'The views expressed are those of the author and do not reflect the official policy or position of the US Air Force, Department of Defense or the US Government.'"

USAFA Harmon Memorial Lecture #36

Codebreaking and the Battle of the Atlantic

David Kahn, 4 April 1994

This is the story of World War II's Battle of the Atlantic and the intelligence effort that went into helping win it. The Battle of the Atlantic was the longest battle of the greatest war of all time. Winston Churchill said it was "the dominating factor all throughout the war. ...Battles might be won or lost, enterprises might succeed or miscarry, territories might be gained or quitted, but dominating all our power to carry on the war, or even keep ourselves alive, lay our mastery of the ocean routes and the free approach and entry to our ports." In the attempt to keep these sea lanes open, codebreaking played an important role.

The story begins- as do so many things in World War II- in World War I. In August of 1914, the first month of that war, a German light cruiser, the *Magdeburg,* stranded itself a few hundred yards off the island of Odensholm at the mouth of the Gulf of Finland. Today that island, now called Osmussaar, is part of Estonia, but then it was part of Russia, with whom Germany was at war. To free his ship, the German captain threw everything he could think of overboard -the coal, the mine laying rails, the bulkhead doors, ammunition, the drinking water. He rocked his vessel. He had the crew collect at the stern to lift the bow. Nothing worked. His radioman could hear the calls of Russian ships from nearby Reval (now Tallinn) approaching. He had one codebook burned and two others thrown overboard. But, as he ordered his crew to abandon ship, he forgot one in his own locker. Only one of the demolition charges he had set went off, and the Russians boarded the damaged cruiser. A search turned up the neglected codebook. This the Russians sent by courier to their allies, the British, who, the Russians thought, as the primary sea power could well use it. It was officially delivered in London to the First Sea Lord, a position equivalent to the American Secretary of the Navy, then held by a politician named Winston Churchill.

With this codebook, the fledgling organization that the British had set up to read coded German naval radio messages got its real impetus. Room 40, as it was called for its early quarters in the old building of the Admiralty, was soon revealing the plans of Germany's High Seas Fleet.

This knowledge kept the Germans from surprising the Royal Navy, perhaps from defeating it in a great sea battle that would end Britain's dominion of the seas and so in effect winning the war in a day. Instead the British were able to bottle up the Germans in their North Sea ports. This kept the Germans from victory, and the British, French and Americans went on to win the war.

The end of that struggle brought a few hints that the Germans had lost at sea in part because of codebreaking, but it was not until 1923 that the secret was revealed. Churchill, who had the necessary political clout, received government permission to tell the story in his memoir *cum* history, The *World Crisis.* In his dramatic fashion, and with rather more poetic license than fidelity to facts, he told how the Russians had picked up the body of a German sailor and " clasped in his bosom by arms rigid in death were the cipher and signal books of the German Navy." He disclosed that the *Magdeburg* codebooks had been given to the British and that with them the British were able to detect every potential and actual sortie of the German High Seas Fleet and so frustrate almost every German naval move. This information surprised and dismayed the Germans. The German Navy realized that it had to have some kind of cipher system that would prevent this ever happening again.

Back in 1918, German mariners had been offered a cipher machine with so many combinations that it would prove useless even to an enemy who captured it because it would take too long to run through them all to hit upon the right one. The German Navy had then turned it down as expensive, complicated, and unnecessary. But in the mid 1920s the *Reichsmarine* realized that this machine was exactly what it wanted. So it got in touch with the inventor.

He was an electrical engineer named Arthur Scherbius. He had developed, independently of others in the United States, Holland, and Sweden who had had the same flash of inspiration, a cryptographic principle called the rotor. The working principle requires you to imagine a hockey puck. On one side of the puck are 26 electrical contacts; on the other, 26 more. They are connected at random to one another through the body of the puck. The puck is held between two plates. One of these gets current from a typewriter keyboard; the other sends current to a display device, such as an array of flashlight bulbs that can illuminate a panel with letters printed on it. Now if you shoot in a current from, say, the letter A from a keyboard, it will go in at the top of the plate, enter the puck, twist around inside it, and come out at the contact that will lead to, say, Q. The rotor turns one space. Now you shoot the current in again at the top, from A. This time it comes out at X. Again the rotor turns. Shoot the A current in again; now it comes out at R.

Obviously, the sequence of substitutions is going to repeat after 26 letters- one revolution. But if you line up several rotors, one next to the other, each turning one step only after the preceding rotor has completed a rotation, you will have a complex, internal maze of electrical wiring that will not recur until 26 to the power of the number of rotors you have. In addition, you can vary the order in which the rotors are put into the machine, and then their starting positions. Probably about 1924, the German Navy saw that Scherbius' machine, which he called the Enigma, solved the problem of capture that had led to disaster in World War I. Sometime in 1926, therefore, it adopted the Enigma. It proved so good a machine that the army too adopted it, instituting its use on 15 July 1928.

Near the end of World War I, Poland had reappeared in Europe. It had been reborn from Germany and Russia, which had partitioned the country near the end of the 18th century. Both Germany and Bolshevik Russia were infuriated at losing this land. The Bolsheviks in fact invaded Poland, in part with the desire of turning all Europe Red. Poland, using every weapon at her disposal, evolved a codebreaking bureau that helped her armies under General Jozef Pilsudski defeat the Russians. During the 1920s, as Germany, never reconciled to the loss of her eastern lands or to the Polish corridor, thundered out ceaseless propaganda about rectifying the frontiers, Poland developed her codebreaking further to get information about German plans. At first her cryptanalysts had been able to solve several German Army cryptosystems. Then, on 15 July 1928, the codebreakers saw a change in the characteristics of the German cryptograms. One of the old systems had merely shuffled the letters of the German originals and so the cryptograms contained about the 40 percent vowels of ordinary German text. The new intercepts had only about 20 percent vowels -the number to be expected at random. This told the codebreakers that they faced a complex cipher system in which the letters of the original German message were replaced with substitutes in an almost random fashion. They guessed that the cipher was generated by a machine, perhaps the Enigma, which they knew from Scherbius' failed attempt to sell it to businesses. Intelligence sources confirmed this, and the Poles attacked the cryptograms. But they made little progress.

While they hammered unsuccessfully upon the intercepts, a German whose soap factory had gone bankrupt had been given a civilian job in the German Army's Cipher Center, which his brother had previously headed. This job included creating, distributing, and accounting for the Enigma machine keys- the order of the machine's three rotors, their starting position, and other

elements that had been added. Needing or wanting money, this man, Hans-Thilo Schmidt, decided to sell the valuable information that he had about the Enigma to the French. They bought from him the basic operating instructions for the machine. But this did not include the actual starting positions, and so it did not enable the French cryptanalysts to break the system. They gave the material to their friends the British, who had no more success with it than had the French.

Now France had had, since 1921, an alliance with the Poles that threatened Germany with a two-front war if she made trouble either for France or for Poland. The French may have known of a 1928 Polish publication revealing Poland 's cryptanalytic successes in her defeat of the Bolsheviks and may have thought that the Poles might put Schmidt's material to good use. In any event, the French gave it to them. At first the Poles could do little more with it than the French and the British. But in 1929, to a greater degree than any other country in the world, the Poles brought mathematicians into their cryptologic service. In 1932, one of them, Marian Rejewski, represented the Enigma encipherment with several simultaneous equations. Aided by some keys that Schmidt had sold and by a lucky guess, he solved the equations- and thereby determined the wiring of the right hand, or "fast" rotor, and then of the others. He had uncovered the heart of the Enigma machine.

But Rejewski 's work had, in a sense, just begun. The advantage of the Enigma was that, even if the enemy were given a copy of the machine, he would not be able to crack messages enciphered in it quickly enough to be of use. Now Rejewski had, in effect, obtained an Enigma. But he and his colleagues now had to ascertain each day 's keys- and that in less than the hundreds of millions of years that the Germans' studies had told them that that would take.

They cracked this problem, in part because an element of the German system of keying intended to offer extra security in fact opened a chink in the cipher's armor. Three letters of the key that had to be sent from encipherer to decipherer were repeated- for example, WSX WSX- to help correct any transmissions errors. The six were then enciphered at a common, prearranged setting of the rotors. But different encipherments of identical letters gave the Polish cryptanalysts a wedge with which to break into the encipherment. Their ingenious analysis, accelerated by special mechanisms, enabled the Poles to do what the Germans thought nobody could ever do, namely, read messages in Enigma in a day. They continued to do this throughout the 1930s, keeping up with the constant complications that the Germans introduced. But, in part for fear of a

leak that might infuriate the Germans, they said nothing about this to the French or the British. After several years, however, two things happened that caused the Poles to change their minds. On 15 December 1938, the Germans put two more rotors into service, giving them five possible choices, not just three, to pick from to insert in the Enigma's three rotor positions. This multiplied the Poles' work by 10 and outstripped their financial and personnel resources. And on 15 March 1939, Hitler, who had promised after he'd taken the Sudetenland, the German-speaking fringe of Czechoslovakia, that he would never annex any part of the world that wasn't German-speaking, marched into the rest of Czechoslovakia. The French and the English finally saw that he was not to be trusted. They guaranteed Poland that, if Hitter attacked her, they would come to her aid.

This promise dissolved Poland's reluctance to share her great cryptanalytic secret, even though Germany's cryptographic improvements had rendered it almost moot. Britain and France, on the other hand, had both the resources and, if war were to come, the need, to exploit the Polish work. The Poles built new mechanical cryptanalytic aids, called bombes, for their allies, as well as Enigma replicas, and, in a sensational meeting outside of Warsaw in July 1939, gave them to their astonished but delighted new allies.

On I September, Hitter attacked Poland. The British and French guarantee went into effect. World War II began. The Poles broke some Enigma messages. But these did not enable Poland to stop the Nazi *Blitzkrieg.* This is a sad but significant instance of the rule in intelligence that, no matter how good a nation's intelligence may be, without military strength, no country can win a war. So Poland was defeated. A few months later, so was France. Not, however, before the British and the French, exploiting a weakness in the German Air Force's Enigma keying system, solved some cryptograms.

Britain, then, protected by the sea from invasion, and augmented in her stymied cryptanalysis of Enigma by the Polish solution, endeavored to crack the German machine. By 1939, she had followed the Polish example and recruited mathematicians to help in this work. She was lucky- or wise- to have in her cryptanalytic agency, the so-called Government Code and Cypher School (G.C. & C.S.), not only a collection of extraordinarily brilliant young men and women, but one authentic genius. This was Alan Turing, the intellectual father of the computer and the man who devised a better way to solve Enigma messages.

Turing modified the Polish bombe mechanism to perform a much more powerful cryptanalytic method. It required imagining what the original German language might be for a particular cryptogram. The bombes- each of which was in a sense a collection of Enigmas- would then run rapidly through all the possible rotor combinations to see if any would yield the known ciphertext from the presumed plaintext. If one did, that combination represented the day's settings for that key net, and it would unlock all that day's messages on that net. But how did Turing guess the original German message? That was, after all, what the Germans were trying to keep secret. There were a number of ways. Sometimes the Germans sent the same message in two different cryptosystems, one in a low-level system for small units that did not hold an Enigma machine, one in Enigma for higher-echelon units. If the British had solved the lower-level system, they had the plaintext they needed to crack the Enigma message. Sometimes German commanders sent the same message or address or message-start at a set time every day, such as "Situation unchanged" or "Morning report" or "To the General of Aerial Reconnaissance." Some of these were known from solutions from the Battle of France; others could sometimes be guessed.

Of course, many days the needed plaintext could not be divined, and Turing's system failed. Moreover, though it worked often with the *Luftwaffe,* where radio operators' chatter and earlier solutions gave insight into the possible plaintext, it worked rarely with the *Kriegsmarine.* The German Navy's radio operators, most of whom had served for many years, were much more disciplined than the newly recruited *Luftwaffe* personnel. Some fortuitous document captures- from a couple of armed trawlers- had made a few solutions possible. These helped in reading a handful of subsequent messages, but there was no wholesale solution of U -boat traffic. In view of the importance of the Battle of the Atlantic, this was fundamental. What could the British do?

A man whose name has become well known as a creative author had an idea. Perhaps, suggested this man, then an aide in the Naval Intelligence Department, we should attempt to capture some of the German Navy's keys. Then we could read the messages directly without having to guess plaintexts and run the messages through the bombes. This man, Ian Fleming, later the creator of James Bond, proposed luring out a minesweeper by faking a crash at sea with a captured Heinkel bomber, then overpowering the minesweeper's crew and seizing the needed documents. The opportunity never presented itself. But, the idea didn't die.

A longish-haired undergraduate named Harry Hinsley (later a Harmon Memorial Lecturer), had been plucked from his studies at Cambridge's St. John's College to work at G.C. & C.S., and was studying German naval activities on the basis of German naval communications patterns. He knew that the Germans had deployed weather ships in the North Atlantic to gather data on the air masses that moved from west to east and that affected bombing raids on Britain and the coordination of German airpower with ground forces throughout Europe. These ships were isolated and unescorted. One day Hinsley realized that these ships carried Enigma machines and thus naval Enigma keys. The Admiralty was persuaded to send a task force to seize the weather ships and nab the keying documents. Twice during the summer of 1941 such task forces were dispatched, and twice, after brief encounters in the northern seas, they came home with the papers Hinsley hoped they would obtain. In addition, a fortuitous capture of a submarine, the U-110, provided additional documentation. The results were dramatic. When the first set of keys in service arrived at Bletchley Park, home of G.C. & C.S., on 1 June, solution times fell at once from 11 days to 5 hours. As the solutions began pouring out- they were codenamed ULTRA- the British began getting a comprehensive view of German naval communication phraseology, inestimable in its importance for providing cribs for the bombes for future solutions when the captured keys expired. Perhaps more to the point, the British began building up a picture of how the U -boats operated.

Did the fast solutions of June and July immediately produce a drop in the number of Allied ships sunk because the British knew where the U-boat wolf packs were and diverted the convoys around them? No. The Battle of the Atlantic involved too many factors for the effect of just one to be so determinative. The cryptanalysts contributed their part, but no one-to-one correlation existed between them and the sinking rate. Still, the Admiralty was glad to have the solutions that G.C. & C.S. produced for the rest of 1941 after the running start the captures had provided. For the solutions did help convoys to avoid U-boats. For example, Convoy HX 155, with 54 ships out of Nova Scotia in October 1941, changed course on the basis of ULTRA at least twice during its crossing to avoid sub-infested waters- and arrived in Britain with its cargoes of gasoline, fuel oil, sugar, steel, copper, and grain entire and intact.

For many months, ULTRA flourished in part because weather reports formed some of its best cribs. G.C. & C. S. had worked them as follows: All German warships sent in meteorological observations. They condensed each of these into a few letters by means of their

so-called Short Weather Code. These coded reports were enciphered in Enigma and transmitted to a headquarters, where the German weather men deciphered them. They then broadcast the weather reports. The British intercepted these. They had captured the Short Weather Code from the U-110, so they were able to convert the broadcasts back to the same form into which the warships had put them. This constituted the plaintext of an Enigma transmission, which G.C. & C.S. could run on the bombes to find that day's key. But in the fall of 1941, the *Kriegsmarine* introduced a new edition of the Short Weather Cipher. This precluded the conversion into Enigma "plaintext," and the useful weather cribs vanished.

Meanwhile, the German cryptographers were growing worried about the increase in their communications volume- an increase sustained by all combatants. They knew that, in general, the more cryptograms one intercepts, the easier it is to solve a cryptosystem. Though the cryptographers never believed that the British might be reading their messages, they wanted to take no chances. So on 1 February 1942, the *Kriegsmarine* changed the configuration of the Enigma. The original had three rotors in it. The new one had four. This multiplied the work of the codebreakers by 26. Together with the loss of the weather cribs, the new mechanical twist blinded the British.

They remained blinded throughout almost all of 1942. Unable to know what the U-boats intended, the Allies could not take remedial action. Convoys sailed straight into wolf packs. Sinkings in the second half of 1942 were quadruple those of the same period a year before, when Enigma messages were being read.

Then, in the fall of 1942, the British got a break. In the eastern Mediterranean, Royal Navy destroyers forced a submarine, the U-559, to the surface. A rating and an officer swam to her and climbed down into her control room. They passed up documents before the vessel unexpectedly sank, taking them down with her. (They received the George Cross for their heroism). But among the documents they had salvaged was the new edition of the Short Weather Cipher. With this, obtained at so high a price, the cryptanalysts of G.C. & C.S. could again perform their weather crib trick. And they were helped now by U.S. Navy cryptanalysts in Washington, D.C. These were supported by dozens of high-speed bombes, weighing about 2 1/2 tons each and produced by National Cash Register in Dayton, Ohio. The British and American cryptanalytic centers, linked by cable and radio, shared the work. The Allies were producing ULTRA solutions faster than before and almost continuously. Once again, convoys were

dodging wolf packs. More supplies were getting through than ever before. A typical case was that of Convoy SC 127. Its 57 ships sailed from Nova Scotia on 16 April 1943, carrying tanks, grain, explosives, steel, lumber, sugar, phosphates, and fuel oil. Its original route would have taken it through an area in which the codebreakers discovered an estimated 25 U-boats. Its course was altered so it sailed around this square, and eventually the convoy arrived in its British ports without the loss of a single vessel. Its commodore happily signaled: "All arrived."

The Allied intelligence advantage was augmented by the growth in Allied air cover over the Atlantic. Some of this came from very long range patrol planes. These aircraft closed the black hole in the mid-Atlantic in which U-boats had operated free from the fear of air attack. Flying over the convoy routes, the aircraft kept the U-boats submerged, greatly restricting their mobility and their effectiveness. More air cover came from airplanes from escort aircraft carriers. And these, for the first time in the Battle of the Atlantic, used codebreaking offensively. The Allies knew that Germany's supply submarines, the U-tankers, or *"Milchkuhe"* (milk cows), greatly extended the combat time-on-station of the U-boats. Codebreaking revealed with almost pinpoint precision where these U-tankers were to rendezvous with the combat U-boats to give them fuel and other supplies. On the basis of this information, airplanes from the escort carriers attacked the U-tankers, often when they were on the surface refueling. In the middle of 1944, of the 10 *Milchkuhe* in the Atlantic, nine were sunk. Each sinking caused U-Boat Command to go through contortions of resupply, with U-boats having to meet and give up precious fuel to one another so that all could return to Germany.

The consequence of all these converging efforts was that, between mid-December 1943 and mid-January 1944, U-boats sighted not one of the 10 convoys that sailed close to their patrol lines and sank only one isolated merchant ship. In the first three months of 1944, U-boats sank only three merchantmen in convoy out of 3,360 that sailed- at a cost of 36 submarines. By then vast convoys, sometimes hundreds of ships stretching from horizon to horizon, proceeded majestically across the Atlantic, bringing to Britain the men and material that would drive a stake through the heart of the wickedest regime the world had ever seen. This was done by the brave men who sailed the ships and flew the planes and by the American shipwrights who built more ships than any fleet of submarines could have sunk. But their bravery and their efforts were supported, and their sacrifices ameliorated, by the backroom boys, the boffins, who broke the German U-boat codes.

David Kahn is a senior editor for Newsday, a Long Island daily newspaper. He earned his A.B. at Bucknell University and a Ph.D. in modern history at St. Antony's College, Oxford University. In addition to his work at Newsday, he has contributed to the New York Times and the International Herald Tribune. Dr. Kahn has also taught courses on military intelligence at Yale and at Columbia 's graduate school of International Affairs. He is the author of numerous books, articles, and reviews, including Seizing the Enigma: The Race to Crack the German U-Boat Codes, 1939-1943 (1991), Kahn on Codes: Secrets of the New Cryptology (1984), Hitler's Spies: German Military Intelligence in World War II (1978), and The Codebreakers: The Story of Secret Writing (1967).

**AUTHOR'S BIBLIOGRAPHICAL NOTE**

This lecture is based upon my book, *Seizing the Enigma:* The *Race to Break the German U-Boat Codes,* 1939-1943 (New York: Houghton Mifflin, 1991), 336 pages. Sources for the statements in the lecture may be found therein.

But it might be useful to comment on some of the other works dealing with ULTRA. Only books- not articles- will be listed.

Fundamental is F.H. Hins1ey et al., *British Intelligence in the Second World War: Its Influence on Strategy and Operations,* History of the Second World War (London: Her Majesty's Stationery's Office, 1979-1988), 3 volumes in 4 parts (plus 2 volumes on deception and counterintelligence). Though this official history covers more sources of intelligence than just cryptanalysis, and within that more than just naval Enigma solutions, it details the effects these intelligence operations had on the war at sea. It is based on documents, but Hinsley 's work with naval intercepts during the war also informs the book, which is thorough and well indexed but rarely develops the personalities involved. This not only omits an essential dimension but makes the work needlessly dry.

Some of the human aspect is found in Patrick Beesly's admirable *Very Special Intelligence:* The *Story of the Admiralty's Operational Intelligence Centre,* 1939-1945 (London:

Hamish Hamilton, 1977),271 pages. Beesly served in the Operational InteIligence Centre's Submarine Tracking Room as a deputy to the room 's commander, and his memoir *cum* history gives a colorful picture of the use of codebreaking in the fight against the U-boats.

A remarkable conference in Germany in 1978 brought together specialists in many areas of ULTRA, including the Battle of the Atlantic. The proceedings have been published in *Die Funkaufklarung und ihre Rolle im Zweiten Weltkrieg,* ed. Jiirgen Rohwer and Eberhard Jackel (Stuttgart: Motorbuch Verlag, 1979),206 pages.

The story of the German who disclosed the secrets of the Enigma to the French, and France's subsequent cryptanalytic relations with Britain and Poland was first revealed by the Frenchman who was at the center of it all, Gustave Bertrand, in his *Enigma, ou la plus grande enigme de la guerre* , 1939-1945 (Paris: PIon, 1973), 295 pages. Additional details are in former French counterintelligence officer Paul Paillole's *Notre espion chez Hitler* (Paris: Laffont, 1985), 287 pages. A solid secondary study, correcting some of the chronological errors found in Bertrand and establishing a list of the spy's meetings with the French, is the final edition of Gilbert Bloch's *Enigma avant Ultra* (1930-1940) (Paris: self-published, 1988), 130 pages.

The account of the original Polish solution of the Enigma is given best in Wladyslaw Kozaczuk, *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War II,* translated and edited by Christopher Kasparek (Frederick, Maryland: University Publications of America, 1984), 348 pages; it includes appendices on technical details of the solution by the man who did it. A German translation, *Geheimoperation Wicher: Polnische Mathematiker knacken den deutschen Funkschliissel "Enigma"* translated by Theodor Fuchs, edited by Jiirgen Rohwer (Koblenz: Bernard & Graefe, 1989), 365 pages, provides additional documents and updates the text. Jozef Garlinski 's The *Enigma War* (New York: Scribner's, 1980; British title: *Intercept),* 219 pages, offers some additional color. Krzysztof Gaj gives the best publicly available explanation of the mathematics of the solution and of the operation of the Polish and British mechanical aids to solving in his *Szyfr Enigmy: Metody Zlamania* (Warsaw: Wydawnictwa Komunikacji i Lacznosci, 1989), 183 pages; only pages dealing with these matters have been translated. C.A. Deavours' *Breakthrough* '32: The *Polish Solution of the Enigma* (Laguna Hills, California: Aegean Park Press, 1988), 85 pages, takes the student step by step through the cryptanalysis, which Deavours has reconstructed. C.A. Deavours' and Louis Kruh's *Machine Cryptography and Modem Cryptanalysis* (Dedham,

Massachusetts: Artech House, 1985), 259 pages, a fund of information about cipher machines, deals in detail with the mechanics and mathematics of the Enigma in chapter ill, pages 93-150. Jack Levine's invaluable listing, *United States Cryptographic Patents,* 1861-1989 (Terre Haute, Indiana: Cryptologia, 1991), 113 pages, in effect places the Enigma in the context of other cipher machines.

The people and operations of Bletchley Park are described in several works. *Codebreakers:* The *Inside Story of Bletchley Park,* ed. F.H. Hinsley and Alan Stripp (Oxford: Oxford University Press, 1993), 321 pages, has 17 chapters (pages 1-137) on Enigma and the production of ULTRA intelligence that include many personal details. One of the great scientific biographies of our times, Andrew Hodges' *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 587 pages, in addition to profiling the mathematician who made a fundamental contribution to the solution of the Enigma, explains what this contribution was and describes his other work at Bletchley Park.

Two books deal with ULTRA and the war at sea. John Winton's *ULTRA at Sea: How Breaking the Nazi Code Affected Allied Naval Strategy during World War II* (New York: Morrow, 1988), 212 pages, regrettably does little more than concatenate the intelligence information in Hinsley et al's official history with the operations described in S. W. Roskill's official history of *The War at Sea,* 1939-1945 (London: Her Majesty's Stationery Office, 1954-1961), from which all references to ULTRA had been excluded, without really integrating the two. Alberto Santoni's *Il Vero Traditore: Il ruolo documentato di ULTRA nella guerra del Mediterraneo* (Milano: Mursia, 1981),378 pages, maintains that the true betrayer of the Axis naval powers in the Mediterranean was ULTRA. It has been translated into German by Theodor Fuchs: *Ultra siegt im Mittelmeer: Die entscheidende Rolle der britischen Funkaufklarung beim Kampf um den Nachschub fur Nordafrika von Juni 1940 bis Mai 1943* (Koblenz: Bernard & Graefe, 1985), 381 pages.

Recent studies of the Battle of the Atlantic incorporate ULTRA intelligence into their narratives. Two good ones are Dan van der Vat, The *Atlantic Campaign: The Great Struggle at Sea,* 1939-1945 (London: Hodder & Stoughton, 1988), 424 pages, and John Terraine, *Business in Great Waters:* The *U-Boat Wars,* 1916-1945 (London: Leo Cooper, 1989), 841 pages. In preparation is a study by Clay Blair with great promise. On the German side are Jochen Brennecke's bitter *Die Wende im U-Boot-Krieg: Ursachen und Folgen,* 1939-1943 (Herford:

Koehler, 1984), 361 pages, and Gunter Boddeker's *Die Boote im Netz: Der dramatische Bericht uber Karl Donitz und das Schicksal der deutschen U-Boot-Waffe* (Bergisch Gladbach: Lubbe, 1981), 383 pages.

Other books tell the non-naval aspects of the ULTRA story. Gordon Welchman, one of the most ingenious of the early Enigma cryptanalysts, reveals some of his technical breakthroughs in The *Hut Six Story*: *Breaking the Enigma Codes* (New York: McGraw-Hill, 1982), 326 pages. Peter Calvocoressi, *Top Secret Ultra* (New York: Pantheon, 1980), 132 pages, explains the ULTRA operation at Bletchley Park for German army and air force messages; the operation for German naval messages was similar. Two books by Ralph Bennett tell how the German Army and Air Force ULTRA was used by Allied commanders in battle: *Ultra in the West: The Normandy Campaign,* 1944-45 (New York: Scribner's, 1980), 304 pages, and *Ultra and Mediterranean Strategy* (New York: Morrow, 1989), 496 pages. Lieutenant Colonel Haines of the U.S. Army Air Force wrote what was called an "ULTRA history of USAAF vs. G.A.F." (German Air Force) in 1945; this has been published as *ULTRA and the History of the United States Strategic Air Force in Europe vs. the German Air Force* (Frederick, Maryland: University Publications of America, 1980), 205 pages. Diane T. Putney edited *ULTRA and the Army Air Forces in World War II: An Interview with Associate Justice of the US. Supreme Court Lewis F. Powell, Jr.*, USAF Warrior Studies (Washington: Office of Air Force History, United States Air Force, 1987), 197 pages, which includes, besides the interview with the wartime codebreaker, a study by Putney on ULTRA.

Two German books by Heinz Bonatz, for part of the war head of the German naval cryptanalytic service, tell of the work of that organization: the narrative account *Die Deutsche Marine-Funkaufklarung,* 1914-1945 (Dannstadt: Wehr und Wissen, 1970), 174 pages, and what amounts to little more than notes from documentary sources, *Seekrieg im Ather: Die Leistungen der Marine-Funkaufklarung,* 1939-1945 (Herford: Mittler, 1981),376 pages.

Finally, there exists a technical history of the solution of Enigma, in several volumes, reproduced by the Ditto process, with numerous diagrams, that was probably written just after the war, perhaps by the British. It seems never to have been mentioned in unclassified print before. Perhaps this notice will alert persons who are interested in this subject and who would have access to this history to its existence, enabling them to deepen their studies of what was probably the greatest sustained intelligence feat of all time.

'The views expressed are those of the author and do not reflect the official policy or position of the US Air Force, Department of Defense or the US Government.'"