SWEDEN CRYPTOGRAPHIC SUPERPOWER A BOOK REVIEW*

Frode Weierud†

ADDRESS: 4 Le Pre Vert, 1041 Rte de Mategnin, F-01280 Prevessin-Moens, FRANCE.
Email: Frode.Weierud@cern.ch.

Beckman, Bengt. *Svenska kryptobedrifter (Swedish crypto achievements)*. Albert Bonniers Förlag, Stockholm, Sweden. 1996. 289pp. ISBN 91-0-056229-7. Skr. 292. In Swedish.

Sweden has been solidly linked to cryptography for more than 70 years largely due to the efforts of Arvid Damm, Boris Hagelin and Yves Gyldén. Back in 1966, David Kahn wrote: "Quite possibly the finest feat of cryptanalysis performed by the Swedes, and the most far-reaching, was Arne Beurling's solution of the German Siemens machine"; thus showing us the tip of the Swedish cryptanalytical iceberg. Now, Bengt Beckman, the former chief of FRA's (Försvarets Radioanstalt) cryptanalytical department, has given us all the details about this magnificent feat and much more. The book contains a well of information. It starts with a short and clear introduction to ciphers and codes followed by an overview of Swedish cryptanalytical history including detailed accounts of how several of the breaks were performed. The second part of the book consists of three chapters dedicated to Professor Arne Beurling. Arne Beurling was clearly a genius, just like Alan Turing, he worked from first principles, however the similarity ends there. Arne Beurling was clearly a ladies' man who liked an enjoyable evening in town, but he could also be stubborn and difficult; he is even known to have ended some arguments with his fists. Despite these flaws, Arne Beurling comes through as a very likeable character with a striking personality.

The Swedish cryptanalytical achievements are top class and therefore it is only appropriate to put Sweden in the same league as the other cryptographic 'superpowers' at the time: Poland, England and USA. Arne Beurling broke into

*The article was published in *Cryptologia*, 22(1): 25–28, January 1998.

†This article represents the views of the author but not necessarily those of his employer or any other third party.

the Siemens T52A/B traffic in June 1940, based on a set of messages in depth intercepted on 25 and 27 May. The first T52 or Sturgeon traffic to be read by Bletchley Park passed between Sicily and Libya in 1942 [1]. BP observed, as did Arne Beurling, that the Germans had the habit of sending large numbers of cipher messages on the same key. BP's first break was with a depth of 40, while later they also improved their techniques to allow breaks with depths of 4 or 5. As BP first broke the Lorenz SZ40 traffic in January 1942 it is probably safe to say that Sweden was the first ever to break modern, on-line teleprinter ciphers. It is indeed a historic achievement, but they did not stop there. On 9 April 1943, they broke the Lorenz SZ40 traffic that passed on their cables, while in June and September they did the same with the SZ40 and SZ42 radio traffic [2]. They also continued to break the improved T52 machines, T52C and T52CA, but when the much improved T52D was introduced in December 1943 they had to give in to defeat. The German keying practices had greatly improved and the intermittent wheel movements of the Siemens T52D machine proved too much for the Swedish techniques. It should be stressed that all these machines were broken by hand and that the Swedes only automated the deciphering of the messages by building 'replicas' of the T52 machines themselves. The Lorenz SZ40 machine was simulated by a real 'Heath Robinson' machine using twelve bicycle chains of different lengths.

Like Alan Turing, Arne Beurling was making the initial breaks and leading the way, but afterwards he got other duties and interests thus other Swedish cryptanalysts took over the work. It was a group of three people, Carl-Gösta Borelius, Tufve Ljunggren and Bo Kjellberg, under the leadership of Lars Carlbom who broke the Lorenz SZ40 machine. Before Arne Beurling decided to take on the T52 problem, he had worked on superenciphered Russian codes together with Åke Lundquist. The Swedish cryptanalysts made great inroads into the Russian codes and cipher systems. They were especially successful with the crypto systems used in the Baltic, the Arctic Naval codes and the Red Army's crypto traffic. They were a variegated group of professors in Slavic languages and literature, mathematics and astronomy including a few art historians. Not to forget all the young ladies of 'good' families who like at BP tended to the more menial tasks.

The Finns were also great experts on Russian crypto systems and from an early stage, there was a Swedish-Finnish co-operation. The will to complete openness and co-operation was lacking, but the contacts resulted in operation "Stella Polaris" [3], the evacuation to Sweden of the complete Finnish cryptographic and signal intelligence organisation. On 22 September 1944, three ships arrived at Härnösand in Sweden. A few days later yet another ship arrived in Gävle. A total of 750 people arrived,comprising the Finnish intelligence staff and their families together with 700 crates of signal intelligence equipment, Russian codes and other cryptographic materials. Sweden had never expected such a massive exodus and the Finns were not to succeed in their expectation of continuing their intelligence activities from Swedish soil. The outcome was that many of them re-

turned to Finland, while only about 15 cryptographers and radio specialist were employed by FRA, who also bought technical material for 252875 Swedish kronor. The code and cipher material and other archives were stored at various places by FRA and others. A part of the archives was photographed and it is known that the Finns also sold code and cipher material to several countries, among those are France, Japan, Great Britain and USA. Two of the Finnish intelligence chiefs, Aladar Paasonen and Reino Hallamaa, went for a short time in French service, while later Hallamaa went to Spain and Paasonen to Portugal. Six of the other Finnish experts also went to work for the French intelligence service. Several countries had much to gain from Stella Polaris, while for the Finns it was more like a catastrophe, many of them never fully recovered from their disappointment. The chief of the Finnish cryptanalytical department, Erkki Pale, ended up in prison for 20 months, once he finally returned to Finland.

Bengt Beckman has decided to draw the line at the end of the war, stating that what comes after still remains classified. However, during the war Sweden had gained considerable experience in cryptography and cryptanalysis. In addition, with the influx of the equally talented Finns they were clearly uniquely equipped to target their next enemy, the Soviets. It is therefore not surprising that at the beginning of 1946 the Swedes started a close intelligence co-operation with the Norwegians [4], which continued well into the 1960s [5]. In those early days, the Norwegians were well placed for intelligence collection. They mainly intercepted Russian military radio traffic and telegram traffic to and from the various East European embassies and offices in Oslo; while the Swedes were doing most of the cryptanalytical work. Later on the share of the work was much more balanced, but how successful they were is still largely unknown. There are of course a number of stories circulating about both of the counties' prowess in intelligence collection and cryptanalysis. For instance it is said that the Swedes followed every step of the Russian rocket shipments to Cuba in 1962, but to know the real truth we will probably have to wait for some time yet.

The book is well written and at times it reads like a good thriller. It has got a good reception in Sweden and it is already in its fourth edition with a total of 20000 copies sold which is quite an achievement. There has been several radio and television interviews of Bengt Beckman and his book has received favourable reviews, but across the border in Norway the book is virtually unknown. Early this year, attempts were made to have the book reviewed in some of the Norwegian daily newspapers. Although the book contains new and unpublished information about Sweden's direct involvement in the illegal radio traffic to Norwegian agents and secret forces, the respective editors found it largely uninteresting. It is a great pity if Norwegian future generations will continue to believe that the only help they got from Sweden during the war was *svenskesuppen*, the Swedish soup.

REFERENCES

1. Unknown author. 1944. *Sturgeon – Type Ciphers*. Addendum to Walter Fried Report No. 116; IR4054, 17 Nov. 1944. NARA, NSA Historical Collection NR. 2612, Box 880.

2. FRA Monograph. 1997. *A Swedish Success, Breaking the German Geheimschreiber during WW2*.

3. Hedin, Sven Fredrik. 1996. Stella Polaris. *Kungl. Krigsvetenskapsakademiens Handlingar och Tidskrift*. pp. 97-108.

4. Lund, Kjetil. 1996. *Lund Kommisjonens Rapport*. Parliamentary Commission for the inquiry into the Norwegian secret intelligence services. Para. 13.3.1 - 13.3.7, History, establishment and co-operation after the war.

5. Tamnes, Rolf. 1991. *The United States and the Cold War in the High North*. Oslo: Ad Notam forlag AS. pp. 49-52.

BIOGRAPHICAL SKETCHES

Frode Weierud is employed by the European Organization for Particle Physics (CERN) in Geneva. He works as a programmer in one of the equipment groups. Cryptography has been his main interest for more than 30 years. His cryptological research is focused on cipher machines and cryptanalytical techniques.