TIRPITZ and the Japanese-German Naval War Communication Agreement

Frode Weierud

Preface

This paper has been published in the Summer 1999 issue of Cryptolog the publication of the U.S. Naval Cryptologic Veterans Association (NCVA). It is now published here in its entity as an electronic publication with the full permission of Cryptolog and the NCVA.

Cryptolog reference:

> Frode Weierud, “TIRPITZ and the Japanese-German Naval War Communication Agreement”, Cryptolog, Vol. 20, No. 3, Summer 1999, p. 6, p. 10.

Frode Weierud, © October 1999

COPYRIGHT

TIRPITZ and the Japanese-German Naval War Communication Agreement

by Frode Weierud[*]

The Agreement

During the Second World War the German and Japanese Navies agreed on a joint communication plan which was signed on 11 September 1942.[1] The signatories were the German Vice Admiral Erhard Maertens, Director of the Naval Communication Service, and the Japanese Naval Attaché in Berlin, Rear Admiral Tadao Yokoi. The agreement, entitled "The Japanese–German Naval War Communication Agreement," was a result of the more general Japanese-German Military Agreement which was signed on 18 January 1942. The communication agreement set out in detail how the two forces should communicate and by what means. It dealt with call signs, addresses and signatures. It also gave instructions for the encipherment of call signs, but it did not explain what crypto system would be used. However, deciphered Japanese Naval Attaché communications show that it was originally planned that all the traffic would be enciphered by machine. The machine was referred to as T-Enigma or Enigma model T.[2] It was called TIRPITZ by the Germans and spelled as "TIRUPITSU" by the Japanese. The US Navy named the machine OPAL and the traffic received the designator JN-18.

The Japanese Navy originally placed an order for 800 T-Enigma machines, but this number of machines was never delivered for various reasons. First of all there was an initial delay in the design, production and delivery of these machines. For this very reason it was decided to prepare two manual systems to cover the communication needs in the interim period. Secondly, the Germans started to doubt the security of the machine and they found it increasingly difficult to supply the materials for the production.

The first of the manual systems, Sumatra, was designed by the Japanese and received the title "Japanese-German Navy Joint Use Code No. 1". The first version, Sumatra 1, was active from the signing of the communication agreement in September 1942 to 15 February 1943, when it was cancelled by Tokyo due to fear of compromise. A revised version, Sumatra 2, became operational on 1 August 1943 and was valid until the end of the war. The US Navy never observed any traffic in this system, although the external characteristics were known and were identical for the two versions.

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

[1] The information about the agreement is based on *Study of Japanese-Naval Joint-use of Ciphers During World War II,* (*RIP 209*), National Archives and Records Administration (NARA), RG 457, NSA Historical Collection, Box 580, Nr. 1419.

[2] See David H. Hamer, Geoff Sullivan and Frode Weierud, *Enigma Variations: An Extended Family of Machines*, Cryptologia, 22(3), July 1998, pp. 211–229.

The second manual system was designed by the Germans and was known as TOGO. Its full title was “Japanese-German Joint Use Code No. 2”. Like Sumatra it was divided into the same two periods and it was known as Togo 1 and Togo 2. Also here no traffic was ever observed but the external characteristics were known to the US Navy.

A Security Blunder

The suspected compromise reported on 15 February 1943 happened during the Guadalcanal withdrawal when the Japanese had no time to burn their cipher material. The instructions for using Sumatra and Togo, and the list of call signs, were torn into small pieces, scattered, and buried in the sand close to the shore in three spots, each at an interval of three kilometres. This curious incident is also mentioned in a historical report on Japanese Naval communications.[3] As the history says, while transporting provisions to Guadalcanal Island, the submarine I-1 was stranded on the coast of Kamimbo during combat with an American motor torpedo boat. The responsible persons evacuated some of the top secret documents from the boat and buried them in the coastal sands. This incident was first reported a month later when the crew returned to Rabul. The Submarine Squadron Command issued orders to dig out the documents immediately and destroy them but one or two of the hideouts could not be located. Moreover, as the stranded submarine, which had part of its hull exposed, was still known to contain a considerable number of code books, serial bombardment and torpedoing by submarine was carried out. However, complete destruction was not confirmed.

David Kahn also refers to the incident with I-1 in his book “The Codebreakers”.[4] However, his reference to the submarine I-1 carrying 200 000 code books does not sound credible. In his article[5], “Codebooks From the I-1 Revisited”, Philip Jacobsen has corrected numerous errors in the Operational History as well as in David Kahn’s and other authors’ writings. Far from being an American motor torpedo boat as reported in the Operational History, I-1 was attacked by the New Zealand corvettes Kiwi and Moa. The question about the large number of code books is probably due to a translation or typing error. The Operational History claimed: “The loss comprised many code books for future use in addition to those in current use, totalling 200 000 copies”. Replacing “comprised” with “compromised” might bring us closer to the truth.

Tirpitz – The T-Enigma

The full title for the Tirpitz machine system was “Japanese-German Joint Use Code No. 3”. It consisted of the rules for use, entitled “TIRPITZ”, and the key list which was named “GARTENZAUN”. The rules were effective from 1 August 1943 until the end of the war, while the key list was divided into two periods. The first, Gartenzaun

[3] *Operational History of Japanese Naval Communications, December 1941 – August 1945*. Laguna Hills: Aegean Park Press, 1985, pp.85–86.

[4] David Kahn, *The Codebreakers*, New York: Scribner, 1996, p. 590.

[5] Philip H. Jacobsen, *Codebooks From the I-1 Revisited*, Guadalcanal Echoes, Quarterly Newletter of The Guadalcanal Campaign Veterans Association, P.O. Box 181, Coloma, MI 49038–0181; Vol. 23, Feb.–Mar. 1996, p. 24.

1, was effective from 1 August 1943 to 31 December 1943, while the second, Gartenzaun 2, was valid from 1 January 1944 until the end of the war.

This is the only joint Japanese-German Naval system which was ever observed in use. Between March and August 1944 about 20 messages were sent by Japanese submarines on arriving off the coast of France. These submarines were blockade runners, part of the new Yanagi operation, which tried to maintain a minimum of transport between the two countries.[6] An example of this traffic is the following message intercepted on 5 August 1944.

```
DAN
C″ C″ DAN DAN 63 W12 5/8 1507 BT

KLDSS ANGWY XWMID CRXFC CLQZS UJNRD VJYLG OPFME
TIGPJ DQWIW 01305 01305 AR
```

The repeated group at the end, 01305, contains the message number in the three first digits and the day of the month in the two last digits.

The planning of the joint communication plan probably started relatively soon after the signing of the Japanese-German Military Agreement in January 1942. On 28 March 1942 the Japanese Naval Attaché in Berlin received a message from Tokyo instructing him to add 100 Enigma machines on the shipment which was then being prepared. The message from Tokyo of 15 February 1943 that informed Berlin about the possible compromise at Guadalcanal also informed it about the fate of the Enigma machines on U-Cruiser I-30. I-30 had hit a British mine outbound from Singapore and went down with its entire cargo.[7] However, 16 Enigma machines were landed and safely delivered before the accident occurred. I-30 is known to have left Lorient on 22 August 1942 with 50 Enigma machines on board.

At this time there appear to have been severe problems manufacturing the T-Enigma, as well as questions about its security, and a new machine referred to as “02562-A-Enigma” enters the picture. On 18 May 1943 Tokyo informs Berlin that they are cancelling the purchase of the manufacturing rights for the Enigma type cipher machine, purchase number 02846. It is reasonable to believe that this was the manufacturing rights for the T-Enigma.

The situation about the security of Tirpitz is further explained in a message from Berlin to Tokyo on 15 November 1943. The Chief of the German Naval Communication Service had explained to the Japanese Naval Attaché that after experimenting with the Enigma machine that had been supplied to the Japanese Navy, they had discovered that its security was doubtful if a great volume of traffic was enciphered on it. As it was anticipated that the volume would be considerable, the OKW had issued an order suspending the manufacturing of this type of cipher machine. Furthermore, he noted that manufacturing this machine in large numbers had become difficult due to the shortage of materials. The Germans therefore decided to design a new type of cipher machine which would be satisfactory in security and in the

[6] Ronald Lewin, *The Other Ultra: Codes, Ciphers and the Defeat of Japan,* London: Hutchinson & Co, 1982, p.205.

[7] Carl Boyd, *Significance of MAGIC and the Japanese Ambassador to Berlin: (II) The Crucial Months after Pearl Harbor,* Intelligence and National Security, Vol. 2, No. 2, April 1987, pp.302–319.

materials used. However, they stressed that it would be difficult to build many of these machines quickly and that they would have to be supplied a few at a time. They also expressed their willingness to fill the new Japanese Navy order for 400 machines with the new type. The Japanese Naval Attaché expressed anxiety that the 400 machines of the old type would be rendered useless. Some of these machines had already been delivered, while others were under construction. Here the Chief of the German Naval Communication Service replied: "With regard to this point, the German Navy has given special attention to the convenience of the Japanese Navy. The new type is so designed as to permit joint usage with the old type." He then explained that in the new type there were more plug sockets than in the old type and the number of ways the wiring could be changed was greater. However, by not employing some of the plug sockets the new type could be used like the old type. With this assurance the Japanese Naval Attaché agreed that the new order for 400 machines should be of the new type.

A New Machine, the A-Enigma

It is not known what exactly the new Enigma type looked like but the reference to "02562-A-Enigma" make it reasonable to believe that it was a version of the A-Enigma, which was the standard machine in use with the German Army and Air Force and which was equipped with a plugboard, normally called Stecker. The T-Enigma was not equipped with Steckers. If one removes all the Stecker connections from an A-Enigma all the letters will become self-steckered and the effect of the plugboard will cease. Therefore, if the A-Enigma was equipped with the same wired wheels as the T-Enigma and all of the Steckers were removed, the two machines would be able to communicate. This was probably the solution adopted by the German Navy.

In the dispatch of 15 November 1943 there is also a reference to an order, by the Japanese Army, for the A-Enigma. Furthermore, we find the statement that "ultimately it will be in use by both the Japanese and the German Armies and Navies." As the German Navy used the M-Enigma (M3 and M4) it is likely that this is a general reference to the Enigma type of machines and not to the A-Enigma.

From then on there appear to have been regular but small shipments of Enigma machines to Japan. The Japanese submarine I-29 (U-Kiefer) left Japan on 17 December 1943 and arrived in Bordeaux 11 March 1944. It returned to Japan on 16 April 1944 with German Radar detectors and jammers, sonar decoys (Bolde) and 10 Enigma machines. However, she was sunk on 26 July 1944 near Luzon by USS Sawfish. Other fatal shipments were reported from Tokyo. On 7 August 1944 Tokyo signalled Berlin that MATU departed Shoonan on July 22 but nothing had been heard from her since July 25[8] when she had reported the presence of an enemy submarine in her area. The passengers on this vessel left in Shoonan and continued to Tokyo by plane, while all the cargo was kept on board. Tokyo reported that the suspected loss of this ship with its entire cargo was a severe loss which would be greatly felt by both the Imperial Army and Navy. It is not clearly stated that the MATU carried any Enigma machines but it is quite likely and the cargo list for the ship to follow, GINMATSU, contains the following item:

02561-A-ENIGMA (New Model) – 6 machines.

[8] The document RIP 209 indicates June 25 which we believe to be a mistake for July 25.

However, if the Japanese Navy were now shipping mostly the new A-Enigma to Japan the older T-Enigma had not entirely been abandoned and the rest of the previous production run was still being prepared for shipment. In the summer of 1944, probably at the beginning of August, several T-Enigma machines were captured in a warehouse in the vicinity of Lorient.[9] There are conflicting claims as to how many T-Enigmas were captured, but it probably was about 70 machines.

Conclusion

It seems that Japan was attempting to make a decisive move to using cipher machines for its operational tactical traffic and that the machine selected for this purpose was the German Enigma. However, the message of 28 March 1942 instructing the Japanese Naval Attaché in Berlin to immediately ship 100 Enigma machines makes it clear, that it was not irresponsible journalism in the *Chicago Tribune*, or for that matter secret documents raided from the Australian steamer *Nankin*, that initiated this move.[10] The Japanese decision to adopt the Enigma machine for some of its cipher communications must have been taken well ahead of both of these incidents. Furthermore, Nelson MacPherson's analysis of the implication of a move to the Enigma machine is seriously faulted. He states: *"This was a most fortuitous turn of events for the US Navy, since Enigma was also penetrated by the Allies. Hence, the Nankin documents eventually proved more damaging for the Japanese war effort than they did for the American war effort; the Japanese adoption of a thoroughly compromised cipher system meant that the USN's cryptanalytical effort was rescued from disaster and allowed to resume effectively in 1943."* This only illustrates the danger of using cryptographic information in historical research when the basic cryptographic principles have not been fully understood. On the other hand, Ralph Erskine's analysis of the *Nankin* incident and the consequences should Japan adopt the Enigma machine, shows a good understanding of the cryptanalytical problems that would result.[11] If this move had happened at an early stage, for instance before the start of hostilities in the Pacific, it could have had a dramatic outcome. Breaking Enigma type ciphers was not easy and the complexity of this operation could easily have overloaded the cryptanalytical capacity of the allied forces during the war. The original T-Enigma without Steckers was of a lower cryptographic complexity than the A-Enigma or the M3 and M4 Enigmas in use with the German Navy. However, an A-Enigma equipped with T-Enigma wheels, each having five notches and therefore resulting in a more irregular movement of the wheels, would have been a very difficult machine to break. It is most likely that even the US Navy Bombes would not have been up to the task and that other methods would have had to be devised to deal with this threat. The Japanese reticence to move to cipher machines for tactical use might also be linked to the problems involved with encoding their language on machines with Latin alphabets. The Japanese did develop one rotor machine with a Katakana alphabet, but Tirpitz was not converted in this way. Luckily, the Japanese move to the use of cipher machines for tactical traffic came far too late and neither she nor

[9] See note 1, *Enigma Variations*.

[10] B. Nelson MacPherson, *The Compromise of US Navy Cryptanalysis After the Battle of Midway*, Intelligence and National Security, Vol. 2, No. 2, April 1987, pp.320–323.

[11] Ralph Erskine, *Letter to the Editor*, Cryptologia, Vol. 15, No. 2, April 1991, pp.156–160.

Germany was in a position to fully implement this plan and to insure a steady supply of machines.

Acknowledgements

I am indebted to Ralph Erskine for sending me a copy of the main parts of RIP 209 and his many comments and suggestions. Furthermore, I am grateful to Philip Jacobsen for giving me a copy of his article about the I-1 incident as well as his detailed comments about Japanese ciphers.