# BLETCHLEY'S SECRET WAR: BRITISH CODE BREAKING IN THE BATTLE OF THE ATLANTIC

Colleen Carper

*The Battle of the Atlantic was the dominating factor all throughout the war. Never for one moment could we forget that everything happened elsewhere, on land, at sea, or in the air, depended on its outcome, and amid all our other cares, we viewed its changing fortunes day by day with hope or apprehension . . . Amid the torrent of events one anxiety reigned supreme. Battles might be won or lost, enterprises 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 out master of the ocean routes and free approach and entry to our ports.* – Winston Churchill

*The King hath note of all that they intend,*
*By interception which they dream of not.* – *Henry V, Act II, scene ii*. Library, Bletchley Park

## Introduction

The Battle of the Atlantic was the longest, largest, and most complex naval battle in wartime history, beginning on the first day of the war, September, 3, 1939, and continuing until the last on May 8, 1945. The fighting on and under the waves was crucial to both sides, and ultimately could determine the outcome of the war, as control of the Atlantic Ocean was vital for Great Britain. In order to fuel the war effort and feed its population, Great Britain needed supplies and raw materials that were imported from around the world on vulnerable ships. Winston Churchill noted in early 1941: "It is the Battle of the Atlantic which holds the first place in the thoughts of those upon whom rests the responsibility for procuring the victory." [1] To wage a successful war against any enemy, Great Britain would need a steady flow of materials; without vital supplies, Britain could not expect victory in the European theater. In addition to supplies, troops from Canada and Australia would need to be transported to Europe in order to bolster British armed forces.

A victory for Great Britain in the Battle of the Atlantic would mean the secure and regular passage of ships carrying vital war supplies across the ocean, which would further their war effort against the Axis powers. Furthermore, by securing the sea lanes, many Britons hoped for a cross channel invasion which would threaten Germany with a two front war. If the Western Allies did not gain the upper hand in the Battle of the Atlantic, Great Britain might very well have been forced out of the

*Colleen Carper, of Louisville, Ohio, is a 2009 graduate of the Ashbrook Scholar Program, having majored in Political Science and History.*

[1] Andrew Williams, *The Battle of the Atlantic: Hitler's Gray Wolves of the Sea and the Allies' Desperate Struggle to Defeat Them (*New York: Basic Books, 2003), 115.

war because of a shortage of food, troops, and critical supplies. Without Great Britain as an active participant in the war, the end results might have proved disastrous for Allies forces. Therefore, the British Admiralty employed several methods of anti-submarine warfare to combat enemy naval vessels.

For decades after the war, Allied victory in the Battle of the Atlantic was attributed to radar, sonar, long-range aircraft, and improved convoy tactics. However, the revelation of one form of British intelligence in 1974 would rewrite history. To the world's astonishment, the war at sea had not simply been won by military genius and tactics, or by the courage of those individuals who fought for the Allies. It was vital information that was decrypted from encoded German radio transmissions that gave the British the upper hand over the Germans at various stages of the war. Noted by historians as one of the most important sources of British intelligence that the Allies possessed, [2] the information gained from German decryptions, codenamed Ultra, provided the British Admiralty with insight into high-level German intelligence and the location of U-Boats well beyond the range of aerial reconnaissance missions.

While Ultra was not the deciding factor in the Battle of the Atlantic, this work will attempt to understand Ultra's role in British intelligence and its influence on the war at sea. Of all the coded messages that the German military enciphered on the Enigma machine, naval ciphers would prove to be some of the most difficult codes to break during the war. Because of the complexity of the naval Enigma ciphers, British cryptanalysts did experience delays in decryption. Depending on the information that cryptanalysts possessed, it could take hours, days, or even weeks for ciphers to be decrypted. While British cryptanalysts were able to build on the decryption methods previously used by Polish intelligence, it would require the capture of code books and vital information regarding the Enigma machine's daily settings that would result in British breaks into the German cipher system.

Deciphering thousands of messages throughout the duration of the war, British intelligence worked to decrypt German transmissions quickly enough for them to be operationally useful. The information gained from Ultra decryptions not only allowed the British admiralty to reroute convoys which were in the path of German U-Boats, but it also aided in the destruction of various German vessels. Without this important source of intelligence, the British would have a suffered a greater loss of men and material during the Battle of the Atlantic.

## Early Breaks into the Enigma Cipher: 1932-1939

The practice of cryptology, the method of changing text so that it is unreadable to others,[3] was not a new idea in World War II. Early coding systems were developed by Julius Caesar to conceal messages, and various ciphering techniques were used in the Franco-Prussian War, the Boer Wars, and World War I. In World War I, methods of encrypting messages centered on words, syllables, phrases, and code words. After the war, code breaking became mechanized, employing mathematical knowledge and ciphers or the method of substituting individual letters in a message.

[2] Ralph Erksine, 2000, Afterword to *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre 1939-1945;* or *Codebreaking in the Battle of the Atlantic,* by Patrick Beeley (Annapolis: Naval Institute Press, 1977), 263.

[3] Rudolf Kippenhaun, *Code Breaking: A History and Exploration* (New York: The Overlook Press, 1999), 31.

The practice of ciphering converts a message into symbols that have no meaning without the key that was used to encipher the message. Without knowledge of the cipher key, messages would appear as a jumble of meaningless letters to enemy interceptors. The radio transmissions of the German military and government in World War II were enciphered on a machine named the Enigma. Resembling a typewriter housed in a wooden box, the Enigma later became one of the best known cipher machines of the time. Over the course of the war, Germany used over 80 variations of codes, all enciphered on the Enigma machine.

The Enigma machine itself was developed and patented by Arthur Scherbius, a German electrical engineer, in 1918. Reportedly named for *Enigma Variations*, a piece composed by Sir Edward Elgar, the first Enigma machines were used by German railway systems and banks to keep the details of monetary transactions secure. These Enigma machines were unclassified and could even be purchased commercially in the 1920s. Weighing only about fifteen pounds, and with dimensions of 4.5 by 10 by 10.75 inches, the secret to this enciphering machine was its interior. The Enigma consisted of a Continental QWERTZU keyboard and another board with lights that corresponded to each letter of the alphabet. The machine was powered by batteries, and pressing one letter such as an "a" would light up another letter such as "p." Inside the machine were three removable rotors. Each rotor possessed a non-conductive wired code wheel with twenty-six electrical contacts–one for each letter of the alphabet–that were randomly connected to another twenty-six contacts on another rotor. The random internal wiring of rotors was secret, and thus determined the final output code. Past enciphering machines would often use rotors; however, what set the Enigma machine apart from the machines of the past was that the rotor or code wheel in Scherbius's machine could rotate. After a letter was typed on the keyboard, the rotors would turn so that entered double letters would not produce the same output letters. For example, a double "b" might result in a "y" then a "d." However, an early weakness of the Enigma machine lay in the use of the twenty-six letters of the alphabet. If the same letter was hit twenty-six times, the first output letter and the twenty-seventh output letter would be the same. Scherbius soon recognized this weakness, and a second rotor was added to the machine. This complex rotor was different than the first in that it turned one rotation after the first wheel had made twenty-six complete turns. In this model, the first output letter and the 677th output letter were the same. With the addition of rotors, the number of times a letter must be hit before the sequence of code letters repeated lengthened by a factor of twenty-six. Therefore, if four rotors were a part of the Enigma machine, the first and 456,977th output letters would be the same; with five rotors the first and 11,881,377th output letters aligned.

In the late 1920s, German engineers Paul Bernstein and Willi Korn made various improvements to the Enigma machine. Bernstein created a removable ring with indicator letters on each rotor; this ring could be locked into place in any of the twenty-six positions around the rotor. Thanks to this innovation, the indicator letters no longer had any relation to the position of the rotors, so that a particular letter did not mean that a rotor was in any particular position. This improvement made the position of the alphabet ring on the rotor now part of the cipher key. Bernstein also moved the notches, or contacts, on the rotor to the ring that surrounded the rotor. This change eliminated the relationship between the rotor movement and the rotor enciphering method, which created a larger obstacle for code breakers to overcome. In an attempt to make the machine's ciphers even harder to break, Willi Korn designed rotors that were removable. The leftmost rotor was now known as the reflector rotor and would not turn. This rotor would send the electrical current back through the rotors on a different path from which it came, further enciphering the original message. It also only had thirteen connectors instead of the twenty-six possessed by the other rotors.

This new method of enciphering created both advantages and disadvantages. The idea of sending the electrical current back through the rotors complicated the system–a letter could go through up to seven substitutions before the output letter was revealed, eliminating the possibility for a simple cipher substitution. Furthermore, the change also eliminated the possibility of enciphering text when the machine was set in deciphering mode. At the same time, this method allowed for the revealing of some plaintext when it was discovered because no letter could represent itself. This disadvantage made it possible to find solutions by eliminating possibilities that were not probable. Scherbius in 1918 wrote to the navy: "They key variation is so great that, without knowledge of the key, even with an available plaintext and cipher text and with the possession of a machine, the key cannot be found, since it is impossible to run through 6 billion keys [based on seven rotors]."[4] If one did not possess the cipher key and wanted to figure out the code, with an Enigma machine with seven rotors and the ability to test a different key setting every half minute on 100 machines, it would take 5.8 years to break just one sent code.[5]

The German army and navy realized the potential of the Enigma machine and officially adopted it to encode classified messages by 1928.[6] However, concerned with both external and internal security issues, the German military's aim was to prevent its enemies from reading its messages, while at the same time, preventing other German units from reading messages that were not intended for them. While all of the messages were encrypted on identical Enigma machines, the army could not read the messages from Hitler's private army, the SS, or *Schutzstaffel*. Therefore, different keys were used for different types of military radio traffic. However, messages were transmitted on the same radio waves. In order to alert Enigma operators if they had the key to read a message intended for their organization, three letters were used before the enciphered message in the unenciphered text. Operators would first look at this group of letters to determine if the message was directed to them. Furthermore, after a series of improvements to make the device more secure, the Germans considered it an advantage that even if an Enigma machine was captured, it could not be decrypted unless the other operator possessed a machine with identical settings.

In 1925, the German navy ordered the production of the Enigma machine with not only regular letters but also umlauts. Originally, the army did not use umlauts in its Enigma machines and employed the QWERTY keyboard while only using three rotors. Only officers could set the key positions, which guaranteed further security. In order to avoid superimposition–that is, the method of having many messages encrypted in the same way–officers chose starting key positions that were far apart in distance on the keyboard. The lower the

[4] David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes 1939-1943* (New York: Barnes & Nobel Books, 1991), 33.

[5] Ibid, 33.

[6] Joseph E. Persico, *Roosevelt's Secret War: FDR and World War II Espionage* (New York: Random House, 2001), 107.

rank of the officer, the fewer keys he possessed. The Germans also utilized a plug board, a board consisting of twenty-six double jack plugs, which added extra substitution. Twelve letters were chosen by commanders and these letters could be substituted for another one of the twelve which further enciphered the message.

The Enigma machines used by the German navy were more complex than those of the other military branches. In August of 1934, the navy, instead of using three rotors like the army, chose to use seven. In late 1939, improvements were made to the sixth and seventh rotors. Notches were added in the alphabet rings next to the letters H and W, which caused the rotor to move one space when it reached those letters in the previous revolution. This important advance reduced the possibility of a successful superimposition. To further the complexity of the codes, different cipher keys were used for home waters and foreign waters. Furthermore, generals and officers often possessed their own plug board settings, while staff possessed different inner settings. To add to the security, the rotors and the boxes in which the Enigma machines were held were heavily guarded. Men who were in charge of the rotor settings were ordered to keep the information secret and were threatened with charges of treason if the information was leaked. The act of setting the inner workings of the machine was also closely monitored. On top of all of these safety precautions, any naval cryptographic materials, such as the log books, which contained the month's Enigma settings, were printed in water soluble red ink on pink paper. If the book would be submerged, the text on the page would bleed out and be unreadable to enemy forces if recovered. With the improvements that were made to the Enigma machine, enemy forces now needed to possess five key elements to successfully read ciphers: an Enigma machine, a code book which held the setting list for the machine, the position of rotors and indicators, the tables for enciphering indicators, and the ring position.

While other branches of the German military during the early years of the war used Enigma machines with only three rotors, the naval Enigma operator had eight rotors to choose from, any three of which could be used for the day's setting. Therefore, the daily number of possible rotor order settings for the naval Enigma machine was 336. This additional security measure made the ciphers of the German navy some of the most complex and sophisticated codes of the war. German naval cipher clerks were responsible for sending out encrypted messages in Morse code. Often, original messages from German headquarters were encrypted to specific submarines or the entire fleet, or messages were sent from submarines to headquarters. Each submarine had an identical Enigma machine in which the operator would enter the encrypted code into the machine. The daily keys that Enigma operators received from the German High Command listed the three rotors that were to be used for the day and their order from left to right. The key also revealed the starting position of each rotor with a single letter; the rotor's alphabet ring would then be turned so the letter indicated would show through the hole in the machine. Finally, the key gave the operator the plug board settings, which further substituted letters.

In order to set up the machine, the Enigma operator had to follow a long, complex procedure which involved the random selection of three letters as an indicator group and their encipherment with the aid of the bigram tables listed for the day in order to establish the message key. Once the operator possessed the key, the three letters were pressed on the keyboard, one after another, and the letters that lit up as a result were recorded. The Enigma rotors were then reset so the enciphered three letters that showed though the top of the machine were the recorded letters. Finally, the machine was ready to encrypt messages. Enigma operators on the receiving end would have their Enigma machines set up in the same way, using the same daily keys. Then the process would be completed in reverse; as ciphered text was pressed on the machine, plaintext letters were illuminated, revealing the original message. Messages were often repeated every half hour or hourly past the original transmission time to ensure that they were decrypted properly. However, without knowledge of the daily key, the intended message could not be read by the receiver. The mere possession of an Enigma machine would not reveal the daily key, and unless one possessed all of the required elements for decryption, coded messages could not be read.

To the Germans, the Enigma already seemed like an impossible cipher tool to break. Because of the trillions of possibilities that the machine could produce, the German military and high command were confident that the ciphers produced by the Enigma could not be deciphered and read on a regular basis. With many key possibilities available, by the time messages would be solved, weeks or months would have already passed, thus making them militarily worthless. There were no fewer than 10.5 quadrillion possible keys for each message. Ultimately, even with 1,000 cryptanalysts, each of whom possessed four captured or copied keys that they tested every minute of every day, it would still take 1.8 billion years to test them all.[7] However, code breakers normally would only test the plaintext until about halfway through the message, when they would realize that the jumble of letters was a product of the incorrect key. If this fact was taken into account with cryptanalysts in the same situation, it would only then take 900 million years to break one message.[8]

By the beginning of the 1930s, French and British intelligence had received little information, mainly generalities, about the Enigma machine. However, in 1931, the *Deuxieme Bureau*, the French Secret Service, was approached by Hans-Thilo Schmidt, who worked in the Cipher Office of the Defense Ministry in Berlin. Fond of money, Schmidt was willing to sell secret German documents to the French. Over the next few years, Schmidt would provide over 300 secret documents over the course of nineteen meetings, including the instructions for the Enigma machine, photographs of the plug board and descriptions of how it worked, and examples of enciphered and deciphered text. [9] From this information the French learned that the Enigma machine possessed at least three rotors with movable alphabet rings. They had also deduced that the reflecting rotor did not possess the capability to turn, and that the machine utilized a plug board which was different than the commercial Enigma machines. However, the French did not possess an Enigma machine itself, and without the machine, they could not discover where the electrical circuit traveled within the rotors. Furthermore, because the ciphered messages were different from the linguistically coded messages of the First World War, and French intelligence lacked mathematical cryptanalysts, they did not know how to further work on breaking the ciphers. However, mathematicians in Poland, a French ally, did have a background in mathematical ciphers, so the French passed along information about the Enigma to Polish intelligence in hopes that they could produce a solution.

[7] Kahn, 68.

[8] *Ibid.*

[9] Michael Smith, *Station X: The Codebreakers of Bletchley Park* (London: Pan Books, 1998), 32.

Marian Rejewski, a Polish mathematician and cryptologist, was assigned to attempt to find a solution to the Enigma machine. In 1932 along with Rejewski, fellow mathematicians and cryptologists Henryk Zygalski and Jerzy Różycki also worked to recover daily key codes. In addition, the Polish team was given replicas of early commercial AVA Enigma machines which were produced by the Radio Manufacturing Company. Though the Germans had adapted their machines from the comercial Enigma, the commercial machines were a start to revealing the inner workings of the Enigma. Early on, the Poles deduced that the initial key was repeated over the air waves in case the receiver on the other end missed the initial key code or if the code was lost in static or transmission. The Poles also understood that the Germans also managed to change the rotor order every three months, while the key changed daily. To send a new key, the Enigma operator would turn the rotors so that the past day's key would appear in the cover. The key usually was a combination of three non-adjacent letters such as "pdj" or "rsn." Then the new key was sent twice: "hwmhwm" which would then be received as "pdnmzz." The operator would then enter "pdnmzz" into the Enigma to receive that day's key: "hwm" and then change the letters that appeared in the cover window accordingly.

Eventually Rejewski discovered that strings of letters in the coded messages created chains in the first and fourth letters of indicators because the plug board connections, rotor order, alphabet ring and rotor start position were the same. The chains would eventually close and appear if enough letters were used. Using high level algebra and theorems in the theory of groups, Rejewski was able to discover that the plug board, which the Germans thought added to the security of the Enigma, could be ignored in his equations. Setting up six equations that upon solving would reveal the wiring on the fastest moving rotor, Rejewski worked around the clock to discover a solution. The twenty-six elements of the equations–the values–were unknowns. However, these unknowns could be reduced to groups: the numbers representing the wiring of the fastest rotor, the numbers representing the combined wiring of the middle and left rotors and the reflector, and the connection of the six pairs of the plug board.

The last unknown was the order of the letters on the alphabet ring on the rotor. However, upon gaining from Schmidt Enigma key settings and plug board settings for both that September and October, the equation was simplified. The Poles then discovered that the alphabet ring simply followed the alphabet–A, B, C, etc. While the Germans could have arranged the letters in millions of ways, they chose to simply follow the alphabet. This important piece of information made the solution of the wiring of the fastest or leftmost rotor possible. Without the keys that the Poles had gained, they would not have been able to solve the wiring of the first rotor. Rejewski later wrote: "To this day it is not known whether equation 3 [the order of the letters on the rotor] is solvable… It required the possession of messages from two days of identical or very similar settings of the rotors; therefore, finding the wiring of the rotors would depend on luck."[10] Later, Schmidt was able to provide the Poles with materials and information that led to the construction of the wiring in the Enigma's rotors and reflector.

The order of the rotors was the next challenge for the Poles. In a normal day, code breakers needed 60-100 intercepts in order to begin to break the day's key code.[11] If enough messages were intercepted,

[10] Kahn, 66.

[11] *Ibid*., 70.

incorrect settings of the Enigma machine could be eliminated, leaving the correct setting for the day. In these intercepts, chains of letters were created. The Poles would convert these chains of letters into tables that would reveal the first two letters of the three lettered key. This method, however, only revealed which letters appeared through the window of the Enigma lid, not the numerical position of the rotors. In order to solve the positions of the rotors, cryptanalysts used a grille, which was a sheet of paper with six horizontal slits with the first chain of letters written on it. These sheets were compared to the alphabet tables. At each position, the Polish cryptanalysts would attempt to find pairs of letters. If they could find six pairs on one table, they could determine which rotor was the fastest, as well as that rotor's position. While this seemed like a logical method for revealing the quickest rotor and its setting, it was tedious work. It would take up to ten minutes to test one setting of one rotor. Cryptologists had twenty-six more settings on each of the three rotors to test. The entire process would then have to be repeated in order to find the middle rotor and its starting position.

Another challenge for the Poles was to reveal where the alphabet rings were set on the rotors. Each rotor possessed notches that turned the rotors to the left. Moreover, each letter possessed its own notch, so in order to break the codes, the cryptanalysts needed to know which notch was specifically set on each rotor. The ring setting could be revealed in two ways. The first consisted of the Poles guessing where the message began by using the word "*an*" (the German word for "to") followed by "x" or the word separator. One out of five messages began in this way, which left only 676 (26 x 26) positions of the other two rings to test. If the Polish cryptanalysts did not try to locate "*an*," they would have to test 17,576 ring positions.[12] Ultimately, if the code breakers could discover the rotor order, the rotor setting, and the ring setting, they could decipher a message in a day rather than years. The plug board, which was another security measure added by the Germans, only used twelve letters. If cryptanalysts with possession of all key components needed to break the codes of the Enigma machine, they could easily decipher the plug board settings. For example, a non plug board deciphered text would read: "slarm larts dmpaqmd." Cryptanalysts could simply look at the quasi-plaintext and be able to solve the plug board wiring, which would reveal the message to read: "spare parts delayed."

Furthermore, while many German officers and government officials believed the Enigma was impossible to crack, their overconfidence in the machine often led to carelessness in practice and protocol when using the Enigma machine. Fewer ideas for key changes meant keys were often duplicated to cut down on new enciphering methods. Furthermore, Enigma clerks often made up simple keys such as "zzz" or "qqq", in order to remember them more easily. These keys, which could be solved by superimposition, were soon prohibited when the German high command discovered that simple keys were being used. Finally, Enigma signal operators or clerks often sent messages that contained common or anticipated plaintext. For example, weather reports or ship movement each started with the same phrases or messages could begin or end with "Heil Hitler!" German military procedures actually made it easier for cryptologists to guess the content of messages. The carelessness of enemy operators who neglected security procedures to take shortcuts to deliver messages could enable enemy cryptanalysts to figure out their coding system. However, in an attempt

[12] *Ibid.*, 71.

to add more security to the Enigma, on February 1, 1936, Hitler demanded that the Enigma's rotor order be changed monthly instead of quarterly. This change reduced messages sent in the same settings by one-third. Furthermore, plug board variations could now range from five letters to eight. Later that year, orders came to change rotor settings daily. These changes put even more pressure on cryptanalysts as the race between the code makers and code breakers escalated. In the past, solutions to current codes could take years. Now enciphered messages would have to be broken in months and days in order to keep up with the rate in which messages were sent. With the new changes to the Enigma machine, the number of codes successfully deciphered was reduced by forty percent.[13]

Despite the changes, some ciphers, such as "asd" or "qaz", did not appear random on a QWERTY keyboard. If these patterns were chosen for keys, cryptanalysts would only have to test thirty to forty settings in order to break the code.[14] Also, Zygalski noticed that groups of letters in ciphered text had certain letters in common. These common letters were nicknamed "females." Because a "female" could not be naturally produced by the Germans, each one represented a setting that could not be used for the Enigma setting. In order to record the "females," Zygalski created two cardboard sheets, each 51 spaces by 51: enough for A-Z to be written on the top and A-Y down the side of each. Each sheet recorded possible positions of rotors and a hole was punched in to the sheets were where a "female" was expected to occur. Once all possible settings were reviewed, the sheets were aligned on top of each other over a light source. The positions where light shone through all of the sheets indicated a possible correct rotor sequence and ring setting. However, this possible solution did not reveal the plug board settings and each sheet could have around 1,000 holes punched in it. Furthermore, with twenty-six positions for each of the six possible rotors, 156 sheets were required.

While the Zyglaski sheets were effective, the process was tedious and time consuming, and when the Germans added more rotor possibilities to the Enigma machine, the Poles could not keep up with coded messages. In an attempt to decipher codes more quickly, the Poles used a cyclometer, which consisted of two linked sets of Enigma rotors to test possible settings. This discovery accelerated the recovery of the order of the rotors and their settings. The Poles understood that if the combination of two Enigma machines accelerated the rate at which codes were solved, adding more machines should further accelerate the process. Therefore, efforts were made to create a machine that would be able to test six sets of Enigma rotors at once. When the machine would produce a possible solution, code breakers would use the key on the enciphered text. If plaintext was produced, then the machine had discovered the correct key. It would take these machines, called "bombs" because of the ticking noise it made during its operation, up to two hours to discover a possible solution. While this method seemed like an effective method, two problems arose. First, cryptanalysts had not taken into account the fact that indicator letters could be changed in the plug board. Second, when five to eight bombs were used, the bombs would only work half of the time because of the primitive wirings of the combined machines in relation to the numerous codes they were testing.

The Poles were able to make these steps toward solving the Enigma codes based purely on analysis and managed to

[13] *Ibid*.
[14] *Ibid*., 72.

keep up with minor tweaks in German security measures. Despite the German alterations, Polish code breaking methods improved, allowing them to solve codes at a much faster rate. However, this all changed on December 15, 1938, when the Germans added two more rotors. Enigma machines still only could hold three rotors, but now the combinations could be chosen from a group of five separate rotors. The overall combination of rotor choices mathematically went from six to sixty. The worst news of all was that the wiring of the two new rotors was unknown. However, the Poles soon discovered that the *Sichnerheitsdienst* (SD), the Nazi Party's Intelligence Service, were still using the old methods to assign the rotor order and settings, ring setting, and plug board settings. Because the wiring was the same as the other rotors, the Poles could reconstruct the writing of the first rotor and the two new rotors. This revealed yet another weakness of the Enigma machine. The rotor wiring went simply from A to Z, instead of a random alphabetical order on each rotor. If the wiring on each rotor was truly random, the ciphers that the machine produced may have never been broken. Now with two new rotors, Polish cryptanalysts would now need sixty bombs and 1,500 sheets or grilles to successfully decipher messages. To make matters worse, on the first of January 1939, the plug board connections rose to ten.

The Poles soon realized they would need the aid of much larger countries with the funds available to crack the German ciphers, and on April 27, when Germany renounced its non-aggression agreement with Poland, the Polish cryptanalysts realized that they now must share their deciphering methods with France and Great Britain. The Poles invited both British and French intelligence to Warsaw on July 24. The cryptanalysts hoped that the larger countries would have the funds to provide them with more bombs in hopes of solving the codes at a faster rate. In the meeting, the Poles revealed the replicas of the Enigma machines they had created, as well as the bombs. Amazed at the feats of the Polish cryptanalysts, the British agreed to aid the three cryptologists. When the Germans invaded Poland just a few short months later, the Polish cryptanalysts evacuated their work station, burnt any unnecessary documents, packed up their Enigma models, and began to travel east toward France. In October, the Poles resumed their enciphering methods in France at Chateau de Vignoles, twenty-five miles northeast of Paris. This villa was named P.C. (*Poste de Commandement)* Bruno and consisted of the Polish "Z-team," seven Spanish Republican Cryptanalysts designated the "D-team" and French cryptanalysts and personnel. Any findings that were uncovered would also be reported to British intelligence via typewriter line by British liaison officer, Captain Kenneth Macfarlane. P.C. Bruno would closely work with Britain in the years to come in deciphering German Enigma traffic.

British intelligence at this time had its own code breaking agency, which in the late 1930s made significant breakthroughs in solving enemy codes. The British first established the Government Code and Cipher School, or G.C. & S.C., as a permanent code breaking agency in 1919 under the direction of the director of naval intelligence, Captain Hugh "Quex" Sinclair, who later would become the chief of the Secret Intelligence Service. Located at the Broadway Buildings complex, which was a few blocks from Westminster Abbey, the G.C. & S. C. employed anywhere from 39 to 500 individuals with an annual budget of 100,000 pounds.[15] Members of the G.C. & S.C. were regularly reading decoded messages from the United States, France, Spain, Japan, Italy, and Hungary. However,

[15] *Ibid*., 80.

the one country's messages that British intelligence failed to read was Germany. Most of the men employed at the G.C. & S.C. did not see this failure as an issue. Because Germany had been stripped of its armed forces after World War I, British intelligence saw the country as defeated with no need for interception. Furthermore, German army radio traffic was difficult to intercept near the British Islands. Finally, while Germany did possess a small navy, opportunities for naval intercepts were slim. These discouragements led British intelligence to focus its attention and efforts on the coded messages from France, Italy, Japan, the Soviet Union, and the United States. World events also drew attention away from German interceptions. In 1936, during the Spanish Civil War, British intelligence focused heavily on Italian traffic. Viewing Italy as a threat to India and British territory, British intelligence focused their efforts on breaking the weakly coded Italian messages.

In later years, the large amount of messages to be deciphered, coupled with the need for security and quiet, forced Sinclair in July of 1939 to purchase Bletchley Park. Built by businessman Sir Herbert Leon, Bletchley Park was located halfway between Cambridge and Oxford, which attracted the attention of Britain's code breaking agency. Furthermore, though the MI6, Britain's secret intelligence service, and the Government Code and Cipher School had offices in London, Sinclair desired an alternate location safe from German bombing and spies. Bletchley Park was given the cover name "Station X" because it was the tenth site acquired by MI6 during its wartime operations. It was also the center of a web of intercept sites around the country where wireless operators recorded German radio messages before sending them to cryptanalysts by teleprinter or motorcycle courier. These intercept sites, known as "Y Stations," were operated by all branches of the British military.

Those individuals who were recruited to work at Bletchley Park possessed competency in clerical work, managed electronic equipment, were skilled in enemy languages, and were able to quickly solve word or math puzzles. Mathematicians, linguists, novelists, chess champions, and academics were hand recruited and employed to decipher various coded enemy messages. The *Daily Telegraph*, famous for its regular readers, held a contest asking contestants to solve one of their crossword puzzles in less than twelve minutes. Those who did well were invited to an interview with the G.C & C.S. Gwen Davis, who was employed at Bletchley Park, noted: "At least half of the people there [Bletchley Park] were absolutely mad. They were geniuses, no doubt many of them were extremely, extremely clever, but my goodness they were strange in ordinary life."[16] The mansion itself could not accommodate the British intelligence staff, so workers assembled temporary one-story, narrow, wooden huts around the grounds in an attempt to give all of the employees their own workspace.[17] Employees themselves were housed in communities near the area and were not to inform friends or family of the workings of Bletchley Park. By the start of the Second World War, many men and women who worked on ciphers at Bletchley Park would only see a piece of the puzzle, not knowing what exactly they were decrypting.

[16] Michael Paterson, *Voices of the Code Breakers: Personal Accounts of the Secret Heroes of World War II* (Cincinnati: David & Charles, 2007), 73.

[17] By 1944, Bletchley Park would employ over 7,000 people.

## The Battle of the Atlantic: 1939

The Battle of the Atlantic began on September 3, 1939, and lasted until the end of the war on May 8, 1945. It was fought all across the 32 million square miles of the Atlantic Ocean, making it the longest, largest, and most complex naval battle in history.[18]

Control of the Atlantic Ocean was vital for Great Britain. In order to further the country's war efforts and feed its population, Great Britain needed supplies and raw materials that were imported from around the world on vulnerable ships. Oil, a critical supply, had to be carried over thousands of miles from the Middle East, the United States, and the Dutch East Indies. Without safe waters, the tankers bringing oil to Britain would be lost amid the waves. Churchill told the country in early 1941: "It is the Battle of the Atlantic which holds the first place in the thoughts of those upon whom rests the responsibility for procuring the victory."[19] To wage a successful war against any enemy, Great Britain would need a steady flow of materials; without vital supplies, Britain could not fight overseas battles and expect victory in the European theater. In 1939, economists calculated that Great Britain needed to import 55 million tons of goods by sea in order to support its population's current way of life.[20] Furthermore, a fleet of 3,000 merchant ships was required in order to transport needed supplies for any given week, and each day around 2,500 of these required 3,000 ships were at sea.[21] In addition to supplies, troops from Canada and Australia would need to be transported to Europe in order to bolster British armed forces. Later in the war, troops would travel from America by convoy, a practice that involved assembling ships into organized formations with escort vessels.

With a victory in the Battle of the Atlantic, many Britons hoped for a cross channel invasion which would threaten Germany with a two front war. Winston Churchill after the war wrote: "The Battle of the Atlantic was the dominating factor all throughout the war. Never for one moment could we forget that everything happening elsewhere, on land, at sea, or in the air, depended ultimately on its outcome, and amid all other cares, we viewed its changing fortunes day by day with hope or apprehension."[22] If the Western Allies did not gain the upper hand in the Battle of the Atlantic, Great Britain very well could have been forced out of the war due to a shortage of food, troops, and critical supplies. Without Great Britain as an active participant in the war, Germany would have been the supreme power in Western Europe. Furthermore, if Germany controlled the Atlantic Ocean, it is a possibility that Great Britain and America would not have been able to send supplies to aid Russia. Moreover, the 1944 invasion of France would have been nearly impossible without safe waters. A victory for Great Britain in the Battle of the Atlantic would mean the secure and regular passage of ships carrying vital war supplies across the ocean which would further their war efforts against Germany and the Axis powers.

The Germans were aware that control of the Atlantic was crucial to Britain. Lieutenant Commander DE Balme of the British Royal Navy noted: "The Germans recognized that the Atlantic was the vital artery for Britain to obtain supplies of food, fuel, and raw materials for our factories. If they could cut that line, they could win the

[18] Williams, 6.

[19] *Ibid*., 115.

[20] John Keegan, *The Second World War* (New York: Penguin Books, 1989), 105.

[21] Barrie Pitt, *The Battle of the Atlantic* (Alexandria: Life-Time Inc., 1977), 17.

[22] Kahn, vii.

war."[23] Without the material and men to defeat Hitler's armies, Great Britain would starve. Grand Admiral of the German Navy Erich Raeder noted: "Great Britain's ability to maintain her supply lines is definitely the decisive factor for the outcome of the war" and was convinced that German *Untersee-boots* or U-Boats "are the decisive weapons against Great Britain" because they gave the Germans the element of surprise in battle; they would later become one of the main enemies of the convoy.[24]

Karl Dönitz, who commanded of the German Submarine Fleet, and who would later become Grand Admiral and Commander in Chief of the German Navy, believed that the best way to blockade Great Britain was through the use of these submarines. Taking only nine months to build and costing about a half million dollars each, U-Boats were inexpensive weapons. These submarines were ordered to a designated area in the ocean, and then patrolled that area waiting for passing ships or for orders to assemble for a larger attack. They would only return to port when fuel or ammunition was low. Only twenty-five to thirty men would live in the small quarters of the submarines for up to three months.[25]

Throughout the course of the Second World War, Germany produced thirty-four types of U-Boats ranging from minelayers and supply submarines to open ocean vessels. On average, these underwater vessels could reach a speed of eighteen knots on the surface and a range of 11,000 miles while running on diesel engines. They could spend up to about twenty hours underwater running on electric batteries but only could reach speeds of two to three knots. It took these submarines about a minute to reach 250 feet below the surface.[26] The deeper a U-Boat sank under the waves, the longer it would take for a depth charge, a bomb detonated by certain water pressure, to reach the submarine, and this offered a better chance for its survival. Only one small break in the submarine's pressure hull could spell doom for the vessel and her crew.

The British used a number of methods of defense against the U-Boat. ASDIC, which was named for the organization that developed it, the Anti Submarine Detection Investigation Committee, was used to detect a submarine that had submerged. Pulses of sound were sent out from a dome located under the ship, and if the sound pulses came in contact with an object, they reflected back to the ship. The sound beams could be reflected off objects other than submarines such as rocks or shipwrecks, but it was up to the operator and the range recorder to determine if the object was moving. ASDIC's ping would become a sound familiar to submarine operators.[27]

With the developments associated with ASDIC, the submarine's advantage of "invisibility" underwater had ended. However, this early version of sonar had serious technical problems. The farther away a submarine was from the hunter ship, the more likely it would be spotted, because the sound beam that was sent out from ASDIC widened with distance. As the two vessels moved closer to one another, the contact with the enemy submarine was more likely to be lost. Moreover, ASDIC could only be used underwater; it could not locate submarines which had surfaced. Therefore, Dönitz ordered his U-Boats to attack Allied ships in surface night raids. U-Boats were not only less visible and not audible to

[23] Paterson, 101.

[24] David Westwood, *The U-Boat War: The German Submarine Service and the Battle of the Atlantic, 1935-1945 (*Philadelphia: Casemate, 2005), 114.

[25] PBS, "NOVA," November 14, 2000, "Hitler's Lost Sub," Roy Scheider.

[26] *Ibid*.

[27] The Americans also developed their own version of ASDIC, which they called sonar.

ASDIC, but could travel at a faster speed than when they were submerged.[28]

With the faith that the British placed in ASDIC, the use of aircraft in anti-submarine warfare initially seemed unnecessary, so crews of the Royal Air Force Coastal Command received little training in anti-submarine operations. In addition, most of the aircraft at the start of the war were unable to travel long distances–a vital aspect in ocean patrol. Also, the bombs that the planes carried proved to be a greater threat to the pilot of the plane than the U-Boat. In order to cause major damage, the bomb needed to fall six to eight feet from the U-Boat, which required pilots to fly at low altitudes. However, when dropped, the bomb would often bounce off of the water and back up towards the plane and explode. A replacement bomb would not be made until 1940.[29]

British commanders also employed radio intelligence in a method called direction finding. Local antennas on the coast and on British ships would be rotated until enemy radio signals were heard. British intelligence then identified the location of submarines by using a "line of bearing." In order to determine the location of a U-Boat, two or more antennas needed to sense the same U-Boat radio signal. Lines were drawn out from both antennas to the perceived location of the U-Boat. The area in which the lines met revealed the approximate location of the enemy craft. But while this method seemed effective in theory, direction finding often had a twenty-five-mile or more margin of error. Furthermore, most ships were not stationed at fixed locations; they moved across the open waters, which made U-Boats more difficult to track. Most British sea vessels were located 60-1000 miles offshore or in the open ocean.[30] Finally, direction finding proved to be an ineffective method of defense against U-Boats because although the technique detected the approximate fixed location of a submarine, it could not inform British intelligence of the direction in which the U-Boat was traveling.

The final method that British forces possessed for defense against U-Boats was to break the ciphered messages that the U-Boats sent out via radio, which could reveal their location or mission. However, during the late 1930s, British intelligence was not capable of deciphering ciphers quickly enough to make this method effective. The lower-level ciphers which were broken by the G.C & C.S. included reports on the weather, damage to German merchant ships, troop transportation, and the departure times of U-Boats and fleets, but neither the position nor the movement of German vessels. However, this method, with improvements, would eventually prove of invaluable use in the Battle of the Atlantic.

At the dawn of the Second World War, the Royal Navy realized it would need to employ any anti-submarine warfare methods it could in order to gain the upper hand in the Atlantic and surrounding waters. Only about ten hours after Great Britain's declaration of war, U-30 torpedoed the British liner *Athenia* on its way to its port, mistaking it for a troopship. In months that followed, U-Boats began targeting merchant ships that were vital for the survival of Great Britain. However, merchant ships were not the only targets for German submarines. In mid September, U-29 sank the aircraft carrier HMS *Courageous* while on patrol, and a month later the battleship *Royal Oak* went down at the hands of U-47 while anchored at Scapa Flow. These successful attacks were a warning to the Royal Navy that no ship was safe.[31]

[28] Pitt, 21.

[29] Williams, 61.

[30] Kahn, 4.

[31] Robert C. Stern, *Battle Beneath the Waves: The U-Boat War (*London: Arms and Armour, 1999), 82, 91-93.

In 1939, Germany possessed the ability to sink British warships, but such sinkings did not add to the amount of tonnage that needed to be destroyed to strangle British supply lines. At the outbreak of war, U-Boats were still abiding by the terms of the Hague Convention, which prevented any attacks without warning on merchant and passenger ships. However, on September 23, Hitler declared that all merchant ships, which could use radios to report the location of U-Boats should be taken captive or sunk.

At the outset of the war, the German navy only possessed fifty-seven U-Boats; of these, thirty were short ranged submarines fit only for coastal missions, leaving only twenty-seven that could venture out into deeper ocean waters.[32] Therefore, only a small number of U-Boats patrolled the Atlantic during the first months of the war. Dönitz pressured his superiors for faster production of U-Boats. His plan was to wage a "tonnage war" against Great Britain with the goal of sinking as many tons as possible per submarine per day without regard to route or cargo. Ultimately, Dönitz hoped his sinkings would exceed British replacement rates.

Dönitz also understood that in the North Atlantic a single U-boat would not be able to inflict much damage on convoys of merchant ships guarded by escorts. The First World War had proven that when merchant ships were organized and escorted by warships, shipping losses were cut by eighty percent.[33] Convoys would travel in a wide rectangle of eight to twelve short columns about 1,000 yards apart, with about 400 to 600 yards between each ship. Most convoys would consist of roughly forty ships, of which thirty to thirty-five would be merchant vessels; the navy could only spare up to five escorts per convoy. Convoys of this size would cover an area around four miles across by two miles wide.[34] However, most of the available escort vessels were patrolling the open ocean, so many ships in the early weeks of the war traveled without escorts. During the first month of the war, an average of only two Royal Navy escorts was destroyed each day, roughly 1.3 Allied ships per convoy.[35]

Although World War I revealed that the use of convoys lowered the success rates of U-Boats, Dönitz had devised a method that he thought would overcome the convoy. A single submerged U-Boat traveled at a slower speed than that of merchant ships in a convoy. Therefore, if a U-Boat captain could not reach a convoy due to an inaccurate position, the crew might have to wait days before another convoy appeared. Also, even when a second convoy arrived, there was no certainty that it would travel in the same path as the first. Therefore, U-Boats would need to travel in concentrations that Dönitz called "wolf packs" to inflict the maximum amount of damage on the ships of a convoy. With the improvement of radio communications, U-Boats on the surface could communicate with headquarters, as well as with other submarines located hundreds of miles away. In order for a wolf pack to complete a successful attack, efficient radio communication and coordination were required. Dönitz ordered that every convoy which was sighted be reported to headquarters, and once a convoy was located, headquarters could radio the location to other U-Boats in preparation for an attack.

As soon as other submarines reached the identified convoy, they could attack when an opportunity presented itself. It often took many hours for other U-Boats to reach a central area, as they were often over

[32] Keegan, 105.
[33] Pitt, 21.
[34] *Ibid*., 96.
[35] *Ibid*., 21.

300 miles apart.[36] Therefore, the U-Boat that first signaled headquarters to a convoy would shadow the formation of ships, often reporting its position for the U-Boats that were heading toward it. Dönitz understood that British intelligence could intercept the large amount of German radio traffic that was generated, but this was a risk that he was willing to take because of his faith in the complexity of the naval codes. No attack was made until all of the U-Boats which were ordered to arrive were present. Most of the attacks were then staged at night so the men aboard the ships in the convoy would not be able to detect the submarines. U-Boats also chose to attack on the surface to avoid sonar detection. Therefore, U-Boat captains were relying on the eyes of convoy lookouts, hoping they would not be detected or that they would be too small to see. The more U-Boats that could attack at the same time led to confusion and lowered the chances of ships in the convoy escaping. Dönitz observed: "The greater number of U-Boats that could be brought simultaneously into the attack, the more favorable would become the opportunities to each individual attacker."[37] Often the wolf pack would attack the same convoy on consecutive nights.

In order to locate convoys in large open waters and attack with effectiveness, Germany would need to produce large numbers of U-Boats. Dönitz believed that 100 U-Boats could do more damage than all of Germany's surface ships, and that 300 U-Boats could cut Britain's supply lines altogether.[38] However, at the outbreak of the war, the navy was third to the Army and Air Force in terms of material and funds. Furthermore, Hitler only gave top priority to surface vessels, particularly battleships. Despite the fleet's second-class status, Dönitz made several attempts at a successful wolf pack attack, but British convoys would often change direction with short notice. It was not until September 1940 that wolf packs began successfully locating and attacking convoys.

## Early Code Breaking Efforts at Bletchley Park: 1940

In the early months of 1940, at Bletchley Park, the work of two men–Alan Turing and Gordon Welchman–would produce two significant breakthroughs in British code breaking methods. The head of the Government Code and Cipher School, or G.C & S.C., in the late 1930s, Alastair Denniston, had realized that the messages that British intelligence was attempting to decipher were coded based on mathematics, not linguistics like the messages of the past. Therefore, he concluded that British cryptanalysts should not specialize in linguistics but math. In 1938, Denniston held a series of courses in cryptology for mathematicians. King's College mathematician Alan Turing, who was in his late twenties at the time, attended these classes. On September 4, Turing would join Alfred Dillwyn Knox, an experienced linguist and British code breaker, Peter Twin, an Oxford Graduate in mathematics, and John R. F. Jeffreys, a Cambridge mathematician at Bletchley Park, to work on deciphering the Enigma codes. Turing's breakthrough in the Enigma decoding method came late in 1939 as he ran the bombs that tested possible Enigma keys. Turing invented electrical multipliers for the cipher system that would eliminate the results from the bombs that led to contradictions. The keys that the bombs ran tested whether the enciphered messages of the cryptogram were consistent with the unknown basic key setting that was trying to

[36] Williams, 83.

[37] David Fairbank White, *Bitter Ocean: The Battle of the Atlantic, 1939-1945* (New York: Simon & Schuster Paperbacks, 2006), 19.

[38] Pitt, 22.

be discovered. The bombs would then reject any keys that produced inconsistencies. Bombs could eliminate thousands of key possibilities based only on inconsistencies. However, this would leave a few keys that were contractions that would have to be tested to see if the ciphertext produced plaintext when the key in question was used on the ciphertext.[39]

Turing's method was based on a technique that cryptanalysts used to break coded messages. Cryptanalysts assumed that within a coded message existed a probable word in the form of a plain word or phrase such as "attack" or "enemy." Probable words included ways of reporting, greetings, referral to units, or signing on or off. This probable word could then be employed as a stepping stone to recovering the full text or key of the cryptogram. This same method had been used by the Poles before their use of bombs when Polish cryptanalysts would assume that messages from the German Enigma would begin with "*an"*–"to" in German. This method was used to reduce the number of trials that the Poles would attempt in trying to find probable positions on the alphabet rings. Turing used this method of matching a word or phrase to part of the intercept and testing whether the rotor position would allow for the word or phrase. Now code breaking methods would change from finding non-contradictive links between known and assumed unknowns to recover keys to non-contradictive links between plaintext and assumed keys. In order to achieve goal, Turing added a test register, a set of twenty-six electrical relay points, to each rotor position on the bombs. The test register looked at the voltage of each of the twenty-six points which were equivalent to the output lights on the Enigma machine. If voltage would run on all of the twenty-six points or all but one, this would equal a non-contradiction between the assumed plaintext and the position of the rotor, which ultimately would equal a possible key solution. Once this non-contradiction was discovered, the key was used on the ciphertext to see if the result was German plaintext. If plaintext was not produced, the bombs would be restarted and the process continued.[40]

The idea for a probable word came from the cryptanalysts imagining a possible plaintext phrase or word that code breakers called a "crib." These words came from knowledge of German communication which was gained through direction finding, radio messages, past Enigma solutions, and captured documents. Cryptanalysts might use the crib *nichts zu melden*, "nothing to report," or the message's recipient–*dem general.* The crib would then be written letter by letter above the ciphered text. Then the cryptanalyst would look for a loop of letters or connected letters that in assumed plaintext and ciphertext could be chained together, linking the first letter with the last.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Crib: | n | i | **c** | h | **t** | s | z | u | m | **e** |
| Ciphertext: | k | r | **t** | b | **e** | l | w | s | u | **c** |

For example, the first *c* in the crib is linked to the *t* in the ciphertext, then to the *t* in the above crib, to the *e* below, to the *e* above, and to the *c* below, which would create the loop "ctec." Once a loop was discovered, the bomb would be set up in the basic position using the rotors, I, II, and III, in that order, and set to AAA. The rotor order and their position, ring setting, and plug board settings were all unknowns. During this time, the ring positions could be ignored, because cryptanalysts hoped that the middle rotor would not be a part of the crib. Voltage would then be applied to one of the bomb's positions that represented a plug board

[39] Kahn, 94-5.

[40] *Ibid*., 95.

substitution in the first letter of the crib. The electricity would then pass through the bomb's rotor arrangement, through the reflecting rotor, back through the rotors, and on to the second pair of letters in the loop. The voltage would then pass through the third letters of the loop, and then back to the first pair of letters. The number of spaces separating the looped letters also played a key role. It was assumed that if the number of spaces between the first and second looped pair was two, the number of clicks the second rotor would have to be from the first or faster rotor would then be two. While voltage passed through the loop of letters, it also passed through Turing's test register. If the rotor arrangement and the plug board substitutions were guessed correctly, the voltage would appear as a single circuit or as one test point. This was one of the two conditions needed for a correct match void of contradictions. If a bomb displayed this condition, the machine would automatically stop to allow cryptanalysts to use the current rotor position to test the coded message. Because of the number of plug board solutions, many substitutions would have to be made to plaintext, but the message itself should resemble enough German that the validity of the message could be tested.[41]

Upon the solution of all of the plug board settings, the code would be broken. If cryptanalysts had the rotor order wrong in the bomb, the voltage would pass through the first rotor and exit the letter as if it was on to the next letter in the loop. However, the incorrect rotor order would prevent the voltage from completing the loop and channel it instead in a non-looped point. When the voltage would enter the end rotor at a non-looped point, the point in which it emerged would again be another non-looped point. This process would continue until all twenty-six points were lit. Then the machine would stop, and cryptanalysts would attempt to figure out the correct rotor order. If the rotors were in the correct order but the plug board substitutions were not guessed correctly, the voltage would spread out in the same method as an incorrect rotor arrangement, with the difference being that the voltage would not be able to enter the one correct test point. With all of the points lit but one, this produced the other condition that would cause the bomb to stop. More often cryptanalysts would find the machine stopped at this scenario. Turing's method freed cryptanalysts from finding any special settings in the message keys such as repeated letters in certain positions in the text which the Polish cryptanalysts called females. The test register also reduced the time that was previously required to solve a coded message, thus making the chances for a solution higher.[42]

The second British breakthrough was discovered by 34-year-old Gordon Welchman, a Cambridge mathematician. Welchman spent most of his time at Bletchley Park intercepting German army messages. In the frequencies of the radio messages, call signs, message indicators, addresses, and signatures of the messages, Welchman discovered patterns within the structure of the German army. Welchman observed that different command structures used different keys using a technique that would later be called traffic analysis. This method made the case that common phrases or words that were located at the beginning of the text could be used as cribs. Furthermore, if a message was transmitted on a lower level system of the German military that had already been broken, it was most likely repeated on a radio using the Enigma machine. If the text of the same message from the lower level system and the Enigma machine could be matched up in what was known as a "kiss," it provided a crib for the message and led to the eventual solution of the Enigma's key

[41] *Ibid.*, 96-7.

[42] *Ibid.*, 97.

settings for that day. Another method used by Welchman was nicknamed gardening. Cryptanalysts at Bletchley Park would choose a certain location at sea and request that mines be dropped into the area. If the German High Command discovered the location of the mines, they alerted U-Boat fleets via radio to avoid the area. After these messages were intercepted, cryptanalysts could use the mines' location as a crib to help them decipher the message keys.[43]

Using perforated sheets, Welchman devised another method, almost identical to the idea of the Polish Zygaliski sheets, to narrow the number of possibilities for the rotor order and settings. Welchman called his sheets the "Jeffreys sheets" for John Jeffreys, the staff member who prepared the sheets for him. The Jeffreys sheets accelerated the number of Enigma solutions that were discovered. The method also revealed that Enigma solutions were reciprocal. For example, if the plaintext b produced the ciphertext K at a certain rotor order and position and a certain plug board setting, then a plaintext k should produce a ciphertext B at the same settings. Welchman's discovery was used to take advantage of the letters in a crib that were not part of the loop in the bomb machine. Welchman used a wooden board with 676 contact points for the A-Z letters across the top and the A-Z letters down the side. Wires would then connect points such as row G, column K and row K, column G. This connection would automatically send voltage through the pairs that were connected and would ultimately reduce the number of faulty stops in the bombs.[44]

Welchman's method was then incorporated into the bombs themselves. The machines soon grew to over four feet wide, as each bomb could hold twelve Enigma machines plus Welchman's diagonal board. With the use of five bombs, all sixty rotor possibilities could be tested. The first machine of this size was introduced in Bletchley Park in Hut 11 in on August 8, 1940. Soon four bombs were installed and ran keys from fifty-nine radio networks, some of which changed keys every twenty-four hours, while others changed every twelve hours.[45]

Enigma messages that were intercepted and decrypted at Bletchley Park were by this time known by their codeword, Ultra. Most of the work towards decoding these messages was performed by Wrens (Women's Royal Navy Service). Over 1,000 Wrens worked with the bombs around the clock in eight-hour shifts to decode messages.[46] British Prime Minister Winston Churchill took special interest in reading decrypts from Bletchley Park. He would often have several deliveries of decoded messages send to his home daily. Churchill had called earlier German intercepted codes "Boniface," a name designed to make the enemy believe that source was an agent, not a deciphering system, an early attempt to keep Ultra and its decrypts a secret.[47] Churchill often referred to Ultra messages by this name long after the term Ultra had become standard.

As the G.C. & S.C. expanded, the military and naval sections of code breaking were split into two sections: cryptanalysts who would crack cryptograms and intelligence analysts who would pull out important information from the deciphered codes. Teams at Bletchley Park were then known by their hut number. The Naval intelligence analysts were located in Hut 4. Turing, who headed the naval cryptanalysis, was located

[43] Kahn, 98.

[44] *Ibid*.

[45] Stephen Harper, *Capturing Enigma: How HMS Petard Seized the German Naval Codes* (Phoenix Mill: Sutton Publishing, 1999), 16.

[46] Perisco, 102.

[47] *Ibid*., 159.

in Hut 8. There, he spent most of his day attempting to discover new cribs, searching for loops in plaintext and ciphertext and running tests on bombs. In Hut 8 mathematicians Shaun Wylie and Leslie Yoxall, statistician Irving John "Jack" Good, International Chess Champion, Harry Golombek and cryptographer Rolf Noskwith worked alongside Turing around the clock in an attempt to break the German naval ciphers. However, despite their efforts, these men were unable to decrypt the messages at a regular and frequent pace. It would take the capture of Enigma key settings and other vital documents to finally break the ciphers at a pace which would make their content effective to the Royal Navy.

In the same month that Turing read the first cipher in April of 1940, cryptanalysts at Bletchley Park received their first captured materials from U-Boats.[48] It is arguable that these captures, known as "pinches" by the staff at Bletchley Park, made a greater contribution to the operational use of decrypted messages in the Battle of the Atlantic than the sluggish mathematical work of cryptanalysts. Both time and cryptanalytic efforts could be saved if the enemy code books could be captured. Therefore, boarding parties entering ships or U-Boats were often sent to the communication room to seize any documents they could find. Most of the men who risked their lives in the race against time in a sinking ship or U-Boat had never heard of an Enigma machine; they simply carried out orders to bring back anything that looked important. Often Enigma machines themselves were unable to be salvaged because they were bolted to tables, but any loose parts and paperwork was gathered. These captured documents and Enigma parts would prove priceless to cryptanalysts at Bletchley Park.

An early break or "pinch" had already occurred by February 1940. The crew of U-33 had been ordered to lay mines off of the coast of western Scotland. This was a dangerous mission, not only because the U-Boat was entering enemy waters miles from shore, but if the U-Boat were spotted in such shallow water, it could not dive to escape. Therefore, the possibility of capture was on the mind of the captain and crew.

This was a risk that Dönitz had taken before. Earlier in the war U-26 was sent on a similar mission in the waters south of England. After the mission, the U-Boat had failed to make contact with headquarters for several days. The submarine eventually made contact, but afterwards Dönitz ordered mine-laying U-Boats to leave their Enigma machines behind. Mine-laying U-Boats now were ordered to travel directly to the location of their missions, and upon completion, return to their bases. During the duration of the operation, the U-Boat would not be able to send or receive messages from other U-Boats or the base. Dönitz later wrote in his war diary: "The consequent disadvantages and difficulties which will be experienced when working together with other boats have to be accepted, as the risk of confidential books and cipher material falling into the enemy's hands, if the boat is lost in shallow water, is too great."[49] However, this strict protocol was not enforced with U-33. It is arguable that the rule was not enforced with this submarine because U-33 was not merely a mine-laying submarine,

[48] The practice of capturing enemy codebooks and secret documents had been used before by British cryptologists in World War I. In November of 1914, the German cruiser *Magdeburg* ran aground in Baltic waters patrolled by Russia. The Russians boarded the ship and retrieved code books, which they promptly relayed to the British Admiralty. These captured documents enabled Room 40, the British center for naval intelligence, to break German naval ciphers.

[49] Hugh Sebag-Montefiore, *Enigma: The Battle for the Code* (New York: John Wiley & Sons, Inc., 2000), 61.

but also was capable of traveling in vast ocean waters and possessed torpedoes. Regardless of Dönitz's reasoning, the U-33 departed with an Enigma machine aboard.

In the early hours of February 12, lookouts on the U-33 spotted what resembled a British destroyer heading directly for the U-Boat. However, the HMS *Gleaner* was not a destroyer; it was a survey ship fitted with the best anti-submarine technology the British possessed at the time. Hours later, the U-33, badly damaged by depth charges, was brought to the surface and the crew ordered to abandon ship. Before the crew abandoned the submarine, the captain ordered that the rotors of the Enigma machine, plus the extras that were not being used for the day, be given to crew members. These men were instructed to drop them into the sea as they jumped off of the submarine. Two of the men were able to do so. However, British sailors recovered three rotors from Friedrich Kumpf, who in the stress of the situation, forgot to throw his rotors into the sea. After the *Gleaner* picked up Kumpf, he told Heinz Rottmann, one of his surviving officers, that he had forgotten to throw the wheels away. When the two men checked Kumpf's pants, the pockets were empty and the Enigma rotors were gone. After Kumpf had removed his waterlogged clothes, British officers searched his pants before returning them to him. The officers, after discovering the rotors in his pockets, were unsure of their use, but made arrangements for the captured items to be sent back to Britain. Little did these German sailors know the precious find was soon on its way to the huts at Bletchley Park. After analysis, it was discovered that these rotors revealed the wiring of sixth and seventh wheels, which until then was unknown to those individuals working at Bletchley Park. While these rotors helped Hut 8 understand the Enigma machine, they did not lead to a complete solution to the naval Enigma. Without knowledge of cribs, the cryptologists could not break any Enigma messages, and without breaking Enigma messages, they could not identify any cribs.[50]

Stuck amid a catch-22, Turing and his team soon realized that they would need to capture Enigma documents so the work done at Bletchley Park could be completed in a timely fashion. However, in order to successfully capture documents from a U-Boat, the submarine had to be brought to the surface by depth charges. If the vessel sank too quickly, no documents could be recovered. Furthermore, in the midst of the chaos, British intelligence had to hope that key documents or codebooks were left behind. It was German protocol that all Enigma documents were to be destroyed or thrown overboard in the event of a capture. The men and women of Bletchley Park only hoped that the stress of the situation would prevent U-Boat crews from making this important task a priority.

On April 26, 1940, British destroyers spotted *Polares,* a trawler flying the Dutch flag. Days before, another British destroyer reported being fired upon by the same vessel. Suspecting this ship was a German vessel in disguise, the HMS *Griffin* sailed close enough to send a boarding party. The men of the *Griffin* not only found concealed gun decks on the ship, but also an unusually large crew for a regular fishing ship. Furthermore, a crewman was seen throwing canvas bags overboard. While one of the bags sank, the other was recovered by British sailors. It was later discovered that the captured bag contained cipher forms. Other cipher forms were found during a search of the ship, later identified as the German *Schiff 26.* These cipher forms contained not only ciphertext but also its matching plaintext. The documents were

[50] Kahn, 111.

immediately sent to Bletchley Park, allowing the cryptanalysts to break into the naval ciphers from April 22 to 27. The first of the messages to be broken was dated April 23; it was successfully broken, translated and read on May 11, making the first official break into the naval Enigma with the aid of a "pinch."[51] It was later determined that the delay in reading the message stemmed from the absence of plug board connections.[52] The settings for April 26 and 27 were broken after two weeks using the bomb and cribs discovered in previous decoded messages.[53]

While these messages held little military value because of the rate of their decryption, the documents that were captured from the *Polares* helped Turing to better understand the naval Enigma machine and the ciphers that it produced. Turing produced a new method, which he called Banburismus, since the sheets that were used in the process were manufactured in Banbury. Banburismus took advantage of a weakness of the German naval Enigma: messages indicating new settings were sent using old rotor settings from the day of the transmission. In the process, long printed sheets with vertically printed alphabets with the letters divided by horizontal lines were used to make calculations. Like the Zygalski Sheets, holes punched in the sheets corresponded with the enciphered text; one letter per column of text until the message was complete. After punching a certain number of sheets, they were placed over one another and examined to see where holes existed, which indicated where letters were repeated. This allowed for the message's sequence to be studied and eventually the day's settings to be determined. Peter Twinn noted: "You can either find out the wiring of a brand new wheel or you can work out with a reasonable degree of accuracy what the messages might be saying."[54] After the process was completed, British cryptanalysts could ignore as many as 336 possible rotor orders that might be used that day.[55] The positions that were left were then tested on a bomb, which eventually revealed the correct settings for the day.

## The Battle of the Atlantic: 1940

With the fall of France in May 1940, German forces seized ports on the English Channel, the coast of the Bay of Biscay, and Atlantic ports such as Lorient and St. Nazaire, which were soon put into service as U-Boat bases. From these ports, U-Boats could operate in Atlantic waters for longer periods of time, reaching as far as Newfoundland and America's east coast; German production of U-Boats would in turn increase with the ownership of these new ports. France's exit from the war also eliminated the French Navy from the Battle of the Atlantic. Finally, U-Boats would no longer have to make the seven-day voyage across the North Sea and around Great Britain to reach the war zone in the Atlantic. The time that U-Boats saved could be used to attack shipping in the area.

From the start of the war in 1939 to the fall of France in 1940, Germany's U-boat fleet had been unable to venture far into the Atlantic due to geographical constraints and Hitler's unwillingness to violate the territorial waters of still-neutral Belgium and the Netherlands. Furthermore, the fleet could not enter the Channel due to mine fields in the Dover Straits. Therefore, the only way to reach the Atlantic was to travel north around Scotland, and few U-Boats possessed the range to successfully complete

[51] Sebag-Montefiore, 76

[52] The settings for the plug board were recovered, but cryptanalysts overlooked these settings which were scribbled on a small sheet of scrap paper.

[53] Sebag-Montefiore, 76.

[54] Paterson, 105.

[55] Sebag-Montefiore, 77.

the journey. Of Dönitz's fleet, only eight submarines could travel over 12,000 miles; no more than eighteen boats could reach the Strait of Gibraltar, while thirty could not even leave the North Sea.[56] Despite these limitations, by the end of 1939, U-Boats, mines, and surface raiders had destroyed over 215 merchant ships equaling more than 748,000 tons.[57] Without knowledge of U-Boat positions or courses from decrypted enemy messages, British shipping blindly sailed into the paths of German submarines.

In June of 1940, U-Boats sank sixty-two ships totaling 284,000 tons – the highest monthly total to date. U-Boat crews called the period that followed the "happy time" due to their successes against British shipping. Operating from French bases, U-Boat commanders began to run high tallies of tonnage. Between July and October only two U-Boats were sunk, and young U-Boat commanders such as Jürgen Oesten alone sank 20,000 tons by August.[58] Dönitz later wrote: "I was anxious that not one single day should pass without the sinking somewhere or other of a ship by one of the boats at sea."[59] The staff at Dönitz's U-Boat Command would keep the day's log of British shipping activity, and if more than two days passed in an area without a convoy sighting, Dönitz ordered the U-Boats to move to another area of sea. By October, the average tonnage sunk per U-Boat per day was 920.[60]

On average there were only six U-Boats operating against British shipping routes at any given time. However, from May to December, eighteen separate U-Boat commanders were responsible for the sinking of nearly 300 ships totaling more than 1.6 million tons; a third of that total was sunk by only five U-Boat commanders.[61] Dönitz later wrote: "Out there in the Atlantic a handful of U-Boats was being called upon to fight a battle that would decide the issue of the war."[62] The losses of Allied shipping boosted the morale of the men aboard the submarines and led Hitler to invest more in the production of new boats. However, a larger and more formidable U-Boat fleet would not be ready until late 1941 due to Hitler's plans to invade the Soviet Union, and his decision to assist Italy in North Africa and Greece.

During the fall of 1940, cryptanalysts at Bletchley Park determined that key documents had to be captured in order to make frequent breaks into the naval Enigma. Therefore, British intelligence began to brainstorm other ways of capturing key Enigma settings. Ian Fleming, who worked at the Admiralty as an officer in Naval Intelligence, spent his time planning operations to steal code books. One of his more famous plans was Operation Ruthless, which involved obtaining a German bomber with a crew, including a telegraph operator and word-perfect German speaker. The crew would be dressed in damaged German Air Force uniforms complete with bandages and liquid that resembled blood. The plane would then be crashed into the English Channel after sending out an S.O.S. message. When a German rescue boat found the plane, the British crew would shoot the crew of the vessels, commandeer the boat, and seize key documents.[63] As the plan developed, more realistic details were added such as a mock attack on the bomber by British Spitfires. Although Churchill himself approved the operation, the circumstances for the plot never presented themselves, and

[56] Keegan, 110.
[57] Pitt, 8.
[58] Williams, 79.
[59] *Ibid.*, 103.
[60] *Ibid.*
[61] *Ibid.*
[62] *Ibid.*
[63] Kahn, 124.

Operation Ruthless was eventually cancelled.[64]

Despite the abandonment of Operational Ruthless, Turing's Banburismus would prove extremely useful to cryptanalysts in the upcoming months. However, the key to the Banburismus was the naval bigram tables. Though the *Polares* capture did not give Turing a copy of the tables, he was able to mathematically reconstruct them. After messages were decrypted, the gaps in the bigram table could be determined. In November of 1940, the Banburismus procedure broke into the naval settings for the first time by breaking the ciphers for April 14, May 8, and June 26.[65] However, to the dismay of the cryptanalysts, the messages on June 26 revealed that new bigram tables would be issued on July 1. Therefore, Banburismus could not be used on future messages until the new bigram tables were captured. Future messages could only be broken with the capture of new codebooks or the discovery of a regular source of cribs. Even though Bletchley Park's cryptanalysts were in the same position as they had been before the captures from the *Polares,* Turing and his team now knew that the naval Enigma could be broken.

In 1940 alone, U-Boats, which now had the capability to travel farther and longer, sank 375 ships totaling 1,804,494 tons.[66] Winston Churchill confessed that he had feared in the winter of 1940-41 that "the U-Boat peril" might "reach the point where our life could be destroyed."[67] Before the war, Great Britain imported 60 million tons of food and raw materials each year. By the end of 1940, the country was only importing 45.5 million tons, and in the following year the number would drop to 30.5.[68] The successful U-Boat campaign coupled with German air raids on British cities, were taking a toll on the morale of British citizens. Food imports dropped from prewar levels of 22 million tons to under 12 million, which was regarded as the minimum requirement for British survival.[69]

By the end of the year, Britain had begun to look to the United States for their long term shipping needs. In December, Winston Churchill wrote to Franklin Roosevelt, informing the President that "the gift, loan or supply of a large number of American vessels of war, above all destroyers already in the Atlantic, is indispensable to the maintenance of the Atlantic route."[70] On December 29, Roosevelt told the nation that "If Great Britain goes down, the Axis powers will control the Continents of Europe, Asia, Africa, Australia, and the high seas. And they will be in a position to bring enormous military and naval resources against this hemisphere. It is no exaggeration to say that all of us in all the Americas would be living at the point of a gun."[71] In February of 1941, the U.S. Congress enacted Franklin D. Roosevelt's program of Lend-Lease, which allowed Britain to borrow materials for war with the promise of repayment after their victory. With a neutral country now openly assisting the British cause, U-Boats now had to contend with American ships clearly loaded with goods on their way to Great Britain.

For the American and British ships traveling in the Atlantic, convoys only offered partial protection from wolf packs.

[64] Despite the cancellation of Operation Ruthless, Flemming did manage to earn fame by later penning the James Bond novels.

[65] Sebag-Montefiore, 77.

[66] White, 22.

[67] Williams, 105.

[68] *Ibid*., 106.

[69] White, 72.

[70] Franklin D. Roosevelt Presidential Library and Museum, "FDR Letter Regarding British and American Efforts for the War 12/7/40," http://www.fdrlibrary.marist.edu/website_online_version/psf/box34/a311s02.html (accessed February 6, 2009).

[71] Williams, 108-09.

Only two or three destroyers could be spared to escort each convoy, and these vessels would be overwhelmed when attacked by multiple U-Boats. Furthermore, early forms as ASDIC were ineffective beyond 1,000 yards and revealed range, but not depth, which was key when releasing depth charges. With the French ports of Brest, Saint-Nazaire, La Rochelle and Lorient in German hands after June, the fleet could operate in the Eastern Atlantic near western Africa, and occasionally venture into the Mediterranean. With the capture of the Bay of Biscay, U-Boats could attack shipping routes from South America, South Africa, and the United States. These ports allowed U-Boats to directly attack British shipping routes. Even though cryptanalysts at Bletchley Park were beginning to read few German transmissions in late 1940, the men of Huts 4 and 8 were not able to break the codes quickly enough to make their information operational. Therefore, U-Boats succeeded in sinking thousands of tons of British shipping that year. Cryptanalysts at Bletchley Park needed to acquire new documents in order to gain the upper hand in the battle.

## British “Pinches” in 1941

While the winter of 1940-41 brought powerful storms in the Atlantic, it provided British shipping with some relief from German submarines. However, soon after the start of the New Year, the assault on British shipping resumed with a new vigor. Out of a total of forty-six operational boats in a commissioned fleet of eighty-nine, only seven U-Boats were sunk between December 1940 and March 1941.[72] U-Boat production was now finally higher than U-Boat losses. Great Britain was slowly beginning to realize how deadly Dönitz’s U-Boat arm could be. Winston Churchill on March 6 announced at a weekly meeting of the Battle of the Atlantic Committee: “We must take the offensive against the U-Boat and the Focke-Wulf [German long range bomber] … the U-Boat at sea must be hunted, the U-Boat in the dock must be bombed.”[73] Churchill understood the danger of U-Boats and ordered the submarine’s destruction. It was now a race against time to stop the thousands of tons of British shipping that were being destroyed each day.

In the early months of 1941, Britain was losing ships three times faster than shipyards could produce them.[74] The odds were clearly swinging towards Germany. Out in the Atlantic, U-Boat aces such as Günther Prien, the commander of U-47, had sunk over 245,000 tons by March 1941.[75] Furthermore, U-Boat production had been raised from an average of three a month to fifteen and was scheduled to rise to twenty in the coming months.[76] While only about a third of the U-Boat fleet was available for Dönitz’s current operations in the Atlantic, another third was involved in training programs which produced skilled officers and men for the anticipated fleet. The final third of the fleet drilled future operations and practiced mine laying techniques in the Baltic. Therefore, the total number of U-Boats in the Atlantic at any given time rarely exceeded thirty. Of those thirty, several were on their way to operations or returning back to port; others were on patrol in the South Atlantic and off the coast of Africa, causing British merchant ships and convoys to use the North Atlantic. Despite these figures, submarines were sinking an incredible amount of British shipping.

[72] Westwood, 117.

[73] Williams, 114.

[74] White, 26.

[75] Brown, 76.

[76] Padfield, 149.

However, in March of 1941, cryptanalysts at Bletchley Park gained the break they had been searching for. On March 4, British destroyers off the coast of Norway identified the German trawler *Krebs*. After opening fire on the ship, the engine room was soon hit, and the ship was abandoned. A group of men from the HMS *Somali* boarded the ship to find that the few crew members left aboard had surrendered. When searching the ship, Lieutenant Sir Marshall Warmington entered the captain's quarters and ordered the boarding party to collect the documents strewn around. Before leaving, Warmington noticed a locked drawer. After shooting off the lock, he pocketed the discs he found inside; without knowing anything about an Enigma machine, Warmington and his men had managed to capture key documents such as German naval grids, a set of spare rotors, and Enigma key tables for February.

Although the Enigma machine itself had been thrown overboard, the Enigma key tables and naval grids were a key find for cryptanalysts at Bletchley Park. The German navy employed a special grid map to encode positions of their U-Boats. A section of ocean was grouped into zones, and each zone was divided into squares that were assigned a two digit number. Then those squares were further broken down and given a number one through nine. Finally each square in the one through nine grid was broken down and numbered one through nine. Therefore, a U-Boat could be located in zone AK in square 8226. With the captured naval grids, the British were able to accurately locate U-Boats. Within five weeks, cryptanalysts at Bletchley Park were using the captured documents to read past naval traffic from February and later some of the traffic from April and most of May.

The men in Huts 4 and 8 knew that the Germans were monitoring the weather in the North Atlantic using trawlers that sailed from Iceland. While they did not report their readings on Enigma machines, they did use the machines to receive messages from base, and, therefore, had the current code books aboard their ships. While the navy had already sunk two of these weather trawlers, Bletchley Park's Harry Hinsley suggested that these ships might carry naval Enigma keys because they stayed at sea for months at a time. In a formal report to the Admiralty, Hinsley stated: "The seizure of one of these ships, if practicable would … offer an opportunity for obtaining ciphers."[77] Cryptanalysts knew that if those weather ships could be boarded, vital code books could be captured that might help cryptanalysts break the naval codes. Therefore, plans were soon made to intercept vulnerable German weather ships in hopes of capturing more documents. The target that British intelligence chose was the *München*, which was to be at sea through May and June. If an armed naval party could board the ship quickly, it was unlikely that the Germans would be able to destroy all of the secret Enigma materials. Even if the code books were thrown overboard, the codes were changed every month, so it was expected that only the codes for May would be thrown overboard. Then the boarding party could search for the hidden book of June codes. On May 7, the *Edinburgh* located the trawler and fired on it, causing the crew to board the lifeboats, while the crew of the destroyer *Somali* boarded the ship. The *Edinburgh* later sent its own boarding party. Colin Kitching of the HSM *Edinbugh* recalled the capture: "The *München*'s captain had thrown the Enigma machine and the May coding tables over the side as *Somali* approached, but the settings for June were in his desk; these were collected by Captain Haines [of Naval Intelligence], who knew exactly what he

[77] Sebag-Montefiore, 128.

was looking for."[78] Haines was later flown to London with the captured documents and reached Bletchley Park by May 10. These captured documents allowed Bletchley Park's cryptanalysts to read German signals with little delay for about six weeks until the keys were routinely changed. In order to keep the capture secret, the British reported: "One of our patrols operating in northern waters encountered the *München*, a German armed trawler. Fire was opened and the crew of the *München* then abandoned and scuttled the ship. They were subsequently rescued and made prisoner."[79] German intelligence, which at the time was reading British communications, knew nothing of the captured documents.

Yet another "pinch" came just two days after documents were captured from the *München,* and resulted from Dönitz's westward deployment of U-Boats. On May 9, 1941, British destroyers *Aubretia, Broadway* and *Bulldog* were escorting the outward bound convoy OB318 south of Iceland. The U-110, which was also patrolling the area, had sunk seven merchant ships totaling over 39,000 tons in the last four days.[80] Aboard the U-Boat, Second Lieutenant Ulrich Wehrhöfer was in charge of changing the Enigma settings every night at midnight. Though Wehrhöfer would retrieve the documents from the safe, he often left the task to the crew telegraphists on duty. Ignoring protocol, Wehrhöfer did not supervise the change of the important codes. The radio operator for U-110, Heinz Wilde, recalled: "We were told that the chances of breaking in [to the Enigma codes] were one to one trillion. Today you would say that breaking in was as likely as winning the jackpot in the lottery. But the jackpot exists."[81] The lax attitude toward security would soon prove fatal for the submarine.

After U-110 fired on the convoy, it was detected by underwater direction finding radar. Depth charges from the corvette *Aubretia* and two destroyers, *Broadway* and *Bulldog,* eventually brought U-110 to the surface. Upon reaching the surface, the U-Boat commander, Fritz-Julius Lemp, noting that he was surrounded by British warships, gave the order to abandon ship. It was Lemp's responsibility that his vessel and its important documents such as cipher material would not be captured by the enemy. Cipher material was to either go down with the submarine or be tossed over the side in a weighted bag. Radioman Georg Högel recalled the scene: "Lemp was standing over the hatch, looking down into the control room. My comrade, who was the radio officer, and I were shouting upwards: 'What's to be done with the secret items?' He shouted to us: 'Leave everything. Leave everything. Get out, get out, get out.'"[82] Lemp also told Wilde to leave the Enigma and documents for the ship was sinking. However, instead of sinking, U-110 continued to float.

Instead of finishing the job and destroying the vessel, the captain of the HMS *Bulldog,* Joe Baker-Cresswell, decided to send a boarding party to the U-110. Lieutenant Balme, a gunnery control officer, led the party, and spent around six hours aboard the U-Boat. Balme noted: "The U-Boat had obviously been abandoned in great haste as books and gear were strewn about the place… Meanwhile the telegraphist went to the W/T office… This was in perfect condition, apparently no attempt having been made to destroy books or apparatus… The coding machine was found here,

[78] Paterson, 116.

[79] Harper, 23.

[80] David Brown, *Atlantic Escorts: Ships, Weapons, and Tactics in World War II.* (Annapolis: Naval Institute Press, 2007), 68-69.

[81] Williams, 130.

[82] *Ibid*., 133.

plugged in as though it was in actual use when abandoned."[83] The documents retrieved from U-110 were some of the best kept secrets of the war. The German prisoners had no idea that their U-Boat had been boarded and were confident that it had sunk before anyone could reach it. Furthermore, Dönitz and German code experts never knew the British had managed to capture a working Enigma machine with all of its parts. CJ Fairrie of the HMS *Bulldog* noted: "Charts, codes, names of spies, U-Boat bases, knowledge of movements of our convoy–an enormous coup–turning point in the Battle of the Atlantic! Materials seized from the U-Boat [were] passed up from hand to hand. Among them was a wooden box that looked like a typewriter. At no time were we aware that a German Enigma machine had been captured."[84] Along with the Enigma machine, a stack of code books was retrieved that detailed the keys to reading the U-Boat's short signals and weather reports for April and June. The tables for May were most likely destroyed accidently in transport to the *Bulldog* upon the water soluble ink's contact with water.[85] Also, a set of bigram tables was recovered and, most importantly, the "Offizier" short signal code settings for June. Sensitive material was encoded with the "Offizier" settings and then enciphered again with the regular settings.

Extremely beneficial to British intelligence, the finds would prove priceless. Hut 8 received the captured documents by May 13. Combined with the documents from the *München*, the material gained from U-110 allowed code breakers at Bletchley Park to read U-Boat messages eleven days after they were sent.[86] Furthermore, when the settings for June became operational, cryptanalysts were reading messages six hours after they were received.[87] More importantly, changes to the naval Enigma were communicated through the "Offizier" codes among other messages of the highest security. British cryptanalysts now had the ability to read the same messages as the German High Command. Furthermore, Balme and his boarding party also manage to collect radio logbooks, charts indicating the positions of German minefields (which would prove valuable for coastal raids), and charts detailing the fixed positions of U-Boats in the Atlantic and those U-Boats that were designated to refuel them. Fifteen of these refueling subs would be sunk in the following weeks. With the capture of the documents aboard the U-110, British code breakers were reading messages in June almost as fast as the Germans, even when the monthly tables changed. From these messages, the men in Huts 4 and 8 gained knowledge of U-Boat tactics, patrol routes, operational routines, supply arrangements, and plans for attacks. The information deciphered from Bletchley Park was sent to the Admiralty's Submarine Tracking Room and could be used to reroute convoys away from wolf packs. Soon convoy routes would be checked with the intelligence gained from Ultra decrypts.

While Ultra decrypts offered insight in to the enemy's operations and plans, the Submarine Tracking Room could also gain information from Intercept Stations located along the shore line. The enemy signals gained from these stations were sent directly to Bletchley Park. Analysis from signal intelligence gained from direction finding – strength of the signal, length, time and number–also provided the British Navy with a part of the overall puzzle. By June, cryptanalysts were reading German messages in "real time." A message intercepted at 12:18

[83] Peter Padfield, *War Beneath the Sea: Submarine Conflict During World War II (*New York: John Wiley & Sons, Inc., 1995), 128.

[84] Paterson, 118.

[85] Padfield, 129.

[86] Harper, 25.

[87] Sebag-Montefiore, 144.

a.m. on June 1 was deciphered in Hut 8, translated in Hut 4, and dispatched to the Operational Intelligence Centre by 4:58 a.m.[88] Furthermore, HYDRA, the code used for German ships in the North Sea and Baltic, minesweepers patrolling the Norwegian coast, and all U-Boats was being read at a similar pace.

These breakthroughs came at a desperate time for Great Britain, for in Spring of 1941, the total number of shipping losses from all causes, including U-Boats, aircrafts, mines, and surface raiders averaged over half a million tons a month. In May alone, U-Boats alone managed to sink 324,550 tons British shipping.[89] Extrapolating those numbers, the British Admiralty expected further losses of 4 to 5 million tons in the fall. To make matters worse, British shipyards did not have the capacity to produce more than a million tons a year. And although the United States was offering some assistance, it would take the Americans around eighteen months to create a mass production program that would be effective against the Germans. Planners estimated that by the end of the year, Great Britain would face deficits of 7 million tons of raw materials, including 2 million tons of food and over 300,000 tons of oil. [90] Unless the number of sinkings could be reduced, the Germans might win the war.

By the summer, however, the situation was far from hopeless. With the use of early high frequency direction finding and timely Ultra intercepts, the location and movements of German wolf-packs could be pinpointed. In order to monitor the activity of wolf packs, the German control system depended on the use of a high frequency radio. While the Germans were aware that simple direction finding could reveal the positions of the submarines, the machinery that was needed to carry out direction finding was too large to be fitted onto a ship. Furthermore, the distance of the ocean would create inaccurate readings. However, with the use of high frequency direction finder, an operator could fix the bearing of a signal sent out by a U-Boat. If two operators could pick up the signal, an intersecting point could be determined.

The revealed location of U-Boats and their refueling vessels in an area often led to their destruction. In June of 1941, U-557 was running low on fuel and ordered to meet the *Belchen,* a German tanker, near the southern tip of Greenland to refuel. U-557 did refuel and continued on with U-109 and U-93 southward. Later, the U-Boats were to learn that the *Belchen* was sunk by British ships. Unbeknownst to the U-Boat commanders, the destruction of the *Belchen* and her supply network was the result of the finds from U-110. Surface vessels were also intercepted by British ships with the aid of deciphered Enigma messages; the *Lützow,* for example, suffered damage that would keep her in port for months.

During the weeks that followed, Dönitz ordered the area that the *Lützow* patrolled to be searched for convoys, but nothing was reported. Earlier in April, a possible leak in security occurred to the U-Boat command when the British began to change the course of convoys. However, Dönitz was certain that convoys were successfully passing by U-Boat wolf packs with the aid of superior long range radar. He still believed the Enigma was impossible to break. While the captures from the *München* and U-110 proved useful, they were not a permanent solution to the naval Enigma. In late June 1941 the German navy began to use a new set of bigram tables. Therefore, Bletchley Park's cryptanalysts would need another two to three months of naval Enigma settings in order to continue

[88] Harper, 25.
[89] White, 289.
[90] Padfield, 150.

breaking the enciphered messages after June. In light of the success from "pinches," Hinsley urged British destroyers to board the *Lauenburg,* another German weather ship. Sailing from Trondheim, a Norwegian port, three British destroyers finally spotted the ship on June 28. However, radio operators in the *Lauenburg* heard the British radio messages and the crew was ordered to evacuate. The radio operator and cipher clerk managed to throw the Enigma machine overboard and the cipher documents into a furnace. When the ship was boarded, it appeared that nothing could be recovered. However, the order was given to collect every document, charred or not. After filling thirteen mail sacks, it was determined that the Enigma keys for July were still readable, as well as plug board settings for the month and internal settings. When the documents reached Bletchley Park on July 2, Huts 4 and 8 were able to be successfully read German naval messages within three hours of their transmission for the rest of the month.[91] Often after the capture of documents, the Admiralty would wait to see if the German High Command would be alerted to the capture and question whether the British had indeed captured enemy code books. However, every time, the Germans remained silent. While talk of a security breach was whispered throughout the lower command, Dönitz refused to alter the security of either his naval Enigma or the procedures for encipherment.

The speed of decryption slowed in August because of failed attempts at capturing more "pinches" in the English Channel, but the documents Balme and his men retrieved allowed cryptanalysts to decipher most of the messages for the rest of the year. Ultimately, U-110 has been regarded as one of the most valuable captures of the war. "Pinches" led to the sinking of tankers, supply ships, surface raiders, and long distance U-Boats on patrol in the South Atlantic.[92] The information about the U-Boats themselves gained from captured documents helped the British navy's chances of destroying them. Upon the capture of U-570 in August, the vessel was towed to Iceland, where it was discovered that this new model of U-Boat could reach depths of over 600 feet. Depth charge settings were then adjusted accordingly.

Once Bletchley Park's cryptanalysts broke the naval code, the impact on the tonnage sunk by the Germans was noticeable. With a 320,000 tons loss in June, the number quickly dwindled to 98,000 tons in July, and 84,000 tons in August.[93] Sinkings of Allied merchant ships also dropped abruptly. In June, sixty-eight ships had been sunk, but only twenty-five ships were sunk in August and only ten in November.[94] Unbeknownst to Dönitz, the British were successfully breaking the naval Enigma codes. By reading the messages between headquarters and the submarines, the Admiralty in London could determine the position of every U-Boat and their patrol lines and could reroute convoys around wolf packs. At the same time, Ultra decrypts alerted the Admiralty to the position of German surface raiders. For example, in November of 1941, the German raider *Atlantis,* while on her way back to Europe, was ordered to refuel U-Boats in the South Atlantic. Through Ultra intercepts, British intelligence was alerted to the ship's change in course and could identify her new location. On November 22, a seaplane accompanying the British cruiser *Devonshire* identified the *Atlantis,* which was disguised as a Dutch ship. While the U-Boat dived, the *Devonshire* opened fire on the German raider, eventually sinking her. The

[91] Harper, 28.

[92] Padfield, 129.

[93] White, 128.

[94] *Ibid*., 121.

crew of the *Atlantis* radioed for help, and the radio signals were intercepted and deciphered to reveal the location of the rescue and U-Boat supply ship. Days later the ship, *Python,* would also be sunk by the *Devonshire*'s sister ship, HMS *Dorsetshire,* while attempting to refuel U-Boats on her way to the wreck of the *Atlantis.*

By this time, convoys were also beginning to employ additional escort ships. More escort ships were being produced and their crews were better trained in anti-submarine warfare. Furthermore, with more protection, the minimum speed for a convoy rose from thirteen to fifteen knots because the Admiralty realized that slower ships were at much greater risk to U-Boats than faster traveling vessels.[95]

In addition to Ultra decryptions and the improved speeds and protection of convoys, Dönitz did not possess proper aircraft to locate Allied convoys; he relied only on his U-Boats on distant patrols to identify convoys. The lack of aerial reconnaissance for the German navy was at a serious level; it was vital to search the sea. After stating his case for aircraft, Dönitz only received one group of the Luftwaffe, and of the pilots he was given, many could not navigate well over the sea. Furthermore, the pilots often gave Dönitz incorrect coordinates for convoys. Therefore, the attacks by German airplanes on Allied convoys were few.

By November 1941, Dönitz was becoming frustrated with the continuing failure of his U-Boats. In his war diary, Dönitz later wrote: "coincidence always seems to favor the enemy."[96] Moreover, he noted in his diary on November 19 that individual U-boats were finding convoys, but the carefully formed U-Boat patrol lines were finding it impossible to locate a convoy unless there had been a previous sighting by a U-Boat. "Chance alone it cannot be–chance does not always fall on one side, and experience extends over almost ¾ of the year. A likely explanation would be that the English, from some source or other, obtain knowledge of our concentrated dispositions and avoid them, thereby running into boats proceeding singly."[97] Dönitz had already eliminated the possibility of treason because of its heavy penalty and continued to ignore the idea that the British had broken the Enigma; to Dönitz the task was mathematically impossible. Dönitz believed that the British were using high level radar or locating U-Boats by aircraft. Even if the British had managed to capture Enigma documents, so many safeguards were built into the process that decryption would be impossible. For example, even if the British had the rotor settings that were changed each month, they would also need indicator lists and bigram tables, which also were changed often. Dönitz believed it was impossible for the British to gain all items, along with an Enigma machine with its eight working rotors, let alone continue to capture the key documents every month as the settings were altered. Ultimately, Dönitz and the Naval Staff failed to realize the lengths that the British were going to and the scale and speed of the operation to break the naval Enigma. The German system was infallible in the eyes of the high command.

It is questionable whether the U-Boat and Luftwaffe attacks on British shipping and ports could have eliminated her from the war without the regular decryption of Ultra. The statistical projection of losses and the increase of operational U-Boats suggested that this might be the case. British wartime intelligence noted: "It was only by the narrowest of margins that … the U-Boat campaign failed to be decisive during

[95] Brown, 68.

[96] Williams, 157.

[97] Padfield, 166.

1941."[98] However, this idea does not take into account the improved methods of defense such as improved anti-submarine warfare methods, particularly the use of long-range aircraft. With Hitler moving towards Russia, the majority of the Luftwaffe operations moved east; therefore, the number of shipping losses from aerial attack dropped. Furthermore, the number of U-Boat losses dropped due to the rerouting of convoys from information gained from Ultra, higher speeds of vessels, and the great number of U-Boats that were transported to the Baltic and Arctic to aid in the campaign in the east.

U-Boat historian Dr. Jürgen Rohwer considers this time to be a turning point and gives credit to Ultra as one of the factors that determined the outcome of the battle of the Atlantic. Clay Blair, an American historian, estimated that of the 3700 merchant ships that traveled in the Atlantic in 1941, only fifty-four were lost to U-Boats. Harry Hinsley estimated that during the second half of 1941 deciphered Enigma codes saved 1.5 to 2 million tons of shipping,[99] and about 350 vessels were saved from U-Boat torpedoes.[100] While Dönitz further blamed his losses on the transfer of submarines to the Mediterranean and Arctic, the real decline in numbers was thanks to the British use of Ultra and advances in anti-submarine warfare. However, despite these statistics, by the end of the first two years and four months of the war German U-Boats had managed to sink 1124 ships – 5.3 million tons of British and neutral shipping.[101] With the entrance of a new ally into the war, Great Britain could only hope that the coming months would bring better news.

## Shark Blackout of 1942

By the start of 1942, new U-Boats were being produced at a rate of twenty a month.[102] At the same time, the number U-Boat veterans was dwindling as many died in battle at sea, were captured and sent to POW camps, promoted to positions on Dönitz's staff, or given flotilla commands. The majority of the newer U-Boat crews consisted of young, ambitious men eager for battle at sea. Often service on a U-Boat would lead to the promise of early command elsewhere in the navy. Now, with the entry of the United States into the war, more U-Boats were needed to attack American shipping. U-Boat High Command saw American involvement as a short term advantage, but a long term danger. The United States would have to assemble convoys for its east coast shipping, which could provide prime targets for the newly produced U-Boats and their young crews. However, it was only a matter of time before American industry reached its peak and the number of new merchant ships and escorts would outnumber those sunk.

At the same time, the success of cryptanalysts at Bletchley Park from the gains of "pinches" would be short lived. On February 1, 1942, all U-Boat cipher operators were instructed to abandon HYRDA in order to tighten security. The Germans introduced a new model of the Enigma, the Triton M4, which had the capability to hold four rotors at one time instead of three. The codes produced by the new machine, code named SHARK, were unreadable when subjected to past methods of deciphering. Turing calculated that in order to break the new codes at the same rate as the old ones, cryptanalysts would need bombs that were twenty-six times as fast as the ones they were currently using.[103]

[98] *Ibid*., 153.
[99] Brown, 75.
[100] Paterson, 127.
[101] Williams, 160.
[102] Stern, 116.
[103] *Ibid*.

While the men and women at Bletchley Park were in the dark thanks to the new naval Enigma codes, high frequency direction finding could still track some U-Boats so that their future positions could be assumed by their movements. However, with Dönitz launching more U-Boats than ever before from a fleet of over 270, cryptanalysts needed once again to read German intercepts in order to keep submarines from sinking thousands of tons of shipping.[104] At this time, the four-rotor Enigma machine was used for U-Boats operating in the Atlantic and Mediterranean. Therefore, it was possible that a U-Boat operator who enciphered a message in the four-rotor Enigma transmitted the message to another U-Boat which only possessed a three-rotor machine before realizing the error. Therefore, the message had to be transmitted again with the key for the three rotor Enigma. Using these two intercepts, cryptanalysts were able to determine that a fourth rotor was added to the naval Enigma machine. However, the wiring of this fourth rotor had been unknown. Moreover, with the addition of the fourth rotor, the number of possible solutions increased by a factor of twenty-six and successful "cribs" were slim to none. Now bombs would take twenty-six times longer to run the possible keys for a machine that used four rotors through a three-rotor bomb. This use of the bombs took valuable time away from the efforts to break the codes of the Army and Luftwaffe. However, new bombs were quickly made that were able to perform twenty-six times as many tests on keys in only twice the time. The first four-rotor bomb was installed in June 1943.

As early as February 1942, Dönitz began moving his U-Boats into the Gulf of Mexico and the Caribbean Sea. U-Boats crept close to America's east coast in Operation Drumbeat, or *Paukenschlag*. That month 154 ships were destroyed by U-Boats and German surface raiders–a total of 680,000 tons.[105] Most of the tonnage was lost in the western Atlantic; however, those ships on their way to Great Britain from the United States were often sunk off of the American coast, not as they convoyed across the Atlantic. [106] June of 1942 saw an all time high for the U-Boats in terms of tonnage. German submarines had managed to sink 124 ships totaling 623,545 tons in the Atlantic, Mediterranean, and Arctic.[107] A large proportion of the ships sunk were tankers that contained needed oil for the Allies. With an end-of-the-year shortfall of 2 million tons, compared to the amount of oil needed to continue the war in European and Pacific theaters, domestic oil was rationed until tankers could successfully reach their destination.

With the cryptologists still in dark at Bletchley Park for the majority of the year, losses and the number of operational U-Boats would only continue to rise. U-Boat situation reports from the week of February 23 noted: "In the absence of Special Intelligence [Ultra decrypts] an accurate estimate of the number or disposition of U-Boats operating in the Atlantic is not possible."[108] However, it can be argued that the British were fortunate that Dönitz tightened security on the Enigma by adding a fourth rotor at the same time during what is known as the U-Boat's second "Happy Time." Dönitz would still concentrate his U-Boat forces against Atlantic convoys, and if Allied convoys were unable to avoid wolf

[104] White, 298.

[105] Williams, 174.

[106] *Ibid*.

[107] Samuel Eliot Morison, *The Atlantic Battle Won: May 1943-May 1945* (Boston: Little, Brown and Company, 1956), 8.

[108] David Syrett, ed. *The Battle of the Atlantic and Signals Intelligence: U-Boat Situations and Trends, 1941,1945* (Aldershot:Ashgate,1998),13.

packs as before, Dönitz could have come to the conclusion that the British had been intercepting and successfully reading the earlier radio signals. The secret of Ultra was still safe because independent ships were still being sunk by single U-Boats. Thus, the success of the "Happy Time" that occurred near US waters may have preserved the secrecy surrounding Ultra.

With only three U-Boats sunk from January to May 1942,[109] Allied naval commanders realized that normal navy training was not enough to destroy the submarines. Seamen needed to be proficient in not only naval tactics but also sonar, radar, depth-charging, and air bombing. New recruits and the best navy men were given refresher training in hopes of tipping the scales in the U-Boat war. However, despite this new training, the Germans were still producing U-Boats faster than Allied forces could sink them. By July, Dönitz finally possessed more than his target number of 300 U-Boats and deployed most of them in the central Atlantic, where the Allied escort force was the weakest because most British ships in the area had been transferred to Eastern Sea Convoys.

In August, U-Boat production rose to twenty-one a month; the fleet itself had a strength of 342 submarines. However, fifty-nine were being used for training, while 131 were on mission in the Baltic or on test trials. Of the 152 remaining operational U-Boats, Hitler had ordered that twenty-three be placed in the waters around Norway in case of an invasion and sixteen were ordered to the Mediterranean for the Italians to aid in the interdiction of Allied supplies to North Africa.[110] While, Allied forces managed to sink thirty-two submarines in the last six months of 1942, the Germans managed to complete 121 new U-Boats in that same time period. [111] Convoy losses continued at a rate of 26 ships of 155,000 tons each month until the end of the year.[112] Losses for the entire year included 1,006 ships totaling 5,471,222 tons; the worst figures for the Allies to date. In addition, Britain had over 2.5 million tons of work in repairing damaged ships.[113] Yet, the staggering losses were not enough. Dönitz had calculated that his U-Boats needed to sink 700,000 tons per month to cripple the convoy chain; the British Admiralty had predicted 600,000 tons per month. Throughout 1942, the Germans averaged sinkings of 456,000 a month, with five months exceeding 500,000 tons.[114]

In late October, a "pinch" would once again aid the men of Huts 4 and 8. On operation in the eastern Mediterranean, the British destroyer HMS *Petard* on October 30, 1942, detected a submarine in the vicinity. Depth charges soon forced U-559 to the surface off of the coast of Port Said. With her crew already abandoning ship, three men from the *Petard* decided to board the submarine. Lieutenant Anthony Fasson, AB Colin Grazier, and NAAFI assistant Tommy Brown managed to recover books and documents from the abandoned U-Boat. However, Fasson and Grazier lost their lives when a rush of water entered the sinking submarine. Brown still managed to recover a short signal codebook and the 1942 short weather cipher from the U-Boat. The short weather signals were still transmitted with the three-rotor Enigma machine, but cryptologists cracked the ciphers within six weeks of receiving the material from U-559, making it easier to figure out the setting for the fourth rotor. After ten months in the dark on naval traffic, by December 13, six weeks after the capture of the material from U-559,

[109] White, 291.
[110] Padfield, 274.
[111] White, 291-92.
[112] Morison, 9.
[113] White, 177.
[114] *Ibid.*, 177-78.

cryptanalysts at Bletchley Park were once again reading the naval Enigma. And by January, cryptologists were deciphering messages quickly enough to be used operationally.

This capture of key Enigma documents ended the lack of intelligence about U-Boat movement and operations that had spanned more than 10 months. During that period, U-Boats had been sinking Allied merchant ships twice as quickly as new ships were being built. These sinkings threatened to reduce British rations to even lower numbers than the year's current figures and disrupt the flow of materials, weapons, and troops for an invasion of German occupied territory.[115] Once again, British intelligence, which was aware of the communication between U-Boats and Karl Dönitz, could reroute convoys away from dangerous U-Boat packs. Furthermore, with the location of U-Boats revealed, so many submarines were successfully sunk that U-Boats were ordered to leave the North Atlantic for safer areas. Ralph Erskine, a naval signal intelligence authority noted: "From December 1942 to June 1942, these [captured code books] were the only means by which Bletchley Park could find 'cribs' with which to break SHARK.... This helped turn the course of the war, and played a major part in winning the war. Few acts of courage by three individuals can ever had such far reaching consequences."[116]

By winter, German production of U-Boats had reached an all time high. Twenty-four new U-boats were now being launched each month, and with a fleet of 416 – 110 at sea at any time and fifty permanently in the Atlantic–Dönitz believed he had finally met the quota he desired. During this time *Funkbeobachtungsdienst*, or *B-Dienst*, Germany's code breaking agency, was breaking British messages, which allowed Dönitz to find and destroy many more ships in convoys. On the other hand, America was by now sending Liberty Ships across the ocean at staggering rates. In 1941, 794,000 tons of shipping was built in American shipyards.[117] Great Britain could only hope that these Liberty Ships could be produced faster than Germany could sink them, thus tipping the scales in favor of the Allies.

After December 1942, cryptanalysts at Bletchley Park read U-Boat messages every day except for the occasional failure to find the day's entry code. British cryptanalysts were often able to read enciphered German codes within hours of their transmission, which gave naval commanders vital information as to the location of German submarines. With renewed access to the U-Boats' radio messages, the British Admiralty could once again reroute convoys around U-Boat wolf packs. From July 1942 to May 1943, Allied forces rerouted 105 of the 174 North Atlantic convoys, placing them completely out of danger. Furthermore, attacks on fifty-three convoys were minimized, leaving only sixteen that sailed directly into German wolf packs and, therefore, endured multiple sinkings.[118] Ultimately the success of Allied rerouting depended on the accomplishments and skills of cryptanalysts at Bletchley Park.

[115] Harper, 8.

[116] *Ibid*., 8-9.

[117] Twenty-one million tons of American shipping would be assembled over the course of the next three years. Richard Overy, *Why the Allies Won* (New York: W.W. Norton & Company, 1995), 62.

[118] Keegan, 111.

## Allied Victory in the Battle of the Atlantic: 1943-1945

In early 1943, after Dönitz replaced Grand Admiral Raeder as the Commander-in-Chief of the German navy, it was clear that Britain could not be forced to surrender by means of starvation, so the chief objective of the U-Boats became to prevent the United States from deploying its full strength in Europe. American troop buildup could be restricted by targeting convoys in the North Atlantic. Dönitz's fleet rose to 409, with 178 U-Boats patrolling the Atlantic. From January to March, Allied ship sinkings rose from 203,000 tons to 627,000 tons, while convoy losses averaged forty-nine ships per month. Meanwhile, *B-Dienst* had broken the Admiralty's newest convoy codes, allowing the Germans to read convoy rerouting orders and daily U-Boat reports. By this time, *B-Dienst* was reading eighty percent of British signals traffic.[119]

At the start of 1943, *B-Dienst* began sending Dönitz reports from British intelligence on the positions of German U-boats that was unusually accurate. Dönitz quickly ordered an evaluation of the security of the naval Enigma. This evaluation, performed by Admiral Kurt Fricke, the Chief of the Naval War Command, reassured Dönitz that the Enigma ciphers were unbreakable. He was convinced that the accuracy of British intelligence was due to reports from spies and observations from fishing vessels. Dönitz later wrote in his memoirs in 1958:

> Our ciphers were checked and rechecked to make sure they were unbreakable, and on each occasion the Head of the Naval Intelligence Service at Naval High Command adhered to the opinion that it would be impossible for the enemy to decipher them. And to this day, so far as I know, we are not certain whether or not the enemy did succeed in breaking our ciphers during the war.[120]

Despite his beliefs that the Enigma ciphers were unbreakable, Dönitz pushed for tighter security surrounding the codes. Because of the heightened security for Enigma ciphers, the German High Command would spend less time entertaining the possibility that the enemy was breaking their codes. Cipher clerks were ordered to pay more attention to their transmissions to avoid mistakes. Furthermore, security measures surrounding the transportation and distribution of daily cipher keys were also examined.

For ten days in January, naval Enigma settings could not be read. U-boats sank at this time two American cargo vessels heading for Britain, amounting to the loss of forty-two tanks, 428 tons of tank parts and supplies, 236 pieces of artillery, twenty-four armored cars, 5,210 tons of ammunition, 600 rifles, 2,000 tons of stores, and 1,000 tankloads of gasoline. In order for a convoy to experience similar destruction by bombing, it is estimated that the enemy would have to conduct 3,000 sorties.[121] Moreover, cryptanalysts at Bletchley Park were unable to break the naval Enigma settings on February 8 and would not break them successfully until February 17. As a result, three Atlantic convoys were intercepted by U-Boats and suffered significant losses. One of these, SC118, lost twenty-two percent of its original ships.[122] During this blackout, seven tankers were sunk totaling 55,000 tons and carrying over 100,000 tons of fuel–a seventy-seven percent loss over three days. This was the

[119] Harper, 85.

[120] *Ibid*., 84.

[121] Persico, 160.

[122] Padfield, 318.

highest proportion of any convoy lost during the war.[123] Cryptologists experienced other isolated unsuccessful days from March 10 onwards. Two convoys in mid March, SC122 and HX229, sailed directly into U-Boat wolf packs. Had cryptanalysts been successfully reading intercepts, these two convoys could have been rerouted. As a result, twenty-two ships were sent to the bottom. That month 108 ships totaling 476,000 were sunk in the North Atlantic.[124] The success of wolf pack tactics and the accomplishments of *B-Dienst* put the Germans back on top.

By April, air defenses over the North Atlantic had improved because the Allies began using for convoy duties a large number of escorts and aircraft that previously had been held in reserve. The "air gap," that is, the part of the Atlantic that previously could not be covered by aircraft, disappeared with the improved production and numbers of long range aircraft flying from Iceland, the Azores, Ireland, and Newfoundland.[125] Furthermore, escort ships and patrol aircraft were being equipped with improved radar that could detect a U-Boat at a greater range depending on the antenna height. The introduction of higher frequency radar doubled its effective range, to the point where a periscope could be detected in a calm sea. Also "Huff Duff," a high frequency direction finder that could be found on most ships of the Royal Navy, allowed Allied forces to target and destroy U-boats at a faster rate. Because of these developments and improvements, U-Boats lost their ability to surface near convoys, which weakened their offensive capability. Moreover, when a U-Boat was detected and forced to dive beneath the waves, it could now be tracked more easily due to improvements in sonar. Later in the war, depth sonar and Doppler sonar helped operators determine the depth and the speed of their target. Overall, improved convoy defenses made it more difficult for U-Boats to get close enough to attack.

By late spring of 1943, the amount of tonnage produced per month by Allied forces surpassed that of the tonnage lost to U-Boats. In April, U-Boat losses were still considered sustainable; however, the effectiveness of these U-Boats, in terms of the amount of tonnage sunk per day, dropped by half in comparison to previous months.[126] Americans produced more than one million tons of merchant shipping, which was four times the nation's output in 1939.[127] Naval vessels at this time were designed for better defense against U-Boats. With more ships being produced that were capable of reaching faster speeds, escort vessels now traveled in front of and behind the convoy, and offered further protection against U-Boats.

Slowly Allied forces were making progress. Germany lost fifty-five submarines in April and had only managed to produce eighty-three during that same month.[128] At the same time, U-Boats were only sinking on average 127 tons per U-Boat per day. Even if U-Boats could maintain this average, it would take 325 U-Boats to sink the 1.3 million tons a month that were needed to keep up with new Allied ships.[129] Dönitz in April only had 207 U-Boats in the Atlantic, and with only twenty-seven new boats being produced every month, it would take over ten months before the total in the Atlantic would reach 325. Bletchley's monthly report stated: "Historians of the war are likely to single out the months of April

[123] Harper, 81.
[124] *Ibid*.
[125] Stern, 131.
[126] *Ibid*.
[127] Pitt, 182.
[128] Morison, 10.
[129] Padfield, 329-30.

and May 1943 as the critical period during which the strength began to ebb away from the German U-Boat offensive, not because of the low figure of shipping sunk … but because for the first time the U-Boats failed to press home their attacks on convoys when favourably situated to do so."[130] Dönitz's tonnage war was quickly becoming unwinnable.

In the following month, U-Boats were being sunk faster than they could be built, and Allied shipping losses had reached their lowest point since 1941 in what the U-Boat command called "Black May." U-Boat losses nearly tripled during the month. Losing thirty-eight U-Boats, Dönitz decided to withdraw his submarines from the North Atlantic and place them to the south and west of the Azores to be used against American shipping routes. With a third of his fleet destroyed in the spring of 1943, Dönitz decided to fight on. "The U-Boat arm could not along stand aside and watch the onslaught, of which it had hitherto borne the brunt, now fall in all of its fury as an additional burden on the other fighting services and the civilian population," Dönitz later wrote in his memories, *Ten Years and Twenty Days.*[131] Allied forces were now gaining the upper hand over the German submarines.

By the end of 1943, U-Boats had failed to interrupt or cut off supplies from the Western Allies to Russia, to prevent America's attacks on Africa and Italy, or to prevent American troop build-up in Great Britain. Moreover, they had become less aggressive in their attacks on Allied shipping. By the end of the year, Allied forces also had adequate numbers of escort carriers and destroyer escorts with better trained crews and improved anti-submarine equipment. With the addition of naval air-craft, convoys acted as a unit. On December 30, German radio reported: "This year the British and Americans managed after three years of preparation to gain a success against the U-Boat. In the second half of the year, as far as U-Boat exploits were concerned, sinkings have considerably fallen off."[132] The broadcast went on to state that total sinkings were only twenty percent less than 1942. The real number was fifty-six.[133] Dönitz later wrote, "We had lost the battle of the Atlantic. Events in May 1943 had shown beyond dispute that the antisub-marine organization of the two great sea powers was more than a match for our U-Boats."[134]

By June the tonnage of merchant ships sunk was below 100,000, and of the 429 U-Boats in the fleet, only half were available for operations, with the remainder of the submarines in repair, on training missions, or testing new technology or upgrades.[135] By the end of the year, the Allies had only lost 3.2 million tons of shipping, but had built 43.59 million.[136] However, Dönitz still hoped an improvement would save his U-Boats: the snorkel. Created by a Dutch naval officer, the snorkel and enabled the submarine's diesels engine to receive air and carry away exhaust fumes. The snorkel was later refined, which enabled it to be lowered when it was not in use. The invention made it more difficult to detect U-Boats and allowed them to travel for longer periods of time. While the Germans saw the snorkel as the best weapon against Allied air power, the mechanism took time to be manufactured and installed in U-Boats. Regardless of the improvements that the Germans were making to their submarines, U-Boats were becoming less and less

[130] *Ibid*.
[131] White, 233.
[132] Morison, 247.
[133] *Ibid*.
[134] White, 232.
[135] Brown, 108.
[136] Paterson, 126.

effective at sinking Allied merchant ships. As they were forced underwater, the snorkel allowed them to continue to operate, but did not improve their effectiveness in sinking enemy ships.

In 1943, the tide turned completely against Dönitz as cryptanalysts at Bletchley Park had once again broken the naval enigma ciphers, allowing convoys to be successfully rerouted. From August 1943 until the end of the war, the naval Enigma was deciphered without significant interruption.[137] Furthermore, escorts, anti-submarine aircraft and long-range patrol aircraft became more plentiful, and improved ASDIC, radar, and depth charges all contributed to the shifting of the battle to the side of the Allies.

By 1944, the amount of intelligence from enigma ciphers decreased because U-Boats were able to maintain radio silence for longer periods of time. However, by this time the Allies had already gained the upper hand in the Battle of the Atlantic and were preparing for a successful invasion of Europe with the help of cryptanalysts at Bletchley Park. In the last two years of the war, codes were being broken within hours, with a record time (thanks to the use of over 200 bombs) of 14 minutes.[138]

In early 1944, Dönitz was more concerned about producing U-Boats that would simply survive the journey to and from battles than he was about waging an effective campaign against Allied shipping.[139] Admitting defeat in his pack tactics, Dönitz sent U-Boats out in smaller amounts instead of packs, still believing that convoys were being rerouted due to the Allies' superior radar systems, not the work of cryptologists. On January 1, Hitler in his Order of the Day to the German armed forces, claimed that "the obvious decline in U-Boat successes has been due to only one invention of our enemy."[140] Hitler was referring to the invention of ASV radar (Aircraft to Surface Vessel), but this was only one small part of the defeat of the U-Boat. Intelligence, research, advanced training, and higher level of production all played their own part in winning the Battle of the Atlantic. In the first three months of the year, U-Boats only sank three of 3,360 merchant ships in Atlantic convoys. In comparison, thirty-six U-Boats were sunk.[141] Until May of 1944, only forty-three U-boats were at sea, out of a fleet of around 450.[142] When the Allied invasion occurred in June 1944, the Allied constant air and sea patrol, coupled with the small number of submarines in the area, led to a minimal effect on the large shipping presence in the Channel and surrounding areas. The average of tonnage sunk per day also dropped between twenty and thirty tons per U-Boat.[143] Furthermore, the life expectancy of a U-Boat fell to only two to two and a half months from June until the end of the year, as Allied forces manage to sink 112 U-Boats. By the end of the year, 241 U-Boats had failed to return to their home bases.[144]

Though Dönitz continued to send his U-Boats into battle, the Battle of the Atlantic itself would downshift during the last battles of the war. Many U-Boats remained in action until the end of the war, but from January 1945 until Germany's unconditional surrender, the victories achieved by German submarines were not substantial. "Their achievements were not large, but they carried the undying hope of stalemate at sea … Nevertheless, when Dönitz ordered the U-Boats to surrender, no fewer than forty-

[137] Harper, 89.
[138] *Ibid*., 16.
[139] Stern, 164.
[140] Morison, 247.
[141] Harper, 93.
[142] Brown, 109.
[143] *Ibid*.
[144] Harper, 93.

nine were still at sea … Such was the persistence of Germany's effort and the fortitude of the U-Boat Service," wrote Winston Churchill during the last days of the war.[145] On May 7, the last U-Boat of the war, U-3503, was sunk. The last merchant ship to be sunk, the Canadian ship, *Avondale Park,* went down on May 8, the last day of the war.

Overall, Allied forces lost 2,452 merchant ships in the Atlantic totaling 12.8 million tons.[146] Of the 1,171 U-Boats that went to war between 1939 and 1945, 666–about 57 percent–were lost.[147] Overall, 36,000 merchant ship sailors were lost, but the casualty rate for German U-Boat serviceman was the highest of any military unit since the time of the Romans. Of the 40,000 German officers that went to sea in U-Boats, only 7,000 survived.[148] While Germany did manage to keep Britain to almost minimum subsistence levels, the British prevailed in the Battle of the Atlantic. But they did not do so alone. The United States by the end of the war had transported million tons of shipping to Great Britain, providing ships faster than the Germans could sink them. Moreover, American advances in technology, which included radar, communication methods, and aircraft, also aided in the defeat of the U-Boat. While improvements in technology and military strategy played a role in the Allied victory in the Battle of the Atlantic, Ultra decryptions also were critical to the British. The information gained from German intercepts would prove to be vital to the Allies in their battle against the U-Boat.

# Conclusion

Thirty years after Second World War ended, the British government revealed one of the greatest secrets of World War II: Ultra. In previous years, the successes of the Battle of the Atlantic were attributed to radar and high frequency direction finding.[149] However, in 1974, F.W. Winterbotham published *The Ultra Secret,* which revealed that British intelligence was able to read German radio communications. According to Winterbotham, Ultra intelligence lay at "the hub of the whole Atlantic Battle," because it gave the Allies knowledge of the positions of U-Boats at sea.[150] Shortly after Winterbotham's publication, the British government lifted the secrecy restriction on Ultra. To the world's astonishment, the war at sea had not simply been won by military genius and tactics, or by the courage of those individuals who fought for the Allies. It was vital information that was gained from the enemies' coded messages that turned the tide at various stages of the war. The result of the release of the secret work performed at Bletchley Park was the rewriting of history and a reevaluation of those men and women who had worked around the clock in a race to reveal the inner workings of the German military. Thanks to these men and women, who had never before received public recognition for their war efforts, most historians regard the interception and analysis of German radio communication as one of the keys to victory over Hitler's U-Boats.[151]

[145] White, 271.

[146] Harper, 99.

[147] White, 2.

[148] *Ibid*.

[149] Jürgen Rohwer, "Signal Intelligence and World War II: The Unfolding Story," *The Journal of Military History* 63, no. 4 (1999): 941, http://www.jstor.org/stable/120557.

[150] David Syrett, *The Battle of the Atlantic and Signals Intelligence: U-Boat Situations and Trends, 1941-1945* (Aldershot:Ashgate, 1998), x.

[151] David, Syrett, *The Battle of the Atlantic and Signals Intelligence: U-Boat Tracking Papers, 1941-1947* (Aldershot:Ashgate, 2002), 1.

Throughout the war, no effort was more urgent or given higher priority than the race to break the Enigma codes.[152] Decryptions from Ultra revealed the positions of U-Boat fleets and information about future German naval operations. Historian Patrick Beesly noted that the steady stream of decrypts "made it possible, for the first time … to build up a comprehensive and accurate picture of the whole operational U-Boat fleet."[153] In 1939, the men and women of Bletchley Park received around 192 messages a day; in 1942, the daily message count averaged around 1,200; by 1943 the number of intercepted messages was soon on its way to doubling again.[154] At the height of its operations in late 1943, Bletchley Park was decrypting over 84,000 messages a month.[155]

Before Enigma decryptions were being read at a regular pace, "the rate at which ships were being sunk … far exceeded the rate at which they could be built" and it was feared that Britain would be starved into submission.[156] First Sea Lord, Dudley Pound, stressed "if our Z [Enigma] information failed us at the present time it would, I am sure, result in our shipping losses going up by anything from 50 to 100%."[157] With Ultra decryptions, however, the British Admiralty was able to successfully reroute many Atlantic convoys during the war. In the second half of 1941, H. F. Hinsley notes, some 1.5 million tons of shipping was saved thanks to Ultra decrypts.[158] In addition, U-Boats only sighted one of every ten convoys during this time.[159] With the rerouting of convoys in the latter half of 1941, Ultra decryptions clearly helped to tip the scales in favor of the British.

Another critical time for Ultra in the Battle of the Atlantic occurred in 1943 after cryptanalysts broke the SHARK ciphers. Many German historians agree that this turning point in the battle would not have occurred without the aid of Ultra.[160] Between December 1942 and January 1943, it is estimated that deciphered SHARK messages saved between 500,000 and 750,000 tons of shipping.[161] Professor Jürgen Rohwer noted that with the help of Ultra, "105 convoys or about sixty percent, out of the total number of 174 scheduled North Atlantic convoys running between the middle of May 1942 and the end of May 1943 were clear of German U-Boat patrols so that they were not intercepted."[162] Moreover, not every convoy that traveled in the path of U-Boats suffered heavy losses. Of the sixty-nine convoys that were intercepted, twenty-three escaped without loss and forty more suffered minor damage. Only sixteen convoys lost more than four ships during this time.[163] In June 1943, Winston Churchill would later write, "The shipping losses fell to the lowest figure since the United States had entered the war. The convoys came through intact, and the

[152] White, 197.

[153] Hervie Haufler, *Codebreaker's Victory: How the Allied Cryptographers Won World War II (*New York: New American Library, 2003), 82.

[154] Kahn, 209.

[155] Persico, 108.

[156] Stephen Howarth, "Germany and the Atlantic Sea-War: 1939-1943" chap. 5 in *The Hitler Options: Alternate Decisions of World War II,* edited by Kenneth Macksey (Mechanicsburg: Stackpole Books, 1995), 120.

[157] F.H. Hinsley, *British Intelligence in the Second World War* (New York: Syndicate of Cambridge University Press, 1993), 307.

[158] W.J.R. Gardner, *Decoding History: The Battle of the Atlantic and Ultra* (Annapolis: Naval Institute Press, 1999), 172.

[159] Kahn, 216.

[160] Hinsley, 307.

[161] Harper, 80-81.

[162] Patrick Beesly, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre 1939-1945* (Annapolis: Naval Institute Press, 1977), 185.

[163] *Ibid*.

Atlantic supply line was safe."[164] Without the aid of Ultra, the battle would have been far costlier for Great Britain. The Intelligence and National Security Report in 1988 noted: "Without special intelligence from Triton [SHARK] the U-Boats would still have been defeated in the long run, but the cost in human life in the global conflict at large would have been even more terrible than it was."

The decryptions from Ultra not only allowed the British Admiralty to reroute convoys, but they also aided in the destruction of various German vessels such as the tankers and suppliers for the *Bismark,* as well as warships such as *Tirpitz, Scharnhorst,* and *Atlantis.*[165] Furthermore, Ultra also played a large role in major convoy battles in 1943, which would ultimately turn the tables in the Battle of the Atlantic against the Germans. By August of 1943, a U-Boat, whose location was revealed through Ultra in five days or less, was three times more likely to be sunk. In addition, the rate at which merchant ships were being sunk was one-sixth what it had been during black-out periods.[166]

Even during periods of time when cryptanalysts experienced black-outs in deciphering, Ultra decrypts would still prove useful. Though not all decryptions would prove useful operationally, information from these messages provided details about the U-Boat fleet in terms of its size, state of training, and operational methods.[167] During times of black-outs, the Admiralty still gained information from U-Boat sightings, attacks, and the few direction-finding transmissions that were available. In 1942, information from POWs and captured documents gave British intelligence specifics on the performance levels of new types of U-Boats, the experiences of certain commanders, and where they often patrolled.

Of course, Ultra was not perfect. Cryptanalysts did experience delays. Depending on the information that cryptanalysts possessed, it could take hours, days, or even weeks for ciphers to be decrypted. In addition, the diversion of a convoy sometimes was not possible due to the timing of the order. At best a convoy in 1943 could cover 240 miles in twenty-four hours; U-Boats at full speed could cover between 320 to 370 miles.[168] Also, the Admiralty could experience up to three days of delays after learning that U-Boats had altered course. Rerouting a convoy to avoid the new path could then be impossible. With more U-Boats in operational use, the Admiralty often chose to reinforce convoys that traveled into the path of U-Boats. While a convoy itself might not be able to be rerouted in time, escorts could be transferred from unthreatened convoys to reinforce those in the path of a large wolf pack of U-Boats.[169] Therefore, Ultra should not be judged on the failures to eliminate the destruction of convoys, but the extent to which it reduced the frequency and scale of the disasters.[170]

In addition, not all of the information gained from Ultra could be used operationally. Not every U-Boat position which was revealed in Ultra could be compromised, because a sharp rise in British sinkings would certainly alert the Germans that their communication system was not

[164] Haufler, 85

[165] Ralph Erskine, "Breaking the Naval Enigma (Dolphin and Shark)," http://cryptocellar.web.cern.ch/cryptocellar/bgac/HMTR-2066-2.pdf (Accessed, February 7, 2009).

[166] Kahn, 227.

[167] Gardner, 202.

[168] Hinsley, 309.

[169] J. David Brown, "The Battle of the Atlantic, 1941-1943: Peaks and Troughs" chap. 9 in *To Die Gallantly: The Battle of the Atlantic,* edited by Timothy J. Runyan and Jan M. Copes (Boudler: Westview Press, 1994), 139.

[170] Hinsley, 311.

safe.[171] Therefore, the British would allow some U-Boats to escape as they strategically chose their targets. Often, spotter planes or search boats would first enter the area, which would then justify the destroyer which would appear hours later. Many cover stories, reconnaissance missions, and false messages were created to keep Ultra a secret. Furthermore, the black-out periods that men and women of Bletchley Park experienced in 1942 most likely concealed the fact that the Enigma codes were being broken. From February to December of that year, when cryptanalysts were in the dark to the operations and locations of U-Boats, the German Navy was enjoying considerable success along the east coast of America. If U-Boats at this time had continued to focus on the Northern Atlantic instead of the American coast, the Germans would have noticed the continued improvement against British convoys and linked it to the change from the three to the four-wheeled Enigma.[172]

Historians over the years have debated whether Ultra decryptions during the Battle of the Atlantic helped to shorten the war at sea. Many historians note that if cryptanalysts had not broken SHARK, Allied forces most likely would not have established naval supremacy in the Atlantic until the second half of 1943 at the earliest, which might as well have delayed the invasion of Europe at least until 1945.[173] English cryptanalyst Harry Hinsley wrote:

> The U-Boats would not have done us in, but they would have got us into serious shortages and put another year on the war. Operation Overlord would certainly not have been launched in June 1944 without Ultra. Or at least, if it had been launched, it would probably not have been successful. My own belief is that the war, instead of finishing in 1945, would have ended in 1948 had G.C. & S. C. not been able to read the Enigma ciphers and produce Ultra intelligence.[174]

Others agree that without the shipping that was spared by Ultra, vessels would have to be pulled from the Pacific and other waters to avoid a delay in the invasions of Italy and Normandy.[175] With a prolonged battle in the European theater, other historians question whether the first atom bomb might have been dropped on a German city such as Berlin instead of Hiroshima.[176]

The work done at Bletchley Park was also crucial in saving Britain from starvation and early defeat at the hands of the Germans. Without the defeat of the German U-Boat, American troops and material, along with aid from the rest of the British Empire and Canada might never have reached the European theater. Furthermore, U-Boats in the Atlantic would have been able to harass the supply lines to Russia costing more men and material, which might have had disastrous consequences for the Eastern Front. The British Joint Intelligence Staff at the end of the war concluded: “without Special Intelligence the war would have been much longer, and more costly, and indeed might never have been won.”[177]

[171] Simon Singh, *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography* (New York: Doubleday, 1999), 184.

[172] John Winton, *Ultra at Sea: How Breaking the Nazi Code Affected Allied Naval Strategy During World War II* (New York: William Morrow and Company, Inc., 1988), 109.

[173] Harper, 9.

[174] Kahn, 278.

[175] *Ibid*.

[176] Gardner, 217.

[177] Winton, 196.

It is also important to note that there was no single capture of Enigma documents that caused cryptanalysts to break the naval ciphers once and for all. Each "pinch" or capture gave the British cryptanalysts another piece to the puzzle and the capacity to break ciphers until the next change in procedure. Therefore, many captures were necessary for Great Britain in order to continue to successfully read German transmissions.[178]

Moreover, it is undeniable that there was a connection between the careful rerouting of Allied convoys and the contents of Enigma ciphers. Though the British Admiralty used the highest level of secrecy surrounding Ultra and continuously relayed false cover stories over the airwaves, if Ultra had been used over a long period of time, the Germans would have certainly caught on to the Admiralty's secret. However, they did not for various reasons.

Throughout the war, Dönitz demanded constant radio communication to keep tactical control of his boats, despite the high risk of interception and decryption by the Allies. U-Boats would transmit radio signals detailing their positions, enemy air, naval, and merchant traffic, weather, and harbor defenses. This radio traffic effecttively denied the U-Boats their chief tactical advantage–the element of surprise. Yet while constant ship to shore communication lowered security, it also made Dönitz's wolf pack tactics possible.

Furthermore, the confidence that Dönitz and the German High Command had in the Enigma was staggering. Many historians believe that psychological blocks played a role in the lack of suspicion concerning the Enigma.[179] The Enigma and its codes were secure because the German High Command and Enigma operators believed that it was secure. The assurances of invulnerability from the German High Command also led many to believe that the enemy would never be able to read the secret messages communicated on the Enigma machine. In addition, very few of the U-Boat Command staff knew the exact details of the Enigma communication system. The fact that vital codebooks, printed on soluble paper, were kept in separate locations was another security measure that added to the confidence of the U-Boat Command.

The U-Boat command was also certain that if the British were indeed breaking into their codes, Germany's own code breaking efforts would have revealed this fact. In addition, they believed that there was no way that British intelligence could be reading their superior codes when their own codes were being broken. The *Funkbeobachtungsdienst*, or *B-Dienst*, the German naval code breaking center, had broken the Royal Navy's Number 3 cipher periodically from the outset of war until early 1943, which gave the details of the location of convoy routes, launch sites and times. This break in the British ciphers gave German U-Boats a considerable advantage. However, the Admiralty later changed its codes in June 1943, leaving the *B-Dienst* in the dark. Moreover, during the last third of the war, British intelligence improved the security of its coding methods, so that by 1944, *B-Dienst* was unable to decipher the two main British code systems. Soon afterward, the Germans were unable to decode lower-echelon messages, and eventually stopped trying to intercept top level messages.[180] Because no mention of Ultra was made in British transmissions that were decoded, German intelligence assumed that their codes were not being broken.

[178] Sebag-Montefiore, 2.

[179] Winton, 104.

[180] David Kahn, "Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes, and Their Effects," *The Historical Journal* 23, no. 3 (1980), 625, http://www.jstor.org/stable/2638994.

The security of the Enigma also played a large role in German complacency. In order for an enemy to decipher a message, the enemy not only needed the Enigma machine itself, but also daily keys and wheel orders, rings and plug board settings. The Germans believed that it was impossible for an enemy to collect all of these items month after month, let alone from cryptanalytic means from the cipher text itself.[181] After the month's codes expired, the code breakers would be back to square one.[182]

However, most of the leads into the decryption of the Enigma stemmed from procedural errors. Various weaknesses in the security of the machine's operating procedures, message handling, and monitoring of message transmission each brought crypt-analysts one step closer to decryption.[183] Because of routine reports and orders, many Enigma operators became sloppy in their operating procedures and message handling. Therefore, stereotypical addresses, signatures, and content appeared in daily messages. The staggering number of ciphering possibilities kept the operators complacent and allowed for errors to occur.[184]

However, while the Germans did try to tighten the security for the Enigma machine, future codebooks detailing code making instructions could be captured. Upon attack, many sailors forgot about protocol concerning the Enigma machine and codebooks as they struggled to escape the U-Boat alive. In addition, many U-Boat commanders were not trained properly on how to dispose of codebooks when the order was given to abandon ship, and the German Naval Command, which dictated Enigma protocol, did not always stress the importance of following protocol. Many German commanders believed that an attempt to sink the vessel should be tried first before any secret code material be destroyed or thrown overboard.[185] However, in many circumstances, the U-Boat could be boarded before it sank. This error allowed for the capture of vital code books. If the German Naval Command had further adapted the Enigma machine so that captured code books could not produce a quick solution, the failure of the ciphers may not have been as imminent.

Overall, few German investigations were made into the security of the Enigma machine. However, the results of each were the same: the ciphers had not been broken. Furthermore, even if weaker ciphers had been broken, this would have no more than temporary effects. In addition, these temporary breaks were attributed to carelessness in the German ranks, which was to be investigated.[186] While the German high command understood that Enigma operators could be lazy, and the capture of documents in wartime was a reality, they still viewed the Enigma and its complexity as the "most resistant of all known methods for secrecy in military communications."[187] Years after the war, Dönitz himself denied any possibility that the codes had been broken. In his post-war memoirs, he wrote: "our ciphers were checked and re-checked, to make sure that they were unbreakable: and on each occasion the Head of the Naval Intelligence Service at Naval High Command adhered to

[181] Stephen Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War II* (New York: Simon & Schuster, 2000), 249.

[182] Beesly, 67.

[183] Gordon Welchman, *The Hut Six Story: Breaking the Enigma Codes* (New York: McGraw-Hill Book Company, 1982), 163.

[184] Jim DeBrosse and Colin Burke, *The Secret in Building 26* (New York: Random House Trade Paperbacks, 2005), 13.

[185] Sebag-Montefiore, 3.

[186] Ronald Lewin, *Ultra Goes to War* (New York: McGraw-Hill Book Company, 1978), 212.

[187] Kahn, 206.

his opinion that it would be impossible for the enemy to decipher them."[188] Instead of believing that their cipher system was compromised, High Command continued to believe that the contents of their secret messages were being delivered to the Allies by German spies or an advanced radar system.[189] Over the years, this ignorance toward the breaking of the Enigma ciphers would lead the British to perfect their strategies in decryption and the tactical use of information from German transmissions; therefore, making Ultra one of the keys to the defeat of Hitler's U-Boats in the Battle of the Atlantic.

Though Ultra was one of the more critical methods of anti-submarine warfare employed by the British, it was not the only factor that led to the defeat of the U-Boat. Furthermore, signals intelligence, high frequency direction finding, radar, sonar, long-range aircraft, Huff-Duff, improved convoy tactics, and American liberty ships all lead to German defeat at sea. Superior Allied strategy, tactics, technology, and intelligence played their own role in Allied victory. The information gained from Ultra shaped military strategy and operations and removed guesswork from Allied commanders' decisions.[190] Ultra decrypts also gave the British Admiralty insight into high-level German intelligence, the location of U-Boats well beyond the range of aerial reconnaissance missions, and was trusted more than spies.[191] The battle could have been won without intelligence such as Ultra, but at a greater cost of men and material.

Not only have historians commented on the importance of Ultra, but many commanders also praise Ultra intelligence. Decades after the war, Franz Halder, the Chief of the German General Staff notes Ultra was "the most copious and the best source of intelligence." Dwight D. Eisenhower informed the men and women of Bletchley Park that the intelligence from the operation was of priceless value. Finally, American General George Marshall believed that the decryptions from the Enigma machine "contribute[d] greatly to the victory [of the Allies] and tremendously to the saving of American lives."[192]

The work performed at Bletchley Park during the Second World War was unparalleled to any other code breaking effort the world had seen. The men and women of Bletchley Park beat staggering mathematical odds in a race against time between the code maker and the code breaker. Winston Churchill after the war wrote: "If we had not mastered its [Ultra's] profound meaning and used its mysteries even when we saw them only in the glimpse, all the efforts, all the prowess of the fighting airmen, all the bravery and sacrifice of the people, would have been in vain."[193]

[188] Lewin, 213.

[189] Winton, 195. Syrett, 261.

[190] Haufler, 308.

[191] David Kahn, "Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes, and Their Effects," 639.

[192] *Ibid*.

[193] Haufler, 6.

# Bibliography

Beesly, Patrick. *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre 1939-1945.* Annapolis: Naval Institute Press, 1977.

Brown, David. *Atlantic Escorts: Ships, Weapons, and Tactics in World War II.* Annapolis: Naval Institute Press, 2007

Brown, J. David. "The Battle of the Atlantic, 1941-1943:Peaks and Troughs." Chap. 9 in *To Die Gallantly: The Battle of the Atlantic,* edited by Timothy J. Runyan and Jan M.Copes, 137-57. Boudler: Westview Press, 1994.

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II.* New York: Simon & Schuster, 2000.

DeBrosse, Jim and Colin Burke. *The Secret in Building 26.* New York: Random House Trade Paperbacks, 2005.

Erksine, Ralph. 2000. Afterword to *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre 1939-1945;* or *Codebreaking in the Battle of the Atlantic,*by Patrick Beeley, 261-284. Annapolis: Naval Institute Press, 1977.

Erskine, Ralph. "Breaking the Naval Enigma (Dolphin and Shark)." http://cryptocellar.web.cern.ch/cryptocellar/bgac/HMTR-2066-2.pdf (Accessed, February 7, 2009).

Erksine, Ralph. "Captured *Kriegsmarine* Enigma Documents at Bletchley Park."*Cryptologia* 32 (2008): 199-219.

Franklin D. Roosevelt Presidential Library and Museum. "FDR Letter Regarding British and American Efforts for the War 12/7/40." http://www.fdrlibrary.marist.edu/website_online_version/psf/box34/a311s02.html (accessed February 6, 2009).

Gardner, W.J.R. *Decoding History: The Battle of the Atlantic and Ultra.* Annapolis: Naval Institute Press, 1999.

Harper, Stephen. *Capturing Enigma: How HMS Petard Seized the German Naval Codes.* Phoenix Mill: Sutton Publishing, 1999.

Haufler, Hervie. *Codebreaker's Victory: How the Allied Cryptographers Won World War II.* New York: New American Library, 2003.

Hinsley, F.H. *British Intelligence in the Second World War.* New York: Syndicate of Cambridge University Press, 1993.

Howarth, Stephen. "Germany and the Atlantic Sea-War: 1939-1943." Chap. 5 in *The Hitler Options: Alternate Decisions of World War II,* edited by Kenneth Macksey, 105-124. Mechanicsburg: Stackpole Books, 1995.

Kahn, David. "Codebreaking in World Wars I and II: The Major Successes and Failures, Their Causes, and Their Effects." *The Historical Journal* 23, no. 3 (1980): 617-639. http://www.jstor.org/stable/2638994

Kahn, David. *Seizing the Enigma: The Race to Break the German U-Boat Codes 1939-1943.* New York: Barnes & Nobel Books, 1991.

Keegan, John. *The Second World War.* New York: Penguin Books, 1989.

Kippenhaun, Rudolf. *Code Breaking: A History and Exploration.* New York: The Overlook Press, 1999.

Lewin, Ronald. *Ultra Goes to War.* New York: McGraw-Hill Book Company, 1978.
Miller, A. Ray. *The Cryptographic Mathematics of Enigma.* Fort George G. Meade: Center for Cryptologic History – National Security Agency, 2006.

Morison, Samuel Eliot. *The Atlantic Battle Won: May 1943-May 1945.* Boston: Little, Brown and Company, 1956.

National Security Agency. "How Mathematicians Helped Win WWII." National Security Agency. http://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/publications/how_math_helped_win.shtml. (Accessed February 23, 2009).

Overy, Richard. *Why the Allies Won.* New York: W.W. Norton & Company, 1995.

Padfield, Peter. *War Beneath the Sea: Submarine Conflict During World War II.* New York: John Wiley & Sons, Inc., 1995.

Paterson, Michael. *Voices of the Code Breakers: Personal Accounts of the Secret Heroes of World War II.* Cincinnati: David & Charles, 2007.

PBS, "NOVA," November 14, 2000, "Hitler's Lost Sub," Roy Scheider.

PBS, "NOVA," November 9, 1999, "Decoding Nazi Secrets," Live Schreiber.

Persico, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage.* New York: Random House, 2001.

Pitt, Barrie. *The Battle of the Atlantic.* Alexandria: Life-Time Inc., 1977.

Roberts, Chuck. “Battle of the Atlantic: Allied Communication Intelligence December 1942 - May 1945.” HyperWar Foundation. http://ibiblio.org/hyperwar/ETO/Ultra/SRH-009/index.html (accessed July 2, 2008).

Rohwer, Jürgen. “Signal Intelligence and World War II: The Unfolding Story.” *The Journal of Military History* 63, no. 4 (1999): 939-951. http://www.jstor.org/stable/120557.
Sebag-Montefiore, Hugh. *Enigma: The Battle for the Code.* New York: John Wiley & Sons, Inc., 2000.

Schofield, B.B. “The Defeat of the U-Boats during World War II.” *Journal of Contemporary History* 16, no. 1 (1981): 119-129. http://www.jstor.org/stable/260619.

Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography.* New York: Doubleday, 1999.

Smith, Michael. *Station X: The Codebreakers of Bletchley Park.* London: Pan Books, 1998.

Stafford, David. *Churchill and Secret Service.* New York: The Overlook Press, 1997.

Stern, Robert C. *Battle Beneath the Waves: The U-Boat War.* London: Arms and Armour, 1999.

Syrett, David. *The Defeat of the German U-Boats: The Battle of the Atlantic.* Columbia: University of South Carolina Press, 1994.

Syrett, David, ed. *The Battle of the Atlantic and Signals Intelligence: U-Boat Situations and Trends, 1941-1945.* Aldershot:Ashgate, 1998.

Syrett, David, ed. *The Battle of the Atlantic and Signals Intelligence: U-Boat Tracking Papers, 1941-1947.* Aldershot:Ashgate, 2002.

Welchman, Gordon. *The Hut Six Story: Breaking the Enigma Codes.* New York: McGraw-Hill Book Company, 1982.

Westwood, David. *The U-Boat War: The German Submarine Service and the Battle of the Atlantic, 1935-1945.* Philadelphia: Casemate, 2005.

White, David Fairbank. *Bitter Ocean: The Battle of the Atlantic, 1939-1945.* New York: Simon & Schuster Paperbacks, 2006.

Williams, Andrew. *The Battle of the Atlantic: Hitler's Gray Wolves of the Sea and the Allies' Desperate Struggle to Defeat Them.* New York: Basic Books, 2003.

Winton, John. *Ultra at Sea: How Breaking the Nazi Code Affected Allied Naval Strategy During World War II.* New York: William Morrow and Company, Inc., 1988.

The women code-breakers of Bletchley Park knew all the secrets -- but couldn't let on.Â  Witness to World War II code-breaking 07:02. Wartime Prime Minister Winston Churchill famously described the team at Bletchley as "the geese that laid the golden eggs, but never cackled." It was only decades later that their story became widely-known, thanks to books and movies like the Oscar-winning "The Imitation Game," starring Benedict Cumberbatch as computing pioneer Alan Turing.Â  Betty Webb, who was sent to Bletchley while serving in the Auxiliary Territorial Service (ATS) -- the women's section of the British Army -- remembers being made to read and agree to the Official Secrets Act as soon as she arrived. The British codebreaking team was astonished when the Poles were able to tell them detailed information about the Enigma and how it might be broken, even though the Poles could not yet decrypt the three-of-five-wheels version. The Poles even produced a working version of the Enigma itself.Â  The German surface forces were never a serious factor in the Battle of the Atlantic. Of more importance, at the outbreak of the war Germany had 57 U-boats.Â  Thanks to the breaking of the naval code and inventions such as sonar, the German U-boat menace began to be reduced. In addition, the B-Dienst success in breaking the British convoy codes supplied U-boat command with the routes and speeds of British convoys. Bletchley Park was the intelligence nerve centre of the Second World War, but what happened to Alan Turing and its other operatives after the war ended?Â  Bletchley had run a world-wide operation; secret listeners in stations on every continent intercepting every coded communication, listening to every enemy plan and manoeuvre. On top of this, the code-breakers had (almost as a side-effect) kick-started a new age of computing. Their efforts to find a mechanised means of decoding Nazi messages led to the creation of the first programmable proto-computers.Â  Or indeed had been pivotal in Bletchleyâ€™s Hut 8 throughout the Battle of the Atlantic. By the time GCHQ moved to Chelteham, it was a vital part of defence, says Sinclair McKay. (Photo by David Goddard/Getty Images).