ARMED FORCES SECURITY AGENCY

111/50/TOPSEC/AFSA-14

Copy No. 31

From: AFSA-14

To: OOT

CONVOY TRAFFIC OF THE ALLIES IN WORLD WAR II
AND THE GERMAN NAVAL INTERCEPT SERVICE

1. The attached is an Armed Forces Security Agency translation of an article by W. F. Flicke entitled: "Der Geleitzugfunkverkehr der Alliierten im 2. Weltkrieg und der deutsche Marine-Horchdienst." The original was transmitted along with several other items through the Chief, Army Security Agency from the Chief, ASA Europe by letter, subject: "Material by Wilhelm Flicke" dated 12 September 1950 and is held by AFSA-14.

2. Contributions by Flicke prior to August 1950 have been issued in parts under the general short title: DF 116. Those received after the publication of the list of TICOM translations DF 210 will be grouped under the number DF 219 and the parts designated as before by letters. An earlier paper on the German Naval Intercept Service was issued as DF 116-X.

October 1950
Translated: R.W.P.
Distribution: Normal

35 copies

8 pages

DF 219-A

CONVOY TRAFFIC OF THE ALLIES IN WORLD WAR II
AND THE GERMAN NAVAL INTERCEPT SERVICE

The Weaknesses and Defects of
the Allied Convoy Traffic

Lessons for the Present and the Future

Naval Intercept Service and Radar

By Wilhelm Flicke

The Intercept Service of the German Navy (B-Dienst) played no less a role in World War II than the Intercept Service of the other branches of the Armed Forces. It provided its Command with information which could have been decisive in naval warfare if the German Navy had had at its disposal a sufficient number of ships and especially of submarines.

Many details of the practical work of the Naval Intercept Service are not merely interesting and noteworthy but also instructive. Especially so is the chapter on the monitoring of Allied convoy traffic.

This chapter appears all the more significant today when the general world situation brings the employment of convoys into the realm of possibility or even probability once more. Parallels to World War II result which merit increased attention because today the situation appears still more serious: the power which appears as potential opponent of Allied convoys has at its disposal means enabling it to make better use of the results of the intercept service than the German Navy could.

— — — — —

In assessing the work of the German Naval Intercept Service it is usually assumed that the direction finding service played the decisive role. This, however, was not the case. The Naval Intercept Service did, to be sure, have at its disposal a whole network of very good direction finding establishments. Many bearings were taken. But if we regard this complex from the standpoint of its usefulness for the conduct of naval warfare, then we find only meagre results. Operationally the Naval Direction Finding Service played no great role.

3

DF 219-A

We must, it is true, mention one exception here: at the beginning of the war the English and French naval forces in the North Sea radioed around a great deal so that the movements of these fleet units could be followed readily. With the beginning of the campaign in the West this ceased to be the case and the situation did not recur.

— — — — —

The decisive source from which the German Naval Intercept Service drew its information during the entire war was the field of cryptanalysis and traffic analysis. And these lines of endeavor found their broadest field of activity in connection with the convoy traffic.

Two cipher (cryptographic) systems served as basis for German crypt-analytic work in this direction. The one was called by the Germans "Verfahren Köln". It was a cipher system of the English Navy and its proper designation never became known to us. The system was solved analytically in Berlin. From the messages which were enciphered in this system and decrypted by us the distribution of the English fleet could be recognized currently in very complete manner.

The second cipher system, which was also solved by analysis, was termed by us "Verfahren Frankfurt." In this case a common English-American cipher system was involved which appeared after America's entry into the war. It was introduced to take care of the radio traffic between England and America, or between English and American offices (stations), which was necessary in connection with the convoy system. It was a 5-digit code which was enciphered with an additive sequence.

Both systems — "Köln" and "Frankfurt" — could be deciphered at all times down to about the middle of 1944. Later the "Frankfurt" system was complicated through the fact that a general, consecutively used (durchgehender) additive sequence was no longer used for encipherment, but instead the additive which was found was used only for one message. For encipherment there was a whole book of "individual additive sequences".

From mid 1944 on this made decipherment far more difficult; consequently from this point on decodes were rarely timely, they always limped along behind.

DF 219-A

From late 1944 on it was no longer possible to decipher messages in this system.

- - - - -

Already at the beginning of the war (1939) the Cryptanalytic Service of the German Navy was in a position to follow English convoys quite well. Hence we can state that from the fall of 1939 to mid 1944 the Cryptanalytic Service was able to furnish the Naval Command all the data necessary for combatting convoys.

The tragic feature - if we may call it thus - lay in the fact that, while all convoys could be clearly identified, they could not be attacked due to lack of submarines.

The German Naval Cryptanalytic Service scored one of its greatest successes in the spring of 1942 when a convoy of 9 ships on the way from Trinidad to England could be wiped out completely on the basis of decrypted radiograms.

- - - - -

The weakness of the convoy traffic of the Allies lay in the system which was used continuously and almost without change. This point cannot be stressed too emphatically, because under the conditions of today and tomorrow one must count on a repetition of those mistakes. If at that time the Western Allies had faced an opponent who could have committed a much stronger force of submarines, then no convoy would ever have reached its destination.

The first mistake lay in the fact that the socalled convoy radiograms were transmitted by two fixed stations (which were always the same). So far as I recall, these were Halifax for the USA and a station near Bristol in England.

The second mistake lay in the fact that the convoy radiograms were so characteristic in their outward form, that they could be clearly recognized as such even before decryption. Incidentally it may be mentioned that even after decryption became impossible (1944) it was possible without further ado to get first rate clues from the undecrypted radiograms. This assertion - which may sound incredible - brings us to the third mistake made by the Allies.

DF 219-A

The structure of the convoy messages was stereotype and fixed. Short letter groups were used for designating the convoys; these designated the date and time of sailing, port of destination, composition of the convoy, number of ships, number of the routes, distance between ships, and route expressed in degrees of longitude and latitude, cargo, escort forces, name of the commodore, assembly points for stragglers, etc. Worst of all was the serial number of the convoy.

Interpretation of the groups was usually quite simple. Thus HX signified Halifax, SC — Sydney Canada, OG — outward Gibraltar, HG — homeward Gibraltar.

These letter groups gave information regarding the port of departure and port of destination. But they revealed still more. If the group ON (outward North Atlantic was transmitted, that gave at the same time the speed, i.e. the normal speed of about 8.5 nautical miles. On the other hand if the group ONS (outward North Atlantic Slow) appeared, then a slow convoy with a speed of about 7 nautical miles was involved.

OS meant outward South Atlantic, i.e. with speed of 8.5 knots. SL — Sierra Leone to England with normal speed. SLF — Sierra Leone Fast, i.e. with speed of 9.5 knots. UGF — United States Gibraltar Fast, while the reverse route was GUF — Gibraltar United States Fast.

In this situation one could always calculate the exact location of the convoy and impart it to the lurking submarine packs.

Of exceptional importance in this connection were the socalled assembly points; these were fixed and radioed in order to give stragglers (those which had fallen behind due to engine trouble etc.) a chance to join the convoy by the shortest route. From a knowledge of the appointed assembly points one could deduce where the convoy would pass and that made possible the commitment of submarines.

The fourth weak point in the convoy traffic lay in the rhythm of the convoys; this was so clearly recognizable that one was in a position to calculate for weeks in advance the days on which convoy Nr. X would put out to sea.

DF 219-A

This was facilitated by the fifth weak point in the Allied convoy traffic, namely the radio traffic which regularly appeared during the assembly of the convoys and which could be recognized just by the 5-letter groups of the radio names (call signs) and afforded clues. It was possible to draw from the radio names the reliable inference that a convoy was being gotten together and where it was heading (from the convoy rhythm).

These secondary characteristics remained throughout the entire war and were helpful, even after the change of cipher. The Cryptanalytic Service of the German Navy in conjunction with the Evaluation Service had become so well schooled that the radiograms which appeared were "readable" to a certain extent without having to decrypt them. For instance, when a message appeared, one knew which convoy it concerned, where it was going, whether "slow" or "fast" or normal, etc.

Only the situation had changed meanwhile with the introduction of radar equipment on the part of the Allies. The best results of the Naval Intercept Service were no longer of any use.

- - - - -

It is not without interest that the Naval Intercept Service recognized very early the use of radar devices by the Allies. About the beginning of 1943 it was recognized from the decryption of a series of radiograms that the enemy had at his disposal some means or other for fixing hostile submarines. The messages from which this was deduced were enciphered by the English-American Convoy Code (which we called "Frankfurt"). Submarine situation reports were radioed every day in this code.

Now, however, it was striking that the positions of the German submarines were suddenly given with astonishing precision. Moreover the word "detected" kept coming up in the messages. That was all the more noteworthy because the submarines remained under water virtually all the time and sent no radiograms; there was only radio traffic within the pack when a boat made contact with the enemy; there was communication with Berlin or with the flotilla chief only on orders from Berlin. (Operational orders to submarines came only from Berlin, via Wilhelmshaven, Bordeaux, etc.).

DF 219-A

It became especially clear that the enemy had new technical means of spotting submarines when we had picked up convoys by our intercept service and our submarines prepared to attack; then a change of route ensued at once, which was promptly recognized by our intercept service.

It could not possibly be a case of enemy decryption; in the first place the above mentioned reasons argued against this, then, too, the fact that the enemy used such terms as "seen", "detected" etc., although the submarines were under water.

The essence of the new foreign technique and the method were still unknown, to be sure, but the fact was established that there was something or other in existence for spotting submarines.

A little later a British aircraft was shot down over the Atlantic. In this case we succeeded in capturing the English Air Code. In this volume we found for the first time the expression "radar"; the term "detecting" also appeared here.

Now it was recalled that even before the war it had been noticed that the English were instituting experiments with a radio measuring device, and indeed for short distances. There was a peculiar ticking observed on the submarines body when a radar beam hit it. Then, shortly before the war one had a Zeppelin fly along the English coast; this time, too, it was observed that the airship was made the object of bearings.

It was also recalled that at that time the English had bought up a whole year's production of Braun tubes. Now one knew of what type the new device must be.

— — — — —

8