryptographers.
	"Elements of Cryptanalysis." Probably the work of Major W. F. Friedman. Another "must" book.
Webster	Definitions of terms. Webster's Unabridged International Dictionary, and Encyclopaedia Britannica. Authority for references to limited number of English sources, Encyclopaedia Britannica

MILITARY CODES AND CIPHERS--THEIR DEVELOPMENT AND USE

1. INTRODUCTION.--It is necessary for the purposes of this monograph to strictly limit the subject matter. I presume that I have access to about ten per cent of the material available in English, yet the material available to me would have been sufficient for a twenty thousand word exposition. Collection of material should have included other original sources, particularly in French, in German and (the Renaissance writers) in Italian; selection of material should have been the work of an expert cryptanalyst; and, finally, the proper collation of material would have taken more time than was available.

In this monograph I have covered briefly:

a. Definition of terms.

b. Historical cryptography; military cryptography; the first cryptographic bureau.

c. The cryptographic background and pre-war preparation of the great powers.

d. A selected historical example of the effect of intercepted messages upon a command decision.

e. A study of cryptography on the Western Front.

f. American cryptography of the World War period.

g. Conclusion.

2. DEFINITION OF TERMS.--The cryptographic literature I have read contains a confusion of terms which no two writers seem to use in exactly the same way.

a. A cipher is a private alphabet or a system of characters contrived for secret writing; a cryptograph; broadly used to include all cryptographic material. (1)

---

(1) Webster

b. A code is a system of signals for communication, as in telegraphy; also a system of words or other symbols arbitrarily used to represent words or phrases for brevity or secrecy. (2)

c. Cryptography. The act or art of writing in secret characters; also secret characters or cipher. (3) Cryptographic is the proper adjective listed, but cryptographist is the only noun listed. Since there is no such word listed as ~~cryptographer~~, cryptanalyst, or cryptanalytic, I am taking the liberty of defining them in accordance with their usage in cryptographic literature.

d. A cryptographer is one who practices the art of secret writing; in a restricted sense, one who formulates cryptographic systems.(2½)

e. Cryptanalysis is the science of reading secret writings without prior complete knowledge of the system or key used by the cryptographer.

f. A cryptanalyst is one who practices the art of cryptanalysis.

g. These last three terms are used very loosely. There are references to "enemy cryptographers" in official texts, when, in accordance with the usage of most of the literature on the subject, "enemy cryptanalyst" is meant. The word decipher appears in the dictionary, but the word decode does not. Both are commonly used in English cryptographic literature. Encode and encipher are not listed but I have often seen them in use. I will attempt to use only the terms listed in standard dictionaries with the necessary addition of the terms ~~cryptographer~~, cryptanalyst, cryptanalytic, decode, encipher, and encode.

---

(2) (3)(2½)Webster

3. CRYPTOGRAPHIC HISTORY.--The art of cryptography is almost as ancient as letters. Probably before the first cryptographer had finished his "secret" message the first cryptanalyst tried to read the message. The secret writer probably thought his work could never be read without the key. After some early cryptanalyst did read the cipher (or code) the cryptanalyst probably turned cryptographer long enough to invent a "perfect" cipher. The secret is that the inventor of a cipher is nearly always sure it cannot be solved by cryptanalysis. Laymen generally feel the same way. Voltaire sneered at those who presumed to be able to read the secret writing of others; Caesar used a very simple substitution cipher. In fact, any bright school boy could have read Caesar's cipher.

Military cryptography is means to an end. The purpose of military cryptography is to facilitate command by making it impossible for the enemy to read certain communications, while the addressee, by means of a key, can read the communications. Successful military cryptography includes:

a. Selection of the cipher or code to use.

b. Prescribing methods of use.

c. Training of personnel to use it.

d. Constant testing of the system.

e. Constant supervision of the using personnel.

One point worthy of emphasis is that, when a tactical blunder is made, only those near-by are directly affected, while a cryptographic blunder may and probably will affect the cryptographic security of those on a distant battlefield who may, through ignorance or necessity, use the compromised code or cipher.

The Renaissance produced a cryptographic literature much of whicm is still classic. Following the Renaissance

little or no progress was made until about 1880 when two forces began to actively affect cryptography. Electrical communication placed a premium on messages in which the text was secret. The second force was the feverish struggle for military and diplomatic supremacy of the great powers. The World War itself so stimulated the cryptographic efforts of the nations involved that it would be safe to say that the four years, 1914-1918, changed cryptography from a desultory activity to weird combination of exact science and art.

The first cryptographic bureau that I can find a record on existed in Venice in the 15th Century. This bureau had two sections, one for cryptography and one for cryptanalysis. The ciphers used by the Venetians were superior to many used by major powers just prior to and during the World War, and the cryptanalytic methods employed disclose a keen scientific understanding of the fundamental problems involved. At the same time an equally effective bureau existed at the papal curia in Rome. Both of these bureaus leaned toward cryptanalysis, and even the personnel who devised cipher systems were first taught the structure of ciphers through the practice of cryptanalysis. This, according to Glyden, explains their success. (4)

4. CRYPTOGRAPHIC PREPARATION FOR THE WORLD WAR.--a. Germany had the most generally effective military machine in Europe in 1914. Cryptographic preparation had not been ignored but it was not very effectively carried out. The German mind, remarkable for its thoroughness and orderliness, is not the best type of mentality for work in a field where logic and orderliness must be combined with originality of method and intuition.

---

(4) Glyden, p 8

The Germans had three bureaus engaged in general cryptography prior to 1914. One was attached to the General Staff of the Army, one was attached to the General Staff of the Navy, and one was within the Ministry of Foreign Affairs. There was little or no cooperation between the Army and Navy, and the regulations of both forces prohibited cooperation with civilian experts. Neither of these bureaus had cryptanalysts worthy of the name; in fact, officers were assigned the task of devising safe cryptographic systems who had never, themselves, solved even the simplest ciphers. The cryptographic bureau in the Ministry of Foreign Affairs employed cryptanalysts to solve foreign cryptographic matter, but the bureau as a whole relied on clues obtained by secret agents rather than on pure cryptanalysis.

Summarizing, this is the case against the German cryptographic system as a whole:

(1) Lack of cooperation between bureaus.

(2) Failure to utilize the services of every able German cryptanalyst.

(3) Failure to employ skilled cryptanalysts to prepare the systems to be used.

(4) Failure to test their own cryptographic system by constantly pitting the best available cryptanalytic brains against it.

(5) Adoption of systems which possessed high theoretical safety from a mathematical point of view, but which, in service, were too complicated to use, or, when used, were so full of errors that the using personnel resorted to clear text messages.

(6) Failure, in time of peace, to select and train the personnel who were to actually use the cryptographic system in the field.

(7) Failure to properly train cryptanalysts to decipher enemy messages.

The degree of cryptographic preparedness seems to vary quite regularly in each country with the quantity and quality of the cryptographic literature produced. Germany had no great modern writers in the field of cryptanalysis. German writers concentrated on analysis of the theoretical safety of certain systems, and never considered the basis or framework upon which the systems hung. Quoting Glyden, "Without being guilty of underestimation, we can safely state that the authors of the German School after Kasiski (1863) 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." (5)

b. Most of the available data on Austrian pre-war preparedness comes from the writings of General Ronge, war-time Chief of the Austrian Military Intelligence Service and peace-time Chief of the Evidenz Bureau.

Steady progress was made from the beginning of the 20th Century, with cryptography generally leading cryptanalysis. Cryptanalysis was, however, materially aided by pre-war use of intercept stations which procured a mass of foreign material, and the desire on the part of the government to have this material deciphered caused a slow but healthy growth of the Evidenz Bureau of the General Staff. The Evidenz Bureau had acquired considerable skill in deciphering Russian, Italian, and Serbian material prior to the war, and had devised a fairly effective cryptographic system. Spies were effectively used to steal codes, cipher keys, and clear texts of messages. The Chief of Bureau, being himself a skilled cryptanalyst, understood the

---

(5) Glyden, p 14

importance of rapid cryptographic mobilization. Austria outstripped Germany by a wide margin in this phase of preparedness, chiefly because cryptanalysis was employed in conjunction with cryptography. (6)

c. Russia had no military cryptographic system worthy of the name. Peculiarly enough the Russian diplomatic service had a cryptographic bureau particularly well organized and capable of performing its mission. Prior to 1914 these Russian cryptanalysts successfully solved the Turkish, Austrian, British, and Swedish diplomatic codes. (7) In spite of this the ciphers recommended for war-time military use were so complicated and cumbersome that the using services either sent mixed text, clear text, or resorted to use of their pre-war cipher system. To complete the picture of fatal cryptographic unpreparedness, there was no central military cryptographic bureau and apparently no peace-time effort was made to teach the army as a whole the principles of cryptographic security. (8)

d. Pre-war Italy presents a sad picture of faded cryptographic glory. Italy possessed no modern cryptographic literature, and had neglected the Italian classics of the 15th and 16th Centuries. Their military cryptographic bureau, established early in the 20th Century, was headed by Colonel Felice de Chaurand de Saint-Eustache. Glyden speaks very slightingly of both the cryptographic and cryptanalytic work of this bureau, and classes Italy, Russia, and Germany as unprepared for war from a cryptographic point of view. (9)

e. Prior to the World War the British Intelligence Service was very little known, even to British statesmen. In fact, the British Intelligence Service managed to guard

---

(6) Glyden, p 21
(7) (8) Glyden, p 20
(9) Blyden, p 23

their exact organization so carefully that the truth about their cryptographic preparation is not yet available. There seem to have been at least four ~~or five~~ other cryptographic bureaus. The Army and Navy each had a well organized and highly centralized bureau. The Foreign Office and the Department of Criminal Investigation (Scotland Yard) each employed cryptanalysts and, in addition, in the case of the Foreign Office, skilled cryptographers. Whether or not a fifth bureau existed within the British Intelligence Service is a matter for pure conjecture. In any event, no agency on earth is, or has ever been, more expert at gathering, handling, and using information; therefore, it is safe to assume that a wealth of material was available for analysis and was probably analyzed. Furthermore, the Foreign Office and the British Intelligence Service have gone their separate ways on several occasions, so I would assume that both cryptography and cryptanalysis were well organized within the Intelligence Service itself.

Singularly enough there was no great modern literature in English on cryptanalysis. On the other hand it is evident that the French literature on the subject was extensively read, at least by the British civilian cryptographers. At the outbreak of the war these cryptographers were rapidly mobilized and skillfully organized, showing a thorough prior study of war-time cryptographic needs. (10)

f. Cryptography in France, 1880-1914, would be a very interesting monograph subject for an amateur cryptographer and French scholar, since most of the cryptographic literature of this period is in French. Six well organized cryptographic bureaus existed prior to the war in the Army, the Navy, the Ministry of Foreign Affairs, the Ministry

---

(10) Glyden, p 19

of Interior, the Ministry of Posts and Telegraphs and the Sûreté Générale. The so-called "Black Chamber" in the Ministry of Posts and Telegraphs intercepted, and turned over for analysis, a constant stream of material. Army and Navy officer cryptographers were trained under the civilian experts, and were organized as a joint board of ten members to determine military cryptographic policy.

The Fremch method of approach was quite distinct from that of the German school. In France cryptography was based on a study of cryptanalysis. Germans favored a purely mathematical basis for determining the resistance to solution of a cipher or code. The French constantly tested their proposed ciphers and codes by submitting them to friendly analysis. The Germans kept their proposed systems secret. The French entered the war with military ciphers and codes of known dependability and known workability. The Germans entered the war with no military codes and a military cipher system so complicated as to be unworkable. It was, in fact, filled with theoretical complications which actually helped the enemy cryptographers. The French encountered difficulties and discovered weaknesses in their cryptographic system during the war, but due to their careful pre-war preparation, and the wealth of personnel already trained, they avoided the most costly mistakes. (11)

g. United States. The bibliography of this monograph contains all of the source material in The Infantry School Library. A bibliography suggested by Encyclopaedia Britannica contains very few additional English works, except a number of technical papers by Major W. F. Friedman, Signal Corps Reserve, who incidentally wrote the article for the latest edition of the Encyclopaedia. In other words there

---

(11) Glyden, p 9.

does not seem to be a very flourishing cryptographic literature in the United States at present. When one considers that Hitt's Manual for the Solution of Military Ciphers is the earliest work listed (1916), one understands the statement of Yardley which follows:

"I quickly began to devour all of the books on cryptography in the Congressional Library. These were interesting but of no practical value.

* * * * * * *

At last I found the American Army pamphlet on the solution of military ciphers. This pamphlet was used as a text-book for a course in cipher instruction at the Signal Corps School at Fort Leavenworth. The book was full of methods for the solution of various types (of ciphers). The only trouble was that the types of cipher it explained were so simple that any bright school boy could have solved them without a book of instructions. I was at the end of the trail." (12)

Perhaps the best way to sum up American cryptographic preparedness is to recall that Herbert O. Yardley, an obscure telegraph operator and amateur cryptanalyst, was commissioned and selected by then Major Van Deman to head the Military Intelligence subsection, MI8. During the World War M.I.8 acted as the central American cryptanalytic bureau. Since Yardley claims to have solved the American diplomatic code just for practice while still a telegraph clerk, it would seem that our cryptographic preparation left something to be desired.

5. CRYPTOGRAPHY IN THE WORLD WAR.--In this section I will briefly describe:

---

(12) Yardley, p 20. (Col. Parker Hitt's book is not the one referred to. T.F.W.)

a. An important World War decision and its cryptographic background.

b. Cryptography on the Western Front.

c. Solution of a cipher.

d. American participation.

(1) A command decision, Tannenberg; Eastern Front, 1914 (refer to Chart No. 1).--The Russian mobilization was not complete when the Russian commander, Jilinsky, ordered an invasion of East Prussia. For dispositions see Chart 1 (a). On August 17, Rennenkampf crossed the frontier with eleven and one-half divisions of infantry and cavalry. After an indecisive battle at Gumbinnen August 20, the Germans withdrew, and on the same day Samsonov crossed the frontier with eight infantry and three cavalry divisions.

This news caused the German Commander-in-Chief, Von Prittwitz, to decide on a retreat behind the Vistula. However, when Von Prittwitz telephoned his decision to the German High Command at Coblenz, he was at once relieved, so his decision was never carried out. Von Hindenburg, new Commander-in-Chief and Ludendorff, new Chief of Staff were soon trundling across Germany, planning as they came, and wiring corps commanders to temporarily "go it on their own".

In the absence of other orders, the German Staff reinforced the German right (south) flank by moving troops from the German left (north) flank, thus initiating the strategy that was Tannenberg. (See Chart 1 b.) (13)

This German Staff decision, after the relief of Von Prittwitz and before the arrival of Ludendorff and Hindenburg, was influenced by the constant stream of Russian clear text radiograms intercepted. The authenticity of these orders and reports intercepted during the first few days of the

---

(13) Hart, p 122. Liddell Hart credits Lt Col Max Hoffman with giving proper weight to the Russian clear text telegrams and initiating these troop movements.

campaign was confirmed by air observers, cavalry and spies. The Russians were being slowed down by bad roads, lack of trains and supplies, and poor liaison between commands. Fortunately for the Germans, Ludendorff, whose preconceived plan coincided with the half-executed plan of the German Staff, confirmed everything. To emphasize the effect of intercepted messages on Ludendorff's decision, I quote Liddell Hart, The Real War, page 125: "Then on the 25th, intercepted wireless messages showed him (Ludendorff) the slowness of Rennenkampf's movements, and he began to think that he could use the XVII Corps (Mackensen) also, leaving only the cavalry to watch and hoodwink Rennenkampf." Ludendorff did use the XVII Corps, and enveloped both flanks of the southern Russian army commanded by Samsonov. (See Chart 1 c.) As a result, Tannenberg was a complete German tactical victory, and partial strategic exploitation halted a serious Russian threat at a critical time.

I have attempted to show that the basic German decision which made Tannenberg possible was, to a very large extent, influenced by intercepted clear text Russian radio messages. The Germans would not have had such a thorough knowledge of the Russian dispositions if even elementary ciphers had been used since the Germans had no organized cryptanalytic service in the field at the time. That came later. Rather than praise the Germans one must blame the Russians, who sent armies into the field with an ineffective cryptographic system operated by incompetent cryptographic personnel.

(2) The Western Front, 1914.--Since I am unable to find another suitable example of a specific command decision being influenced by cryptographic success, I have chosen to discuss generally the cryptographic work on the Western Front.

We have already noted that the French and British far outstripped the Germans in cryptographic preparedness. As long as the Germans were able to use their own telegraph lines there was very little suitable cryptographic material intercepted by the Allies. With the invasion of Belgium and Northern France the number of radio messages increased, but the French intercept stations, located principally in the border fortresses further south, were out of range. The French at once converted many of their field radio stations to interception service with considerable success.

At first the Germans laboriously and doggedly enciphered everything, but the time consumed in enciphering, transmitting, and deciphering was excessive, sometimes as much as twenty-four hours per message. This was partially due to poor cipher clerks and radio operators, but an even more important fault lay in a cipher system so complicated that a mistake of one letter made decipherment almost impossible for the average clerk. Soon some corps started sending clear text or mixed text and the French cryptanalysts were able to start the work which, on October 1, 1914, resulted in the complete analysis and solution of the German military cipher. From that time on a change of keys only cost the French experts a few days' work, and when the Germans changed systems on November 18, 1914, it took the French cryptanalysts exactly three weeks to read the first cipher. (14)

Meanwhile the French and British used telegraph almost exclusively. Numerous codes and ciphers were used for specific purposes, ranging from carefully guarded two-part codes for strategic messages to simple ciphers in lower units. In 1915 stabilization on the Western Front had

---

(14) Glyden, Chap. 2, p 28

enabled the German Signal Corps to use safer methods (wire) of transmission and the value of the decrypted messages decreased.

Let me emphasize here that close cooperation between the French and British in cryptography and cryptanalysis made possible the excellent results achieved. Moreover, the Allies never halted their drive for cryptographic security. On the other hand the Germans, starting late, with few previously trained cryptanalysts, never caught up. As the Germans switched to codes and a few improved ciphers in 1916, they met a vastly improved Allied cryptographic organization in which skill could largely replace the luck of 1914.

(3) How the first German cipher was solved.--On the subject of clear text messages, Glyden says: "Clear text messages must not be used no matter how safe such telegrams may appear to personnel unacquainted with methods used in cryptanalysis."(14.1) In searching for an example of the method by which a cryptanalyst actually uses a clear text telegram, I found that a very short clear text radio "WAS IST CIRCOURT?" was intercepted, probably in September, 1914, by the French. It was turned over to a bureau headed by Major Cartier, later French cryptographic chief and which included the skilled cryptanalysts Olivari, Freyss, and Schwab. First they sought the probable reason for the message being sent. They found that on a certain map, known to be in German hands, Circourt was abbreviated "C". A previously intercepted radio from a point also near Circourt was available. Using the "Bazeries" or intuitive method, these cryptanalysts guessed that the preceding (and also very short) radiogram was an order or report involving the word Circourt. The assumption was correct, and the first complete breakdown of the order of letters of the German cipher key phrase followed on October 1, 1914.(14.2)

(14.1) Glyden Page 41 (14.2) Glyden Page 35

It should be remembered, however, that these cryptanalysts already knew the type of cipher probably used and that they had previously been able to partially decipher many messages. From this point on, however, the French read German ciphers as easily as the Germans themselves. Meanwhile the French cryptanalysts were gaining a very intimate knowledge of how certain German commanders varied the rigid German phraseology of command, and the errors that certain cipher clerks were apt to make. With these aids a new German key was often solved in from one to three days and a whole new system was actually solved in three weeks.

(4) American mobilization and participation.--Amid the general reorganization and expansion which took place when America entered the war a central cryptographic bureau was formed as a Military Intelligence subsection (M.I.8). Major General Van Deman, retired, was the Military Intelligence Officer responsible under the Assistant Chief of Staff, G-2. As previously noted, this bureau was forced to start practically from scratch. Captain Yardley, who was selected by then Major Van Deman to head M.I.8, organized it into sections as follows:

(a) Code and cipher compilation.

(b) Communication.

(c) Shorthand (solution of intercepted shorthand documents).

(d) Secret-ink laboratory.

(e) Code and cipher solution (cryptanalysis).

Later a separate section was organized to devise safe communication systems for the exclusive use of Military Intelligence personnel, and to instruct agents in secret communication. (15)

---

(15) Yardley, p 47

Initially the lack of a pool of trained cryptanalysts was a most serious obstacle, which, quoting Yardley, was finally overcome with great difficulty: "Judging from the letters I found in the files of the War College, nearly everyone in the United States had dabbled in ciphers... I quickly selected a few scholars who appeared to have a superficial knowledge of ciphers, and ordered them commissioned... Here was a problem (cipher solution) not found in the classroom and not many of them would succeed. Scholarship, I suddenly discovered, was nothing more than an ability to absorb learning. These scholars were faced with a quite different problem, for there was not a great deal of learning to absorb. They would be obliged to make their own discoveries. For this reason most of them were dismal failures." (16)

This statement is reinforced by the opinion of Glyden: "...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... In reality there is no science or profession which is particularly suitable as a recruiting field for cryptanalytic experts... For instance, in France the four most expert civilian cryptanalysts were a paleontologist (Painvin), an archive research worker, a criminologist and a philologist,..." (17)

Soon after M.I.8 was organized, the British called the attention of our War Department to serious weaknesses in the War Department code in use. Yardley says that his investigation revealed (1) that a code book had been stolen in Mexico in 1916, and that a photograph of the code was reported to be in German hands, and (2) that an analysis of

---

(16) Glyden, p 38
(17) Glyden, p 19

the code by cryptanalysts in M.I.8 revealed that, due to poor technical construction, the code could have been easily solved in any event. Work was at once initiated on a new War Department code.

Meanwhile the school for cryptanalysts was successful to a limited degree. The most promising students were sent to France, but only a few were capable of independent work. Yardley warns that training, while necessary to give the cryptanalyst his basic knowledge, does not guarantee ability to later solve new problems. One of the early students (18) whom M.I.8 sent to France did, by solving for test purposes the ciphers used by the Expeditionary Force prior to the Saint Mihiel Offensive, prove to the Army Staff the necessity for a change of system.

In addition to the code and cipher compilation section in Washington, an additional section was organized in France in January 1918. Initially the personnel working on code and cipher compilation consisted of a captain, three lieutenants, and one enlisted man. After several changes in personnel (two of the lieutenants were transferred from this section to take charge of the message center sections of the First and Second Armies) the section at the close of the war consisted of a captain, a first lieutenant, two second lieutenants, and three enlisted men. These men actually devised, printed, and distributed 80,000 copies of nineteen different codes ranging from a 30,000 word staff code to simple two and three letter codes for front-line use and other special uses. (19)

No data is available to show whether the men engaged in formulating these codes were trained cryptanalysts, or whether the codes were ever submitted to friendly

---

(18) Name of cryptanalyst not available
(19) May have included ciphers; Chief Sig Off not explicit

Century American authorities have contributed anything of importance to our cryptographic literature: Hitt, Friedman, and Yardley. This would seem to indicate little or no national interest in the subject. I personally know only two line officers who are amateur cryptographers.

b. Anyone can devise a cipher system or a code. Only a skilled cryptanalyst can tell whether or not the system is worthless.

c. In 1914, France led the world in cryptographic preparedness, chiefly because of:

(1) Effective central bureaus working in close cooperation.

(2) Wide civilian interest, denoted by the number of excellent French books dealing with cryptanalysis and cryptographic history.

(3) A system of training officer cryptographers under the recognized experts, which, in time of war, accomplished two things: (a) these officers formed a pool of trained cryptographic executives, and (b) the basic theory of cryptographic security was understood thoroughly by a few officers in every grade and in every organization.

(4) The French systems of ciphers and codes were inherently flexible and were designed and tested by cryptanalysts who worked with a background of basic theory and sound practical experience.

(5) The French not only tested the effectiveness of their system from a cryptanalytic viewpoint, but in maneuvers, tested its practical workability. (25)

Even this careful preparation did not immediately lead to unqualified success. The French were forced to make many changes after August, 1914, due not only to a close

---

(25) Glyden, p 11

(4) Trained cryptographic personnel must be present in every command echelon.

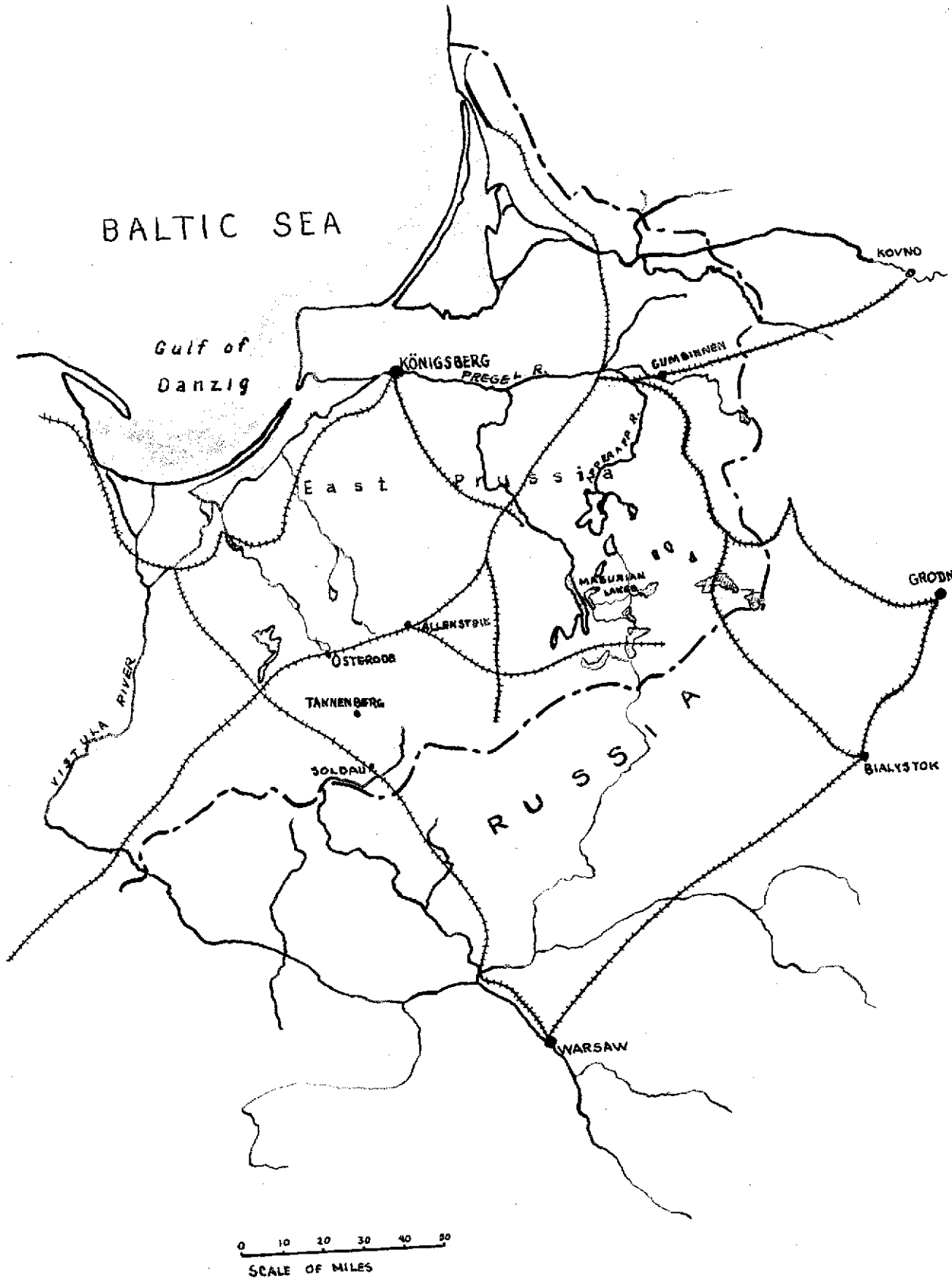
(5) All cryptographic personnel must work in close cooperation; civilian bureaus, military bureaus, intercept and goniometric stations, monitor services, espionage and counterespionage services. These services should not exist as water-tight compartments but should function as a team under intelligent leadership.

g. The enemy military cryptanalyst will rarely be able to do timely and effective work in breaking down our codes and ciphers unless we do part of his work for him by relaxing our efforts to maintain our cryptographic security.

h. Only by constant cryptanalysis of every bit of available material, whether it be a projected system of our own or foreign material made available by some means of interception, can we hope to attain cryptographic preparedness for a successful war against a first class enemy.

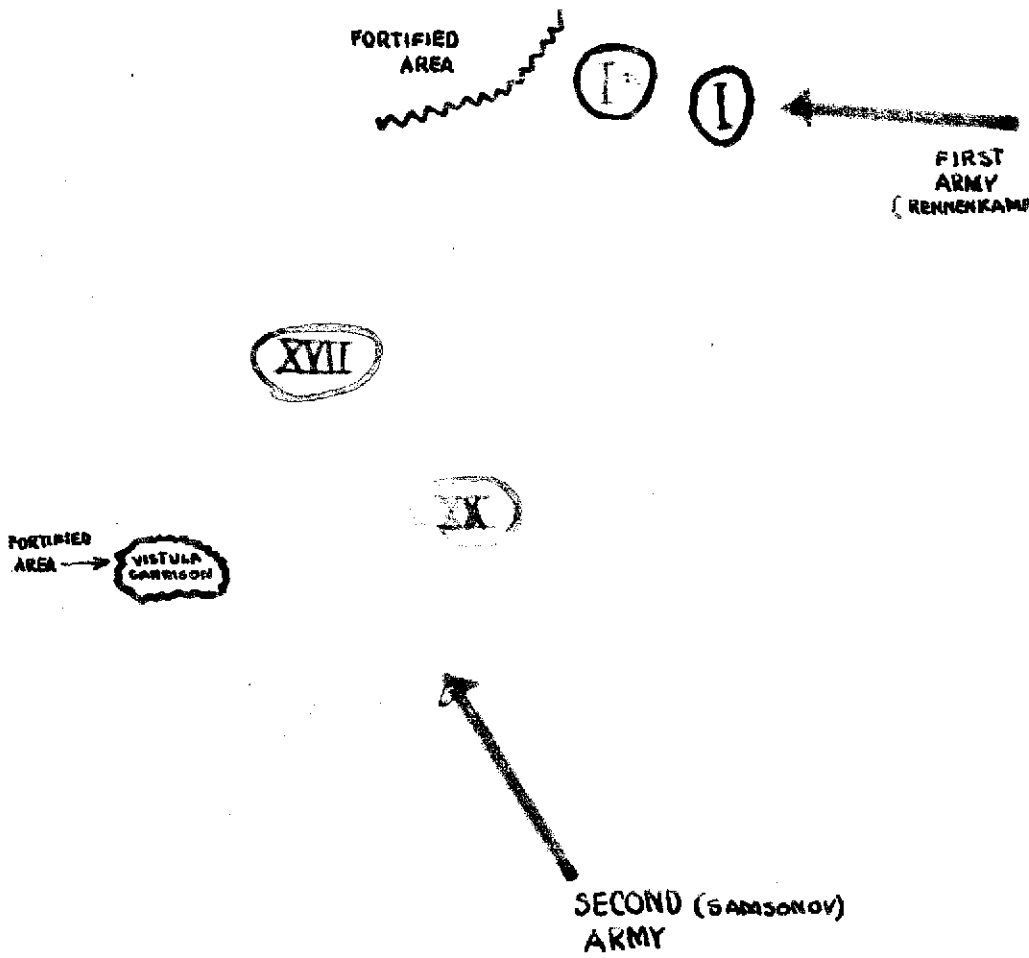
i. Cryptographic security is a negative means of defense, a form of camouflage. Cryptanalysis and its associated services may, on the other hand, help lift the fog of war and make sound decisions easier for the commander to reach.

In conclusion I quote Major William F. Friedman in Signal Corps Bulletin No. 101, and indirectly, General Cartier, wartime head of the French cryptographic service who said: "The interception and solution of enemy messages is indisputably superior to all other means of securing intelligence."



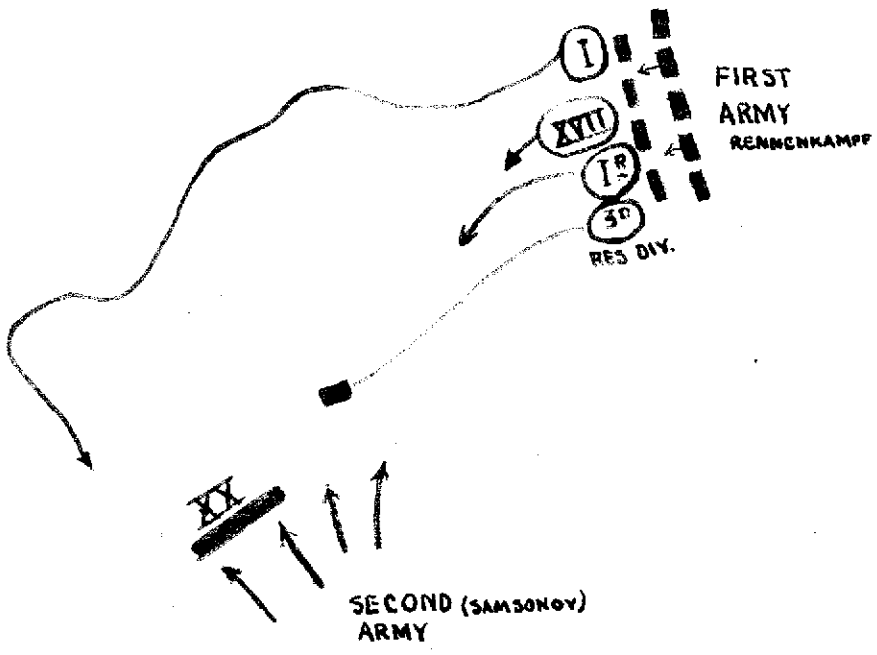
SKETCH No. 1.

THE BATTLE OF TANNENBERG
Strategical Map



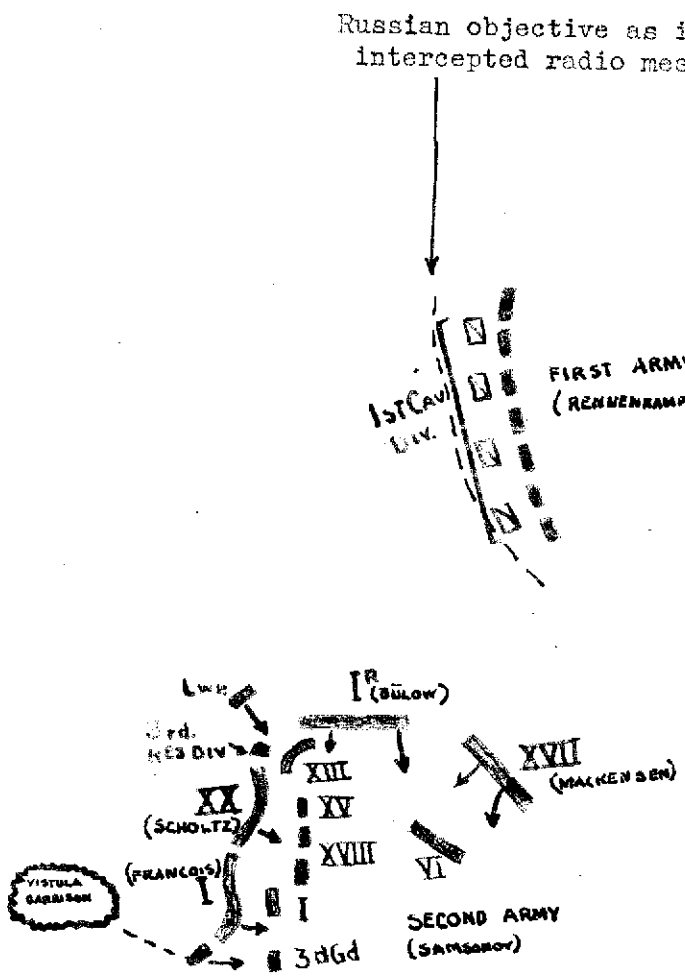
SKETCH No.1a.

RUSSIAN PLAN - BLUE
German Concentration - Red
August 17, 1914



SKETCH No. 1½.

GERMAN RETIREMENT AFTER GUMBINNEN
Samsonov's Advance
August 25, 1914



SKETCH No. 1c.

DISPOSITIONS, August 27, 1914
A double envelopment