Lectures

STANDARD FORM NO. 64

Office Memorandum • UNITED STATES GOVERNMENT

TO : Mr. Friedman

DATE: 7 August 1953

FROM :

SUBJECT:

The attached paper is the one prepared by LCDR P.J. KARL for use with the "Submarine Chart". For your retention.

VR

fort.

(1) See Charts - in A & G file Cabinet

(2) Slides - in small box of slides

Stout

"MONTHLY LOSSES OF BRITISH, ALLIED AND NEUTRAL SHIPPING BY U/S ACTION IN WORLD WAR II"

The chart entitled "Monthly Losses of Shipping by U/S Action" illustrates the relationship between the Allied struggle against the German U-boat menace in World War II and the availability of accurate and timely operational intelligence derived from cryptanalysis (i.e., reading the texts of enemy radio messages). It also takes into account the other principal factors which influenced the outcome of the Atlantic battle.

A significant two-fold comparison of the value of Communication Intelligence (COMINT) in wartime is apparent from an analysis of the chart. On the one hand, it is unmistakably clear that British - U.S. COMINT contributed directly and substantially to the Allied victory over the German U-boat. On the other hand, the staggering losses inflicted on Allied shipping by U-boats, from the outbreak of the war until the summer of 1943, were closely related to the degree of success achieved by the German COMINT organization (the "B" Service) against Allied communications.

Three degrees of COMINT success are represented on the chart for both British - U.S. and German radio intelligence (R.I.), namely low, medium, and high readability. German communications between Naval headquarters and the U-boat fleet were carried exclusively in the German machine cipher (ENIGMA), a high-grade system. In consequence, the combined British - U.S. cryptanalytic attack was concentrated on this

system and the degree of Allied success included not only the percentage of solution but also the time limitation for immediate operational effectiveness of the information. Low readability, therefore, indicates a low state of solution with a time lag in decrypting the messages such that the information obtained is of no value for immediate operational effectiveness. It is useful, however, for building a background of strategic information. Medium readability indicates approximately a 50% solution of the messages, many of which can be read in sufficient time to be of immediate tactical value. High readability indicates that all or most of the messages can be decrypted completely ("solidly") and can be read currently and continuously with a minimum of delay.

Whereas the combined British - U.S. cryptanalytic effort was directed against the U-boat cipher machine, the German "B" Service concentrated on codes and ciphers containing information regarding Allied convoys and merchant shipping. No high-grade cipher machine was available for combined use for this traffic until late in 1943. Hence, from 1941 until late 1943, all of the Allied convoy and shipping information was carried in less secure codes and ciphers, and it was against these that the "B" Service realized its greatest success. Where the chart indicates the Germans' low readability of Allied traffic, it means that intelligence was obtained from reading low grade systems such as merchant ship codes and aircraft reconnaissance codes. Medium readability indicates partial solution of Allied medium grade codes and ciphers. Currency, though desirable, was not of the essence in decrypting this traffic, for the "B" Service stressed the importance of building up a background of

convey intelligence and developing operating patterns. For this purpose, non-current decrypts were obviously of great value. In periods when successive convoys were using approximately the same routes, past knowledge of convoy habits and procedures, together with the known regularity of the convoy sailing patterns, was made to compensate for the lack of current information on individual convoys. High readability indicates complete solution of the British - U.S. high grade Naval cypher using Tables "M" and "S", and decryption of the messages on a current and continuous basis. The "B" Service achieved this degree of success only once during the war - from January until June of 1943.

In addition to intelligence derived from cryptanalysis, the combined British - U.S. effort had available two other sources of information based upon the Germans' heavy radio traffic. These were Direction Finding (D/F) and transmitter identification (TINA and RFP). D/F is a method of locating a transmitter by obtaining simultaneous bearings at several receiving stations and plotting the area of intersection of the bearing lines. TINA is a method of identifying a radio operator by his sending characteristics, while RFP is a method of identifying the radio transmitting station by studying the electrical characteristics of the transmission. Both D/F and transmitter identification procedures were used extensively and effectively against the U-boats. Intelligence from these two sources was available throughout the war. However, its accuracy and application were much more limited than in the case of intelligence derived from cryptanalysis.

From the outbreak of war until August of 1940, the Germans enjoyed a period of medium readability on British codes and ciphers. (This factor is represented by the green plaid column toward the left hand side of the chart.) It is known, for example, that both British Naval Code No. 2 and Naval Cypher No. 4 were approximately 50% readable; during the spring and summer of that year a time lag of only 24 hours was quite common. Thus, valuable information on the disposition of the British Fleet was available. The excellence of the "B" Service in the latter part of this period is high-lighted by two successful German attacks on Naval forces - the sinking of H.M.S. GLORIOUS on 8 June and a less spectacular U-boat operation against the Northern Patrol a week later.

During the first nine months following the outbreak of war, the number of U-boats available for operations against shipping was small, and monthly losses of Allied vessels were relatively light (150,000 gross tons in the heaviest month). However, in June 1940, after release of the U-boats from the Norwegian campaign, sinkings increased steadily until they reached 350,000 gross tons in October of that same year.

Changes introduced into British Naval Code and Cypher in August 1940 resulted in a completely unsuccessful month for the German COMINT effort. Sinkings continued unabated, however, since the U-boats were by now operating out of French ports in the Bay of Biscay. Night attacks on convoys by surfaced U-boats accounted for heavy losses. It was evident that, despite the loss of intelligence from COMINT sources, thorough knowledge of Allied convoy procedures, patterns of operation, and probable

movements enabled the U-boat commanders to continue their raids until German COMINT broke into British codes and ciphers again the following month. However, success this time was on low level crypto-systems (see barred green column) and, as a consequence, the quality of German intelligence began to deteriorate. Even this low-grade success was short lived, for changes introduced into British cipher procedures in September began to have their effect and another drought in German COMINT contributed to an appreciable reduction in Allied shipping losses.

The number of U-boats sunk by Allied action was negligible during the first year and a half of the war. (See shaded green area on extreme left side of chart.). Allied intelligence and anti-submarine operations were not yet up to the task of combatting this undersea menace.

In February 1941, the Germans once more began reading low level Allied systems and again the rate of shipping losses began to mount. The U-boats moved west of 40°W and launched concentrated night attacks on convoys; the month of April saw the first daylight attack on a convoy by a U-boat group. The campaign in the open Atlantic was now in full sway. The availability again of intelligence, exploited with more aggressive tactics, resulted in a marked increase in German submarine successes.

It was in March of 1941 that British cryptanalysts first tasted success against the German ENIGMA. It was a trickle at first, mainly of low readability and non-current, but it soon progressed into medium readability with shorter time lag, then British decryption in volume began (See red column.). With the intelligence now available to the

British from COMINT, the convoys were able to adopt evasive routing tactics, and this factor, together with the provision of escorts and aircraft based on Iceland, caused drastic reduction in shipping losses for two months.

British COMINT was now in a period of high readability, and decryption of the German U-boat messages was placed on a current operational basis in August 1941. In September, the British ceased to encipher the indicators for their own Naval Codes and ciphers and the Germans were quick to spot this weakness. However, an interesting situation developed; despite this new German COMINT success, there was no appreciable improvement in their operational situation at sea. A battle of the COMINT services developed, with the British now holding the upper hand. Moreover, in October, a more secure combined British - U.S. Cypher for convoys was introduced and the effectiveness of the U-boats was further reduced. Allied shipping losses were cut to under 75,000 tons the following month, as against a loss of 10 U-boats. With the failure of their patrol lines, the Germans began now to suspect British Intelligence.

The United States entered the war in December 1941. For about the first six weeks of 1942 there was practically no COMINT available to the Germans. But the Combined Naval Cypher No. 3 became readable in February and was read almost entirely and currently until June, when it was replaced by Naval Cypher No. 5. From an operational point of view the exploitation of Cypher No. 5 was perhaps the greatest achievement of the German COMINT service. U-boat commanders now had the one

indispensable means of locating Allied convoys in mid-ocean. The German reconnaissance problem was solved - on paper- and U-boat strength could be concentrated at the right place and at the right time. The U-boats moved in for heavy attacks in mid-Atlantic and along the eastern seaboard of the U.S.; once more Allied losses began to soar (The chart now shows an area breakdown for losses attributed to German U-boat action, and the heaviest concentration appears in the Atlantic Ocean, shown in black).

It was during this same period that the Germans added a fourth wheel to their ENIGMA machine, resulting in a complete blackout for British cryptanalysis. This bleak period lasted for ten consecutive months. The Germans continued reading British traffic throughout this period and the U-boats enjoyed their greatest successes, reaching a peak of some 750,000 gross tons of shipping in November 1952, of which 625,000 tons were in the Atlantic. Some sporadic relief was experienced by the introduction of U.S. countermeasures and by the effectiveness of U.S. coastal convoys, but, in general, the U-boats continued to maintain the advantage. The U-boat offensive was extended into the Gulf of Mexico and the Caribbean, and Allied losses continued at a high level.

The month of December 1942 marked a turning point in the battle of the Atlantic. Allied losses dropped to one half the total of the previous month. Rough weather was undoubtedly a factor, but the introduction of new combined cipher procedures caused another blind

spot in German COMINT. Meanwhile, the British once again broke into the German traffic and resumed decryption. During the following month, losses were further reduced by evasive routing of the convoys made possible by the new flow of COMINT, and by assistance rendered by very long range aircraft. It was in this same month of January 1943 that the total of Allied new ship contruction passed the total of losses by U-boat action.

In February 1943, the Germans resumed their decryption of British communications and were enjoying a period of high readability. Concentration of U-boats in the northwest Atlantic began, but the U.S. cryptanalytic effort against the Germans was put on a production basis, and this helped to offset the new German success. The number of U-boats sunk began to increase slightly.

The German COMINT effort reached its peak in March 1943 with the rapid reading of valuable convoy messages and the Allied convoys found themselves surrounded by the U-boats. Losses in the Atlantic jumped to 600,000 tons, double the previous month's total. Beginning with this period, suspicions were aroused concerning the security of Allied convoy operations. However, operational success in exploiting the information supplied by the "B" Service was short lived because the British - U.S. effort was becoming increasingly successful. Allied technical superiority in aircraft, weapons, and radar, reinforced by COMINT, made itself felt in increased sinkings of U-boats; losses reached an all-time high for the war in May 1943 when some 41 vessels were sent to the bottom.

It was in May of '43 that the insecurity of the Combined Cypher was proved through renewal of Allied COMINT success, and changes were introduced the following month (June 1943). British - U.S. Naval Cypher No. 5 replaced Cypher No. 3, and in consequence the Germans lost their COMINT during the month of June. However, they were able to resume a period of low readability on Allied systems in July. By combining results from low-level codes with information gained through traffic analysis, the Germans were able to meet the demands of the Operational Command for the next four months. But, the "B" Service lost all readability in the following November and a complete drought in COMINT continued for the duration of the war.

During this same period, the tempo of the Allied offensive increased, on the sea as well as in the COMINT chambers. A combined surface and air offensive in the Bay of Biscay area forced a general withdrawal of the U-boats in favor of less dangerous areas. The loss of so many U-boats in the sinking of so few Allied vessels was becoming a very expensive piece of business for the Germans. In the combined COMINT field, the month of June 1943 saw the first American BOMBE placed in operation in Dayton, Ohio. (This BOMBE, a forerunner of which had been developed in U.K., was a high-speed analytical machine capable of matching an assumed plain text against the enciphered text of a German ENIGMA message for the purpose of obtaining the daily wheel setting.) The time delay in reading ENIGMA traffic was cut from an average of 600 hours to about 150 hours. (See heavy red horizontal line on chart.)

U.S. Navy escort carrier forces could now be directed to the refueling rendezvous of the U-boats in mid-Atlantic with a resultant high loss in refueling vessels. Allied forces could also be brought within effective range of their own search equipment for attacks against the submarines. U-boat losses in consequence continued to be high. By September of 1943, the U.S. BOMBES were operating in full force in Washington, thereby greatly augmenting the combined COMINT effort, and the time lag in reading German messages was slashed to an average of 72 hours. The Combined Cipher Machine (CCM), introduced for combined usage in the late spring of 1943, came into widespread use by the fall of the year.

Results of these achievements were felt in the German operational picture at sea. Although the U-boats returned once again to the North Atlantic shipping lanes in considerable force, the "B" Service could no longer lead them to the Allied convoys. Allied ships and planes, aided by intelligence from COMINT sources, continued the offensive against the U-boats and losses continued heavy for the Germans. In December, they diverted their U-boats to the U.K. - Gibraltar shipping lane, having been driven out of the North Atlantic. German U-boat messages were now being read continuously, completely, and currently, in 18 hours on the average. The Germans' high-grade operational radio communications were now wide open to the Allies. Besides supplying current operational information, ENIGMA messages revealed invaluable technical intelligence concerning the U-boat program. The Allies now had a source of accurate and comprehensive information on new weapons,

such as the acoustic torpedo, as well as on new devices such as search receivers and the schnorchel experiments. With the loss of their own COMINT sources, resulting from increased Allied communication security subsequent to general distribution of the Combined Cipher Machine, the Germans were forced to rely almost entirely on German Air Force reconnaissance for locating convoys. But this alternative proved much less effective than COMINT, and Allied shipping losses in the Atlantic, for eight months subsequent to full-scale operation of the BOMBES, were cut to an average of some 27,000 tons per month.

In January 1944, the first schnorchel U-boat appeared in the Atlantic but the schnorchel experiments at sea were not satisfactorily completed until after the Allied invasion of France. The schnorchel U-boat did not become a serious threat and shipping losses continued at a low level. The Allies continued to maintain the advantage during the critical invasion period. (Losses were so small by June 1944 that the chart no longer shows an area breakdown.) U-boat losses, on the other hand, were consistently heavy. The BOMBES continued their excellent work of recovering daily key settings for the ENIGMA and the time lag never again fell behind a 48 hour maximum for effective operational needs. By August, the U-boats had been evacuated from their ports on the French coast, and the German undersea fleet was greatly reduced after 16 consecutive months of reverses.

Despite these setbacks, the German submarine arm continued its struggle to regain superiority. At sea, a last-ditch effort was made in the autumn of 1944 to resume the offensive by using the schnorchel U-boats, which by this time were steadily increasing in number.

Communication-wise, experiments were made in January 1945 with a new type of transmission, the "Kurier" transmission, in an attempt to prevent interception of U-boat messages. The "kurier" was a system of ultra-high-speed or "flash" transmission, in which a brief but complete message was sent in a fraction of a second.

The new U-boat offensive was concentrated in a blockade of the British Isles. The schnorchel U-boats entered the channels and inland seas of Great Britain where they steadily increased in numbers and effectiveness. But the end of the war was only a few months off. Faced with total collapse in the homeland, the once powerful U-boat fleet was forced to surrender in March of 1945, although it was still a dangerous combat unit, well organized, improved and willing to continue the war.

While it is not feasible to assess precisely the value of COMINT in the Battle of the Atlantic, certain results drawn from operational analysis have indicated that the availability of timely decryption intelligence to the German U-boats increased by a minimum of 250% their effective search ability against convoys especially selected for attack on the basis of such intelligence. This analysis has also revealed that during the period of high readability by the Allies, from September 1943 to March 1944, the contact rate of German U-boats was two-thirds that of the rate during the last six months of 1942, when the Allies were not reading U-boat communications. Moreover, during the same period of high readability by the Allies, the sinking rate (per U-boat day per convoy day) dropped to one-sixth of the level prevailing from July to December 1942 when decryption intelligence was available to the Germans but not to the Allies.

Aside from the vast savings resulting from this great drop in effectiveness of the U-boats during the periods of Allied COMINT success, there were comparable gains in anti-submarine offensive operations. The effectiveness of the limited surface and air searching forces which were available in the Atlantic was greatly extended, and tremendous savings in fuel for these forces were achieved.