Cryptanalysis in the German Air Force

BY OBERLEUTNANT WALDEMAR WERTHER

~~*Top Secret*~~

The report from which this article is taken was prepared after World War II at the request of an Army Air Corps team interrogating former Axis COMINT personnel. The extract is published here for its general interest to readers of the Journal.

1. A SHORT HISTORICAL SURVEY OF THE DEVELOPMENT OF THE EASTERN CRYPTANALYSIS GROUP OF THE GERMAN AIR FORCE

During the period of preparation for the establishment of the intercept equipment of the Air Force in 1936, the first State employees intended for cryptanalysis (who were all of them civilians up to the outbreak of the war) were sent to the permanent intercept posts of the Army in the East for the purpose of basic training. The results of this training were unsatisfactory because the Army was reticent in releasing even the most elementary information, and furthermore, because the individuals sent lacked in most cases the necessary qualifications for their work; the personnel officials made their selections on anything but a proper basis, and appointed many persons who turned out to be completely unsuitable for the work of a cryptanalyst. The creation of a capable and successful cryptanalytic group was accomplished only in the course of the following years of tiresome work, without outside assistance, and through an internal development achieved by dropping numerous unsatisfactory elements.

In the summer of 1937, four cryptanalysts were working on Soviet traffic at the Cryptanalytic Bureau of the Air Force (Chi-Stelle). The other Eastern powers were either treated very superficially, largely as a side issue by our Soviet section, or not processed at all. The cryptanalytic groups of the outstations of the Air Force Intercept Service (cover name: "Radio Weather Receiving Stations") also consisted of a few poorly trained and often incompetent workers. A worth-while organization for breaking new systems was developed only at the cryptographic bureau. The outstations were barely able to decode the encoded messages with the code in front of them.

At the outbreak of the war in 1939, the cryptanalytic groups both in the central office and in the outstations had grown to about 10 men each, and they were included in the newly established intercept companies. The training of the individual analyst was continuously improved through conferences, short training courses, and exchange groups of key men for instruction purposes.

During the occupation of Eastern Poland in the fall of 1939, and during the Winter War in Finland (1939–40), the best men from the outstations were recalled to the Bureau, because the outstation cryptanalytic groups had proved unable to process accurately and quickly enough the current and excessive material. Moreover, a group of mathematicians (made up of about 20 men without language training) was employed at the Bureau during the Finnish Winter War, and these later formed the nucleus for work on the additive systems.

At the start of the Eastern Campaign, Section E–1 of the Cryptographic Bureau (later the Cryptanalytic Section of the 353rd Regiment) was increased to about 40 persons, and during the course of the war to about 90, of whom some were women. The strength of the outstations (later the cryptographic section of the evaluation companies) increased to from 40 to 60 men, women being employed only in exceptional cases.

The intercept companies with the individual air corps ("corps companies" for short) also had small cryptanalytic groups, but they unfortunately had to be staffed with poorly trained personnel, who because of their limited field of work stayed at a low professional level—although their results are by no means to be underestimated.

In the last months of the war, a part of the less qualified personnel was turned over to combat units.

Although at the beginning of the war, the focal point of the work was unquestionably in the cryptographic bureau and the project of combining all cryptanalytic personnel in a central office inevitably kept cropping up, the cryptanalytic sections with the Air Commands went on developing as the war continued, and thanks to the regional systems of the Soviets found themselves in a position to handle the material coming from their own fronts without assistance.

Section E–1, on the other hand, kept losing significance, and fell to the level of an archive and organizational relay point, although it had in its command an excellent staff of cryptanalysts. Its only remaining specific assignment was the processing of material which did not admit of regional processing. But finally, after combined work on this material had been carried on for a time by the air force and/or the army, the processing, which had become useless, was given up and Section E–1 lost its last particular assignment.

2. SOME SUGGESTIONS REGARDING THE IDEAL FORM OF ORGANIZATION

The attitude to be taken on the problem, "Centralization or Decentralization," is determined by the present characteristics of the Soviet cipher traffic (strong differentiation and regional division of cryptographic material).

In the case of centralization, all otherwise unavoidable duplication of work could be obviated, and the personnel could be more logically used. But the disadvantages would be much greater, so long as, owing to the length of the Eastern front, it remained impossible to carry on radio reception at one point. The late arrival of the raw traffic at the central point, due to the insufficient and partly interrupted communications facilities, causes it to lose its timeliness. Moreover, with every transmission of messages by teleprinter, additional sources of error appear which, as experience shows, can hinder the work and lower the value of the cipher material. Lastly, the absolutely essential contact between intercept operator and cryptanalyst is completely interrupted.

For this reason the regional concentration of cryptanalytic personnel in the air fleets for independent processing of their own front sectors can be considered, in fact, as the most satisfactory solution. A small working staff exclusively for questions of organization and training would have had to be formed from the extensive cryptographic section of the regiment; all the other analysts would have found more profitable employment with the air fleets.

Any further subdivision of the cryptanalytic forces, however, is not advisable, and should be avoided except insofar as there may be detached companies with special assignments (e. g., long-range fighters or air defense).

3. ORGANIZATION AND WORKING TECHNIQUE OF A CRYPTANALYTIC SECTION.

a. The Cryptanalytic Section of an Evaluation Company

In this chapter the organization and working technique of the cryptanalytic section of the evaluation company of an intercept battalion will be sketched.

Everything said here is essentially valid for the cryptanalytic section of the intercept regiment (formerly E–1 of the Cryptanalytic Bureau of the Air Force), as well as for the small cryptanalytic groups of detached companies with special assignments.

The cryptanalytic section makes up a platoon of the evaluation company. The head of the section is, when possible, one of the company's officers (Wachoffizier). The prerequisite is, however, that the head of the section be an outstanding specialist, and the question of rank plays but a minor role in this case.

b. The Chief of the Cryptanalytic Section (Chief Analyst)

He is the soul of the whole section. The extent of training, pleasure in the work, and success depend on him. If he cannot continually show proof of his outstanding professional abilities, he soon loses the respect and confidence of his men. Experiences with officers who had

to assume direction of a cryptanalytic group without, or with insufficient, professional knowledge were always thoroughly disappointing. For mere organizational activity (assignment of personnel, arranging work schedules, etc.) without actual professional knowledge leads to constant wrong decisions and has a most harmful effect.

All cryptanalytic work is a matter of trust; a man cannot be forced to decrypt, and the actual amount of work done cannot be exactly measured, since unfortunately, the amount of work spent on cryptanalysis does not always bear a direct relationship to the success achieved. For these reasons, if for no others, the chief must be able to judge his colleagues not only professionally but also as to character.

By means of daily, even though short, conferences the chief must be in a position to be able to follow continually the work of every individual man, in order to be available with advice and assistance when the inevitable stoppages occur. In such conferences, moreover, current organizational ills and desirable transfers of personnel will become evident.

Particularly difficult problems are handled personally by the chief analyst with the assistance of especially good troubleshooters. He is the man who is always there when the wagon gets stuck in the mud; once it gets going again, he can simply turn his attention to new difficulties and leave further work on the old system to his colleagues.

Because of security, the work of the cryptanalyst must always go unrecognized by the outside world. It is all the more the responsibility of the chief analyst to encourage his colleagues by just praise, and to see that the accomplishments of his people are appropriately valued by the "higher-ups" (say, at inspections).

c. Work Shifts

During the war, the personnel of the cryptanalytic section worked on two (early and late) or three (continuous) shifts. The exact division of time depends on the amount of work and the size of the space available, and must be adjusted to new conditions rather frequently.

The assignment of personnel to the shifts takes particular care, because the abilities of the members of the shift must be carefully balanced.

d. The Shift Chief

The shifts take care of the current reading of traffic and the simpler decryptions. The organizational head of the shift is an experienced and responsible man, who as such is responsible for the entire process on his shift. He divides the work coming in in accordance with the instructions of the chief cryptanalyst, and must be able to judge the difficulty of the work processes in order to recognize and adjust over-

or under-loading of his colleagues. Since his organizational duties leave him little time for regular cryptanalytic work, and a long term of duty would tend to make him become a bureaucrat, it is desirable from time to time to "change the watch". It is the duty of the chief cryptanalyst to educate his men so that they see in the assignment as leader of a shift no particular "social advancement" but only a temporary, albeit honorable position. The change of the leader of a shift is neither a punishment nor a sign of lack of confidence, but merely aims at preserving the usefulness of the individual as a worker.

e. The Cryptanalyst-Specialist (Trouble-shooter)

For rush problems or especially difficult problems the chief analyst calls on particularly capable and reliable analysts from the shifts. Generally they work only on the day shift and are continually in closest contact with the chief analyst. These specialists are given more or less freedom with regard to working hours and length of working period,—insofar, of course, as inevitable military demands permit.

The continual change of personnel of the specialist group makes it possible (1) to employ specially capable men in their special fields; and (2) to raise the level of training of the individual by appropriate distribution of the work.

Specialization on the part of the individual cannot be avoided. In and of itself it is desirable. But care must be taken that this specialization is not allowed to become one-sidedness, so that the worker loses his necessary perspective.

f. The Clerical Force

The untiring efforts of a strictly trained clerical force are essential because of the excess of paper and the danger, which springs therefrom, of an "editorial-office order." The force consists of one or two workers, who if possible should have at least a minimum knowledge both of language and cryptanalysis, so that they do not manage, because of their ignorance, to do more harm than good. The duties of the clerical force are the following:

Presorting of the message material received.

Assembling the material by nets on the basis of message designation (net number, breaking of call signs) by the traffic analysis section.

Assembling by systems on the basis of known indicators and other characteristics (recognition books of the cryptanalysis section).

Sifting out of the non-pertinent messages from other fronts and branches/offices of the armed forces and forwarding these to the appropriate offices, or destroying them.

Filing material which cannot be currently read until work on its solution can begin, or until the system has been solved.

Transmission of the decrypted material for exploitation (message archives).

Registry of secret papers, teletypes and other material.

In addition to this work, the clerical force can be called upon to do statistical work when necessary.

g. The "Gadgeteer"

It appears advisable to have a worker in each cryptanalytic section who can make the various aids for additive-encipherment solution, such as sliding tables, drum systems, codes, and so on, in simple and useful forms, and who is always available. By this specialization of one ingenious man much time can be saved, and the neatness and usefulness of the gadgets can be assured.

4. MESSAGE ANALYSIS

a. Presorting and System Recognition

The already marked message material comes from traffic analysis to the cryptanalytic section and is there sorted and identified, first by the clerical staff and then by the analyst, according to the available material for recognition of the codes.

b. Decoding

Insofar as the necessary material is available, the message is immediately decoded, so that there may be no unnecessary time lags, such as may seriously reduce the value of the message.

c. Analysis

Unclear material, and material which cannot be directly read (that is, for which the code has not been broken) is continuously analyzed by means of all sorts of statistical studies.

d. The Break-in

As soon as the material in a given system has accumulated to a point which promises success, attempts are begun to break into it.

e. Analysis of the System and Reconstruction of the Basic Code

As soon as a sufficient number of groups have been determined, attempts are begun to reduce this usually relative material to a true basic, i. e., to reconstruct the original form of the Soviet code. At the same time the recovered key sequences must be compared and collected in a unified system.

f. Further Treatment

By reworking the material returning to the cryptanalytic section after exploitation, the codes are extended by additional recoveries. During the first years of the war, the break-in could be considered as the essential crypto-technical process, but lately the emphasis has shifted more and more to a processing of the system and reconstruction of the codes.

5. SOME GENERAL WORKING PRINCIPLES

a. Team Work

The most fruitful form of cryptanalytic work is the collaboration of a few mutually sympathetic analysts, who naturally get together on the handling of more difficult problems without direction from above, and who supplement each other in their intellectual make-up. Alongside the precise, inexorably logical and constructive systematizer with perhaps only a fair knowledge of the language, there are the superior linguist who may not be so good at putting two and two together and the sensitive artist whose strong point is intuition. When one of these tires and begins to have his doubts, the common work is carried on, nevertheless, by the impetus of the others. Discussions bridge gaps in the ideas of the individual, and arguments crystallize correct knowledge and break down unclear and botched ideas. In short, the problem is illuminated from all sides.

b. The Space Problem

For this reason the demand which is sometimes heard for individual rooms as the ideal, in order to assure quiet and intellectual concentration, is not sensible. On the other hand, a certain spaciousness of quarters is necessary for the work. The rooms must be large enough so that the workers do not interfere with each other, and that big heaps of message and code material do not pile up because of lack of space, forcing the workers to hunt laboriously for the material they need at the moment, with consequent loss of time. Care must be taken in particular to have extra sorting tables and sufficient space for storage. The disciplined quiet of an intellectual institution must be guaranteed in the interest of the work, even though brief but quite necessary recesses turn the serious room into a jovial gossip-shop.

c. Statistics

The statistics are to the cryptanalytic expert at once the essence and the chemical analysis of the message, and the most essential aid in his work. A careless count can be worthless, leading to false deductions, and thus seriously delay the course of solution. For this reason the use of assistants who are employed on the basis of their previous train-

ing and limited intellectual penetration, as "mere statisticians" is extremely dangerous and objectionable. Each cryptanalyst must be required to make the necessary statistics for his own work. The processing of very difficult and extensive systems, e. g., superencipherment with long keys, which requires weeks of mathematical and statistical work, is, of course, an exception.

d. The Responsibility of the Processor

Each worker is bound to process his message conscientiously to the point of readability, and to add his initials when he has finished, in order that the translator and exploiter, as well as the leader of the shift, may direct inquiries to the right person. The processed messages are collected and quickly checked by the leader of the shift or some specially designated person, and then turned over to Content Evaluation for translation.

e. Message Translation

As long as the majority of personnel in the Content and Final Evaluation sections do not know the language well enough—and that, unfortunately, was the situation except in the Regimental Evaluation Unit—all messages solved must be translated.

At first, analysts were made responsible for the translation of their own messages. This procedure, however, proved to be most impractical, for a large part of the cryptanalytic personnel did not have a good enough knowledge of the language to make a satisfactory translation of the difficult and partly garbled message texts.

As a result, mediocre cryptanalysts with very good language ability were gathered together into a special translation group. Working under Content Evaluation they handled all solved material and could be developed into good translation specialists and at the same time used as assistant evaluators. Over and beyond that they became something of a check on the work of the cryptanalytic section.

f. Regarding Allocation of Personnel

Each cryptanalyst should handle the most advanced material and problems that he can—without too much loss of time, of course. That does not, however, exclude the possibility of having even the best cryptanalyst, during periods of mental fatigue, quietly take over simple and primitive work. Generally, however, it is better that a first-class individual should not carry out a system to its finish, but after clearing away all difficulties should turn it over to his less capable comrades and thus again be available for more difficult work.

g. Generally Understandable Individual Work and Notes

In the processing of a system, all essential intermediate information must be set down in writing, and in such an understandable form that in the event of the worker's unexpected absence another man can take over without loss of time. For this reason, if for no other, generally applicable forms and symbols have been introduced for various processes (e. g., summaries of statistics, determination of superencipherment systems, etc.) in order to assure the general understandability for all colleagues of all personal notes.

h. Use of Female Personnel

While a man works for the job, a woman works for a person. Her productivity depends, therefore, much more than does the man's, on released sympathetic or antipathetic impulses. The performance of female workers was therefore dependent on the attitude of the chief cryptanalyst, the other military authorities, and the general living conditions.

Though a goodly number of intelligent women and girls showed good average results, working together and particularly living together under war conditions created an atmosphere which could hardly be called serious and intellectual. Undoubtedly purely male organizations showed better and more substantial results.

i. Military or Civilian Personnel

All cryptanalysts are of the opinion that civilian control would have had a positive effect on results. Because of the military form of life, part of the personnel's energies were diverted into completely useless paths. Thus, for example, military training claimed valuable working hours, but could not turn the mass of cryptanalytic personnel into really well-trained soldiers. Unfortunately, too, there was always very great opposition when recommendations were made for the promotion of meritorious cryptanalysts. The cognizant military authorities consistently—and not without justification—opposed promoting those nominated, because their military bearing, as well as their level of training, left much to be desired. Thus it was not always possible to reward cryptanalysts properly for outstanding performances.

6. THE CRYPTANALYSTS' TOOLS

a. General Aids

In the course of the continuous development of military language the good linguist daily encounters unknown words, expressions and abbreviations. In this case, technical dictionaries, lists of abbreviations, and training manuals of the enemy render, generally speaking, good service. But since the editing of such special aids usually takes a long

time, the cryptanalyst is obliged to help himself: current language problems and obscurities are noted on paper and cleared up at the next opportunity (as by interrogating intelligent prisoners). The interrogation officer of the Air Force is used continually, insofar as there are no other more favorable sources in the vicinity (such as a P/W camp) which make independent steps more convenient.

Net diagrams, callsign interpretations, and D/F results are used not only by the clerical force, but also by the individual worker in identifying the encrypted material.

Maps, lists of place names, and time-tables simplify the break-in and working out of the material. Situation maps and lists, tables of aircraft, type lists of all kinds, and military-unit and name files all serve the same purpose.

b. Special Tools

In working on a country for a long time the classical language statistics (monographic, digraphic, and trigraphic frequencies, etc.) drop into the background. The few rules of thumb which are still used become general property.

Novices and less-sure linguists have used lists, partly prepared by themselves, in which characteristic expressions are analyzed. Sometimes, these "crib-lists" have served a good purpose, but they are looked down on by experienced analysts.

The compilation of a vocabulary from the multiplicity of reconstructed and a few captured code books to form what we may call an "ideal code book," proved to be particularly useful in filling out partial recoveries. Such ideal code books were published a number of times during the war.

In the course of the years, some twenty statistical procedures have been developed, most of which have been used for current operations.

The archives of previously read messages are of great value as visualization material in work on new systems from known nets and in further training of cryptanalysts.

Daily summaries in the form of leaflets or card files on the occurrence of individual systems, on the relationship between systems on the one hand, and call signs, address and signature groups, place names, indicators, characteristic headings and characteristic message construction on the other, complete the list of aids for the cryptanalyst.

c. Exploitation of Captured Material

Although the German Army intercept service captured a great many codes during the advances in the East, the amount of captured material in the Air Force (partly because of the more extensive front) was insignificant, so that no reduction in the work load was noticeable. A

majority of the captured material was either well out of date (during the first days of the War in the East, for example, codes were captured dating from the year 1935) or already superseded because of compromise. Moreover, air-ground tables from shot-down aircraft could very seldom be exploited, because of the short effective period of these tables (usually only one mission).

The transmission of captured aviation codes from intercept units of the army and the intercept liaison officers of the navy staffs and other flying organizations was generally assured.

Sometimes, also, captured orders containing superencipherment instructions for systems still in use were of great value, since they gave a clear insight into the structure of the system in question.

7. COOPERATION BETWEEN THE CRYPTANALYTIC DIVISION AND OTHER PROFESSIONAL GROUPS

a. Cooperation with the Other Groups of an Exploitation Company

A close connection between operators and cryptanalysts has always proven very fruitful. Frequent conferences give the cryptanalyst valuable hints for his work. Knowledge of the quality of the individual operator, the good points of his work or his characteristic mistakes saves the cryptanalyst from many blind alleys. Especially when attacking new systems, it is most important to be able to evaluate the material at hand on the basis of the abilities of the receiving operators. Occasional talks, in a popular vein, on cryptanalysis and the value of perfect message material, given the operators by the chief analyst, had a decidedly positive effect on the zeal of the radio shifts.

The messages are reviewed and marked by the traffic analysis section before their processing by the cryptanalysis unit. Discussion with the traffic analyst can often provide the cryptanalyst with useful hints in individual cases; on the other hand, the cryptanalyst is in a position to aid the traffic analyst in picking up lost nets, by identifying messages on the basis of message and system indicators and characteristic counts. In some cases, D/F results can be of notable value, especially where traffic analysis can give little information.

All card files and other materials of the Evaluation Section can be continuously used by the cryptographic section for their work. Indeed it has been shown repeatedly that in the handling of difficult problems cryptanalysts and exploiters have cooperated and decrypted almost as a team. The daily work conferences under the chairmanship of the commanding or executive officer of the section gave the chief cryptanalyst an opportunity to present hints and wishes for cooperation. Fundamental for all cooperation is the recognition of the fact that each specialized section needs the others for its work, and is also needed by

them; that each technical specialty is, to a certain extent, a tool subject for the others; that an individual section can never work successfully alone. At the beginning of the war, there were attempts for security reasons to keep the various sections separate from each other and prevent any exchange of ideas; this insane plan was dropped very shortly.

b. Cooperation of the Cryptanalytic Group with Other Cryptanalytic Units

Originally the contact between regiment and section in the field of cryptanalysis was very close, because the section had neither the personnel nor the material to meet the demands made upon it. Frequent borrowing of workers, and conferences, guaranteed the transmission of new discoveries and techniques.

Owing to the differentiation of the cipher material, the often excessive distances on the Eastern front, and poor communications, the contact became, in the course of time, less close. The sections were later able to handle their assignments in complete independence.

New systems were exchanged constantly with the regiment by teleprinter, and their designations were selected by the regiment. An exception was made so that the radio star net of the intercept service in the East could be used for the exchange of communications between the sections. A special cipher system was available for encoding radio messages concerned with cryptanalysis. It may be worth mentioning that at times a Soviet code book was used as the basis of this system.

Quarterly conferences lasting several days gave the chief analyst of the sections an opportunity to clear up all technical and organizational problems with the regiment.

The three cryptanalytic sections on the eastern front maintained an active interchange of ideas. Frequent visits back and forth afforded an insight into the work of the neighboring sections and gave a new incentive for one's own. Newly solved systems of air armies which they covered in common were exchanged directly on the teleprinter, and codes for older and processed systems were compared at regular intervals. The fact that the key men in all cryptographic sections had either come from the cryptographic bureau or had worked together elsewhere for years and were well acquainted led to very stimulating and loyal cooperation.

The personnel of detached companies of the intercept section was, in most cases, drawn from the cryptanalysis section, and was later taken care of by the cryptanalytic section of the exploitation company, remaining closely connected with the latter in its work.

c. Cooperation with Other Branches of the Armed Forces and Foreign Intercept Services

Even though the field of work of the individual cryptanalysis sections was definitely limited by the nature of Soviet cryptographic methods, an attempt was made to keep up a current exchange of opinions with the corresponding technical sections of other branches of the armed forces and friendly foreign intercept services, and this led to good results and a broadening of the professional horizon.

Cooperation with the cryptanalytic sections of the "commands for communications observations" in the same area was uniformly good. Again and again, exchange of material between the individual cryptanalytic sections of the Army and the Air Force was arranged. It is true that it never became very effective because mutual interest in individual systems was not great, but the characteristics of the systems, the resulting methods of attack, and the general organization of the work were repeatedly discussed or investigated. Aside from that, message material of interest was continually exchanged.

In contrast to the Air Force, the Army posts had behind them a great tradition, although this very tradition threatened to degenerate into intellectual stagnation and made the organization of the work appear unwieldy. The successes of the Army became smaller in the course of the war owing to increased complication of the army systems and very strict radio discipline on the part of the Soviets. The level of training and the techniques were approximately the same as in the Air Force.

Cooperation with the Navy was not so close, largely because of the difference in technical interests; otherwise, what has been said concerning cooperation with the Army also applies here.

No cooperation existed with the SS. There were rumors of an elaborate cryptographic set-up within that body, and sporadic attempts were made to recruit key men of the other branches of the armed forces for it.

Finnish cryptanalysis was carefully and efficiently organized in a large central station, had available a multitude of excellent personnel and obtained correspondingly good results. Cooperation with the cryptanalysis section of the Finnish First Air Fleet was unrestricted and led to excellent results.

The cryptanalysis force of the Hungarian intercept service consisted of over-age personnel and was unadaptable; the results were meager. Although even before the war a disguised Air Force detachment in Budapest was cooperating with the Hungarians, the relationship could not be characterized as satisfactory because the Hungarians were not sufficiently honest.

8. THE CRYPTANALYST

a. Mental Requisites

The prime requisite is a lively interest in the work. A man without enthusiasm and interest in the work cannot be forced to accomplish anything. He is merely an obstructive foreign body.

The cryptanalyst must be intelligent and mentally very alert, but the ability to associate ideas must be held in check by a well-developed critical faculty. A mere day-dreamer is inconceivable as a cryptanalyst. The ability to work scientifically, i. e. systematically, is a further essential. The peculiar character of the profession all too often involves having the work of days, or even weeks, prove useless and being continually obliged to try new ways of reaching the objective; in such a situation indomitable persistance is the only resource.

Good knowledge of languages is indispensable. At least, if a man has no satisfactory knowledge of languages, he must show a pronounced feeling for languages.

The mathematical ability so often called for or presupposed does indeed belong among the essentials, but this talent is not to be confused with mathematical schooling. The best cryptanalysts with great analytic and constructive talents have, as a rule, no notion of the theory of combinations. The few mathematically trained workers on the other hand often use their knowledge merely to calculate, on the basis of well-known formulae, how many possibilities this or that system permits—the system being generally broken by others.

Two other elements must not be forgotten: intuition and—luck. I mean that luck which in the long run falls only to the lot of the competent. These notes indicate sufficiently that, on the basis of the requirements set forth, the professional ideal can only be reached by very few. Hence in the interests of the work the individual must have a definite community feeling; he must not be a mere lone wolf. Most successes in cryptanalysis are not the exclusive work of an individual but are group accomplishments, which have resulted from technical discussion, from mutual criticism, and from an integration of intuition, systematic work and diligence.

There is no cryptanalyst whose knowledge covers the entire field. The reason for this is to be found less in the mental acumen of the analyst than in the inventors of the systems worked on, and in the accidental allocation of the individual, usually made on the basis of his linguistic knowledge. Each one is master only of the systems and the tricks necessary for the solution of the systems which he has actually worked on, and worked on not for a short time—perhaps at some school or in a course—but in actual practice over a long period. An outstanding analyst, who has worked, let us say, for years only on the substitution systems of a particular group of countries, will only be able to talk in generalities about machine systems, although it must be assumed on the basis of his proven professional ability that he will be able to hold his own in this field too.

b. Choice of Cryptanalytic Personnel

Selection and replacement of personnel is rendered very difficult by the strict demands for secrecy. Special psychological-technical tests are obviously risky, while general intelligence tests lead repeatedly to bad mistakes. After years of experience in the field of personnel selection one must come to the conviction that a ten-minute general conversation reveals the suitability or unsuitability of an applicant better than the most lengthy and comprehensive tests. Of course, occasional errors of judgement cannot be wholly avoided. Many a hopeful novice reveals himself after a few weeks as an untalented bungler and many an unimpressive person with obvious deficiencies (inadequate knowledge of languages, scant general education, and the like) becomes a successful and well-qualified worker. Thus, for example, an undoubtedly highly intelligent language teacher, who composed several textbooks for learning Russian which are recognized as good, failed utterly as a cryptanalyst. On the other hand a young soldier, a metal worker by trade, who had never done any scientific work and was assigned to the intercept service by sheer accident, became one of our most effective cryptanalysts.

One factor which must not be underestimated as a contribution to morale and achievement was the fact that numerous cryptanalysts were either Germans from Russia and the Baltic States, or Russian nationals who had immigrated; all these had had their unfortunate experiences with Bolshevism. For these people, employment in the cryptanalytic section was not simply a matter of bread and butter or obedience to orders, but was an expression of strong anti-Bolshevist feeling.

In the last years of the war, replacements were supplied almost exclusively by the Interpreter Replacement Section of the Air Force. The fact that in this section there was no instructor with the cryptographic background needed to select men who might conceivably be useful as cryptanalytic replacements had bitter consequences. The replacements offered were wholly inadequate.

c. Training of Cryptanalytic Personnel

A cryptanalyst is developed almost exclusively by on-the-job training in a section. He is first apprenticed to some experienced analyst. Of course, he doesn't have everything served him on a platter; he has to inquire and work his way into each new point, and every trick of

the trade. Explanation is not enough. An explanation, for instance, of how a recipherment is solved or how a relative code is adjusted to the presumed original does not, by any means, put him in a position to perform these tasks by himself. If he cannot himself see the problematic character of his work, if he does not feel the desire to force his entry into this undiscovered territory by constant questioning and boring, he will never become a good cryptanalyst. Those who fail in the profession are prone to offer the excuse that this or that was not shown them or not explained to them. It will almost always be true that they did not have the necessary acumen to work out the corresponding problem themselves. As a matter of principle everything is explained, but it must also be understood. Naturally, however, young members of the organization are not mere mental messenger boys, whose time is to be filled out exclusively with sorting messages and making counts the significance of which may perhaps not be explained to them. At the beginning of a long and tedious training it is necessary that the novice be able to share in the exciting, nay, dramatic incidents of this work,—that one try to show him the breaking of a system or the development of a process. Great importance also attaches to having the young analyst learn to make practical and efficient use of the manifold aids afforded by all the other sections, for the best analyst is not the one who works depending upon himself alone and starting from scratch, but the one who can piece together, for his own combinations and constructions, the greatest number of building blocks selected from the results of the other sections. It cannot be over-emphasized that the art consists not in working as "creatively" as possible, but in incorporating as many known technical elements as possible into one's work.

For this reason it is absolutely essential that the cryptanalyst have tactical schooling and be acquainted with the work of the various Evaluation Sections, at least in broad outline. One can only think with horror of the many fellow workers of those first years who, in default of the most elementary knowledge of military affairs, did not hesitate in their messages to subordinate a divisional staff to a regiment and let the regiment issue orders to the staff or to start local reconnaissance planes on a long-range fighter mission—and when their work was criticized, to assert that what they had written agreed with the source and if the text was not satisfactory, so much the worse for the text. One trait of a really good cryptanalyst is his tendency to conservatism— the tendency to cling to methods which have at some time proven good. It is very difficult to convince one's fellow workers that the methods they have used thus far have led to the goal to be sure, but can or must be replaced by others which are better, more logical, and more exact. At such moments, a certain spir-

itual inertia becomes manifest. Introducing the use of substitution tables, for example, or implanting the idea that it is absolutely necessary to attempt the reconstruction of the original code even though decipherment with a relative code has been successful; such reforms require much time, effort, and pedagogical persuasion on the part of the analyst responsible.

Formal courses of instruction seemed desirable, but unfortunately the want of good cryptanalytic personnel was so keenly felt that it was not possible to release a few good men from their daily tasks to set up a permanent teaching staff and institute a long-term training program. All the short term and—in the last analysis—improvised courses in cryptanalysis which were given, revealed their inadequacy and questionable value again and again. It was really only possible to discuss the systems briefly and to show the sort of aids necessary in working them. Any made-up problem is after all only an isolated phenomenon and furnishes training in the use of a particular procedure rather than in flexibility of mind. That was all, and it amounted to very little. Thus the short term courses were, for the most part, merely a means of getting acquainted with the new fellow workers. The product of the courses was never a "trained" cryptanalyst. Such a one develops, as already remarked, only in and by practical work.

As to a text book: no doubt it would have been wise to put into writing the results of practical experience, fundamental ideas, and tricks of cryptanalysis in the form of a guide, and to place this in the hands of not only the novice but the advanced student as a manual for reference work. This project was to be carried out after the end of the war.