Swedish Cryptology II

By KJELL-OVE WIDMAN
Institut Mittag-Leffler, The Royal Swedish Academy of Sciences, S-182 60 Djursholm, Sweden (Retired)

ANDERS WIK
Swedish National Defense Radio Establishment (FRA), S-161 26 Bromma, Sweden (Retired)

In this second installment about Swedish cryptology, we will describe the successes and failures in intercepting, cryptanalyzing, and reading the secret messages of potentially hostile and other countries during WW2. The information gathered aided the government in its quest to stay neutral and kept the military leadership informed about possible threats of invasion.

After warring with Russia on and off since the Middle Ages, Sweden had enjoyed peace since 1809, when Finland was ceded to Russia. Suspicions about the "hereditary enemy" never vanished, fed by inquisitive Russian navy operations close to Swedish marine maneuvers and rumors about Soviet spying.

The Molotov-Ribbentrop pact and the outbreak of the war in September 1939 did not ease these fears. Germany was not seen as a great threat since its interests seemed to be directed east and west, rather than toward Scandinavia. The Russian attack on Finland in November (the "Winter War") and the establishment of Soviet bases in the Baltic countries naturally heightened the doubts about Stalin's intentions. Despite the wish of many strong voices that she enter the war on Finland's side, Sweden contended with allowing a volunteer corps to be formed, as well as supplying her neighbor with materiel, notably airplanes, artillery, and AA guns. Swedish intelligence was to a large extent focused on the threat from the east.

This month's article describes Swedish successes and failures in intercepting, cryptanalyzing, and reading the secret messages of potentially hostile and other countries during World War II.

On April 9, 1940, the situation changed radically. The German occupation of Denmark and Norway suddenly made an attack on Sweden seem possible, even probable, and her intelligence agencies abruptly had two prioritized targets. In addition, Sweden was now cut off from the West, making trade with the outside world difficult even if not totally impossible. The greatest worries were those for food and oil.

Another complication arose in June 1941 when Germany attacked the Soviet Union with Finland joining in to recuperate territories lost in the Winter War. With German soldiers now stationed also in Finland, Sweden was totally surrounded by potentially unfriendly troops.

The government, sturdily hanging on to its policy of neutrality, tried to steer a course between the belligerent parties by showing a conciliatory attitude toward everybody, though in reality angering both sides, for example, by exporting iron ore to Germany and ball bearings to the United Kingdom. Good intelligence was now of great importance in order to successfully maneuver the treacherous waters of a world on fire.

I. SOVIET UNION

Suspicion of the big neighbor in the east made Swedish Sigint peer anxiously out over the Baltic Sea. An attack would have to cross this water, so keeping track of the Soviet Baltic Fleet was of paramount importance.

At that time, the Soviet military, including the navy, was using a number of superenciphered codebook systems. There were two-, three-, four- and five-digit codebooks. The smaller ones were employed on a tactical level, while the five-digit ones were used for transmitting information of more strategic value.

The four-digit code of the Soviet Baltic Fleet was introduced in June 1938 and was immediately attacked by the small staff of the

Date of publication August 20, 2021; date of current version December 8, 2021.
Digital Object Identifier 10.1109/JPROC.2021.3084438

Defense Staff Crypto Section. The superencipherment system used a bigram substitution for which 20 substitution tables with corresponding decipherment tables were used. Inroads were quickly made, in part due to an intercepted message that mistakenly had been enciphered using a decipherment table.

In May 1939 and again in May 1940, new four-digit codebooks were introduced, and then, the cryptanalysts had to start from scratch. The set of substitution tables was first increased to 60, whereas, starting from May 1, 1940, a system of ten tables, renewed monthly, was used.

The 1939 codebook was readable after about six months and provided valuable information, but, when the encipherment tables were changed, the flow of information necessarily ceased until the new ones had been reconstructed. Those of May 1, 1940, were fairly quickly mastered, and when a new codebook was introduced on May 15, it turned out that the superencipherment tables remained in use for the rest of the month, an unforgivable error on the part of the Russians. Therefore, reconstruction of the new codebook could start immediately, aided also by the fact that one message was sent twice: first using the old codebook and then with the new one. Thus, captured messages started yielding useful information after just a few days [1, pp. 54 and 55].

The four-digit codebooks contained around 9000 groups, of which slightly more than half were reconstructed. This was sufficient to make sense of most messages.

The work on the five-digit system, considered much more difficult to break, was led by Arne Beurling. Good progress was made during the fall of 1939. Since it was known that the Finns were also working on this problem, contact was established, and in January 1940, while the Winter War was raging, Beurling went to Finland to see if a cooperation agreement could be reached. During this visit, the Russians introduced a new five-digit codebook, and the combined effort had to be restarted.

The superencipherment system here consisted of a list of 300 five-digit numbers that were added to the code groups using so-called false addition, i.e., "without carrying." The list was changed daily. A different starting point in the list was used for each message. It is obvious that, if many messages were sent during a day, sections of them would be enciphered using the same random numbers, creating so-called *depth*. This was the point of attack, and by May 1940, the new five-digit system was readable.

Toward the end of 1940 and in 1941, the Russians became more careful. For example, the five-digit superencipherment was made more complicated by adding two sequences from the list, each starting from different points. Although these complications were finally mastered, they made decryption considerably more laborious [1, pp. 167–170]. Even more detrimental was the fact that, in the winter of 1941, traffic started to dry up. Due to a compact ice cover, most of the Baltic, including the Gulf of Finland, was unnavigable from February to May, and messages became rare. After Barbarossa—the German attack on the Soviet Union on June 22, 1941—almost complete radio silence was kept as the Baltic Fleet hunkered down near its base Kronstadt, in the Gulf of Finland.

In the glorious year of 1940, over 10 000 messages were decrypted, yielding invaluable information on the positions and movements of Soviet vessels. Rarely, the dispositions of a potential enemy force have been more accurately known by the Swedish military leadership.

When the Baltic traffic dwindled, available resources were redirected to gather more material from the Soviet Arctic Fleet, resulting in over 2000 messages being decrypted in each of the years 1941 and 1942. This yielded interesting insights into the Soviet war machine and information on the allied Arctic convoys bound for Murmansk and Archangelsk.

If the Soviet Baltic Fleet traffic had priority, the air force was certainly second, and many low-level systems were broken. Through the decrypted messages, dispositions of the Soviet air arm could be followed. During the bombing attacks on Finland and Estonia, target directions could be followed almost in real time, something which would certainly have been life-saving, had Sweden, one day, been included in the attacks.

Red Army traffic was also monitored, and many low-level systems were broken. However, due to the plethora of systems and the enormous quantity of messages, the picture formed from decrypted material was rather piecemeal. During parts of the war, Sweden ceased listening to the Red Army since the Finns provided intercepts to cover Swedish needs.

II. GERMANY

A. G-Schreiber

In the early morning of April 9, 1940, the German ambassador to Sweden, Prinz zu Wied, called on the Swedish foreign minister to inform him about the German occupation of Denmark and Norway and to make certain requests. Thus, the Germans demanded that they be allowed continued use of the telephone and telegraph transmission lines from Norway to Germany running through Sweden, in particular the so-called West Coast cable. The supreme commander, General Thörnell, consulted Erik Anderberg who was now the Head of Signaling, and according to his son, he shouted out aloud: "Object like the devil, but thank God for the possibilities that will give us!" Thus, the Germans were given a cautious yes, and preparations for tapping the lines were quickly set on foot.

After some initial confusion caused by the differences in teletype standards, it was found that, besides telephone traffic, six dedicated four-wire circuits were used for two-way teletype communication, initially in plain. Operator chat indicated that, soon, a "secret writer," in German called *Geheimschreiber* or *G-Schreiber*, would be introduced, and shortly thereafter, German traffic became "severely unintelligible," as a Swedish report had it [1, p. 67].

To handle the captured messages, most of which were now encrypted, transmission lines were organized from the tapping points in Göteborg to "Karlbo," a dilapidated apartment house in Stockholm where the main part of the cipher bureau was housed. A number of redesigned teleprinters were set up to record the messages on paper tape (Fig. 1). A contingent of women then took care of gluing them onto paper sheets that were put into cardboard boxes awaiting further analysis. Aptly, the handlers were nicknamed Glue Princesses.

Several people from the crypto-office took a look at the material but could not make any headway. Finally, Arne Beurling was asked to try. He chose the messages from May 25 and 27 since they seemed relatively error-free, wrote them up on squared paper, 60 × 60 cm, with about 60 characters per line, went home, and—to make a long story short—returned two weeks later knowing how the *G-Schreiber* worked and how messages could be decrypted and the daily settings found.

Once the possibilities of this discovery were realized, a small industry was set up. Special deciphering devices, called "Apps," were built (Fig. 2). They emulated the German device and deciphered incoming messages automatically, once the daily keys had been solved by manual means (usually using depth or trying probable words). The resulting plain texts were then cleaned up by people with good knowledge of German, retyped, and then distributed to analysts and the military and civilian government authorities concerned.

From a modest start with the West Coast cable, which served the link Oslo–Berlin, with time, a number of other teletype and telephone links used by the Germans were tapped, joining Berlin, Stockholm, Helsinki, Kirkenes (Norway), Rovaniemi (Finland), and, for a while, Narvik and Trondheim (Norway).

The end points in Berlin were the *AA* (Ministry of Foreign Affairs) and the *OKW* (Military Supreme Headquarters). In Oslo, Kirkenes, and Rovaniemi, they were the local German military headquarters and, in Helsinki, the German embassy and the German military liaison office.

In Stockholm, the Swedish Telegraph Authority set up a local teletype network for the Germans, with seven branches, including the embassy, the offices of the military attaché, and the air attaché (which had two). All lines were tapped. There were also direct connections from the embassy to their colleagues in Oslo, Helsinki, and Berlin [3, p. 136]. The air attaché's equipment was also used by the local *Abwehr* organization which made it possible to get an insight into German spying and the activities of German agents in Sweden.

The official name of the G-Schreiber was T52, or more precisely, for the variant used at the beginning of the war, T52AB, used by the Army, Navy, Air Force, and the Foreign Office.

The organization set up to handle the flow of intercepted telegrams produced decrypted telegrams on an almost industrial scale, culminating in 1942 when, on average, more than 250 a day were delivered to end users. However, on June 17, 1942, the astonished Swedish crew at Karlbo could read about their own activities in incoming German telegrams: *Achtung, die Schweden hören mit!* (Attention, the Swedes are listening in!). A message from the German military headquarters in Rovaniemi stated that no other than the head of OKW/Chi, General Fellgiebel, had visited and personally given the order to send T52 messages on cables avoiding Sweden or, if that was not possible, to encipher with another machine, the Lorenz SZ40.[1]

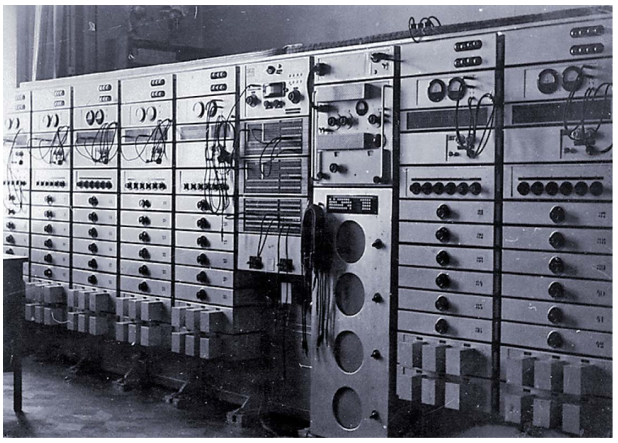

Fig. 1. *Receivers capturing German enciphered teletype messages.*

The source of the unfortunate information to the Germans is believed to have been the Finns who, through their close personal contacts within the Defense Staff in Stockholm, in all probability were well aware of the Swedish success story. In fact, it is easy to imagine that, before General Fellgiebel's visit to Rovaniemi, he had been seeing his colleagues in Finland, Reino Hallamaa and Aladar Paasonen, whose organization the OKW/Chi cooperated with closely. Beckman [1, p. 161] records a belief that the German general had accused the Finns of leaking information on German troop movements to the Swedes, and in order to defend themselves, his hosts then revealed what they knew of the matter.

Naturally, the Germans instituted countermeasures. Besides employing another cipher device, these included introducing new and improved ciphering algorithms and keying practices. Thus, a number of variants of the standard T52AB were introduced, named C, CA, D, and, finally, T52E. The Swedes kept pace for a while, reconstructing C and CA and designing new "Apps" for automatic decipherment, but enjoyed scant or no success with the D and E models. The combination of improved algorithms

[1] "Utredning rörande viss inskränkning och omläggning av tyska fjärrskriftstrafiken med anledning av risk för dechiffrering i Sverige." June 30, 1942. [12] SE/KrA/0202/009/01 H/B 2/8.

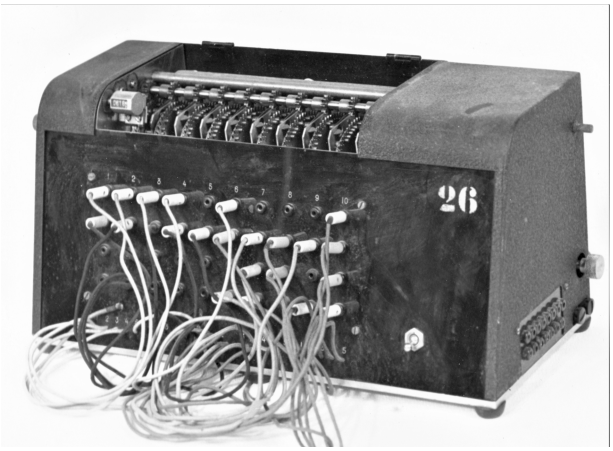

Fig. 2. *"App," deciphering device for messages encrypted by German T52.*

and stricter keying practices caused this source of military intelligence to dry up in the course of 1943, while some diplomatic traffic continued to be read in 1944.

Despite this setback, the results achieved, while luck held, were impressive. The total number of German messages decrypted during the war is estimated to have been around 500 000 [2, p. 154] of which around half were deemed worthy of distribution to the relevant authorities. At the end of 1942, 32 deciphering "Apps" were in use, 16 of which could handle C/CA messages. In addition, a considerable number of plaintext messages were intercepted, some of which were also distributed. The yearly numbers are as follows:

1940	1941	1942	1943	1944
7100	41 400	120 800	98 600	29 000.

Approximately, 80% of the messages were decrypts. On one day in October 1942, 682 telegrams were decrypted.[2] The over 300 000 delivered German messages are neatly archived in the Krigsarkivet (The Military Archives of Sweden) in Stockholm, occupying about 80 linear meters.[3]

Arne Beurling's feat, reconstructing the T52 from scratch, using only intercepted telegrams and operator chat, must be considered to be one of the foremost cryptanalytic achievements of WW2. His experience with cryptomachines had, hitherto, been limited to mechanical devices. His knowledge of teleprinters, or electromechanics in general, was very limited. According to his own account, he had asked himself, what are the simplest ways to encipher five-bit characters? One can switch the positions of the individual bits, and one can XOR a sequence of bits to them. That was exactly what was going on in the T52. His material contained quite a few messages in depth, but, since the ciphering process was not purely additive, the standard method for extracting plain text was not immediately applicable. However, using his hunch about permutation of bits, he managed to wrench out portions of plain text. He then noticed that the presumed additive sequences did indeed exist and were periodic, and seemed to emanate from five pinwheels, a technique with which he was familiar. It also transpired that the permutations of bits were likewise controlled by five other pinwheels.

During the crucial years before Stalingrad and El Alamein, the information delivered by the G-Schreiber decrypts to the Swedish authorities gave invaluable insight into the German war machine in Norway and Finland, its dispositions, manpower, and armaments. However, most of all, it had the potential for answering the essential, vital question of the government, and the military leadership: are the Germans going to attack Sweden, and in that case, when and where? Since, in all probability, such an operation would have had to involve the German troops in Norway, who would need instructions, orders, and alerts, it is estimated that Swedish authorities would have had a two-week head start for defensive measures. Also, German troop movements in Norway, detected through other means, could be ignored since, through the decrypts, they were known to be inoffensive, thus saving on costly mobilizations. Not only information about the local situation was gleaned: regular reports from Berlin headquarters to the commanders in Norway and Finland about the military situation in all the war theaters gave an insight into how the war developed, as seen from a German perspective. After the Eastern offensive had stalled and it was realized that the invincible German war machine had been stretched too far, it allowed the Swedish authorities to take a more aggressive attitude, daring more often to delay or outright refuse German demands.

B. SZ40/42

A new, stand-alone, ciphering machine for teleprinters, manufactured by C. Lorenz AG, and called SZ40 was introduced in mid-1941 and cable traffic picked up in earnest from November 26. From other accounts, it was known that the SZ40 was mainly intended for use with wireless radio, so-called radio teletype, and the efforts to capture such transmissions were, therefore, started in January 1943.

In the beginning, despite repeated attempts, only partial results were obtained in the analysis of the SZ40 traffic, and by March 1943, a 1.5-meter tall pile of undecrypted messages had built up. However, on March 1, 1943, a three-man team mounted a new fresh attack, and by April 9, the functioning of the SZ40 was completely known. As in the case of the T52, the reverse engineering was performed with information gleaned from intercepted messages only and, to some extent, from operator chat

[2]"Distribuerade meddelanden 1940–1944." Undated report [11, p. 10].

[3]"C-papper" [12], SE/KrA/0955/003 H/B XI.

but wholly without knowledge about the actual machine. An enhanced model, SZ42, was successfully reconstructed six months later [2, p. 181].

To decipher SZ40 and SZ42 messages, a primitive mechanical contraption was built, with bicycle chains playing the role of pinwheels. Of course, the settings, i.e. the keys, had to be found first. This required manual intervention, using messages in depth. In the summer of 1943, wireless messages sent from Berlin to military units in the Baltic were intercepted and decrypted, and a certain amount of other traffic was successfully read, but, due to the poor quality of the intercepts and the lack of resources, this source of information never assumed an important role [2, p. 186].

C. Enigma

The German tactical cipher device Enigma was more or less regularly broken and read by the British and American Sigint agencies. The information thus gained had profound importance, in particular regarding the hunt for German submarines. The Enigma was studied in Sweden but was deemed hopeless. The ciphering principle was known from its having been offered to the Swedish military in the 1920s, and material to work with should have been plentiful enough. However, unlike the British, the Swedes had no information on the modifications made in the 1930s, nor did they have access to actual rotor wirings.

D. Diplomatic Systems

As we have seen, the T52 installed at the German embassy in Stockholm was read from the fall of 1940 through 1944 and partially well into 1945 [3, p. 139]. However, important messages were also sent by other means, such as diplomatic mail, and/or encrypted by the standard superenciphered code systems used by the AA, known as *Blockverfahren* (GCE in American parlance) and *Grundverfahren* (GEE, Floradora). The ciphering principles of these systems sought to emulate an OTP system but were nevertheless broken by the Americans but not by the Swedes.

E. Allied Efforts Against German Systems

It is interesting to compare Swedish cryptanalytic achievements with those of the United States and the United Kingdom, whose resources, however, were of a completely different magnitude.

Beurling's achievement with the T52 ("Sturgeon") was repeated by the British two years later, based on radioteletype messages picked up from a link between Sicily and Libya [4]. They were also able to break into the T52D in 1944. However, since the T52 was mostly used on landlines not accessible to the Allies, the value to the war effort turned out to be marginal.

The SZ40 ("Tunny") was broken in January 1942 by the British, a year before the Swedes. To continually read messages, a number of devices were built at Bletchley Park, culminating in the famous "Colossus." Since SZ40, and later SZ42, traffic to a large extent was wireless and, thus, could be more easily intercepted, and moreover, often concerned strategic matters, its value to the Allied war effort was great.

As we have seen, the important Enigma traffic read by the Allies was beyond reach for the Swedes but would, in fact, have been of comparatively little value, given that it was used on a tactical level and a German military attack never materialized.

F. Germans' Own View

In view of the Swedish success against German enciphered teletype traffic, the question inevitably arises: how could a minor actor, such as Sweden, overcome the presumably well-designed products of one of the then technologically most advanced countries in the world?

The answer seems to lie in the lack of a central German authority regarding cryptomatters. In addition to the supposedly central agency OKW/Chi, the Army, Navy, and Air Force, as well as the AA, the Auswärtiges Amt, all had their own cipher bureaus, and internecine competition played a role. The weakness of the T52 was well known in some quarters. Already in the 1930s, a corporal Schulze had made a theoretical study resulting in a negative verdict. Later, Dr. Erich Hüttenhain, the Head of cryptanalysis of the OKW/Chi, concluded in a report from 1939 that security was insufficient.[4] Nevertheless, since OKW/Chi had no power of decision, the T52 was used on a grand scale by the German Army (80 units), Navy (200), and Air force (170) [6, p. 92]. According to legend, the AA cipher section had analyzed the T52 and concluded that its security did not suffice, and its use was prohibited [5]. However, at least 30 machines of this type were employed at the Foreign Office and its embassies, including several in Stockholm [6].

OKW/Chi also had serious doubts about the security of the Enigma and the SZ40/42 but did not have direct insight into or influence on its usage.[5]

III. OTHER SIGINT TARGETS

Although Swedish Sigint and cryptanalysis resources were mainly directed toward the Soviet Union and Germany, neither the Allies nor other countries were neglected.

At the outset of the war, codebook systems, with or without superencipherment, were the preferred method of encryption in the diplomatic world, while the military often used simple handheld gadgets or pen-and-pencil methods. With time, ciphering machines became more common. Germany and the United Kingdom used locally developed devices, while others, in particular smaller countries, bought commercially available equipment, and

[4]TICOM I-31 [10, p. 14].

[5]"OKW/Chi Cryptanalytic research on Enigma, Hagelin and cipher teleprinter machines." TICOM I-45 [10].

this usually meant Hagelin C-36 or C-38. Since the security, in this case, was highly dependent on usage and keying practices, inroads could often be found, sometimes with the aid of operator errors. Swedish familiarity with these machines, of course, aided in their exploitation.

Among the countries receiving Swedish attention in the beginning of the war, France stood out through its diplomatic service using a multitude of codebooks, used with or without superencipherment. The head of the French section was the multilingual Yves Gyldén whose command of the language contributed greatly to the success in reading this traffic. Even after the German occupation of France, the Vichy government and the Free French were successfully targeted.[6]

Due to lack of personnel, other countries were only sparingly investigated first although some British and American codes were read [2, p. 189]. As the German material waned after 1942, resources were freed up so that other targets could be attacked. Over the whole of the war period, inroads were made into military and diplomatic traffic from Argentina, Belgium, Brazil, Bulgaria, Chile, Colombia, Czechoslovakia, Finland, France, Greece, Hungary, Italy, Mexico, The Netherlands, Norway, Poland, Portugal, Rumania, South Africa, Spain, Switzerland, Syria, Turkey, the United Kingdom, the United States, the Vatican, and Yugoslavia. A certain number of messages of Chinese and Japanese origin were also decrypted, but the lack of translators made it difficult to make use of the information gained.[7]

The value of the decrypted information varied greatly. Those diplomatic systems of the major powers that could be decrypted, were mostly of low-level importance, while those of smaller countries could yield surprisingly much, often in the form of indirect information.

A target of particular importance was illegal radio transmissions used by agents and spy rings active in Sweden. Here, paper-and-pencil methods and additive key streams taken from books dominated. A problem in this connection was the need to dissimulate the true origin of the information, which was presented in court. Care was taken to find plausible-sounding sources other than cryptanalysis since, apart from the wish to keep all such activities secret, it was feared that information found by cryptanalysis would not be legally admissible [1, p. 114].

The interception of illegal radio transmissions posed a particular problem since monitoring the entire shortwave spectrum would require large resources. To remedy this, the Swedish engineer Bertil Arvidson—later Technical Director at FRA (The National Defense Radio Establishment)—in 1936 constructed an aperiodic receiver that was able to detect nearby shortwave transmitters regardless of the transmission frequency.[8] In 1944, around 1000 Apes were in use, with 270 covering large parts of Stockholm (Fig. 3). They were connected to a central station where the frequency and the received Morse signals could be registered. The effective range of an Ape was 500–1000 m [3, pp. 191 and 192].

Fig. 3. *"Ape," aperiodic radio receiver used to identify and capture illegal agent radio traffic. Photograph by Johan Antus.*

Weather prediction became adversely affected as soon as the war broke out since most countries immediately started enciphering meteorological observation data sent by radio. Since any prediction valid for more than a few hours needed data from a wide area, forecasting almost came to a halt. The Swedish Meteorological Institute started their own, surprisingly successful cryptanalysis unit, but the results were considerably improved after the FRA took over. Most weather observation data from neighboring countries, including Germany—which, for some time, provided weather observation data from almost all of Europe—could, thus, be collected and used. An unfortunate exception was the United Kingdom, which was thought to have used a one-time system [1, pp. 203 and 204].

IV. COOPERATION WITH FINLAND

During WWI, Sweden cooperated closely with Germany in attacking Russian diplomatic communications. In WW2, Finland became an important partner for Sweden, actually the only Sigint partner. Initially, the common target was Soviet military traffic, but, with time, the diplomatic correspondence of a range of countries was included.

Finland, from 1809 a Grand Duchy under the Russian Czar, was able to break free in 1917 but remained wary of its big neighbor's intentions, fearing renewed efforts by the Soviet Union leadership under Stalin to reincorporate its former dominions. Sigint and cryptanalysis were early recognized as valuable tools to identify potential threats.

As a young navy signaler, Reino Hallamaa became interested in cryptography and Sigint. After finishing cadet

[6]"Distribuerade klartexter 1940–1945" [11] B HB XIX:3. Referenced in [3].

[7]Årsrapporter [11] B HF III:4. Referenced in [3].

[8]A similar device, nicknamed Watchdog, was later in use in the United States; see report by George E. Sterling: The History of the Radio Intelligence Division Before and During World War II. Available at http://61thriftpower.com/riradio/pdf/ridhist.pdf

school in 1927, he was entrusted with building up a small Sigint group, later to be named RTK, which, by 1939, had grown to about 75 members.

The Finns' fears turned out to be well-founded. On November 30, 1939, the Russians attacked, expecting to quickly cut Finland in two and then occupy it within weeks: the Winter War had broken out. Due to valiant efforts by Finnish soldiers supported by excellent Sigint and cryptanalysis work, Stalin's plans were thwarted, albeit with Finland having to cede large areas of land in the southeast when a peace treaty was signed in March 1940.

When Hitler attacked the Soviet Union in June 1941, Finland joined in, in the hope of regaining territories lost (the "Continuation War"). Again, the RTK under Hallamaa was very successful in reading Soviet military communications, but, nevertheless, in the end, Russian military superiority prevailed, and Finland was forced to accept a painful armistice treaty in September 1944.

By the end of the war, the RTK had become a Sigint and cryptanalysis powerhouse with a staff of around 2000, including support personnel. Their German counterparts considered the Finnish cryptanalysts to be their only peers. The prime target was the Soviet Union, with an emphasis on tactical systems when the wars were raging. Among the many other Finnish feats was the successful breaking of the so-called Strip Cipher, M-138, used by the American State Department for embassy communications.

The cooperation with Sweden started in earnest in 1938 and continued during 1939 with the exchange of intercepted Soviet code materials, ciphering methods, call signs, and other traffic analysis findings. Hallamaa's sharing of his experiences in setting up the RTK was highly valued, and as a sign of appreciation, he was nominated for the Svärdsorden (Order of the Sword) by the Swedish King.

Just before the outbreak of the Winter War, Sweden delivered a large batch of Sigint equipment, such as radio receivers, to the Finns in exchange for information on Russian signaling practices, codebooks, and superencipherment methods [2, p. 116].

In the early days of the Winter War, Sweden provided decrypted information concerning the Soviet attacks at Salla and Suomussalmi.[9] The battlefield value of this assistance has, however, been disputed by Finnish sources [7, p. 66]. During the bombing attacks on Finnish towns in January and February 1940, the Swedes read the target orders sent to the airborne Russian airplanes and relayed them to the Finns. Speed was of the essence since the flying time from the bases around Leningrad to Helsinki and other targets was less than an hour. Thus, a hole was sawed in the floor of the Swedish interceptors' office, so captured messages could be thrown down to the cryptanalysts below to be decrypted, reenciphered, thrown back up, and then radioed over to Finland [1, p. 61].

[9]Personal information to the authors from some who took part. See [8, p. 363].

In 1940, Sweden supplied some 50 Volvo covered trucks to be used as mobile interception units together with receivers, transmitters, and direction-finding equipment.

A certain division of effort developed over time. Thus, Finnish capabilities regarding the Red Army traffic were so good that Sweden at times stopped listening and relied on the intercepts provided to them by the Finns [3, p. 149]. On the other hand, Sweden delivered material on the Soviet Baltic Fleet, which remained a Swedish specialty.

In the spring of 1941 [7, p. 222], cooperation in the form of exchange of intercepted diplomatic telegrams was taken up; included were American, British, and German material. Through leakage, probably on the Finnish side [7, p. 222], the Americans became aware of the Finnish–Swedish cooperation and put pressure on Swedish authorities. This led to a decision in March 1943 by the Swedish Foreign Ministry to forbid the delivery of intercepts from the United States, Germany, Hungary, and the United Kingdom to the Finns. Nevertheless, Swedish deliveries of American diplomatic material were restarted a year later, and "in the summer of 1944, the exchange had normalized" [7, p. 223].

Further Swedish deliveries of materiel took place in 1941, with aperiodic radio receivers for agent localization, and in 1942, when American radio receivers were supplied on two occasions.

Despite the mutual benefits, the relationship between the neighboring agencies was not always smooth. Hallamaa's organization had other partners, in particular, the German OKW/Chi, and according to the unwritten rules of the business, information emanating from Germany must not be revealed to the Swedes. Likewise, Sweden was unwilling to share information revealed through their German sources[10] and tried to keep their results on the Siemens T52 secret, probably in vain, since the Finns are suspected of leaking information on this to the Germans. It also seems the Finns often withheld valuable knowledge, suspicious that the Swedes would leak information to the British (which was not without its foundation [1, pp. 161 and 162]).

Fears of an outright occupation by Russia after the armistice of 1944 led to the evacuation of large parts of the RTK and the military intelligence organization under Aladár Paasonen. Personnel, including their families, some 750 individuals, equipment, and archives, were shipped over to Sweden in September 1944, a secret operation codenamed *Stella Polaris*. The Finns expected to continue their Sigint activities on Swedish soil but were prevented by the authorities; this would have been too obvious a violation of the neutrality policy of the host country. Nevertheless, for a while, a small Finnish contingent of interceptors and cryptanalysts worked clandestinely from

[10]A concrete example is that, in sending a report on the Soviet Arctic Fleet in 1942, the Swedes carefully omitted information on station signals that they had extracted from decrypted German messages [7, p. 207].

a hideout outside Stockholm and sold copies of the results to the local OSS office [9].

Important parts of the Finnish archives were bought by the FRA, and about two dozen interceptors and cryptanalysts were employed, substantially increasing the Swedish Sigint capabilities concerning the Soviet Union.

Hallamaa and Paasonen, accused of treason at home and finding themselves without resources, proceeded to sell other parts of their stash, in particular codebooks and other cryptoanalytic material, to whoever would buy them, sometimes selling the same things several times over [9]. Customers included the United States, the United Kingdom, France, and Japan. The two leading figures in the intelligence war against the Soviet Union then had to take refuge abroad, unable to return to the homeland that owed them so much.

For Sweden, the cooperation with Finland was very profitable from an intelligence-gathering viewpoint and would have been extremely valuable under a different war scenario. When considered from a political angle, it, of course, went against the grain of the neutrality principle, just like the German-Swedish cooperation did during WW1.

V. SWEDISH CRYPTOSYSTEMS

Given that the Swedish cryptanalytic efforts must be considered very successful during the Second World War, it is legitimate to ask how well the country's own protection fared against foreign codebreakers. The short answer is that the Swedish systems were not impregnable, but, on the whole, higher level systems seem to have held out well. For tactical systems, the verdict is not so good, but it must be remembered that all countries at this time used many vulnerable systems.

The workhorse for the military was the Hagelin six-wheel C-38 with its keyboard companion BC-38. A hand system of transposition type, HGA, served as backup. In addition, there were tactical level two- and three-figure superenciphered codebook systems, particularly popular in the army, and manual matrix systems of the Slidex type. The navy, for a while, continued to use the B-21, but, since it was no longer adequate, it was phased out in 1941.

On the diplomatic side, apart from some older codebook systems, messages were protected using either an OTP (one-time pad) system or the Hagelin C-38.

In the beginning, both diplomats and the military considered the C-38 very secure. Yves Gylden was the responsible expert. In May 1940, he wrote that "even a preliminary examination would make prospective attackers abandon the idea and turn their attention to more amenable targets." He goes on to state that the five-wheel C-362 and even more the six-wheel C-38 would provide completely adequate protection, given that normal security measures were taken.[11] The relations between Gyldén and Beurling were strained, which probably is the reason that Beurling had never been asked to study the Hagelin systems.

However, in the fall of 1941, reports from London and Helsinki[12] indicated that the main diplomatic C-38 system was not secure. A new evaluation was evidently urgent, and at the beginning of 1942, reluctant superiors at the Defense Staff Crypto Section asked a hot-tempered Arne Beurling to give an opinion. His verdict was crushing: the machine was totally insecure. It could possibly be marginally usable with considerably stricter rules and keying practices, including stringent (and short) message length limits and random key settings.[13]

New regulations were hurriedly put in force.

Due to a rich supply of declassified reports about codebreaking during the war, quite a lot has been revealed about foreign attacks on Swedish systems. It turns out that a certain amount of C-38 traffic was decrypted before 1942 but only rarely thereafter and then mostly when depth occurred through operator errors.

With the possible exception of the Soviet Union, the only country systematically attacking Swedish military traffic was Germany. The Germans thought that they had identified no less than 31 different systems.[14] Most of them remained unread, but there were notable exceptions. Their greatest successes seem to have been scored by an army listening post in Halden, Norway, which claimed having read all the lower level systems of the Swedish army and, occasionally, when operator errors allowed it, a number of C-38 messages. As an example, in July 1944, no less than 1105 low-level messages were decrypted and distributed, while, for C-38 and HGA, the report laconically notes "Keine neuen Erkenntnisse" (no new findings). Nevertheless, the results of the Halden group were such that they claimed having built up a complete picture of Swedish army strength, dispositions, and tactical deployment practices.[15]

The diplomatic C-38 should have been vulnerable to attack in the beginning, but inroads seem to have been small and marginal. Germans, Finns, Brits, and Americans did score some successes, but they were intermittent and decryption never reached regular production level.[16] It is known that the FBI managed on at least one occasion to break into the Swedish embassy in Washington, DC, and photograph key lists (Fig. 4).[17] A British report from August 1944 states that *the keys have not been broken since*

[11] "Yves Gyldén: Allmänna forceringssynpunkter" May 15, 1940. F6:13 [13].

[12] C Kry report to CFST, September 25, 1941, and report from the Swedish Military Attaché in Helsinki, October 18, 1941, both in [12]. Fst Kry Series F II:1.

[13] "Report by Arne Beurling. Received March 19, 1942." S, HF I: 20 [11].

[14] Listing of German results on Swedish WW2 systems in [10], Synopsis, vol. 1, pp. 120–122.

[15] E.-Bericht Nr.7/44 Feste Nachrichtenaufklärungsstelle 9, Br.B.Nr. 2135/44 g.Kdos, August 1, 1944. Available at http://chris-intel-corner.blogspot.com/2012/11/. Accessed December 22, 2020.

[16] Capt. Walter J. Fried Reports. NARA: RG 457, Box 880, NSA Historical Collection.

[17] "Key and instructions for Swedish cipher 'MMA'" 1942-10. NARA: RG 457, Box 153, NSA Historical Collection.

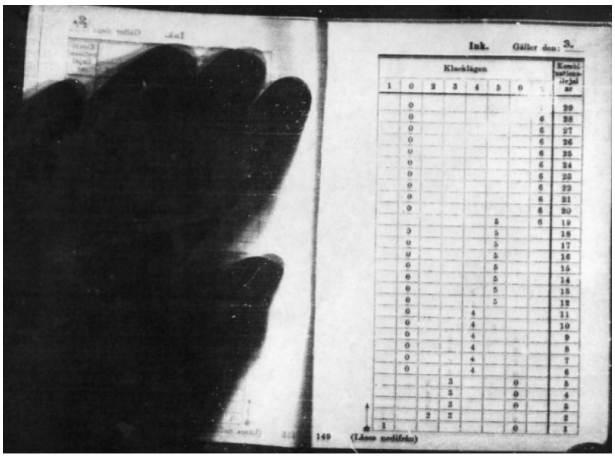

Fig. 4. *FBI photograph of a Swedish key list.*

February 1942 and none of this traffic has been read since June of that year. I understand not much headway has been made in America on this problem [2, pp. 240 and 252], Thus, the efforts to tighten security taken in 1942 after Beurling's analysis seem to have borne fruit.

Of course, Sweden would not be of the highest priority for the warring nations, but, since both the British and the Americans eagerly read other neutral countries whenever they could, Swedish communications should not have been uninteresting.[18]

There is no indication that any OTP traffic was read although the production of random numbers for one-time pads posed great problems for the Foreign Office cipher bureau. FRA stepped in and designed a contraption using a combination of mechanical devices with differing periods, combined with human intervention. It seems that the number sequences thus created were sufficiently random-like to avoid exploitation.

Practically nothing is known about Soviet Sigint and cryptanalysis directed against Sweden during the war. Knowing their predilection for close access operations, theft, bribery, and agent recruitment, it would not be surprising if they, in such a manner, gained insight into both diplomatic and military communications.

VI. CRYPTO TOOLS

To the contemporary cryptanalyst, having access to computing power undreamed of at the beginning of WW2, it might be difficult to imagine the difficulties facing his colleague at the time.

The laborious search processes, involving examination of large quantities of intercepted material while looking for repeats and statistical anomalies, had to be done by hand. Mechanical and electromechanical devices had started to appear, however. In particular, the so-called tabulating machines (Hollerith machines) could relieve the—often female—staff of tedious tasks. Speed was, of course, another factor: in 1944, Åke Rossby, the Head of the FRA Cryptanalysis Section, stated that, without the Hollerith machines, an important system used for enciphering meteorological observation data could not have been decrypted fast enough to be of any value. Ingenious early programmers even managed to use the Hollerith machine for computing trigonometric functions, used for attacks on the Hagelin C-machines.

Unlike Britain and the United States, Sweden did not have the resources to build special machines, such as the Colossus or the Bombe, to be used for codebreaking. However, a step in this direction was taken in 1943 when the FRA proposed to the Swedish Defense Research Committee that Sweden start developing a computing machine using "dual numbers," to be used also for cryptanalytical purposes; rumors of the Eniac project had reached Swedish shores.[19] Nothing came of this proposal.

A problem of a different nature appeared once a system was broken: intercepted messages had to be deciphered fast and economically. In order to cope with the German T52, special electromechanical devices, "Apps," were built which emulated the corresponding cipher machines. The corresponding mechanical device for the SZ40/42 was rather primitive but served its purpose, given the small amount of intercepted traffic.

VII. BIRTH OF AN AGENCY

From a modest start at the beginning of the war, the Sigint and Crypto Sections of the Defense Staff grew considerably and managed to produce high-value intelligence not only for the military but also for the Government, the Foreign Office, and the police.

The dispersion of activities, such as cryptanalysis, processing, and compilation, at around a dozen locations in and around Stockholm made administration and coordination difficult. Also, civilian authorities, such as the Foreign Office, complained that the military control of the distribution of decrypted telegrams at times precluded their having access to all the available information.

Thus, a new, independent civilian agency was established on July 1, 1942, with the purpose to handle all aspects of Sigint activities. New headquarters for the FRA, the National Defense Radio Establishment, were built 15 km outside the Stockholm city center, close to the Drottningholm royal castle.

The FRA is still in the same location. Many things have changed, but the core business remains the same. ■

Acknowledgment

The English-speaking reader may find the first two references of interest for further reading.

[18] FBI provided The Military Intelligence Service with information on Swedish cryptosystems and messages on several occasions. See, in particular, a letter from J. Edgar Hoover to General Edwin M. Watson, Secretary to the President, November 9, 1942. Available at https://sverigesradio.se/Diverse/Appdata/Isidor/Files/83/14100.pdf. Accessed December 23, 2020.

[19] Åke Rossby, the Deputy Director of the FRA, had a brother, Carl-Gustaf Rossby, who was a Professor at The University of Chicago and a well-known meteorologist with insight into the ENIAC project. A hint between brothers can be suspected.

REFERENCES

[1] B. Beckman, *Codebreakers: Arne Beurling and the Swedish Crypto Program During World War II*, K.-O. Widman. Trans. Providence, RI, USA: American Mathematical Society, 2002.

[2] C.-G. McKay and B. Beckman, *Swedish Signal Intelligence 1900–1945*. London, U.K.: Frank Cass, 2003.

[3] J.-O. Grahn, *Om Svensk Signalspaning. Andra Världskriget*. Stockholm, Sweden: Medströms, 2018.

[4] F. Weierud, "Sturgeon, The FISH BP never really caught," in *Coding Theory Cryptography*. Berlin, Germany: Springer, 2000, pp. 18–52. [Online]. Available: https://cryptocellar.org/pubs/sturgeon.pdf

[5] M. van der Meulen, "The road to German diplomatic ciphers—1919 to 1945," *Cryptologia*, vol. 22, no. 2, pp. 141–166, Apr. 1998.

[6] W. Mache, "Der Siemens-Geheimschreiber," *Archiv Für Deutsche Postgeschichte*, no. 2, pp. 85–94, 1992. Accessed: Dec. 19, 2020. [Online]. Available: https://www.cryptomuseum.com/crypto/siemens/t52/files/mache_t52.pdf

[7] L. Lehtonen, T. Liene, and O. Manninen, *Sanomansieppaajia ja Koodinmurtajia*. Jyväskylä, Finland: Docendo, 2016.

[8] D. Kahn, *The Codebreakers (Paper Back Version)*. London, U.K.: Sphere Books, 1973.

[9] M. Aid, "'Stella Polaris' and the secret code battle in postwar Europe," *Intell. Nat. Secur.*, vol. 17, no. 3, pp. 17–86, Sep. 2002.

[10] *Army Security Agency, European Axis Signal Intelligence in World War II as Revealed by TICOM Investigations*, Riksarkivet, NARA College Park, College Park, MD, USA. [Online]. Available: https://www.nsa.gov/news-features/declassified-documents/european-axis-sigint/

[11] *FRA Arkiv*. Bromma, Sweden.

[12] *Krigsarkivet*, FRA, Mil. Arch. Sweden, Stockholm, Sweden.

[13] *Boris Hagelins Privatarkiv*, Krigsarkivet, Mil. Arch. Sweden, Stockholm, Sweden.

ABOUT THE AUTHORS

Kjell-Ove Widman received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from Uppsala University, Uppsala, Sweden, in 1962, 1963, and 1966, respectively.

After holding appointments as an Assistant Professor at Uppsala University from 1967 to 1972 and a Professor of applied mathematics at Linköping University, Linköping, Sweden, from 1972 to 1981, he worked as a consultant in the communications industry, finishing his career as the Director of the Institut Mittag-Leffler, The Royal Swedish Academy of Sciences, Djursholm, Sweden, from 1995 to 2005. His interest in cryptology dates from his time as a conscript at the Swedish National Defense Radio Establishment (FRA), Bromma, Sweden.

Anders Wik received the M.Sc. degree in mathematics from Uppsala University, Uppsala, Sweden, in 1969.

After two years with the Institut Mittag-Leffler, The Royal Swedish Academy of Sciences, Djursholm, Sweden, he took employment as a Cryptologist at the Swedish National Defense Radio Establishment (FRA), Bromma, Sweden, in 1972. He retired in 2007 as the Deputy Director of FRA and has since then, among other things, worked in the field of history of cryptography both within and outside FRA.