The Geheimschreiber Secret

Arne Beurling and the success of Swedish signals intelligence

Lars Ulfving

Translated from the Swedish by Frode Weierud

Original Title: "Geheimschreiberns hemlighet, Arne Beurling och den svenska signalspaningens framgångar"

In "I Orkanens Öga, 1941 - Osäker neutralitet"
edited by Bo Hugemark, Probus Förlag, Stockholm 1992

Translator's Preface

The translation has been kept as close to the original language as possible. Specialist terms and expressions have been retained whenever such terms and expressions exist in the English language. Where this has not been possible, a substitute term with the closest possible meaning has been chosen and an explanation given in the text.

The original notes appear as in the original, as footnotes at the bottom of the page. Other short notes in brackets appear as in the original. Original references are marked with superscript numbers, and the references themselves are placed at the end of the text.

The translator's notes are of two types: short notes included in the text in brackets and in italic (*translator's note*), and normal notes which are marked by italic numbers in square brackets, [*1*].

An appendix and a bibliography has been added as an aid to placing this account in its cryptological context and as an incentive to further study.

Version: 29 January 1997.

The Geheimschreiber Secret

Arne Beurling and the success of Swedish signals intelligence [1)]

by Lars Ulfving

A short historical résumé until spring 1941 [2)]

At the beginning of 1941 Sweden was in a situation that had drastically deteriorated during the previous year. The end of the Winter War (*Russo-Finnish war*) and the signing of peace in Moscow on 13 March 1940 were traumatic events in Sweden as well as in Finland. However, the conditions were not so devastating as they could have been had the Soviet war aims been achieved. Finland survived as an independent state, but within tighter borders.

The surprising and successful German attack on Denmark and Norway on 9 April 1940 brought serious consequences for Sweden. Sweden's political freedom became seriously limited. Threats from new directions had quickly to be taken into consideration. In one area, however, the German demands on Sweden created unexpected possibilities that were exploited well. Their request to hire telegraph lines going through Sweden made great successes for Swedish signals intelligence possible.

In mid-summer 1940, after the French capitulation and the Soviet occupation of the Baltic states, the Swedish intelligence service was faced with two important questions. Would Germany carry out "Operation Seelöwe", a naval invasion of Great Britain, during the autumn? Would the Soviet Union again attack Finland to re-establish Russian borders on the northern shore of the Gulf of Finland while Germany was engaged on the western front? There existed no guarantees that Stalin would wait until the German air war might lead to air supremacy over the British Isles or that he would wait for the German invasion. After developments in the Baltic, Stockholm considered it likely that the Soviet Union would attack Finland at the turn of the month July-August even before, or perhaps even without, a German invasion attempt on Great Britain. Germany would then probably take the same attitude as during the Winter War, i.e. benevolent neutrality. Indications, chiefly reported by attachés from Riga, Berlin and Moscow, showed such a development. The Finnish government was under enormous Soviet pressure, while Moscow-led communists tried to create internal trouble in the country. The pattern was the same as that before the Baltic states were occupied by the Soviet Union in June.

When, on 13 August 1940, Foreign Minister Günther explained the current situation to the Foreign Affairs Committee, his opinion was that there existed a real danger of such an attack. The German military attaché in Riga was given as the source. It is remarkable that no Swedish sources or Finnish military authorities' views were used or referred to. The Defence Staff's intelligence department was therefore also obviously restrained in its written reports to the military command and the government.

German fear of a Russian attack, however, caused Hitler to free the arms embargo against Finland shortly before 10 August. The arms' deliveries that had stopped under the Winter War were now let through. This political change of course indicated a renewed German interest for Finland's continued existence as an independent nation. The tension in Helsingfors was relieved. The immediate danger of a Russian attack was estimated to be over for the time being. As a result it was considered necessary that the Defence Staff's intelligence department concerned with Finland should be strengthened. Now, it was not only Finnish-Soviet relations but also German-Finnish relations that had to be watched. Since neither Finnish nor German military contacts were very communicative any longer, the task was not particularly easy.

The extraordinary Swedish military contacts in Finland were evidently about to be reduced because of Finland's German connections. The attaché reports from Berlin also showed a clear German interest in Finland. Speculations about a German attack on the Soviet Union started to appear in the reports from Berlin. Neither the Swedish attachés nor others could obtain any further information about Hitler's intentions. They were reduced to making assumptions about probabilities and possibilities. A German two-front war, however, was not considered probable by the Defence Staff's intelligence department. In autumn 1940 the situation did not seem particularly alarming to the Swedes. The concessions made, in response to German demands for troop transit and continued iron ore exports, appeared to be sufficient.

The reports from the military attaché in Moscow during the winter of 1940 no longer indicated a Russian build-up and deployment of forces against Finland. The Russian build-up of forces was instead concentrated in the border areas in the south and south-west, against Bessarabia and Bukovina. In Finland, however, they still felt that a new Russian attack was a real possibility.

As a consequence of the commonly perceived threat, the military intelligence exchange between Sweden and Finland which, as already explained, had diminished after the end of the Winter War, was again improved. However, once more the Finnish interest for co-operation diminished considerably during spring 1941, principally during and after April. Attaché von Stedingk in Helsingfors reported simultaneously that German-Finnish relations had dramatically improved. He also reported that Finnish contacts appeared to be prepared to take part in a German war against the Soviet Union, which German contacts said, with a surprising frankness, would start in early or mid-June. Colonel Carlos Adlercreutz, the chief of the Defence Staff's intelligence department, had during a conversation with the chief of the Finnish General Staff, General Heinrichs, clearly seen the possibility of Finland joining in a German attack on the Soviet Union, or being forced to participate in such an attack.

German probes about the transit of German troops from Norway to Finland through Sweden had already taken place in February. Sweden feared that these explorations would change into direct demands, but wondered if Hitler would be content with demands for transit if he intended to start a two-front war against the Soviet Union before Great Britain had been finally defeated.

The uncertainty about Hitler's intentions was brought to a head during the so-called "March crisis" that culminated in a large preparedness alert on 15 March. The alert was actually caused by a German communications error. In fact, there was no other intelligence about a German attack. However, the information obtained through signals intelligence made Swedish preparatory measures possible against regions where German units were positioned in Norway.

The deployment and build-up at the German eastern border now started to be obvious and was difficult to conceal. However, an uncertainty still prevailed as to whether Hitler really intended to attack the Soviet Union before Great Britain was conquered. Perhaps the build-up aimed only at applying pressure — not a two-front war. How — or if — the received information was analysed at the Defence Staff and how — or if — the information in the military reports was weighed together with the rather uncertain and speculative diplomatic information, can no longer be clarified. At a presentation for the government on 21 April General Olof Thörnell, the chief of the Defence Staff, judged that a German-Soviet war was probable, and that in such a conflict Finland would participate on Germany's side. From the presentation it became clear what vague information was the basis for this judgement. The deception measures taken to protect the planning were hard for other intelligence services, including the Swedish, to penetrate.

The Soviet military intelligence service was informed about the coming attack. Nevertheless, Stalin refused to believe that the attack on the Soviet Union would start before Great Britain was conquered.

In one area the Swedish intelligence service was considerably in the lead. In spring 1941 the Swedish signals intelligence service furnished very interesting, extensive, accurate and unique information about German military dispositions in the vicinity of Sweden.

Swedish signals intelligence and intelligence service before and during the Second World War [3)]

In 1936 a resolution was passed about a new defence order which came into force 1 July 1937. The resolution included provision for the establishment of an intelligence department, a signals intelligence department and a cryptology department.

However, the prerequisites for an effective intelligence service were not so good. Swedish intelligence services in the modern sense of the word had indeed been already established in the beginning of this century. The armed forces intelligence service had increased in 1905, during the Union crises, and in the First World War. The General Staff and Naval Staff of that time both had their own signals intelligence and cryptographic units. However, in the inter-war period less and less was done. The knowledge acquired in signals intelligence and cryptanalysis was lost. Politicians of that time did not understand the importance of a well-functioning intelligence service and consequently they did not grant any appropriations for this purpose. Nor did the Defence Commission, which was appointed in 1930 and on whose report the 1936 Defence Resolution was based, take any appreciable interest in the intelligence service. The General Staff's foreign department did not constitute a solid enough foundation for such a service. No special agency for cryptanalysis existed before the Defence Staff was established, although the cryptographic departments at the Naval and General Staffs had some success during the First World War. The encrypted radio traffic of the Russian Baltic Fleet could be broken to some extent. The General Staff probably broke German diplomatic traffic periodically.

The breaking may have taken place even earlier, but solid information about this is missing. These breaks, however, were probably quite sporadic and had a "chamber character", i.e. rather amateurish.

From the summer of 1928 signals intelligence was carried out fairly regularly under naval direction. In the beginning it took place from the warship *Sweden* (*Sverige*) and from the summer of 1929 from several ships in the coastal fleet. From October 1929, signals intelligence was also carried out from naval coastal radio stations.

The first attempts to develop this branch of the intelligence service were made by the Navy. During the years 1930–31, the Naval Staff had already organized a course in cryptology and cryptanalysis. Ships in the coastal fleet started the systematic interception of foreign radio traffic in spring 1931. Later professional intercept operators were trained on the warship *Queen Victoria* (*Drottning Victoria*). The first successful attempts to break foreign cipher traffic were made in spring 1933, when they succeeded in breaking the cipher then used by the OGPU (later the KGB). These breaks into foreign military ciphers were probably the first to be made in Sweden after the First World War. The naval cryptography courses of 1930–31 were repeated in 1932–33 and 1934–35. An agreement was reached between the Naval and General Staffs to run these courses alternatively every second year.

The instruction was based on theory with special exercises. The real material available was too complicated to be used in the teaching. Even if these cryptanalysis courses did not result in real breaks, they were nevertheless of great importance as they created a small cadre of trained theoretical cryptanalysts, consisting of both active and reserve officers together with conscripted students. Later on civilians from the University of Uppsala, among others, were also trained as cryptanalysts. One of these students was the mathematics professor Arne Beurling.

When the future Defence Staff organization was analysed in 1935–36, cryptology-committed interest groups succeeded in pushing through the establishment of a department for cryptography and cryptanalysis — the crypto department. In some quarters a crypto department was considered unnecessary but, in spite of opposition, one was set up during the final stages of establishing the Defence Staff. Sections I to III were intended to deal with the cryptographic security of the Army, Navy and Air Force. The fourth section, crypto section IV, was intended to be a cryptanalytic section. Thus, the foundation was created for a central cryptanalytic organization. It was in crypto section IV that the Geheimschreiber traffic would later be broken.

Radio interception was taken care of by the Defence Staff's signals department. However, the actual signal-intercept work was completely carried out by the Navy, which was the only force with access to qualified intercept personnel.

The crypto department led an ambulatory existence during 1936–40. In the beginning, it was housed in the staff building "Grå Huset" (*The Grey House*) in Östermalmsgatan 87; later in a house on Lützengatan. During the summer of 1939 the approaching war became more evident and the department intensified its mobilization preparations. At the outbreak of war it transferred to the premises of the Military Academy, where it had the top floor at its disposal. Soon it became overcrowded, which is why crypto section IV moved to a property on Karlaplan 4, consisting of a building facing the street and a dilapidated house in the back garden. The conditions were rather primitive. The furnishing was of the utmost simplicity, consisting of folding tables and simple wooden chairs. However, it was here the crypto department was going to perform great achievements.

Photo 1 - Dilapidated house in the back garden on Karlaplan 4.

Breaking of the German encrypted telex traffic - the breaking of the Geheimschreiber [4)]

At the time of the German attack on Denmark and Norway 9 April 1940, Germany demanded that there should be no interruption of their telecommunications transmitted over Swedish lines. After a positive answer, the Germans gradually hired lines in Sweden for the connections Oslo - Copenhagen - Berlin, Oslo - Trondheim, Oslo - Narvik and Oslo - Stockholm. The German embassy in Stockholm already possessed a line for their traffic to Berlin. Later on they hired a line for the connection Stockholm - Helsingfors. The interception of the German telegraph lines was the fundamental condition for the future successful breaking of the German encrypted messages. The Swedes had, by these means, access to large quantities of genuine information. Wartime arrangements allowed foreign rented telecommunication lines passing through Swedish territory to be tapped, without breaking Swedish law.

We shall here for the first time in open literature show the principles involved in the breaking of the Geheimschreiber. The Germans considered this cipher machine to be extremely secure, but their confidence resulted in an imaginary security. German carelessness and Professor Arne Beurling's genius exposed the secret of the Geheimschreiber.

A note about teleprinters

To facilitate an understanding of the subsequent explanations we will give a short technical review of teleprinters.

The first teleprinters were constructed at the end of the 19th century. The principles have remained largely unchanged since then. Every character transmitted consists of a combination of pulses of two types. The number of pulses in a character is always five, contrary to the varying number of pulses in the Morse code alphabet. All pulses are of the same length, and are indicated by positive or negative polarity or alternatively, current or no current. Five pulses taking on two different states give 32 different combinations, but that is not sufficient for all the characters that have to be transmitted. There therefore exists an arrangement with the same function as the letter/figure shift key on a typewriter. A combination of pulses causes all subsequent characters to be received as number or punctuation characters, and another combination signals in a similar way that all the following characters will be received as letters. Several teleprinter alphabets have existed. The one mostly used is called the Murray code after its inventor, or the International Teleprinter Code (*International Telegraph Alphabet No. 2*). The text is punched on paper tape which is fed into the transmitter. 'Hole' or 'no hole' in the tape corresponds to 'current' or 'no current', or to 'positive polarity' or 'negative polarity'.

Teleprinter encryption

Soon after the first teleprinters were put into operation, equipment for the encryption of teleprinter signals was constructed. The method first used was simple. Two identically-punched key tapes, one for the sender, the other for the receiver, are produced. They are then glued together in a loop of manageable length, about 1000 characters. The sender punches his plaintext tape and places it in a tape-reader. He then comes to an agreement with the receiver about how the key tapes will be placed in their respective tape-readers, and the transmission starts. In a simple relay circuit a modulo-two addition is performed on the characters from the sender's two tape-readers. A character on a tape can be regarded as a binary number: a combination of 'holes' representing ones, and 'no holes' representing zeros. A modulo-two addition of two such numbers signifies an addition, without carry, of each bit in corresponding positions. The result of this addition forms the cipher character that is transmitted. The same procedure is used in the receiver. After each transmitted character all tape readers are stepped one position forward and the whole process repeats. The cipher methods gradually evolved. Instead of key tapes a number of code wheels with pins were introduced, e.g. five wheels , one for each channel in the key tape. An active pin had the same function as a hole in the corresponding channel on the tape. Thus it was no longer necessary to punch the plaintext on tape and then transmit it later. The teleprinter could be directly connected to the cipher equipment, hence it was possible to transmit and receive in "real time", so saving a lot of time. In the crypto department this encryption method, consisting of adding a key character to a plaintext character, irrespective of how the key character was generated, was called "overlaying". This term is used in the following text.

The Geheimschreiber

The German company Siemens developed a mechanical teleprinter cipher machine in the 1930s that was the first in a series of such machines. The generic name was "Der Geheimschreiber", which the crypto department called "G-skrivare" (*G-writer*). In addition to the previously mentioned classical type "overlaying", it also made a permutation* of the pulse order as another encryption function.

The crypto department later used the expression "transposition" for this permutation. A polarity inversion was made with five relays, and five others took care of the transposition.[*1*] The relays were controlled by ten coding wheels which, through a set of plugs and jacks, could be connected to relays in an arbitrary way. The principle of transposition of the teleprinter pulses is not suitable for all types of teleprinters. The five pulses must be available simultaneously in the transmitter and the receiver for a permutation to take place. In the transmitter this is not so difficult to arrange, but it is much more difficult in the receiver. However, Siemens had solved the problem for the receiver even without access to modern digital technology. All functions were mechanical in the cipher machines of those days. An incoming character's five pulses, positive or negative, charged five capacitors in sequence. When the fifth pulse was received the information stored in the capacitors was simultaneously transferred to five polarized relays. These relays were part of a circuit that selected the character to be printed. During this transfer it was possible to produce a transposition by changing the connections between the capacitors and the relays.

*Permutation: A permutation of a number (= n) of elements, or of numbers, corresponds to an arrangement of these elements in succession. Two permutations are equal when, and only when, the elements, the numbers, in both are placed in the same order. For n = 2 there are two permutations (1,2) and (2,1), for n = 3 there are six (1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2) and (3,2,1). Generally it can be shown that the number of permutations of n different elements is $1 \cdot 2 \cdot 3 \cdots (n-1) = n!$ (n factorial).

The Geheimschreiber's ten code wheels had the periods 47, 53, 59, 61, 64, 65, 67, 69, 71 and 73. In the first models all the wheels moved one step for each enciphered character. Since the wheel periods were relatively prime, that is they had no common factor, the total period of the machine — the number of steps the machine must make to return to its starting position — was equal to the product of all the individual wheel periods, that is 893 622 318 929 520 960 steps. This number also indicates the number of possible wheel starting positions.

The "transposition circuit", that is the insertion of the "transposition relays" between the rows, could be varied. Eight basic patterns were possible, each with 2 612 736 000 variations.[*2*] The combinations of connections and wheel adjustments were, before the creation of the computer, considered to be extremely large numbers. In addition there were the number of ways of connecting the code wheels to the relays. This may have given the Germans the impression that the Geheimschreiber was a very secure cipher machine. It was probably considered to be more secure than the Enigma machine which was intended for tactical use. The Enigma had, for example, a period of 17576.[*3*]

The Geheimschreiber was gradually developed and several models were brought into service. The first machine the crypto department came in contact with was called T52A/B. Later T52C, D and E came into service. There were also variants of the different models. However, they were all based on the same basic principle.

Photo 2 - "Geheimschreiber" or "G-skrivaren" (*Schlüsselfernschreibmachine T52C*).

At the end of 1941, a new machine designated Z appeared in the traffic. It did not belong to the A/B-serie and it was called Geheimzusatz 40[*4*] and not Geheimschreiber. It was a stand-alone attachment that was connected between the teleprinter and the transmission line. It could therefore have been used together with teleprinters other than the Siemens machine that the Geheimschreiber was based on.

Arne Beurling

Who was Arne Beurling? According to *Svensk Uppslagsbok* (*Swedish Encyclopaedia*) he was "Arne Karl August Beurling, born 5 February 1905, mathematician. Beurling defended his thesis in Uppsala in 1933 (Etudes sur un problème de majoration), senior lecturer same year, Ph.D in 1934, professor in 1937. Beurling is an ingenious and all-round scientist who has attained beautiful results in function theory, prime number theory, modern integration theory and in several other areas." After the war Arne Beurling was offered an excellent position at Princeton University in USA in 1954. In 1965 he was given Albert Einstein's office, No. 115, at The Institute for Advanced Study, a distinction granted very few people. Arne Beurling died in 1986.

It is now known that Professor Arne Beurling was the man behind the breaking of the German Geheimschreiber. David Kahn writes in "The Codebreakers", page 482: "Quite possibly the finest feat of cryptanalysis performed during the Second World war was Arne Beurling's solution of the secret of the Geheimschreiber." Arne Beurling's greatness is given by the fact he had at his disposal only the teleprinter tapes with the cipher text. He had no access to any machine, no plaintext and no knowledge about the logical construction of the cipher machine. Everything had to be reconstructed, something which was done in a remarkably short time.

It is known that he based his analysis on only 24 hours of traffic intercepted on 25 May 1940. A quick analysis showed that the first assumptions probably were correct. A check was made with the traffic intercepted for 27 May. Two weeks later the construction principles for the cipher machine were solved.

On the other hand it is not known how he set about it. That secret Arne Beurling took with him in the grave. However, a reconstruction has been made by FRA (*Forsvarets Radioanstalt*). The credit for this reconstruction goes to Carl Gösta Borelius who served at the Defence Staff's crypto section, later on FRA, from 1941 to 1985. Borelius' description of the reconstruction work is the basis for what is shown here.

The reconstruction

There was, of course, a procedure for indicating the Geheimschreiber key settings. One setting was the inner one, that is the selective connection[*5*] used for the connection between the ten code wheels and the previously mentioned inversion and transposition relays. The inner setting was in force for three to nine days, starting at 9 o'clock on the first day.

When a message was to be transmitted, the code wheels had first to be set to a given position. These settings had to be the same for both sender and receiver. The transmitting station would select a setting for five consecutive wheels. This setting was transmitted to the receiving station with a three-character so-called "QEP indicator". The five remaining wheels were set to a predetermined key value that was valid for all messages during a 24-hour period. This setting was called "QEK". The daily key list indicated which wheel would be "QEP-wheel" and which setting the "QEK-wheels" should have.

It should be pointed out that the number 3 = letter shift, 4 = figure shift and 5 = space in this teleprinter alphabet. This has great importance for the following deliberations.[*6*]

When the transmission of a cipher message was about to start, the transmitting station would present itself with "Hier MBZ" (*MBZ here*) and would then ask if the message could proceed, "QRV". If this was the case, the receiving station answered with "KK". The transmitting station then sent "QEP" succeeded by five two-digit numbers (e.g. 12 25 18 47 52). Both operators then adjusted the wheels in their respective machines, partly the "QEK-numbers" after the key list for the current day, and partly the "QEP-numbers". When the transmitting station was ready it would transmit "UMUM" (umschalten — *switch over*) and when the receiving station was ready it would answer "VEVE" (verstanden — *understood*). Then they switched over to cipher mode and the transmission of the text itself started. The ciphertexts were consequently always preceded by "UMUM" and were therefore easy to retrieve in the large number of signals.

It is possible that Beurling had knowledge of the Siemens & Halske patent, but this is not certain. Borelius recounts that when Beurling visited FRA on 15 November 1976, he reacted strangely to questions about the first break. He evidently did not like the questions to be put. He nevertheless said that he made use of "threes" and "fives" in the texts.

Telecommunication technical problems were a great help during the breaking. The telegraph lines were long, sometimes bad, and therefore often exposed to interference, which could distort a transmitted character. The readability was nevertheless not disturbed except when the character changed to a "4" (= figure shift), because then all succeeding text became an unintelligible sequence of numbers and punctuation characters. If the distortion affected only the receiving station, the transmitting station did not notice anything, and continued the transmission. To reduce the problem, the operators normally used to write "35" (= letter shift, space) instead of only "5" (= space) between the words. Thus the consequence of a false "4" would be restored at the next space between the words.

Beurling discovered that when the plaintext of "3" and "5" had one pulse the same and four different, this had also to be the case in the enciphered state. For a guessed "3" there consequently existed only five possible "5" or vice versa. It was therefore relatively easy to establish spaces between words, which would have facilitated further work. It was probably this which Beurling talked about when he alluded to "threes" and "fives". Hence a guessed "3" gave only five possibilities for Q and V in "QRV", which asked if the message could proceed. In this way further work was greatly eased.

It also seemed natural to suppose that a part of the encryption process consisted of a transposition of the five-pulse-characters pulse positions. A number of comparisons could give the transposition arrangement.

Beurling tried in this case to trace back the cipher character to its appearance before the transposition. Then he made his next observation. The change from one character in the plaintext to a cipher character after the "overlaying" consisted of a change in polarity for some of the pulses of the plaintext character, and for all characters in a column it is always the same character that changes.

We can assume that Beurling now introduced his observations on his "work sheets" (*"avvecklings-papper"*).† In five rows under the examined text he placed

†Avveckling: A technical term for the elements of work that took place between the inter-

in every column a dot for pulses with inverted polarity and a circle for those that did not change. When the emerging five-dot combination resembled a teleprinter character, it was called an “overlaying” character. Under this character was written the permutation order, that is the so-called transposition. Gradually it was detected that the pattern of circles and dots in the five rows of the “overlaying” repeated after a number of characters. Beurling then supposed that the pattern was produced by pin-wheels like those in the Swedish cipher machine, invented by Boris Hagelin.

Subsequently he continued the work with the transposition. It turned out that if for example “pulse 2” ended up on “place 3” then the fourth circuit connection had to be open, otherwise it was not possible. If this circuit connection was controlled by a wheel with even distribution of active and inactive pins, the pulse would end up on “place 3” in half of the events, in the rest it would fall on some other place. A converse conclusion should have been possible, using an inverted argument. The complete circuit and hence the details of the remaining wheels were obtained through hypothesis tests. By these means Beurling would have got the break that revealed the Geheimschreiber secret, as Borelius' reconstruction shows.

Imperfections, errors and laziness

It has been mentioned earlier that the telecommunication connections were bad. But it was not only single characters that were distorted and therefore gave an opening for breaking.

The abundant number of “parallel texts”, that is an enciphered text sent several times with the same key setting on the cipher machine, were a big help in breaking the Geheimschreiber. In extreme cases the same message was sent 20 to 40 times with the same setting. How could this happen? One of the basic rules of cryptological security is never to send the same or a different message with the same key setting. Bad connections and distortions together with laziness gave many openings of this type.

The keying procedures have already been described. It takes a certain time to adjust the wheels by hand. To facilitate the adjustment of the “QEK-wheels”, that is the current key for the day, there existed a cursor that easily could be moved around on the wheel and positioned on an arbitrary key number.

The wheels could be freed with a locking arm. All the wheels could be turned backwards with a handle until their cursors came to a home position when the wheel stopped. This handle sat on the right on the front of the machine under a plate with the inscription “LANGSAM DREHEN” (*turn slowly*). The idea was that every morning the cursors would be set on the five wheels that were intended for the daily key (the QEK-wheels). Later these wheels could quickly be returned

ception of a message and until the plaintext could be extracted. That is, the work consisted of extracting the current cipher key.

to their agreed positions before every new transmission. Unfortunately it became a habit that even when the "QEP-numbers" were set, the cursors were set to the key values and then the wheels were cranked back. This was against the existing rules, as new "QEP-numbers" should be selected for every new message.

Since the lines were long and sometimes poor there were often distortions. These sometimes caused one of the machines to interpret the distortion as a character. The operator of the other machine would not notice anything. One of the machines would then be one step ahead of the other. The cipher machines were no longer in phase and the message became unintelligible. When this happened, it was necessary to break the transmission, switch over to plaintext, choose a new message key and continue the transmission.

Now the big mistake was made. For each break in the transmission of a message due to continuous distortions on the line, the operators chose the easy solution of simply cranking back the wheels to the previous setting. In this way the cryptanalysts got their parallel texts with all their errors and flaws which gave a large number of opportunities for breaking it. The high security of the Geheimschreiber became therefore in many ways simply illusory.

Interception and preparation

As mentioned earlier, the traffic on the German hired telecommunication lines through Sweden was intercepted. It was quickly discovered that apart from plaintext, encrypted text was also transmitted. When Beurling found how the Geheimschreiber functioned, Swedish technicians under the leadership of Viggo Bergström started to construct special machines for decryption after directions from Beurling.[7] These machines very soon made it possible to follow the frequent changes in cipher keys and subsequently quickly extract the plaintext. The machines were later built in quite large numbers in L.M. Ericson's workshop for precision mechanics.

Photo 3 - Decryption unit for German line traffic, ex. "APP".

The German Geheimschreiber traffic was broken and deciphered from June 1940 until May 1943. This went on even when new models were introduced and the key procedures were gradually changed.

The intercepts came from a number of teleprinters in a room in Karlaplan 4 which were connected to the different lines between Germany - Norway, Sweden and Finland. The machines, which were very noisy, were supervised 24 hours a day. The texts came out in a never-ending stream of paper tapes, which were then glued on to big sheets of paper.

The daily routine was the following: In the morning (after 9 o'clock, when the daily key was changed) the cryptanalysts examined the incoming traffic, waiting for a case with sufficiently many "parallel texts" to occur. As soon as possible, the cipher key extraction (“avvecklingen”) took place. When the new key settings were produced they were given to the staff who worked with the deciphering machines, and the deciphering of the day’s harvest could start. Subsequently the plaintexts were cleaned up and typed. They were later given to the various consumers of intelligence.

Photo 4 - The decryption units, “APPARNA”, at their working places.

Photo 5 - In the machine room. (*Room with teleprinter-receiving machines connected to the intercepted lines.*)

As mentioned above, two types of traffic were observed and studied. The most extensive were the military traffic and the traffic between Berlin and the embassy in Stockholm. The diplomatic traffic had the highest priority, as this concerned Swedish-German relations. At least two key settings therefore had to be determined every day.

At first, the teleprinters used in Karlaplan 4 were machines from the American firm Teletype. Teleprinters were, however, in short supply as importing them was difficult during the war. However, the Royal Telecommunication Administration (*Kgl. Telegrafverket*) were persuaded to surrender a number of their teleprinters, which resulted in a return to Morse telegraphy on some lines. When the crypto department later succeeded in obtaining a batch of Siemens teleprinters, these replaced the Teletype machines, which was certainly reasonable considering their use.

As mentioned earlier, when newer versions of the Geheimschreiber were later introduced, attachment units were constructed and connected to some of the deciphering machines that were used for the C model traffic. For the Z-traffic only one deciphering machine was built.[*8*]

Large quantities of messages were decrypted and distributed.

Number of distributed messages.

Year	Encrypted	Unspecified	Unencrypted	Total
1940		7100		7100
1941		41400		41400
1942	101000		19800	120800
1943	86600		13000	99600
1944		29000		29000
Total	187600	77500	32800	297900

The highest number of messages distributed in one day (October 1943): 678.

This extensive traffic resulted in an increase in the number of staff. The number of teleprinters and deciphering machines also increased until they reached a total of 32.

The decryption of the Geheimschreiber traffic developed gradually into a real industry needing a lot of people. In 1941 the staff increased to 500 people and later on it became even bigger from time to time.

> Photo 6 - View from the rack room. (*Room with equipment racks where the intercepted telecommunication lines entered.*)
>
> Photo 7 - Another view from the rack room.

The breaking of the Geheimschreiber was a large contributory factor to the establishment of FRA (formed from the Defence Staff's signals and crypto departments) as an independent authority on 1 July 1942.

In May 1943 the keying principle was changed with the result that further deciphering became impossible. A small group stayed on to handle those messages that for different reasons had not been deciphered earlier.

On the eve of Operation Barbarossa: How was the intelligence used? 5)

What has just been described, it must be emphasised, was a spectacular performance even on an international scale. As far as known the Siemens Geheimschreiber was not broken in any other country.[*9*] It was also an extraordinary yield based on a relatively limited investment. Beurling's reluctance to explain how he did it could be due to the fact that he solved the problem so easily and quickly that he found it too easy to arrive at the solution. But in reality genius shows itself in simplicity and its accompanying excellence.

In 1940 the crypto department had been developed with mostly rather new staff. Its technical and organizational achievements were therefore considerable, since during autumn that year it began to distribute German messages in ever-increasing numbers. German unit compositions and their position, together with military and political deliberations and directives were in this way known to the Swedish authorities, sometimes almost at the same time as the real addressee.

The German traffic was not particularly alarming during the autumn of 1940. Hitler was hardly interested in Sweden politically. The planning for the attack on the Soviet Union was still in its infancy. The directives for Operation Barbarossa were first drawn up in December 1940. This gave the crypto department a respite that was used to build up and render more effective the breaking, analysis and delivery routines. The Defence Staff could therefore prepare methods for handling the decrypted material at a time when it was not under any particular pressure.

Texts "of strategic importance or of an obviously secret nature" were delivered directly to Adlercreutz, as chief of the intelligence department, who normally submitted them to his superiors Commander-in-Chief General Olof Thörnell and the chief of the Defence Staff Major-General Axel Rappe. Then the texts went to the intelligence department's own sections. Routine messages went there directly. Afterwards the messages were burned, apart from those judged to have long-term value or that were of great strategic importance. Otherwise, distribution within the Defence Staff was very restricted. A distribution list was never established. The material was delivered to the recipient after an assessment in each particular case. (Comment: Destruction of the decrypted original texts has probably created problems for modern historical research.)

Distribution outside the Defence Staff, to the Foreign Office and the Security Service, took place in the beginning through Adlercreutz's personal service. The distribution to UD (*Utrikesdepartementet = Foreign Office*) was very restricted as Adlercreutz doubted the Foreign Office's security consciousness. However, that the co-operation between the Foreign Office and the crypto department was as good as it became, was due to the fact that foreign minister Richard Sandler (1932—1939, later governor of Gävle) was a very keen amateur cryptologist although, as a cryptanalyst he had no real success. His great services consisted of arranging for UD to inform the crypto department when important events were under way and when encrypted messages might be sent to Germany. This could assist the cryptanalysts, by allowing them to check that the decrypts were correct.[*10*]

Different considerations contrasted with each other here. The necessity to deliver information to suitable Swedish authorities conflicted with the requirements for secrecy in order to minimize the risk of betrayal of this unique intelligence source.

As the decryption work was done by a department in the Defence Staff, Adlercreutz wanted the intelligence department to be the first to receive all information and even to have a right to direct the work in the crypto department. However the crypto department successfully resisted these attempts to boost the intelligence department's power.

In the beginning, few objections were raised against Adlercreutz's control over distribution. But when the German preparations for Operation Barbarossa eventually came to their final stage, the Foreign Office started to feel that they did not get all the intelligence that they needed. The chief of the crypto department then decided to change the distribution routines after consultation with the Foreign Office, who also suspected that they did not get all the information in time.

During the winter of 1941 the incoming information became more and more alarming for Sweden, much more so than during the autumn and winter of 1940. However, it was now possible to get a continuously clear view from the decrypts of the groups, composition and combat readiness of the German forces in Norway and therefore also of changes in the situation. A lengthy force enumeration, intercepted on 21 April 1941, indicated a general movement of troops towards the north. Nevertheless, as on previous occasions no concentrations or deployment could be shown to be directed against Sweden. Nor was there any indication in the numerous reports from military border patrols, customs officers, police commissioners and officials interrogating Norwegian refugees that a German offensive against Sweden was imminent. The decrypted diplomatic traffic gave no special reason for alarm. The repeated German threatening warnings to Swedish contacts were reflected neither in the incoming intelligence nor in their own signals. During a period when German-Soviet tensions increased rapidly, it was nevertheless impossible to ignore the warnings. The government, principally the prime minister and the foreign minister, as well as the military command, were not prepared to cause trouble and accordingly create German irritation. It was not therefore apparent that they reckoned with a German-Soviet war.

Many analysts consider that war preparations serve only as instruments of pressure during negotiations. However, that ignore the dynamics of future military developments which are created by a deployment as large as that which occurred here. Economic factors and military logistics make it almost impossible to keep large, inactive troop concentrations in place as a trump card during long negotiations, just as it is damaging for the units' fighting spirit. It is too expensive not to use the troops, therefore they must either be used in combat or be demobilized and returned to civilian life. Only victory justifies the price — even if it is high. For example, consider the collapse of the economic, political and ecological systems now affecting the states of the former Soviet Union as a consequence, during a long period, of a highly forced "war economy" that did not result in any gains.

On 4 June a message was received indicating that strong German forces would in the near future be transferred east of Rovaniemi in northern Finland. Units would come from Germany as well as from Norway. The deployment was to be ready for 15 June. However, no demands on Sweden for the transit of troops could be gathered from the messages. Two divisions would be transferred by sea to Stettin, then in turn to Oslo and on to Rovaniemi.

The information in the decrypted messages clearly indicated a German attack on the Soviet Union.

On 11 June three further messages came which showed that this assumption was probably correct, as well as other intelligence revealing that Finland could not avoid becoming involved in the war. On 16 June came a teleprinter message that AOK (*Armeeoberkommando*) Norwegen had taken military command of Finnish Lappland and that the troop transports were going as planned. The same day, 16 June, the teleprinter connection Berlin - Helsingfors via Stockholm was established following an earlier request. In spite of different speculations about a negotiated agreement, the incoming messages in the week before 27 June increasingly pointed towards an imminent outbreak of war.

Despite the intelligence, the Defence Staff did not cancel leave for the midsummer weekend. An assessment that there would be a negotiated settlement, which would not require a high military preparedness, clearly had some validity. However, it is also possible that when the assessment was made that the war would not affect Sweden, it was more important to conceal the possession of this extraordinary source, which consisted of access to the Geheimschreiber traffic. Perhaps, therefore, they took it easy and allowed themselves to be "taken by surprise".

What happened later? When and how was the unique source exposed? [6)]

The decrypted German messages had, as mentioned earlier, been the most valuable sources during the weeks before the German attack on the Soviet Union on 22 June 1941. This situation would remain the position for a few years. With the attack, the teleprinter traffic to the German commands in Oslo and Rovaniemi, as well as the diplomatic traffic Stockholm - Berlin increased. The information received by the Swedish authorities became more detailed than before.

During the first year, from summer 1941 to summer 1942, when the German campaign against the Soviet Union took place, the decryption of the German teleprinter traffic provided extraordinary intelligence. German military plans and German politics towards Sweden could be clarified with the utmost certainty. However, no reliable knowledge was obtained about Adolf Hitler's political and strategic intentions. Intelligence throwing any light on the innermost reasoning of the people close to Hitler rarely or never existed.

The supreme army commands in Oslo and Rovaniemi did not command any of the decisive operations of German warfare. Hitler therefore seldom interfered in what went on in these theatres of operations. Nevertheless, even if the embassy in Stockholm and the commands in Norway and northern Finland were on the periphery of German interests, the intercepted internal German briefings and compilations had a great intelligence value for Sweden.

Adlercreutz's restrictions on distributing the decrypts to external recipients, except for the senior officers of the Defence Staff and the Intelligence Department, were mainly aimed at not exposing this exclusive source. Special instructions about other aspects of handling the material were issued in September 1941 by Samuel Åkerhielm in his capacity as deputy chief of the Defence Staff. The purpose was, of course, not to reveal the source. The decrypted messages had to be communicated and handled in secure ways. It was not permitted to refer to this material in conversations, and even less so on the telephone or in writing. When the messages were no longer needed, they had to be burned in controlled conditions.

The German confidence in the Geheimschreiber's security was, as explained earlier, an illusion. However, even the Swedish belief that the Geheimschreiber's secret still was a secret, except in Sweden, soon also became an illusion.

Some time in August 1941 the Soviet Union obtained access to the decrypted material. The courier Allan Emanuel Nyblad had the task of transporting the decrypted messages from Karlaplan 4 to the Staff building "Grå Huset" on

Östermalmsgatan 87. He was a rather quiet man. He had been recruited as an agent, on ideological grounds, by the Soviet Union. The espionage was carried out in the following manner. On his way to the Grå Huset, Nyblad went to a rented flat situated along his usual route and photographed the messages he carried. The photos were given to the Soviet representatives, who had promised Nyblad a prominent position in a future communistic Sweden. He is not likely either to have received or demanded any money worth mentioning.

It is a reasonable assumption that the Soviet intelligence services (the NKVD and GRU) followed the Swedish success with interest. Moscow must have welcomed the likelihood that Sweden, with the aid of the intelligence, would take as strong as possible a position against Germany. But at the same time, the decrypted texts could also create doubts about Swedish power and will to withstand the German pressure.

Here we may reflect that the Soviet Union was taken by total surprise in 1941. During spring 1941 information about the coming German attack was leaked from Sweden to Great Britain (via the naval attaché) who passed on the information to the Soviet Union. However, General Golikov, then the chief of the GRU (the military intelligence service), actively contributed to the surprise by playing down the warnings from western sources, especially British, for reasons of political expediency. (The British intelligence service, SIS or MI 6, had until the Second World War primarily been working against the Soviet Union. Distrust can therefore be considered to be the explanation.)

Nyblad's spying was exposed in January 1942. It could not be exactly established which messages came into Russian hands through Nyblad, as he could not remember clearly on which days he had copied the material (T. Thorén)[*11*]. It is not known whether the Soviet Union derived any benefit from the information.

Less than six months after Nyblad's spying stopped, the Defence Staff discovered a new leak about the successful Swedish codebreaking activities. This time the leak soon had devastating consequences.

On 22 June 1942, Colonel Carl Björnstjerna, chief of the newly created foreign affairs section, which was directly subordinated to the chief of the Defence Staff, wrote to Major-General von Stedingk, the military attaché in Helsingfors, "A serious mishap has taken place. The Germans have been warned by the Finns that we have succeeded in breaking their G-schreiber. For this reason they are changing keys, message channels and everything ...".

No contemporary information exists about how "the serious mishap" happened. However, one need not be surprised. Swedish service personnel had been so open towards their Finnish colleagues that a leak was made possible. The openness shown during the winter of 1941, when it was conceivable that both Sweden and Finland could have common defence interests, continued after the summer of 1941. The Finnish military attaché, Colonel Stewen, was even treated like an insider in the higher Swedish staffs, and the Germans suspected him of communicating sensitive information to Sweden, who they presumed then passed it on to the USA and Great Britain. However, it was equally possible that both of these great powers were capable of acquiring the alleged "leaked information" themselves. When the Germans criticized their Finnish colleagues for gossiping, the latter defended themselves by revealing that the Swedes had intercepted the teleprinter connections and were breaking the messages. It is even possible that Colonel Stewen had seen decrypted messages; at least he knew about them. The Finnish intelligence about the Swedish codebreaking activity probably reached the Germans some days before 17 June 1942, when the big alert hit the German communications. In the beginning, the counter-measures were quite incoherent, but they were soon concentrated in two directions. One consisted of introducing new cipher machines or attachments to them.

On 21 July 1942 a new machine appeared in the traffic, T52C, "Caesar". In the beginning it appeared on only a few lines, while on the others the old machine remained in use. As time went, more and more C-machines were put into operation.

At first inspection the C-machine appeared to be completely normal. When the crypto department received parallel texts it could attack these as before, but the texts no longer fitted the previously known patterns. The sequences were no longer periodic or they had at least no short periods. Was this a new encryption method?

At last the crypto department hit upon the solution. Two texts had been solved and it appeared that two "pin series" were identical in the long sequences. They had already earlier worked on the hypothesis that the seemingly infinite sequences were generated by addition, modulo-two, of the results of two wheels and hence obtained very long periods. The identical sequences allowed this hypothesis to be tested. This had failed earlier. Was it true that the old A/B-machines' QEK-settings also were used in the C-machine? It was known that the C-machine could be used like the A/B-machine. For the A/B-machine they knew which five code-wheels were QEK-wheels, and also the settings. They then combined the wheels two by two in the ten combinations, but that did not work. However, when this procedure was repeated by leaving out four of the wheels it turned out to be correct. In this way it was possible to reveal the functioning of the C-machine.

The Germans had in a hurry made the mistake of keeping an element from an older, simpler system in a new cipher system. In the C-machine they used the same wheel-lengths and pin-patterns as in the A/B-machine and the keying principle was the same. They should have made the new machine completely independent of the old one, but it is likely that production difficulties created obstacles. The A/B-machine could be connected to the C-machine. Therefore the quick change of machines did not have any appreciable effect.

The other counter-measure taken by the Germans consisted in avoiding transmitting particularly important messages over Swedish telecommunication lines. It was therefore no longer possible to maintain the excellent intelligence about the

German armed forces in Norway and Finland. A further deterioration occurred in October 1942 when all teleprinter traffic to and from Oslo and Rovaniemi was sent over Danish-Norwegian, or Finnish-Baltic cables. In certain cases cables were laid specially for this purpose. However, the teleprinter traffic to and from the German Embassy in Stockholm could still be intercepted and broken.

In October 1942 the Germans ordered the introduction of so-called "Wahlwörter" (*randomly chosen words*). The idea was actually sound. It is a good cryptological practice to avoid stereotype beginnings, which are usually where the codebreaker starts to look for an entry. The "QET-texts" were of course necessarily monotonous. Now the text would begin with a "Wahlwort" and in this way move the stereotype, fixed text further on to an undefined place in the message. However, the good intention failed. Many people follow instructions to the letter. Most people used the word given as an example in the instruction, which probably was SONNENSCHEIN (*sunshine*), as it occurred very often at first. Some managed to produce the word MONDSCHEIN (*moonlight*). The record was the word DONAUDAMPFSCHIFFSFARTSGESELLSCHAFTSKAPITÄN (*Danube-steam-ship-company-captain*). When the procedure with Wahlwörter was used correctly it became more difficult, but not impossible, to decrypt the incoming messages.

In May 1943 such radical changes in the keying procedures were introduced that codebreaking became almost impossible. The breaking of the Geheimschreiber's teleprinter messages therefore diminished considerably. A smaller group was left on the task to try, if possible, to do something with the newly received material. Otherwise they were engaged in decrypting older material that had not been dealt with earlier, and in following the traffic.

During 1944 the Geheimschreiber appeared in versions D and E and a mysterious machine called Y. The crypto department never succeeded in breaking these machines. Models D and E were further developments of the machines that carried the designations A, B and C. The Y-machine[*12*] could perhaps have been a further development of the Z-(Zusatz)gerät (*Z-(additional)device = Z-attachment*). But, as just mentioned, the traffic transmitted with these machines could never be decrypted, only followed.

Other leaks also occurred, but were never of any significance. It was the Finnish military attaché in Stockholm, Colonel Stewen, who exposed the secret.

Experiences and lessons [7)]

When the new Defence Staff started functioning on 1 July 1937 the conditions were not the best for the intelligence and crypto departments. They did not have a solid foundation to build on. The procedures applied in the intelligence department were rather simple: namely, they were suited to producing compilations of open material and to making glossaries. Incoming messages from signals intelligence and e.g. attachés were passed on “in extenso” to the concerned parties without making any overall assessments and conclusions. This was left to the individual reader. The information was therefore not turned into intelligence.

The crypto department worked under very frugal conditions during its first development phase. However, through considerable efforts, where limited means were used in the best possible way, impressive results were achieved.

Swedish military intelligence collection deserves very good marks for the period just before Operation Barbarossa and during its opening phase. The Swedish military attaché in Helsingfors had given a warning in good time about a German attack on the Soviet Union in which Finnish participation was highly probable. The continuous decryption of the Geheimschreiber’s messages also indicated clearly and unambiguously an imminent outbreak of war.

No inquiry will probably ever be conducted to see if the organization was a pure military endeavour, or a common one for the foreign department and the military commands to study and analyse the incoming information jointly. At least no documents exist showing this to be the position. Evidently it was considered adequate to circulate attaché reports and decrypted messages without any attached intelligence evaluation. However, the most essential messages were probably discussed by representatives from the Foreign Office and the military commands at their weekly meetings which they started in the beginning of April 1941.

Yet the incoming information gave the impression that Sweden would not be pulled into the war on the German side. The Swedish government and the commander-in-chief were therefore not surprised on 22 June 1941 as they had been on 9 April 1940. Nor was it necessary for Sweden to take any precipitate measures. They could afford to lie low and show surprise in order not to expose the exclusive source of the decrypted German teleprinter messages. No information exists about this, but the view is not unreasonable.

As mentioned, no organization existed for compilation, study, analysis and synthesis in preparing intelligence evaluations. Nor was the establishment of such an organization considered. The assessment of the circulating messages’ intelligence value and the conclusions were left to the individual readers, whether with good or bad results.

Any long-term analysis and assessment of the war’s course and end was never carried out, but considering the turbulent developments ahead that was perhaps best.

When one looks back to see whether it is possible to learn from that time’s events one must also take into consideration the classical dilemma of a professional intelligence service. Incoming intelligence rarely or never gives information about planning prerequisites, considerations and objectives of the supreme command’s inner circles, and even less about chosen alternatives. For this to be possible one must have access to a traitor or a planted spy in the enemy’s supreme command (e.g. the CIA’s Oleg Penkovski in the Soviet Union or Mossad’s Eli Cohen in

Syria). Normally one is simply reduced to using information which can give intelligence about possible actions and when they are likely to be realized. When different readers, each studying from varying positions, preconceived opinions and needs to assert his preserve, draws intelligent conclusions from raw information which will be the basis for decisions, the result can be disastrous. The lonely decision-maker may very well take non-optimal, irrational decisions. However, if the decision is made in full session, the delay caused by the decision-making process can produce catastrophic consequences before everybody agrees after a long discussion. These are two of the conditions for a strategic attack to succeed, like the German attack on Denmark and Norway. A third risk also exists. A joint, balanced intelligence estimate, which is carried out by a whole organization, can in the end be so diluted that it has no value for the decision-maker. The balance between the different extremes demands a lot from those carrying out intelligence work, irrespective of grade or service rank. It should also be pointed out that it is nearly impossible to assess all undercurrents influencing a historic event so as to make a forecast. Unknown as well as known events, which an intelligence service will not be able to interpret and describe, can create unknown forms of interference in a chain of events so that they can hardly be predicted.

Conclusion

On New Year's Eve 1941, Sweden was seemingly in the same geostrategic situation as the year before. However, a change in the wind was under way. In front of Moscow's gates, the Germans' storm wave had collapsed when Marshal Zhukov's Siberian troops launched a violent counter-attack on 6 December 1941. The Red Army had good help from "General Winter", who would assist in several winters to come. But in reality the strategic initiative was on its way to slipping out of German hands. However, it would take a whole year before this became evident for the world, when a complete German army was annihilated near Volga.

On 7 December 1941, the day after the counter-attack outside Moscow, Japan attacked the American fleet in Pearl Harbor. With that an industrial giant arose in terrible anger - an anger that in the end would turn the fortunes of war.

In the Second World War, the breaking of the cipher from the German Enigma machines and the Japanese Purple machines[*13*] was of crucial importance. The considerably greater intellectual effort needed to break the Geheimschreiber messages, which was accomplished in Sweden, did not in any way have the same decisive significance for the war. Therefore this accomplishment has not been so well known. However, from a Swedish perspective, it was of considerable importance as it actively contributed to keep Sweden out of the war.

Bibliography

Unpublished documents

Documents of various types concerning the breaking of the Geheimschreiber in FRA's secret archives.

Published works

Carlgren, Wilhelm M, *Svensk underrättelsetjänst 1939–1945*, (Stockholm 1985).

Kahn, David, *The Codebreakers*, (New York 1967)

Annotation

The publication of information from FRA's archives has taken place with due permission.

Notes

1. Where no other source is given, the account is based on information from Försvarets Radioanstalt's (FRA) documents.
2. Carlgren, p. 32.
3. Resumé of experts in FRA's documents, compare with Kahn, p. 478.
4. After Carl Gösta Borelius' unpublished documents in FRA's archive.
5. Carlgren, p. 68.
6. Carlgren, p. 80, compare with Borelius' documents.
7. Carlgren, p. 179.

Translator's Notes

1. The author talks about the use of relays for the inversion and the transposition circuits. It was only the T52C and E machines that used relays for these circuits. The other machines, T52A/B and D, used the cam contacts directly on each coding wheel.

2. It is not entirely clear what the author has in mind here. The number of combinations given by the author, $2\,612\,736\,000 = 10!\cdot 6!$, does not appear to refer to the T52A/B machine. Gösta Borelius has not been able to find this number in the available FRA documents. As the author talks about the transposition relays it is possible that he refers to the message-key unit that was used on the T52C machine. The use of the terms 'transposition relay' and 'transposition circuit' does not refer to the machine's permutation of the Murray code elements, but rather to a basic circuit-building block, the transposition unit, which contained a double change-over contact. This basic building block was used to perform all the necessary operations of modulo-two addition and permutation of the teleprinter code elements. A total of fifteen transposition units was used to construct the message-key unit. The T52C machine was the only machine to employ this feature.

3. Due to an anomaly of the rotor movement in the Enigma machine, the 2nd or middle rotor will step twice every time the 3rd or left rotor is advances. Therefore the period is 26x25x26 = 16900 instead of 26x26x26 = 17576, but the machine has a total of 17576 starting positions.

4. There is some slight confusion here about the terminology. The early Siemens T52A/B machine (1937) was called Geheimzusatz while the Lorenz SZ40 and SZ42 machines were called Schlüsselzusatz (cipher attachment). The use of the Z designation for the SZ40 machine probably comes from the German use of the letter Z to describe this machine while setting up an encrypted communication circuit. To set up encrypted communication with the T52A/B they would transmit in clear the Q-code "QEK", while for communication with the T52C and the SZ40 machines they would transmit "QEK C" and "QEK Z" respectively.

5. The author uses the term "transposition connection", which is correct in the sense that it transposes the function of a given code wheel, but it is a term likely to be confused with the machine's permutation circuit or the transposition unit. The translator has therefore decided to call this part the selective or programmable connection.

6. Because the enciphered text can contain any of the 32 possible teleprinter combinations, including the six control signals, the teleprinters used for interception had to be modified. In these specially modified teleprinters the signals *carriage return*, *line feed*, *letters*, *figures*, *space* and *null* were replaced with the numbers 1,2,3,4,5 and 6. All the other combinations were represented by their

corresponding letter as normal. The British codebreakers at Bletchley Park used a similar arrangement where they repaced the six control signals by the characters *4*, *3*, *8 or -*, *5 or +*, *9 or .* and */*. See Appendix A.

7. The construction of the decryption units, Apparna, was led by engineer Vigo Lindstein of L.M. Ericson's cash register department.

8. The breaking of the SZ40 machine was based on intercepted radio traffic, but some SZ40 traffic appeared also on the normal telegraph lines. This traffic covered the period from 26 November 1941 until March 1943 and the first Swedish break into the SZ40 took place on 9 April 1943.

9. The codebreakers at Bletchley Park made a break into the Siemens T52 machine during the summer of 1942. They had followed the use of this machine that BP called Sturgeon for some time. The T52 machine was mainly used on radio teleprinter links belonging to the German Air Force and the German Navy. Due to a question of priorities BP allocated their resources on the German Army links that used the Lorenz SZ40 and SZ42 machines. However, it appears that the Swedish codebreakers were the first to break the Siemens T52 machines.

10. It is more likely that the crypto department was looking for probable words or "cribs" than testing for correct decryption.

11. The author refers here to Commodore Torgil Thorén the chief of the Defence Staff's crypto department. The review of the Nyblad case is part of Thorén's analysis, which is included as Appendix 6 in the 1946 report "Investigation into the Defence Staff's handling of decrypted messages from FRA".

12. It is not entirely clear which machine the 'Y-machine' refers to. It is possible it is the Siemens one-time-tape machine T-43 which towards the end of the war was used on radio communication circuits that also used the SZ40/42.

13. The Japanese machines, Purple, Coral and Jade, were used for high-level diplomatic communications and therefore never carried the same kind of tactically important traffic that was the case for the Enigma. Nevertheless, intelligence from these machines was important for the conduct of the war, and the reports from Japan's ambassador in Germany, Ōshima Hiroshi, contained much information of great strategic value.

Translator's Bibliography

Published works

1. Friedrich L. Bauer. 1995. *Entzifferte Geheimnisse, Methoden und Maximen der Kryptologie.* Berlin: Springer Verlag. German.

2. Friedrich L. Bauer. 1996. *Decrypted Secrets, Methods und Maxims of Cryptology.* Berlin: Springer Verlag.

3. Bengt Beckman. 1996. *Svenska kryptobedrifter (Swedish crypto achievements)* Stockholm: Albert Bonniers Förlag. Swedish.

4. W.W. Chandler. 1983. *The Installation and Maintenance of Colossus.* Annals of the History of Computing. July, 5(3): 260–262.

5. Allen W.M. Coombs. 1983. *The Making of Colossus.* Annals of the History of Computing. July, 5(3): 253–259.

6. Donald W. Davies. 1982. *The Siemens and Halske T52E Cipher Machine.* Cryptologia. October, 6(4): 289–308.

7. Donald W. Davies. 1983. *The Early Models of the Siemens and Halske T52 Cipher Machine.* Cryptologia. July, 7(3): 235–253.

8. Donald W. Davies. 1994. *New Information on the History of the Siemens and Halske T52 Cipher Machine.* Cryptologia. April, 18(2): 141–146.

9. Donald W. Davies. 1995. *The Lorenz Cipher Machine SZ42.* Cryptologia. January, 19(1): 39–61.

10. Cipher A. Deavours and Louis Kruh. 1986. *Mechanics of the German Telecipher Machine.* Cryptologia. October, 10(4): 243–247.

11. Thomas H. Flowers. 1983. *The Design of Colossus.* Annals of the History of Computing. July, 5(3): 239–252.

12. Georg Glünder. 1989. *Als Funker und "Geheimschreiber" im Krieg 1941–1945.* Pionier, Nr.11/12, 1989 and Nr.2, 1990. German. Translated into English by Paul K. Whitaker. Unpublished.

13. Dieter Gollman and W.G. Chambers. 1989. *Clock-Controlled Shift Registers: A Review.* IEEE Journal on Selected Areas in Communications. May, 7(4): 525–533.

14. I.J. Good. 1993. *Enigma and Fish.* In ed. F.H. Hinsley and Alan Stripp. 1993. *Codebreakers, The Inside Story of Bletchley Park.* Oxford: Oxford University Press. pp.149–166.

15. Ken Halton. 1993. *The Tunny Machine.* In ed. Hinsley and Stripp. *Codebreakers.* pp.167–174.

16. Gil Hayward. 1993. *Operation Tunny.* In ed. Hinsley and Stripp. *Codebreakers.* pp.175–192.

17. F.H. Hinsley. 1984. *Geheimschreiber (Fish).* In F.H. Hinsley et.al. *British Intelligence in the Second World War.* London: HMSO. Volume 3, Part 1. Appendix 2, pp.477–482.

18. F.H. Hinsley. 1993. *An Introduction to Fish.* In ed. Hinsley and Stripp. 1993. *Codebreakers.* pp.141–148.

19. David Kahn. 1979. *The Geheimschreiber.* Cryptologia. October, 3(4): 210–214.

20. Wolfgang Mache. 1986. *Geheimschreiber.* Cryptologia. October, 10(4): 230–242.

21. Wolfgang Mache. 1989. *The Siemens Cipher Teletype in the History of Telecommunications.* Cryptologia. April, 13(2): 97–117.

22. Wolfgang Mache. 1992. *Der Siemens-Geheimschreiber — ein Beitrag zur Geschichte der Telekommunikation 1992: 60 Jahre Schlüsselfernschreibmachine.* Archiv für deutsche Postgeschichte. Heft 2: 85–94. German.

23. Wolfgang Mache. 1993. *Lexikon der Text- und Daten-Kommunikation.* R. Oldenbourg Verlag, München. 3rd, revised edition. German.

24. Brian Randell. 1980. *The Colossus.* In ed. N. Metropolis et. al. *A History of Computing in the Twentieth Century.* New York: Academic Press. pp. 47–92.

25. Ernst S. Selmer. 1993. *From the Memoirs of a Norwegian Cryptologist.* In ed. Tor Helleseth. *Advances in Cryptology - EUROCRYPT '93.* New York: Springer Verlag. Lecture Notes in Computer Science. 765: 142–150.

26. Ernst S. Selmer. 1994. *The Norwegian Modification of the Siemens and Halske T52E Cipher Machines.* Cryptologia. April, 18(2): 147–149.

27. Glenn Zorpette. 1987. *Breaking the enemy's code.* IEEE Spectrum. September, 24(9): 47–51.

Documents

28. Oberkommando der Kriegsmarine. 1937. *Der Geheimzusatz der Siemens-Fernschreibmachine T.typ.52.* M.Dv. Nr. 35. Geheim. Berlin, Oktober 1937.

29. Deutsche Wehrmacht. 1942. *Schlüsselfernschreibvorschrift (SFV).* H.Dv. g 422, L.Dv. g 704/3b, M.Dv. Nr. 924a. Geheim. 1.12.42.

30. Oberkommando der Kriegsmarine. 1944. *Die Siemens-Schlüsselfernschreibmachine SFM T52d (T typ 52 d).* M.Dv. Nr. 35IV, D.(Luft) T.g.Kdos. 9105d. Geheime Kommandosache. Berlin, März 1944.

This page is intentionally blank.

Appendix A

Modified teleprinters with International Telegraph Alphabet No.2

Lower Case (letters)	Code elements 1 2 3 4 5	Upper Case (figures)	
A	1 1 0 0 0	-	
B	1 0 0 1 1	?	
C	0 1 1 1 0	:	
D	1 0 0 1 0	"Who are you"	
E	1 0 0 0 0	3	
F	1 0 1 1 0	*\)	
G	0 1 0 1 1	*\)	
H	0 0 1 0 1	*\)	
I	0 1 1 0 0	8	
J	1 1 0 1 0	Bell	
K	1 1 1 1 0	(	
L	0 1 0 0 1	)	
M	0 0 1 1 1	.	
N	0 0 1 1 0	,	
O	0 0 0 1 1	9	
P	0 1 1 0 1	0	
Q	1 1 1 0 1	1	
R	0 1 0 1 0	4	
S	1 0 1 0 0	'	
T	0 0 0 0 1	5	
U	1 1 1 0 0	7	
V	0 1 1 1 1	=	
W	1 1 0 0 1	2	
X	1 0 1 1 1	/	
Y	1 0 1 0 1	6	
Z	1 0 0 0 1	+	
1	0 0 0 1 0	Carriage Return	(BP code: 4)
2	0 1 0 0 0	Line Feed	(BP code: 3)
3	1 1 1 1 1	Letters	(BP code: 8 or -)
4	1 1 0 1 1	Figures	(BP code: 5 or +)
5	0 0 1 0 0	Space	(BP code: 9 or .)
6	0 0 0 0 0	No Action	(BP code: /)

Note: **)* Unassigned, reserved for domestic use.