## 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.

Part. See Charter to mender of Suider of Suider of Suider

The Carrie

San Character Ch

## POSTRET LOSSES OF BEITTER, ALLIED AND MUTHAL LIPPING BY U/S SETTED IN SCALP WAS IT

The chart entitled "Monthly Losses of Shipping by U/S Action"
illustrates the relationship between the Ailied struggle against the
Cerman 5-boot menece in Morld War II and the availability of accurate
and timely operational intelligence derived from cryptanalysis (i.e.,
reading the texts of enemy radio messaces). 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 (CCRINT) in wartise is apparent from an analysis of the chart. On the one hand, it is unmistakably clear that British - U.S. COMING contributed directly and substantially to the Allied victory over the Comman U-boat. On the other hand, the staggering losses inflicted on Illied shipping by U-boats, from the outbreak of the war until the summer of 1963, were closely related to the degree of success schieved by the Serman COMINT organization (the "B" Service) against Illied communications.

Three degrees of COMING 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 Maral headquarters and the U-best fleet were carried exclusively in the German machine cipher (ESIGM), a high-grade system. In consequence, the combined British - U.S. cryptonalytic attack was concentrated on this



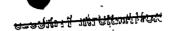
SECULATIVE SHIP Commercial

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 residability, 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 residability indicates approximately a 50% solution of the messages, many of which can be read in sufficient time to be of immediate tectical value. Righ residability 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.

Shereas the combined British - U.S. cryptanalytic effort was directed spainst the B-boat cipher machine, the German \*B\* tervice 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 19h3. Hence, from 19h1 until late 19h3, all of the Allied convoy and shipping information was carried in less secure codes and ciphers, and it was against these that the \*B\* tervice realised its greatest success. Where the chart indicates the Germans' low readability of Allied traffic, it seems that intelligence was obtained from reading low grade systems such as merchant ship codes and sireraft recommissance 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



Soil



THE WOLLD

convey intelligence and developing operating patterns. For this purpose, non-current decrypts were obviously of great value. In periods then 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 \*\*\* and \*S\*, and decryption of the messages on a current and continuous basis. The \*B\* Service schieved this degree of success only once during the war - from January until June of 1963.

in addition to intelligence derived from cryptanalysis, the combined British - U.S. effort had available two other sources of information based upon the Cermans' heavy radio traffic. These were Direction Finding (D/F) and transmitter identification (TIBA 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. TIBA is a method of identifying a radio operator by his sending characteristies, 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.



Sabbatt & oft Branch ....

prom the outbreek of war until August of 1940, the Germans enjoyed a period of medium resolutity 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 Maval Code No. 2 and Maval Cypher No. Is were approximately 50% readable; during the spring and summer of that year a time lag of only 2h hours was quite common. Thus, valuable information on the disposition of the British Flort was available. The excellence of the ABr Dervice in the latter part of this period is high-lighted by two successful German attacks on Maval forces - the sinking of N.M.S. CLOETOUS on 8 June and a less spectacular U-boat operation against the Northern Patrol a week later.

paring 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 tone in the heaviest month). However, in June 1940, after release of the U-boats from the Horwegian campaign, sinkings increased steadily until they reached 350,000 gross tone in October of that same year.

Changes introduced into British Mavel Code and Cypher in August 1960 resulted in a completely unsuccessful menth for the Cerman CCHINT effort. Sinkings continued unabated, however, since the U-bosts were by new operating out of French ports in the Bay of Riscay. Right attacks on convoys by surfaced U-bosts accounted for heavy losses. It was evident that, despite the loss of intelligence from CCHINT sources, thorough knowledge of Allied convoy procedures, patterns of operation, and probable





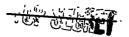
movements enabled the U-boat commanders to continue their raids until German CCHIRT broke inte British codes and eighers again the following month. However, success this time was on low level crypto-systems (see barred green column) and, as a consequence, the quality of German intelligence began to deteriorate. 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-euksarine operations were not yet up to the task of combatting this undersea menace.

In February 1941, the Garmans 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 is the open Atlantic was now in full sway. The availability again of intelligence, exploited with more aggressive tactics, resulted in a marked increase in Garman submarine successes.

It was in March of 1961 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





U.NUE

SECURITY INCURSIATION

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

British COMENT 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 Cermans were quick to spot this weakness. However, an interesting situation developed; despite this new German COMENT success, there was no appreciable improvement in their operational situation at sec. A battle of the COMENT services developed, with the British now holding the upper hand. Hereover, 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 Maval Cypher No. 3 became readable in February and was read almost entirely and currently until June, shen it was replaced by Maval 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





- WE WENTER



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-stlantic and along the eastern meaboard of the U.S.; once more Allied losses began to sear (The chart now shows an area breakdown for losses attributed to German U-boat action, and the heaviest concentration appears in the Atlantic Green, shown in black).

It was during this same period that the Germans added a fourth wheel to their FRICRA machine, resulting in a complete blackout for British cryptanalysis. This bleak period lasted for ten consecutive menths. 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 1962 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

Constitution

THE PARTY OF HEED B C CHESSES

losses by U-boat action. possible by the new flow of CERIFF, and by assistance rendered by losses were further reduced by evasive routing of the convoys made that the total of Allied new whip contraction passed the total of very long range aircraft. It was in this same month of January 1943 the Comman traffic and resumed decryption. During the following south, apet in German COMINI. - Manuabile, the British once again broke into

amk began to increase alightly. oryptanalytic effort against the Cermons was put on a production basis, centration of U-boats in the northwest Atlantic began, but the U.S. communications and were enjoying a period of high readability. (onand this helped to offset the new German success. The number of U-boats In February 1943, the Corresps resumed their decryption of British

reached an all-time high for the war in May 19h3 when a COMME, made itself felt in increased sinkings of U-boate; technical superiority in aircraft, weapone, and radar, reinforced by British - U.S. effort was becoming increasingly successful. information supplied by the vgs Service was short lived because this period, suspicious were aroused concerning the security of Allied to 600,000 tons, double the previous menth's total. Reginning with themselves surrounded by the U-boats. enroy operations. repid reading of relushie convoy messages and the filted convoys found the German GUBING effort reached its peak in March 1943 with the ment to the bottom. Bosser, operational success in emploiting the Losses in the Atlantic jusped TORRES POTITION

It was in May of this that the insecurity of the Combined Cypher was proved through renewal of Allied COMINT success, and changes were introduced the following month (June 1963). British - U.S. Mayal Cypher No. 5 replaced Cypher No. 3, and in consequence the Communa lost their COMINT during the menth of June. However, they were able to resume a period of low reedability 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.

on the see 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 B-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 BORBE placed in operation in Bayton, Ohio. (This BORBE, a forcrumer of which had been developed in U.E., was a high-speed analytical machine capable of matching an assumed plain text against the enciphered text of a German FAICMA 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 \$50 hours. (See heavy red horizontal line on chart.)

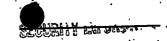
THE STATE OF THE S

SECONDERE COMO CONTRACTOR DE LA COMO

U.S. Navy escent carrier forces could now be directed to the refueling rendervous 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. BORNES were operating in full force in Washington, thereby greatly augmenting the combined CONINT 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 Morth 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-beats 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 new wide epen to the Allies. Hesides supplying surrent operational information, ENICHA messages revealed invaluable technical intelligence concerning the U-boat program. The Allies now had a source of accurate and comprehensive information on new meapons,

WE VE



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

In January 19hh, the first schmorchel U-boat appeared in the Atlantic but the schmorchel experiments at sea were not satisfactorily completed until after the Allied invasion of France. The schmorchel U-beat 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 19hh that the chart no longer shows an area breakdown.) U-boat losses, on the other hand, were consistently heavy. The HOMMES continued their excellent work of recovering daily key settings for the EMICHA and the time lag never again fell behind a h8 hour maximum for effective operational needs. By August, the U-boats had been evacuated from their ports on the French coast, and the Cerman undersca fleet was greatly reduced after 16 consecutive menths 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 19th to resume the offensive by using the schnorchel U-bests, which by this time were steadily increasing in number.

UFINE

Communication-wise, experiments were made in January 1945 with a new type of transmission, the "Eurier" transmission, in an attempt to prevent interception of U-bost messages. The "kurler" 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 Islas. 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 Earch of 1965, 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 pariod of high readability by the Allies, from Ceptember 1943 to Harch 1956, the contact rate of German U-boats was two-thirds that of the rate during the last six months of 1962, when the Allies were not reading U-boat communications. Horeover, during the same pariod 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 1962 when decryption intelligence was available to the Cermans but not to the Allies.



Aside from the wast 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-subscrime 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 aphieved.