Ultra and the Battle of the Atlantic:

In the following pages are the texts of three papers on "Ultra and the Battle of the Atlantic" presented at the Naval Symposium at the U.S. Naval Academy in Annapolis on October 28, 1977. The speakers were Patrick Beesly, former Deputy Chief, Submarine Plotting Room, the Admiralty; Jurgen Rohwer, Director of the Library of Contemporary History, Stuttgart; and Kenneth Knowles, former Head, Atlantic Section, Combat Intelligence, on the staff of the Commander-in-Chief, U.S. Fleet. The session was organized by Professor Harold C. Deutsch of the U.S. Army War College, who served as chairman—and whose article surveying the impact of Ultra on World War II history appears following the three papers.

The British View

Patrick Beesly

First of all, a brief explanation. I shall refer throughout not to 'Ultra' but to 'Special Intelligence,' because this was the term invariably used in the British Admiralty to describe information derived from decrypting enemy signals. You will find virtually no mention of 'Ultra' in the secret British naval records: it was merely a security classification, akin to 'Top Secret,' for outgoing signals. Unfortunately, due to Winterbotham's best-seller, *The Ultra Secret*, the term is now almost universally used in quite the wrong sense. I only mention this because researchers into the secret British naval records, which are now slowly being released, will be misled unless the point is clearly understood.

A number of other misconceptions also stem from Winterbotham's book and from others by authors with even less knowledge of maritime Special Intelligence and its operational uses than Winterbotham. The impression is given in many of them that Special Intelligence was *the* war winner, that from mid-1940 onwards we knew *all* the Germans' moves and intentions, either in advance or at least currently, and that men, ships and aircraft to do the actual fighting were hardly necessary—the cryptanalysts alone would provide.

Far be it from me to underrate the inestimable boon which the ability to decrypt enemy signals bestows on the power that possesses it. Practically no other source of information, at least up to the end of World War II, could possibly provide such valuable raw material from which accurate and sensible appreciations of an opponent's movements and intentions might be built up. But Special Intelligence was only *one* of many sources of information upon which intelligence departments, both Allied and Axis, depended, and it had, like all of them, its own drawbacks and limitations. It was *not* all-embracing, it was *not* complete, it did *not* provide *all* the answers which the naval and air staffs required if they were to anticipate and counter every move made by their enemies. Even when Special Intelligence was in its most informative and current state, a very great deal still depended on the genius, and I use the word advisedly, of a few individuals (two of them, Admiral Denning and Captain Knowles are here today) to piece together, from scraps of information from all sources which were received *in time* to be of operational value, a clear appreciation of what was really going on, or was about to take place, at sea. The raw material needed to be carefully processed before use could be made of it.

There was a further requirement. It could serve no useful purpose, even if the intelligence department did produce an accurate appreciation, if those responsible for

taking the operational decisions did not understand or failed to accept the conclusions to which intelligence had come. In World War I, the British Admiralty's Room 40 decrypted during the night after Jutland sufficient information to show clearly the route back to Wilhelmshaven which the German Admiral, von Scheer, was taking. Room 40, however, was not a true intelligence center and was not permitted to pass the priceless information direct to Jellicoe[1] and the Grand Fleet. The responsibility for doing this rested with the staff of the Operations Division, who were not trained intelligence officers, failed to understand the significance of the information laid in front of them by Room 40, and did not pass it on to Jellicoe. As a result Jutland was not the second Trafalgar, which it otherwise undoubtedly would have been.

In World War II the British cryptanalysis organization, the Government Code and Cypher School, was housed outside London at Bletchley Park. Responsibility for analysing and disseminating the results of its work in the maritime sphere rested, thanks largely to Norman Denning's pre-war planning, with the Admiralty's Operational Intelligence Centre (O.I.C.). This organization did exercise the true and full role of an intelligence center, with enormous benefits to the Allied cause. It communicated directly, not only with the operational authorities in the Admiralty and at the R.A.F.'s Coastal Command, but also with ships and fleets at sea. On at least one occasion, however, there was a reversion to the Jutland attitude. During the ill-fated PQ.17 convoy the First Sea Lord, Admiral Sir Dudley Pound, refused to accept Denning's accurate appreciation that *Tirpitz* and her squadron had not left Altenford to attack the convoy and gave the mistaken order to scatter which led to disaster. Such failures were, however, rare and in fact O.I.C.'s advice was very seldom ignored.

What, then, were the limitations of Special Intelligence? First of all, the German Enigma machine, when it was introduced, was an undoubted improvement on any other cipher system then in use. Nor was there only one variety of it. The German Navy developed its own model with a number of technical improvements compared to the Air Force and Army types, which greatly increased the difficulties of the British cryptanalysts. As a result, although some of the German Air Force ciphers were cracked as early as April 1940, and the Army ones not long afterwards, it was not until the capture, in May 1941, of U-110[2], complete with Enigma machine and accompanying instructions, that any German Naval cipher could be broken. For the first twenty-one months of the war at sea the intelligence scales were weighted heavily in favor of the Germans.

Another misapprehension is that Ultra or Enigma was a single cipher. The German Navy alone had thirteen different ciphers for different types of radio traffic, not all of which were broken during the war. The capture of U-110 did, however, enable us to read currently the main operational cipher, code-named Hydra, then in force. Nor was the German assumption that once the validity of the accompanying instructions had expired our cryptanalysts would once more be defeated, sound. Hydra continued to be decrypted, although with varying delays, throughout the war. There were, however, other ciphers: for units in the Mediterranean, for training U-boats in the Baltic, for specific operations by the heavy ships of the main fleet, for cruiser warfare and blockade runners on the broad oceans. These last two were never, to my knowledge, broken, but most of the others eventually were. The point is that the ability to decrypt one particular cipher did not necessarily or immediately lead to the penetration of all the others.

Nevertheless the cracking of Hydra did produce tremendous results. If it played no significant part in the sinking of *Bismarck*, it did lead, thanks to instructions broadcast to U-boats, to the mopping up of seven tankers and supply ships sent out to support the battleship on her proposed raiding cruise. Hydra also disclosed to us the dispositions and movements of the U-boats and enabled us to use evasive routing of convoys with some success and to gain a far greater insight into U-boat strategy and tactics. Merchant shipping losses in the North Atlantic fell considerably. Operation *Paukenschlag*, the U-boat campaign along the eastern seaboard of the United States after Pearl Harbor, was detected in advance by O.I.C., but although this knowledge was immediately passed on to the Navy Department in Washington, the absence of any American equivalent to O.I.C. resulted in little use being made of the information. With the creation of Op-20-G[3] in June 1942, affairs began to take a very different course, but that is Ken Knowles' story, not mine.

The German successes in the first half of 1942 were not solely due to American unpreparedness. At the end of January that year the U-boat Command introduced an entirely fresh cipher, Triton, for the Atlantic boats. Although we continued to decrypt Hydra and certain

[1] Admiral Sir John Jellicoe was commander of the British Grand Fleet in the Battle of Jutland May 31, 1916.

[2] A German submarine.

[3] Op-20-G was actually in existence for some years before this date.

other ciphers, with varying delays to which I will return later, Triton defeated the Allied cryptanalysts until the first week in December. During these ten months, although we were aware, from the signals in Hydra to and from escort vessels, of the activity of U-boats in and out of German, Norwegian and French ports, and, from Tetis, the Baltic U-boat training cipher, of the ever more rapid increase in their total numbers, we no longer had any information concerning the Atlantic U-boats once they were at sea. O.I.C.'s Submarine Tracking Room under its inspired chief, Commander Rodger Winn, R.N.V.R., and Op-20-G under the equally talented Commander Kenneth Knowles, U.S.N., had to fall back on other sources such as direction-finding, photographic reconnaissance, and sightings and attacks for their daily forecasts of the U-boat situation. Nevertheless, thanks to the almost uncanny ability of Winn and Knowles to read the mind of Admiral Karl Dönitz, commander of German submarine operations, the results were considerable even during this phase.

From December 1942 until the end of the war, the Allies—for the British, American and Canadian Tracking Rooms and their respective Trade Routing Departments worked in close cooperation with each other—were generally able to get a pretty close look at the cards in Dönitz's hand. Despite this, a number of serious handicaps had to be overcome. The first of them was the obvious one that decrypted intelligence could only be obtained from signals transmitted by radio. We could learn nothing of messages sent by land line, or, except subsequently from prisoners of war, of instructions given to U-boat commanders before sailing, or of the deliberations of Dönitz with his staff officers, unless these were signalled to those at sea. This fact could, and often did, leave large gaps in our knowledge.

A second and even more serious limitation was the fact that the cipher settings were changed every twenty-four hours and therefore had to be broken afresh on each occasion. The time taken to achieve this varied greatly at different periods during the war. In broad terms current reading was achieved from the end of May 1941 to July or August. Thereafter time lags of from 24 to 48 hours began to occur, although there was some current reading up to the blackout in February 1942. When Triton was broken in December 1942, delays varied from nil to ten days for the first five months of 1943, when the Battle of the Atlantic was rising to its climax. The longest delay of all, apart from the blackout, was in July 1943—three whole weeks. From then on, the time lags began to decrease, and by the end of that year and throughout 1944 current reading became the rule rather than the exception, such delays as did occur rarely exceeding twenty-four hours.

To be of operational value, decrypting had to be swift. Intelligence that was more than forty-eight hours old was liable to have been overtaken by events and to be of use only as background information. In 1943 the Germans often had more than one hundred U-boats at sea in the North Atlantic alone. In order to be able to divert convoys around the large U-boat packs, spread out on three or four extensive patrol lines which were constantly shifted in the light of the latest information available to Dönitz, we required continuous and up-to-date information, and this, as I have said, was not always forthcoming in the first half of 1943. Without it we had to fall back on direction-finding, on other conventional sources and on intelligent guess work.

Nevertheless the German method of controlling their wolfpacks from ashore in France involved a great deal of signalling between Dönitz and his men at sea. We knew, from the escort vessels' signals, when a U-boat left port. After that it had to report having successfully passed out of the Bay of Biscay or the Iceland-Faeroes passage. It would then be given a fresh point for which to steer, followed, a day or two later, by instructions to join a particular wolfpack. Thus delays in decrypting did not always leave us completely helpless. There were, on the other hand, many occasions when, having carefully routed a convoy clear of the waiting U-boats, our plans would be frustrated by fresh dispositions ordered by Dönitz when the new settings had not yet been cracked and we were 'blind.'

Here I must mention the work of the German equivalent to Bletchley Park, the *B. Dienst*. Just as the Germans had to signal fresh instructions to their boats at sea, so diversions and new routes had to be signalled to the Allied convoys. In 1941 and increasingly in 1942 and 1943, the *B. Dienst* decrypted many of these orders, until, in June 1943 the Allied code was changed. Thereafter, the *B. Dienst* decrypted little that was of operational value, but until then the rather ridiculous situation existed that both sides were decrypting at least some of their opponent's signals without being aware that they themselves were being subjected to exactly the same form of eavesdropping.

Yet another difficulty faced O.I.C. and OP-20-G. German Naval charts were overlaid with a lettered and numbered grid, by reference to which all positions were given. Thus 51 degrees 30 minutes North 25 degrees 40 minutes West would be described as, say AB1234. This represented no difficulty to us once a fragment of a German gridded chart had been captured and the whole reconstructed. However, from November 1941 onwards, the Germans introduced a simple substitution code into their grid reference so that AB1234 became, for example, CD 5678, and these codes were changed frequently. Until

each new formula had been solved we were unable, sometimes only for minutes but often for days, to say exactly which of various perfectly feasible alternatives gave the correct position.

There were other less obvious difficulties in pin-pointing the positions of U-boats and in keeping convoys clear of them. The navigation of the U-boats themselves was not always accurate, nor could we (or indeed Dönitz) always estimate their speed of advance correctly. Despite the volume of signalling, days might elapse before a U-boat on passage would report its position. Similarly our own convoys and their escorts would not break wireless silence unless they thought that their position was already known to the enemy. They might be unable to comply with diversions ordered and not report the fact, or they might, because of gales, be fifty or more miles ahead or astern of their estimated positions on our plots. Those without personal experience of it often fail to realize the meaning of the expression the 'fog of war.' I can assure you that it, and just the 'luck of the game' were often more decisive than many post-war historians realize.

A new situation arose in the second half of 1944. There was then a reversion to individual operations with considerable latitude left to the U-boat commanding officer. This called for far less signalling, and as this phase coincided with the almost universal fitting of the *Schnorkel,* aircraft sightings and attacks also fell almost to zero. Information from cryptanalysis, direction-finding, and aircraft decreased alarmingly, and had the Germans been able to bring their new types of U-boats into operational service, as Dönitz had planned, the results would have been extremely serious for the Allies; all the more so because, despite repeated assurances from his signal security experts that his ciphers were unbreakable, Dönitz began to employ 'Officer Only' and 'one Ship Ciphers' which could not be broken, at least quickly enough. I am only amazed that he did not introduce, even earlier, more radical changes into his ciphering arrangements.

A brief word on sources. The secret British records so far released to the Public Record Office in London, although not complete, contain many fascinating files from O.I.C. and the Naval Section of Bletchley Park. The latter must be treated with discretion since they were usually written weeks or months after the events to which they refer. It should not be supposed that the information they contain was necessarily available absolutely contemporaneously to O.I.C. or OP-20-G. From the point of view of the Battle of the Atlantic, the most revealing papers are the weekly reports to the First Sea Lord which Winn started to write towards the end of 1941. These are *contemporary* documents and show his thinking *at the time.* Again and again one can see his amazing ability to predict Dönitz's next moves. They also show roughly the approximate time lags prevailing week by week in decrypting. In addition there are the reports which the Tracking Room made after every major convoy battle, based almost entirely on the relevant Special Intelligence. They must be one of the most complete records of the German point of view still available. The only American release which I have so far seen is far less revealing of Allied contemporary thinking, but as it consists of a narrative, compiled immediately after the war and based on Special Intelligence, it too adds greatly to our knowledge of German activities.

How much did Special Intelligence contribute to the Allied victory at sea over Germany? It was certainly of enormous benefit in assisting in the evasive routing of convoys, and in the concentration of naval and air forces on the critical convoys and at the decisive points. Without it the victory could only have been achieved (although I believe it would *still* have been achieved) later, and at much greater human and material cost. Who can say what would have happened if the invasion of Europe had been postponed until 1945? But what would have been the result if Dönitz had never had the benefit of the work of the *B. Dienst?*

Special Intelligence and, I *must* emphasize, the way in which O.I.C. and OP-20-G made use of it, was a war winner. It was not the only one. The real heroes of the Battle of the Atlantic were the men of the Allied Navies, Merchant Navies and Air Forces, and, indeed also the U-boat crews. They were the ones who risked their lives and all too often had to pay a fatal price for other peoples' mistakes.

Patrick Beesly was Deputy Chief of the Admiralty's Submarine Plotting Room during World War II. His book, *Very Special Intelligence. The Story of the Admiralty's Operational Intelligence Centre 1939-1945*, was published in England and Germany in 1977.

The German View

Jürgen Rohwer

I appreciate the opportunity to present some results of my researches on the influence radio intelligence had on the Battle of the Atlantic. Many books, essays and TV shows in recent years suggest that, by using Ultra, the Allied High Command almost always had knowledge of German intentions. If true, this would have led to a much earlier end to the war. But it is a common error to believe that with the knowledge about the German cipher machine Enigma and with Ultra, it was possible for the Allied cryptanalysts to decrypt and read any and all German secret messages at once.

Largely owing to Patrick Beesly's excellent book *Very Special Intelligence* and his essays in the *Marine-Rundschau*[1] these misunderstandings are corrected for the Battle of the Atlantic. In his paper he gave a clear introduction to the problems of radio intelligence and its operational use in general on both sides. I think I can underline Patrick Beesly's statements best by showing you first how the German cipher machine "M," which the Navy used, worked, and then, how the radio war influenced the development and outcome of some typical convoy battles and operations.

"Enigma" was the code name for a series of cipher machines developed by a private German firm. The first versions were sold to private enterprises and also to agencies in Poland, Sweden, Great Britain, the United States and Japan. The German Navy introduced another version of this machine in 1926 as *Funkschlüssel C*. But this type, as well as the Enigma-G used by the German Army from 1928 onwards, were not regarded as secure; their three changeable cipher rotors offered too few possibilities. So the Army in 1934 changed to a much-improved machine—Enigma-I, which used three cipher-rotors out of a stock of five and also an additional plug board for up to ten wire connections.

The Navy's similar *"Funkschlüssel M,"* by adding three more cipher rotors to the stock, had many more possibilities for producing different cipher-alphabets without repeating a sequence of letters. The most used machine, M–3, had four different settings, three of which were changed daily, and one of which was changed with each message:

First, the operator could choose three out of eight cipher rotors, permitting 336 different combinations of rotor sequences;

Second, each rotor had a revolving ring with 26 positions to change the inside wire-connections; this permitted for the three inset rotors 26^3 or 17576 ring positions;

Third, there were 1547 possible plug connections on the plugboard;

And *fourth*, the operator could set each rotor to 26 different positions before beginning to encipher; this again gave 17576 possibilities. By multiplying these factors you can get at the theoretically possible total of cipher combinations, which is in the area of 160 trillion.

To try so many combinations to find out the right one would take so much time—the German thought—that cryptanalytic successes would come too late to be of operational value. But the Germans overrated the time needed greatly, because they had no idea of the ingenious inventions which made the cryptanalytic machines possible. The young Polish mathematicians under Colonel Langer had solved the secrets of the Enigma machines used by the German Army and Air Force long before the war. They had reconstructed their working mechanisms, and they knew the interior wire connections of the five cipher rotors. The French section of the *Deuxieme Bureaux* under Major Bertrand assisted by delivering a great number of secret cipher documents—for instance, the printed cipher procedures obtained by a German traitor. The British experts at Bletchley Park used—besides their own good ideas, of course—the Polish intellectual achievements and the French espionage results to develop the ingenious technical means to get decrypts fast enough, and the highly effective organization to make operational use of this intelligence possible.

Patrick Beesly has told us that the additional rotors of the naval machine resisted all efforts of Bletchley Park until the capture of the submarine U-110 in May 1941. And he gave us a clear picture of the first consequences in the second part of 1941, when cryptanalytic successes and

[1] A translation of this article will appear in a later issue of *Cryptologic Spectrum*.

Ultra signals led to the destruction of the German surface supply ship organization and the sinking of the most successful German raider, *Atlantis*, but also to a much more effective evasive routing of convoys.

To show you how the Commander of U-boats directed his wolfpacks by radio messages and how the Allied command used Ultra signals based on radio intelligence to re-route convoys, I selected an example which may be of special interest to Americans. You will remember the Kearney incident.[2] But it may be new for you to learn that the first American deaths in the Battle of the Atlantic—seven weeks before Pearl Harbor—had to do with Ultra.

On October 6th, 1941, most of the German U-boats were chasing a Gibraltar convoy, so the North Atlantic convoy route was almost free of U-boats. The Allied convoys east of 30° West were escorted by British Escort Groups, those to the west were escorted by American Task Units and Canadian Escort Groups.

At this time the German decrypting service *(xB-Dienst)* could decrypt Allied signals with considerable time lag only. But they got enough dates to reconstruct the convoy time-table. So the U-boat command intended to block the way of the next pair of convoys expected around the 15th of October. Its first step was to signal a "heading point" southeast of Greenland for some U-boats coming out from Norway.

On this day—October 6th—the estimate of the U-boat-situation by the Submarine Tracking Room seems not to have been very accurate. The positions of only four outgoing boats south of Iceland were plotted fairly well, after decrypting the signals of escort vessels, which had reported the release of those subs off Norway some eight days earlier.

On the 8th of October the Canadian-escorted slow convoy SC.48 had cleared the Belle Isle Strait. It was to go along a convoy route recommended by the Admiraltry's Trade Division on the 26th of September, and approved by the Convoy & Routing section in Washington (OPNAV 38S) on the 28th. But during the night of the 8th to 9th October, Bletchley Park decrypted the "heading point" signalled by the U-boat command three days earlier, and this point was exactly on the convoy route. So the Admiralty on the 9th recommended re-routing SC.48 to the south, to evade the U-boats running for their "heading point". OPNAV concurred.

On the next morning the Canadian Senior Officer Escort (S.O.E.) received new course instruction from OPNAV 38S. The Admiralty instructed the west-going convoys ON.23 and ON.24, running on the British side of 30° West, to go south also, after effecting the exchange of escort groups at the pre-arranged point. Later on the 10th, the U-boat command signalled to the three U-boats first arriving an "attack square" and ordered an adjacent "heading point" for the next four boats. These signals were decrypted during the morning of the 12th. With three U-boats in position and four more nearing the southern end, the Submarine Tracking Room estimated that the U-boat command was trying to establish a patrol line across the course of SC.48.

Only two hours after the recommendation of the Admiralty, OPNAV 38S ordered the S.O.E. to turn SC.48 immediately southeast, and again two hours later gave a new route instruction. This re-routing order led to some problems on the 13th, because SC.48 would pass very close to the west-going ON.23, and a fast troop convoy, TC.14, would have to go round both these convoys. Some re-arrangements had to be made. In turn, on the 13th, the U-boat command ordered separate "attack squares" also for the next four U-boats, and on the 14th the area of these attack squares was exactly known to the Submarine Tracking Room.

The three convoys were passing close to the southern end, while the next west-bound convoy, ON.24, was ordered to make a short detour to the southeast, to get out of the way of TC.14 and SC.48. All seemed to be set for a cleverly planned and well executed evasive routing operation. But then, in the early light of the 15th, two ships were torpedoed. The attacking U-553 had met the convoy by chance, running up to its position in the new patrol line the U-boat command had ordered only a few hours earlier for the seven boats in the area and six additional boats coming up from France. Intelligence gained by decrypting could not prevent such chance contacts, even if the U-boats situation plot was—as in this case—fairly accurate.

In 1941 the escorts were not equipped with high-frequency direction-finders, which later were used so effectively to shake off the first shadower, and they had no radar which could distinguish between a U-boat and the wave echoes at distances of more than four miles. So U-553 began to send its hourly contact signals, providing a homing signal for the nine U-boats which the U-boat command had ordered to close and attack. But the signals of U-553 were also intercepted by the Allied shore listening stations. Without decryption, which needed too much time anyway, the signals could be identified by

[2] The USS *Kearny*, on convoy duty in the North Atlantic, was torpedoed Oct. 17, 1941. Seven Americans were killed.

their prefix "B-bar" and by their bearings to be shadowing signals from SC.48.

The Admiralty was thus able, by using this other form of radio intelligence, to send in the afternoon of the 15th two corvettes of convoy ON.25 and two destroyers of convoy TC.14 to the assistance of the threatened convoy SC.48. In the evening also OPNAV 38S ordered the commander of the American Task Unit 414, escorting the ON.24, to disperse his convoy and to take his five destroyers to help the attacked convoy. This could be done, because the U-boat situation map clearly showed no dangers from U-boats ahead of the dispersed ships.

Fifteen hours later Captain Thebaud, commander of Task Unit 414, reached the convoy, which was continuously shadowed by the U-boats and had lost a third ship during the night. He took command of the combined escort group of American, Canadian, British and Free French destroyers and corvettes. In the night following, the U-boats sank six more ships, and U-568 torpedoed the *Kearny*.

This example, besides providing new information on the otherwise well known Kearny incident, may serve to demonstrate the influence radio intelligence had on many of the convoy battles, its potential as well as its limitations.

Patrick Beesly described the "big black out" in the decrypting of U-boat signals from January 1942 to December 1942. The expansion of German territories and the increasing number of ships and U-boats at sea led to a dramatic increase in the number of transmitted military communications, which rose from a daily average of 1000 in 1939 to almost 9000 in 1943. Notwithstanding the fact that any message which could be sent by telephone or teleprinter was forbidden to be sent by radio, the share of the wireless traffic grew from 12% in 1940 to 29% in 1943. But only this part of the secret messages was, of course, accessible to special intelligence.

In 1939 it was possible to encipher all of the daily average of 192 wireless U-boat messages with two cipher circuits—home and foreign. But the rising volume of this wireless traffic—in 1940, 310; in 1941, 473; in 1942, 1200; and in 1943, 2563 in the daily average—made it necessary to establish, first, additional traffic circuits with separate frequencies, and, second, also new separate cipher circuits, to reduce the number of signals enciphered with the same cipher settings. So in January 1942 the new cipher circuit Triton was introduced for the Atlantic U-boats.

Fears of cipher compromises led to additional security measures: the publication of a new codebook for the U-boat short-signals and the super-encipherment of the square-grid code. Also some preparations were initiated to improve the cipher machine.

The big black out had only limited consequences up to July 1942, because the German U-boats were operating during this time independently off the Americas, and there was no great need for operational radio communications. But when the German U-boats came back to the North Atlantic convoy routes, the black out was of great importance. In May/June 1942 the first experimental group, Hecht, only six U-boats, intercepted five out of six slow west-bound convoys.

In the period from July to December 1942 there were 24 U-boats on the average on the North Atlantic convoy route, few more than in the second half of 1941. But against only 4% of convoys intercepted during the time of current reading of German signals in June to August 1941 and the 18% intercepted during the following period of decrypting with short time lags to the end of December 1941, in the second half of 1942, without decrypting, the U-boats intercepted 34% of the running convoys. Fourteen percent of these convoys were attacked by more than two U-boats. Most of the other 20% could shake off the shadowers by skillful use of HF/DF, which was, I think, of greater importance than radar in most of the convoy operations of this period.

Then, in December 1942, Bletchley Park succeeded again in solving the main problems of the Triton cipher circuit. It is not clear at this time if it was a success of cryptanalysis alone, or if it was arrived at by a new capture of cipher materials, perhaps of U-559 in the Mediterranean. But we know from the newly released American study, which was made by OP–20–G at the end of the war, that the average time lag in decrypting the German U-boat traffic was up to three days at the end of December 1942; then, in January 1943 decrypting was very often current, although it dropped off somewhat towards the end of the month, but from the 5th to 28th February the traffic was decrypted with seldom more than 24 hours time lag. This led to a sharp drop in convoy sightings during January. The number of operating U-boats rose to an average of 40, but the number of convoys sighted dropped sharply to only 20%, and only 4% had larger losses. All others were reported outside or at the edges of German patrol lines, so that no successful operation was possible.

But at this time the German *xB-Dienst* also came to its most successful period: it could decrypt many of the routing and re-rerouting signals and also many of the U-boat situation reports sent daily by the Admiralty or COMINCH. Even if only 6 to 10% of the decrypts came in time to be of operational value, this had important

consequences, as an example of operations in February 1943 may illustrate.

On the 11th the U-boat command ordered group Ritter to establish a patrol line, going southwest, from the 14th. Four days later he ordered a second line Neptun for the 18th. Both were to search for the convoy HX.228, expected according to the time table.

On the 16th the German *xB-Dienst* decrypted a position of this convoy going northeast, so the U-boat command ordered the group Ritter north and the group Neptun to take its position immediately. But Bletchley Park decrypted this order on the 17th. The HX.226 was re-routed north of the German lines. Also the west-going convoys, ON.166 and ON.167, the routes of which were planned to go through the area of the German lines, were re-routed south of group Ritter.

On the 18th the German *xB-Dienst* reported a position of the ON.166, and the U-boat command now ordered Ritter and Neptun to a long patrol line along 30° West, to cover both possible routes on the estimated passing date, the 20th. On the 19th this new German order was decrypted by Bletchley Park, and the ON.166 was re-routed again south of the combined line. But on the same day the *xB-Dienst* decrypted a new position of the convoy, indicating the southwestern direction of ON.166. So the U-boat command ordered four new boats to form immediately an additional short patrol line—Knappen—southeast of Ritter. This new order was also decrypted at Bletchley Park on the 20th, but now it was too late.

While the next re-routing order was going out, U-604 already had established contact, and the U-boat command had ordered Knappen and Ritter to close and to attack. In a fierce convoy battle which lasted for six days and covered 1100 miles, the U-boats sank 15 ships and lost two of their number to the counter-attacks of the escorts.

With the number of U-boats operating on the North Atlantic convoy routes reaching 60 in the first half of March, it became more and more difficult to evade the patrol lines even with the almost up-to-date intelligence from Bletchley Park. But at this time the Germans had finished the preparations to set the fourth rotor of their new cipher machine M–4 to work, which raised the possible rotor sequences from 336 to 1344.

When Bletchley Park deciphered the key-word in the first days of March, there was at first a great fear of a new and long-lasting blackout. Without decryption on the Allied side, evasive routing might now become almost impossible. In the first twenty days of March, out of four east-going convoys of 202 ships, the U-boats sank 40, or 20%. Such losses for another month or two, and the whole convoy system, backbone of the Allied strategy to win the war, might collapse. To prevent this catastrophe, in Bletchley Park all energies now were concentrated to overcome the problems of the fourth rotor, and in only about ten days the experts arrived at the solution.

This was—I think—the greatest and most significant success the cryptanalysts at Bletchley Park had during the whole war. It was accomplished partly because the Germans made some incredible mistakes. At the beginning they introduced only a small part of the technical possibilities of the new machine. There was some overlapping in the use of the old and the new machines, and of the ciphers used for weather planes of the Air Force and the new ones for the U-boats. It was about the 20th of March when the new ciphers were broken. Evasive routing again could be based on decrypts. This was the beginning of the turning of the tide. Now also the Allies could confirm their suspicions that the Germans were also decrypting: there was a decrypted German signal to U-boats which gave references to their own radio intelligence results, an unpardonable carelessness.

The British undertook at last the task of changing all signal security rules and cipher systems, and there was an almost complete blackout for the German cryptanalysts from the 1st of June 1943. The consequences were not felt so heavily on the German side, because one week earlier Grand Admiral, Dönitz had to admit his defeat in the convoy battles against the combined work of the convoy escorts, the support groups with escort carriers and the very long-range aircraft, all equipped with the new ten-centimetric radar. But he did not know anything at the time of the roles played by D/F and by Bletchley Park and the O.I.C.

But in analyzing the last two years in the Atlantic, we must not assume that any and all German wireless messages were decrypted in time to be of operational value. At the end of 1943 the German Navy alone was using up to forty different ciphers, twenty-four of which were based on Schlüssel-M. All had different daily settings, and most had two or three security grades: general, officers only and staff only. To use their own capabilities most economically and efficiently, Bletchley Park had to attack the different ciphers and their changing traffic volume according to established priorities. Surely the U-boat signals always had some priority. Most of them could be read. But current deciphering was often interrupted by time lags of two or three or even seven days. Also some short blackouts came, the longest-over three weeks—in July 1943.

How difficult it is to come to sound conclusions I learned during my studies of the convoy operations of September 1943. After reading the summary report of the Submarine Tracking Room on the convoys

ON.202/ONS.18, based on German decrypts, one gets the impression of complete and up-to-date information on the Allied side. But when one compares this with the German, British and American operational documents, one discovers that much information which seemed to have been obtained in time for counter-measures nevertheless led to complete failures, because the Germans had changed the orders after two days, while the decrypts became available only after five days and still two days off from the operation as originally planned.

Now for conclusions: What was the role of radio intelligence in the Battle of the Atlantic? Of course, all the battles and actions during the six years had to be fought by the men in the U-boats, the ships and aircraft with their many weapon systems, produced by the unnamed workers at home on both sides. But I am sure, without the three pillars of radio intelligence—direction-finding, traffic analysis and decryption—that neither the commander of U-boats could have used his U-boats as effectively as he did, nor could the Allied commands on both sides of the Atlantic have routed their convoys so successfully around the German wolfpacks.

But my detailed studies of all the convoy battles have led me to conclude that radio intelligence was of much greater influence on the operational and tactical decisions taken on the Allied side than on the German side. If I have to place the many factors which decided the outcome of the Battle of the Atlantic in the spring of 1943 in an order of precedence, I would place Special Intelligence or Ultra at the top. I am sure that, without the work of many unknown experts at Bletchley Park and men like Norman Denning,[3] Patrick Beesly, Kenneth Knowles and last but not least, the late Roger Winn,[4] the turning point of the Battle of the Atlantic would not have come as it did in May 1943, but months, perhaps many months, later. Then the Allied invasion of Normandy may not have been possible in June 1944. There would have been a chain of developments very different from the ones we experienced. Of course, there would have been an Allied victory in the end, but this end may have been introduced by dropping the first atomic bomb on Berlin. But this is speculation; Ultra was a reality, and that is what counts in history.

[3] Vice-Admiral Sir Norman Denning was chief of the British Naval Intelligence Division during WWII.

[4] Commander Roger Winn, R.N.V.R., was chief of the Admiralty's Submarine Tracking Room.

Professor Rohwer is Director of the Library of Contemporary History, Stuttgart. During World War II he served in the German Navy. One of the leading scholars specializing in World War II naval history, he recently wrote an article, with Mr. Patrick Beesly, "Special Intelligence and the Destruction of the *Scharnhorst*," which appeared in the October 1977 issue of *Marine Rundschau*.

The American View

Kenneth Knowles

As events recede into history, few of them retain a significance worthy of recall, but the life-and-death struggle known as the Battle of the Atlantic certainly does. Throughout it were woven technical achievements of the highest order, giving advantages and breakthroughs first to one adversary and then to the other. But transcending all of these skills was Ultra intelligence, the breaking of the German U-boat cipher. It gave first to the British and then to the Americans the edge of victory at sea; and from it flowed victory in Europe. Without it the British could have been beaten to their knees. No wonder Churchill considered Ultra intelligence his prime and sacred weapon—his Excalibur.

Not having experienced the harrowing war years 1939–41, we Americans viewed the U-boat conflict, at least at our entry, more as a challenge than as a struggle for survival. We recognized the seriousness of the U-boat weapon and the vital importance of Ultra intelligence, but we controlled its security and use differently from the British. That is, we were far more selective in those who had "need to know" about Ultra, but we made use of Ultra more directly in anti-submarine operations.

Before I proceed further, it might be well to look into the American naval organization developed specifically for the Battle of the Atlantic: The Tenth Fleet, whose commander was Admiral King and whose Chief of Staff

was Frances Low. The Tenth Fleet was set up within COMINCH[1] Staff, using but a small segment of that staff. For example, my job was Head, Atlantic Section, Combat Intelligence, COMINCH, and designated F-21. While still wearing that hat, I also wore a second hat as Chief, Intelligence Staff, Tenth Fleet.

The Tenth Fleet was organized by the normal staff functions—plans, intelligence, operations, *et cetera*—but it also included two important additions: Convoy and Routing, and Operations Research.

A distinct advantage of the Tenth Fleet organization was the ability to use the highest command level for anti-submarine operations. This enabled us to issue orders directly to U.S. task groups in the Atlantic Theater without incurring the delays caused by passing dispatches down through the chain of command. Of course, all related commanders were kept informed.

Another advantage of the Tenth Fleet organization was the integration, through the two-hat system, of related tasks involving the staffs of COMINCH, CNO, and Tenth Fleet.

A third advantage of this organization was the security afforded Ultra intelligence. Within all staffs at supreme headquarters, only three persons actually dealt with Ultra intelligence: myself, my dupty John Parsons, and an enlisted man to handle files and other secretarial duties. Perhaps a half dozen senior officers within the combined staffs had knowledge that Ultra existed. None of the operational commands were so informed. These restrictions were deemed necessary in the American Theater because of the wide separation of commands and the difficulty of maintaining communications security among them.

On the British side, it was customary for Cmdr. Roger Winn, Chief of the Admiralty's Submarine Tracking Room, or Patrick Beesley, Winn's deputy, to talk to Western Approaches, Liverpool, and other shore-based commands on a daily basis when necessary, and this could be done by scrambler telephone without loss of security within the well disciplined and relatively tight command relationships. Also, the British permitted a far more open knowledge of Ultra intelligence among those assigned to operational intelligence than did we Americans. This enabled the British to operate with considerable freedom and convenience within designated areas.

We in the Tenth Fleet received Ultra intelligence when available by secure teleprinter from our communications center, situated in a former girls' school on Nebraska Avenue. We also received facsimile of high-frequency direction-finder (HF/DF) fixes when occurring, from the center, as well as any so-called fingerprint signatures of U-boat radio operators, obtained by comparison of oscillograph recordings (called TINA).

The communications receiving end in Tenth Fleet was in a small, locked room adjacent to the Atlantic Theater combat intelligence center. As previously noted, only three persons were permitted to enter and use this room. We were able to maintain a security screen around Ultra intelligence largely because of tight restrictions of those requiring a "need to know," and the convenient cover of HF/DF fixes and U-boat sightings, as well as TINA fingerprint signatures.

How did we use this sensitive yet powerful intelligence? At times more directly than did the British, yet at no time without back-up evidence, either from HF/DF fixes or sightings. We skated on some pretty thin ice in one instance later in the war when it became imperative that we gain decisive victory as soon as possible. The occasion was a rendezvous in a remote area of the western South Atlantic involving a "milk cow" (U-boat tanker) and a group of 740-ton U-boats coming in for refueling.

As I recall, the "milk cow" and two of the 740-ton U-boats were sunk. We felt the results justified the security risks, since the operation broke up very destructive U-boat attacks in that area and saved valuable shipping and cargoes. It should be remembered, too, that most of our losses were occurring in the western South Atlantic during this period. Subsequently, the commander of a U-boat which survived this attack questioned the security of German U-boat communications, but nothing came of it, as the high command was confident of their cipher system.

In ordering that attack we did have a questionable aircraft sighting and a partial HF/DF fix that could be associated with it. But, in our determination to destroy this dangerous U-boat concentration, we certainly went out on a limb. I remember Commander Winn's cryptic yet appropriate signal, "Too true to be good". In retrospect, however, I feel that Admiral King's philosophy based on "the calculated risk" was sound, and certainly paid off in rich dividends, culminating in the capture by Dan Gallery's task group of U-505. She was towed with superb seamanship from the vicinity of the Cape Verde Islands to Bermuda, where Admiral Low and I inspected her. Among our finds were the first German acoustical torpedoes and their new location charts only recently put into use.

Let me digress for the moment and speak of the German U-boat cipher. Produced in the first instance by the Enigma, it yielded a completely random cipher at any setting. In addition, U-boat positions and areas of operations were designated by coded location charts. Thus, even though the Enigma cipher were broken, the

[1] Commander-in-Chief, United States Fleet (Also Admiral King).

geographic position of a U-boat and its operating area were generally unknown unless we possessed the coded chart. Over a period of time, we could laboriously reconstruct portions of the chart from U-boat attack and sinking reports and HF/DF fixes. The capture of those newly issued charts in U-505 was therefore of inestimable value to the British and us.

Again, possession of the deadly acoustical torpedoes aboard U-505, which had wreaked such damage among our escort vessels and small carriers, was most fortuitous. After exhaustive tests of the acoustical torpedoes, we developed a counter to them called "Foxer"—towed metal bars which vibrated intensely at the proper frequency and became the sound target for those torpedoes instead of the ship's propellers.

While Ultra intelligence gave us an advantage over the U-boat that no technical skill could surmount, there were frequent lapses when no Ultra was forthcoming, in some cases of several months' duration. We did, however, receive on a regular basis from Cmdr. Winn reports of U-boat arrivals and departures to and from their French and Norwegian basis, as well as new U-boats departing the Baltic. These gave us continuing and reliable count of U-boats at sea, and usually their individual identities.

During the gaps in Ultra intelligence, we relied on operational patterns developed from previous Ultra, and when these grew dim in time, we leaned heavily on HF/DF fixes. As I recall, we had some 30 to 35 reporting stations extending from South Africa to Iceland and around to Brazil on the western periphery. Normally, we received by facsimile a preliminary fix of three to five bearings within half an hour of the U-boat's transmission, and a more precise fix of perhaps eight to twelve bearings within the hour. The fixes were designated as to accuracy, the best being characterized as "within 50 miles." Perhaps 15 to 20% came within this degree of accuracy.

Historians generally consider the turning point in the Battle of the Atlantic came after the summer of 1943, following the sinking of some 90 U-boats. The spring had been disastrous for us in ship losses, with tonnage exceeding any previous period. The U-boat fleet was at its prime, while we had not yet attained necessary strength in aircraft and surface escorts and carriers. Also Ultra intelligence had been exceedingly sparse. After that period we certainly had the distinct edge, especially since the Germans had lost so many of their experienced U-boat captains. However, in the background was emerging a whole new ball game: a fleet developing of highly sophisticated Type XXI 1600-tonners and smaller Type XXIII U-boats, with new schnorkels, permitting underwater speeds exceeding most of our escorts. Once these boats became operational, it would be touch-and-go all over again.

In addition to these technical advances, including a new high-speed acoustical torpedo, the Germans were improving their surface radar and radar-detection and introducing a revolutionary communication method of flash transmission—an entire message of 50 groups being sent in perhaps ten seconds. Such brief radio transmissions would have literally scrapped our whole system of HF/DF bearings and fixes, and could have cut seriously into the interception of U-boat radio traffic—the very grist of our Ultra mill.

It was imperative, therefore, that we crush German seapower before these ominous developments could become operational. Here is where Ultra intelligence did, indeed, do yeoman service, for it enabled us to so weaken the German Navy after 1943 that we could hasten the European victory while there was still time. I cannot emphasize too strongly the crucial importance of this time factor. It was providential that the periscope/schnorkel vibration problem of the new U-boats so delayed their development that but one Type XXI 1600-tonner became operational by the German surrender. Both the British and ourselves used Ultra intelligence for defensive as well as offensive operations. Our primary defensive operations were concerned with routing convoys and the "Queens"[2] which, because of their high speed, operated independently. We in combat intelligence were in constant touch with the convoy and routing watch officers. A change in U-boat dispositions, such as the German wolfpacks, would immediately be noted and routing changes made. When the Germans started reading our convoy dispatches, they became suspicious of these route changes just when a new wolfpack line was established.

So there was always the danger, in using Ultra intelligence in operations, that the Germans would change their cipher system, and they did begin changing their Enigma keys every few hours instead of once a day. We were more aggressive in our use of Ultra intelligence than the British and got more mileage from it, but then they had so much more to lose. Perhaps it is fair to say that the British were more clever in its use, we more daring. The teamwork between us was superb, and we were ever grateful for their more experienced counsel and advice.

Yet, in spite of every safeguard, there were occasional disasters. The one that still haunts my memory concerns the first convoy of aviation gasoline tankers enroute from Trinidad to the Mediterranean, designated TM-1. We had routed it south of the Azores. However, the short-legged escorts needed refueling when they got to that general area, so the escort commander chose the northern

[2] The famous steamships. *Queen Elizabeth* and *Queen Mary*.

lee of the Azores for refueling to avoid the heavy weather farther south. By the time we received his change of route signal, it was too late. The wolfpack hit hard over several days and nights, and it only took one torpedo hit on a tanker for her to become a flaming holocaust. As I recall, only two tankers reached port. The irony of this disaster was that the escort commander had just come from a tour of duty in the British Convoy and Routing section.

One factor, often overlooked in the breaking of the Enigma cipher, was the sheer volume of U-boat radio traffic stemming from Dönitz direct control of U-boat tactics, especially those involving U-boat attack concentration, such as the wolfpacks. He not only insisted on complete information from his commanders, but also would himself personally direct individual U-boat tactics. No such volume of radio traffic—so urgently needed by cryptanalysts—would have been available in normal submarine operations. But then Dönitz's methods almost succeeded!

A final observation about Ultra intelligence: I seem to gather the impression from existing books and articles (I have not yet seen that excellent book of Patrick Beesly's) that the British not only succeeded in breaking the German U-boat cipher, with the acquisition of an Enigma machine and the capture of the U-boat location chart, but continued to break the cipher and sort of spoon-feed us Americans with its tremendous benefits throughout the Battle of the Atlantic. Not having played any part in that cryptographic wizardry, I can only speak indirectly, but it is my distinct impression that, once we got into the act, the American contribution to Ultra was at least equal to the British effort. Perhaps someone more knowledgable in that area will speak more directly to the question.

Captain Kenneth Knowles, USN (Ret), served as Head, Atlantic Section, Combat Intelligence on the staff of the Commander-in-Chief, U.S. Navy during World War II.