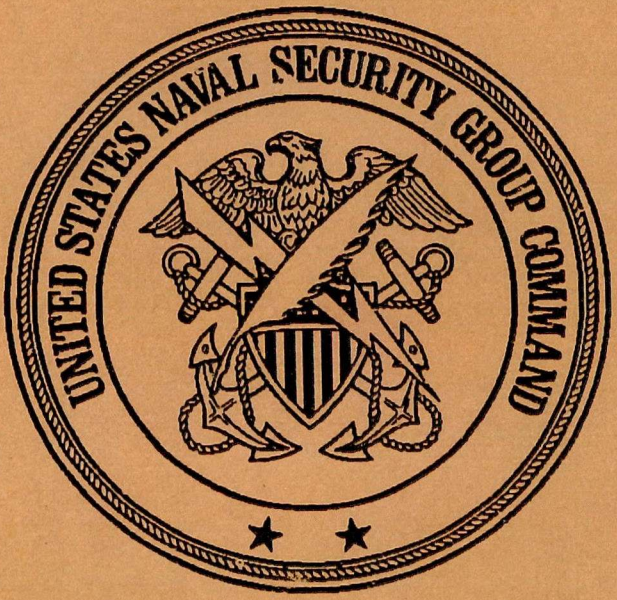
A BRIEF HISTORY OF NAVAL CRYPTANALYSIS



By
Jeffrey Greenhut, PH. D.

Contents of this paper are not necessarily the official views of, or endorsed by, the U. S. Government, the Department of Defense, the Department of the Navy, or the Naval Security Group.

REVIEWED AND CLEARED ON 25 JUNE 1991 FOR
COMNAVSECGRU BY
MR. I. NEWMAN.

THE PRE-WORLD WAR II PERIOD

The Early Years

The first formal code book used by the United States Navy dates from 1848, but a major interest in the codes and ciphers of other nations by the Navy had to wait until technology permitted substantial intercepts of enemy communications. The technological advance that permitted this was the development and widespread use of radio communications by all the industrialized countries. Still, the first part of the twentieth century saw the attention of the Naval officer corps directed toward the transformation of the United States Navy from a coastal defense force into what would shortly become a Navy second to none. Although some attention was paid to the intricacies of cryptanalysis, it took the entry of the United States into World War I before the Naval establishment turned to the obvious requirements of signals security and signals intelligence.

By the time the United States entered the war, the German surface fleet was confined to port, and the British cryptologic effort directed against the enemy submarine threat was well ahead of the Americans. While the Army did direct a significant cryptologic effort against the German armies, the Navy in effect reinforced the British naval effort with Direction Finding (DF) stations. Nonetheless, before the end of the war, the predecessor of DCMS, the Confidential Publications Section had been created and a Code and Signals section placed under the Director of Naval Communications.

Between the Wars

The close of World War I saw the attention of the Navy turn to the Pacific. Ever since the acquisition of the Philippines from Spain in 1898, and the Japanese defeat of the Imperial Russian Navy in the classic battle of Tsushima in 1904, the Navy had gradually increased its attention on the Pacific theater and on Japan. With the close of World War I, and with the great German High Seas Fleet scuttled or sunk, the only possible naval adversary was the Japanese.

However, the world was war weary after the slaughter of the trenches, and the attention of Washington was riveted on disarmament. Fortunately for the State Department, it and the Army had retained Herbert Yardley, the architect of the Army effort during the war, and set him up in New York. By the convening of the Washington Naval Conference in 1920, he and his team had cracked the Japanese diplomatic code. Couriers traveled daily from New York to Washington carrying the decrypts as the Japanese negotiators requested and received instructions from their government. The

resentment of the Japanese over the limited spoils they received at Versailles, a symptom of the extreme nationalism that would drive them into World War II, was balanced by economic troubles at home and a fear of pushing the Americans too far. In the end, they instructed their representatives to settle for a Navy to be sixty per cent of that of the United States or the British. Knowing this, the American Secretary of State, Charles Evan Hughes, simply outstared the Japanese team until they accepted this ratio.

The year of the conference also saw the awakening of the U. S. Navy to the need for cryptanalysis. Captain Andrew Long reported to Washington as the new director of the Office of Naval Intelligence. The office had long been considered simply a post office for sending on reports generated elsewhere. Long had a different approach. Realizing that Japan was the major possible adversary, he increased the number of Naval intelligence and language student officers at the American Embassy in Tokyo.

However, one could not yet state that the cryptanalysis effort of the Navy had been systematized. That step took the arrival, in 1924, at the newly created Research Desk in the Codes and Signals Section of Lt. Laurence Safford. Safford set about collecting a small team to be trained as cryptanalysts, but they suffered from a major constraint, a very limited number of signals on which to practice. After all, code breakers are of limited use unless they are actually breaking codes.

Therefore, the next step was for the Navy to establish a number of intercept stations. The first became operational on Guam in 1925, followed by, two in the Philippines and another in the American consulate in Shanghai. In that same year, Commander (later Rear Admiral) Ellis M. Zacharias tested the effectiveness of a seaborne listening station. It proved so effective that in 1928 Zacharias set up on the cruiser U. S. S. Marblehead to listen in on the Japanese as they fought their annual naval war game.

When Safford left for the sea duty required of all Naval officers of the day, he left behind a brilliant team that included Lt. Joseph Rochefort and Ms. Agnes Driscoll. Rochefort was soon on his way to Japan for a three year language course. He was followed by many others whose contributions to victory in World War II were substantial.

With the intercept stations in operation, it became obvious that the number of naval enlisted personnel capable of accurately and quickly listening to and transcribing Japanese messages was inadequate. So, in 1928, the Navy began a program to train selected men in this skill. Since the training area was located on the roof of the old Navy Department building in Washington, graduates of the

school became known as the "On the Roof Gang." These sailors and marines staffed the intercept stations scattered over the Pacific. By the time war broke out, the 176 men graduated from this program formed a solid and competent corps for the signals intelligence effort.

While the Navy was busy in this area, Yardley continued his activities in the "Black Chamber." Unfortunately, because Yardley was a dissolute character and had become an impediment to the Army's efforts to systematize its signals intelligence efforts, the Army cut off his funding in 1929. Now his only support came from the Department of State. This did not last long. The new Secretary of State, Henry L. Stimson, was outraged when some intercepted and decrypted signals were laid on his desk. Reputedly stating, "Gentlemen do not read one another's mail," he immediately stopped Yardley's remaining funding. Yardley's revenge was not long in coming. He sold to the Japanese his knowledge about the penetration of their code, and published his memoirs.

The Japanese Response and the American Answer

The Japanese were considerably more outraged than Secretary Stimson. More importantly, they began work on an "unbreakable" system. They decided to overlay their codes with a machine based cipher. The first of their cipher machines, like most such systems of the day, was based on a series of rotors each of which had a series of positions around its circumference based on the alphabet. Within the rotor, intricate and complex wiring arrangements meant that the possible number of differently wired rotors for a system based on the Latin alphabet was immense. By creating a machine using a number of rotors, shifting their positions in a prefigured but randomly selected pattern, and coupling the entire system to a typewriter keyboard, the number of possible combinations became so large that decryption seemed impossible.

The Japanese introduced this system in 1931. The foreign office version, known in the United States as the "Red" machine, was quickly broken. Then, in 1937, the Japanese shifted from the rotor principle with an entirely new machine, known as "Purple." Fortunately, they made the profound error of sending identical messages in both systems, giving the Americans the raw material on which to develop their solution.

In these days, intelligence personnel and the cryptanalysts did not always work together. In one case, intelligence personnel stole a Japanese code the cryptanalysts were already reading. Had the theft been discovered, the Japanese would have changed their codes and

blinded the cryptanalysts. Such incidents highlighted the necessity of working together.

By this time, the Army's signal section, under the direction of William Friedman, and the Navy's, once more under Safford, were working closely together. Understanding Friedman's that genius would be best applied to "Purple," the Navy furnished its Purple intercepts, picked up by its intercept stations all over the Pacific, to Friedman and the Army, while it concentrated on the other Japanese diplomatic and naval codes. By the summer of 1940, this collaboration had paid off, and Japanese diplomatic traffic was an open book.

By 1941, the Army had constructed eight analogs of the Purple machine. Four were in Washington, two each for the Army and Navy. Messages were divided up between the two services based on the date of origin in Tokyo, the Army taking even days, the Navy odd. Another machine was in the Philippines, due to its ideal location for interception. The remaining three had been given to the British.

If Japanese diplomatic traffic could be easily read by the Americans, unfortunately, the same could not be said of the Japanese high grade naval code. From 1926 to 1940, the Navy had been able to read the Japanese "flag officer system." However, on December 1, 1940, the Japanese had introduced a new code, JN-25, which still resisted the best efforts of the Navy. Yet the Navy was not totally blind. Rochefort, now in charge of Station "Hypo" at Pearl Harbor, had, through a meticulous study of call signs and signals volume, built up an accurate estimate of the Japanese Navy order of battle, and could track units of the fleet as long as they did not observe radio silence.

If the ability to read the Purple ciphers and codes was of enormous benefit, the system was by no means perfect. Insufficient radio circuits existed to transmit all intercepted traffic to Washington, so much went by airmail, on the single flight from Hawaii to the mainland each week for example. If normal airmail schedules were disrupted, messages might even go by train or ship. Even when placed into plaintext, translation was a serious bottleneck. It is doubtful that the Army and Navy between them had any more than eight or nine translators available at any one time.

At best, Magic, as the effort was called, provided only raw information. Before it became intelligence, it needed to be analyzed, interpreted, and disseminated. Here too lay serious problems. Fear of compromise was so extreme that distribution of the decrypts was severely restricted. Further, there was no system in place to get complete sets of decrypted material from Washington to Hawaii, and

even the partial sets stopped being sent in July of 1941. The slipshodiness of the system was demonstrated by the fact that Admiral Stark, Chief of Naval Operations, was erroniously informed that Pearl continued to get the complete sets. Further, Admiral "Terrible Tommy" Turner, Chief of War Plans Division, a man who richly deserved his nickname, had succeeded in relegating the Office of Naval Intelligence to that of a collection and distribution agency, thereby taking the responsibility for evaluating Japanese intentions out of the hands of people who knew Japan, its language, its Navy, and its people.

To quote Ronald Lewin, Magic "was like some rare and precious object carried on a fragile conveyance that has been tied together by frayed pieces of string."

WORLD WAR II

Pearl Harbor

When it became known that the United States had had access to the Purple material throughout the months leading up to Pearl Harbor, there was an immediate suspicion among some quarters that either the plans of the Japanese were known and deliberately kept from the commanders on the scene, or that an incredible blunder had occurred. An examination of the evidence proves neither true.

Any impartial analysis must start with the fact that although the United States could read the Purple code, that is the diplomatic traffic, the Japanese naval code, JN-25 was still a mystery to American naval cryptanalysts. On the other hand, a number of messages dealing directly with American naval strength at Pearl Harbor were not passed on. Yet it must be remembered that these were lost in volumes of traffic that were concerned with military forces elsewhere. Only in retrospect did these stand out.

Nonetheless, by November 27th, 1941, Washington had become convinced that war with Japan was imminent and so advised Admiral Kimmel and General Short in Hawaii. By that time, Rochefort had lost the Japanese fleet which was either observing radio silence or sending messages designed to hide its whereabouts. On the night of November 30th, another ominous development took place. The Japanese fleet, for the first time ever, changed call signs twice within a single month. Lt. Commander Edwin Layton, Kimmel's fleet intelligence officer, was forced to admit that for all he knew, the Japanese fleet could be rounding Diamond Head.

On December 2nd, the Japanese foreign ministry dispatched a message to its Consul in Hawaii requesting information on the

presence in port of major warships and if they were protected by barrage balloons or barriers. Although this might have alerted Kimmel and Short, the message, although intercepted on December 2nd, was not mailed to Washington until the 11th, and not translated until the 13th.

On December 4th, Washington became aware that Japanese Embassies had received instructions to burn their codes and destroy their code machines. Quite aware of the significance, they immediately informed Kimmel.

Thus, by the first week in December, Hawaii had received a war warning, had lost the Japanese fleet, and had been informed that the Japanese were burning codes and code machines. It was thus clear that Japan was going to war. What was not clear was with whom and where she would strike. Although both Kimmel and Short testified that had they had all the messages available in Washington, they would have better prepared for hostilities, we can only conclude that is hindsight. What is not is that Japan struck at dawn on December 7th and crippled the unprepared and somnolent American fleet. Every one of the eight battleships was sunk or damaged, but in an incredible stroke of luck, all the American carriers were at sea. Not one was damaged. With six carriers available, some defense against further Japanese attack was possible.

However, a glance at the map showed that the Japanese had the advantage of interior lines. Their eight great fleet carriers could be shifted far faster than could those of the Americans. Further, the Americans had a second ocean with which to deal, the Atlantic. Admiral Chester Nimitz, the new commander in the Central Pacific, could never know when one or more would be removed from his control and sent either to the Southwest Pacific theater or to the Atlantic.

In Hawaii, Rochefort and his group finally began to crack JN-25b. There, in a shabby cellar, entered only by two locked doors, they labored in a permanent state of disorder. Rochefort commanded, usually wearing a red smoking jacket and carpet slippers. Existing on three hours or less of sleep, snatched on a cot amid the mess, and living on a diet of coffee and sandwiches, he and his crew gradually began to read the Japanese naval code. They found their clues in Japanese mistakes and carelessness, and by the fact that Japan's new and far flung conquests made it so difficult to distribute new codes that they retained the old ones far too long and used them in conjunction with the new for identical messages.

Even with this, less than fifteen per cent of many individual messages could be read, and their content comprehended only by

intimate knowledge of the Japanese order of battle and the general situation. It was April of 1942 before the pieces finally came together. At that point, Rochefort was able to report the first indications that would lead to the great battles of the Coral Sea and Midway.

Coral Sea and Midway

Before long, Rochefort had infomred Nimitz that three Japanese carriers, one light and two heavy were converging for an operation in the Solomons area. Forces available to Nimitz for his response were limited. He had only four carriers available, and two, the Hornet and the Enterprise, had not yet returned from launching the Dolittle raid over Tokyo. Although he sent them southwest immediately upon refueling and rearming, they were three times the distance from the area of operations than the Japanese. Thus the Battle of the Coral Sea pitted Admiral Fletcher's Lexington and Yorktown against three Japanese carriers.

The results were mixed. The Japanese lost one light carrier which was more than compensated by the loss of the Lexington and the damage to the Saratoga. Yet both the Japanese heavy carriers engaged in the Coral Sea would be unavailable for Midway. It was a Japanese tactical victory that turned out to be a strategic defeat.

Yet the odds were still not in America's favor. Against six large Japanese carriers and eleven battleships available to Admiral Yamamoto for the Midway operation, the Navy could place, at most, only the five remaining carriers of the Pacific fleet, for its battleships either rested on the bed of Pearl Harbor, or were not yet repaired of the damage inflicted on December 7th. Further, Japan had a superior air fleet. The Japanese Zero outclassed all American carrier borne fighters, and their torpedo bombers carried the famous "Long Lance" torpedo, far superior to the American slow, short range torpedoes that often failed to explode even when they hit.

As the days passed, the situation did not improve. Nimitz had to send the Wasp to the Atlantic, and the Saratoga to San Diego for repair. The lineup now was six to three.

Although Yamamoto's intelligence was not as good as that of the Americans, he nonetheless felt assured of a temporary superiority. He was also well aware that this superiority was short lived, for he had spent several years in the United States and did not underestimate its productive capacity. He had to strike now. If he could concentrate all six of his operational carriers against the Americans, the outcome couldn't be doubted. For Nimitz, the problem was acute. He was not strong enough to take the initiative and therefore had to await the

Japanese thrust. But where would it come? Yamamoto had three choices, a move to the south against Australia, a move to the north against Alaska, or finally, an attack in the center against Hawaii or Midway. Each had to be considered.

As Rochefort's team cracked more and more of JN-25b, Yamamoto's objective began to surface. The Japanese referred to their objective as "AF," and although Rochefort was reasonably sure that AF was Midway, he was not sure enough to recommend betting the entire American Pacific Fleet on it. He therefore devised a clever stratagem. Through the reading of Japanese traffic, he knew the Japanese on Wake were monitoring American messages from Midway. Fortunately, the pre-war underwater telegraph cable to Midway was still in operation, so he sent instructions to Midway through the secure cable to broadcast by radio in clear that their water distilling plant had broken down and they were short of water. Sure enough, within forty-eight hours, American intercept stations had intercepted a message from the Japanese advising all commanders that AF was short of water. At least now no American carriers would be off chasing wild geese, but even so, six to three was long odds.

Yet the Americans had an additional, if intangible, advantage in the mind of Admiral Yamamoto. Although a brilliant planner and tactician, his skills were clouded by a tendency toward convoluted and overly complicated plans. If the Americans remained ignorant of his plans, and reacted as expected, his victory was assured, but if they knew, they might be able to take advantage of this situation.

As May drew to a close, Rochefort provided Admiral Nimitz with more and more information gleaned from the circumspect Japanese message traffic. Nimitz now knew that Yamamoto had divided his fleet into three task forces, each powerful in itself, but too far apart for mutual support. He also knew that the two carriers moving against Alaska could be ignored as a feint. His three carriers and his air forces on Midway could therefore be concentrated on Yamamoto's strike force of four carriers operating against Midway. Then, toward the end of May, the Japanese once again changed codes. Too late. The rest is history.

The Problem of Security

The great American victory at Midway would have been impossible without the help of Rochefort and the rest of his team at the Combat Intelligence Center. Washington knew that their continued success was contingent on keeping the Japanese ignorant of their code breaking success, but the very nature of American society and the lack of laws on security made such a job difficult in

the extreme. This was demonstrated when, only a few days after the victory at Midway, the Chicago Tribune published the fact that Nimitz had known the Japanese objective, that the Aleutians operation was a feint, and the Japanese order of battle prior to the action, information that could only have come from signals intelligence. Admiral King hit the roof.

Although the Tribune insisted that its correspondent had written his story without access to secret information, investigation seemed to show that he had seen Nimitz's last message to the fleet, and incorporated it into his story. At first, the Navy favored prosecution. After all, they were not reading the new version of JN-25 introduced just prior to the Midway battle so they had little to lose.

Wiser heads prevailed. A trial would certainly had exposed a great deal of the cryptologic effort, perhaps sufficient to convince the Japanese to shift to an entirely different system. The new version of JN-25 would probably eventually yield to the efforts of Navy cryptanalysis, but if the Japanese shifted to an entirely new system, who could say if it could ever be read. Further, such revelations might have also warned the Germans and put the Enigma effort at risk. The matter died.

Upon examination, there was no certainty that any effort aimed at preventing publication of secret information that depended on coercion of the publisher could have much success. The Constitutional requirement for open trials meant that any trial might result in compromise of secrets, and the guarantee of freedom of the press complicated pre-publication censorship. Therefore, efforts would have to be aimed at not letting those without a need to know get the information in the first place.

The first step was to eliminate cryptanalytical units outside the Army, Navy, and FBI. By July 8th, the President had issued orders stopping such efforts by the Director of Censorship, the Federal Communications Commission, and the Office of Strategic Services.

The next was to tighten ship in the services themselves. On June 20th, Admiral King issued a long instruction to his fleet commanders regarding the security of the radio intelligence effort. King's personal interest was important. His passion for discipline was well known, and his temper legendary. His daughter once described him as "the most even-tempered man in the Navy. He is always in a rage." However, if senior naval officers might concern themselves with King, the same could not be said of more junior personnel to whom King was a distant figure, and by the end of the war there were thousands of them. It was inevitable that some would gossip.

The dissemination system could be made more secure though. Only those with a need to know were made aware of the source of much of the information provided, and those few were restricted almost always to senior commanders and those that actually had to handle the transmission of such material to the commanders involved.

Still, there were constant security violations. Some were the inevitable consequence of the operation itself, such as the Yamamoto shoot down. His route could only have been discerned through radio intelligence, and the risk that the Japanese would put two and two together had to be taken if the operation was to succeed. Fortunately, it did and they did not.

Other violations, particulary those that found their way into the newspapers, were usually the result of individual personnel not keeping their mouths shut, or their documents secured. Serious violations appeared in the Washington Post, Time magazine, and even in the Annual Report of the Pan American Union which not only described in full the interception of radio messages from Axis agents in Latin America but also the deciphered signals themselves.

If all this could happen in wartime, in the midst of a popular war, what were the implications for peace?

Organization and Relationships

With war, the Naval cryptanalytic effort expanded greatly, and the Navy needed new quarters for the effort. In the summer of 1942, it took over Mount Vernon Academy, a prestigious girls finishing school on Nebraska Avenue in northwest Washington (still the home of NAVSECGRU). There, a bevy of civilian intellectuals, large numbers of newly enlisted sailors, both male and female, and regular, reserve, and newly commissioned officers coexisted uneasily in a hothouse atmosphere.

At the same time, certain well connected officers in Washington became convinced that control of the signals intelligence assets should be centralized in Washington. Using their proximity to King to the utmost, they began a power struggle with Rochefort. The outcome was never really in doubt. The cryptanalytical unit in Washington, as well as its outposts in the Pacific, were transferred from a loose relationship with the Office of Naval Intelligence to the firm control of the Office of Naval Communication. Rochefort, brilliant, enigmatic, and manifestly difficult, found himself in command of a floating dry dock training center, with Nimitz' recommendation for a decoration "lost." Yet despite the unsavory methods used by some officers in Washington, and their shabby

treatment of Rochefort, their decision was undoubtedly correct. The war was too large, and the cryptanalytic effort too important, to remain in the hands of that small band of experts who had created it before the war.

In the field, expansion took place at an enormous rate. In July, 1942, the Intelligence Center, Pacific Ocean area, was created at Pearl with Rochefort initially in command. In September, it became a joint Army-Navy intelligence center, and Rochefort's station Hypo divided up. The Combat Intelligence Center section was retained in JICPOA, while Hypo, now named FRUPAC, was placed under the Pacific Fleet. The creation of JICPOA did much to break down the distrust the two services had of each other.

The largest remaining problem was that of distribution. The United States here took a lesson from the British, particularly their practice of having "Special Liaison Units" attached to the staffs of every major overseas commander. The men assigned to these units had the responsibility of receiving intelligence from Bletchley Park in a secure cipher, distributing it to cleared personnel, and ensuring that all security requirements were met. A simple copy of the British system, however, would not do. The American Special Branch was a part of the Army, but in the Pacific, the Navy had a, if not the, major role. Also, Nimitz and MacArthur were two very different personalities.

Nimitz proved receptive. Army Special Branch personnel were attached to the Navy at Pearl. Others were assigned to every major Army command in the Central Pacific and permitted to use both Army and Navy communications channels. Finally, a Special Branch link was employed at FRUPAC. The expansion of Special Branch units and methods throughout the Central Pacific had Nimitz' full endorsement and support. The same could not be said of MacArthur. Although Special Branch personnel did operate in the SWPA, it took the personal order of General Marshall to overcome MacArthur's strong objection to anyone in his command reporting to or controlled by anyone outside his own chain of command.

The Islands Campaign

In mid-1942, unbeknownst to each other, both the Japanese and American high commands were looking at the same area of the world, the Solomon Islands. Japan wished to secure the area in order to protect its major base at Rabaul, and extend its defensive perimeter so that future American carrier raids on the home islands would be made too difficult. On the other hand, the Allies needed the same

area to clear the supply lines to Australia and New Zealand. The two conflicting objectives would meet on the island of Guadalcanal.

At this point in the war, JN-25b was still a mystery to the Allies. Such a development had been anticipated years prior to the war when Naval cryptanalysts had foreseen at least temporary periods of blindness each time the enemy changed codes. They had therefore made great efforts in devising methods of traffic analysis and high frequency direction finding (HFDF) to gather intelligence. HFDF stations had been established not only throughout the Pacific, but also along the west coast of the United States, as far north as Alaska and the Aleutians to as far south as San Diego. All this, coupled with reports of Australian Coast Watchers, and the Navy's continuing ability to read lower level codes and ciphers, gave the Allies a pretty good picture of Japanese intentions.

An examination of one month, July, 1942, gives some idea of just how good this information could be. By the beginning of the month, signal intelligence was reporting a marked increase in Japanese activity in the Solomons. On the second, fifteen warships had been identified, and on the third, the allies knew that a landing force and two cruiser divisions were earmarked for the operation. By the eleventh, the allies knew that the commanders of two Japanese fleets were in the area, and that the carriers would not be included in the operation.

This information galvanized the allies into action and the Marines landed on Guadalcanal before the Japanese could fortify the beaches. Throughout the long battle for the island, traffic analysis continued to provide vital intelligence. If it was not of the same quality that could have been obtained from decryption of messages themselves, it was nonetheless a vital factor in the eventual victory.

Guadalcanal became the home of the Marine Corps' 1st and 2nd Radio Intelligence platoons. Formed and deployed at the end of 1943, they were to be part of Marine division and corps signal companies and have the missions of intercepting Japanese military and naval communications, conducting RDF operations, and monitoring friendly communications to ensure security.

Unfortunately, when they arrived at Guadacanal, no one was quite sure how to use them, and they received no taskings relating to Marine tactical intelligence. They therefore decided upon their own missions and forwarded the results directly to Pearl Harbor. The 3rd through 6th platoons deployed to the Central Pacific and were better used.

Many of the platoons participated in amphibious assaults. The 2nd Platoon suffered thirty per cent casualties on Pelieu and was

disbanded. The 1st participated in the assaults on Guam and Iwo Jima. The 3rd Platoon was in on the battle on Okinowa, and the 6th on Saipan and Tinian.

In the Southwest Pacific Theater, the Navy began with a nucleus of cryptologic persponnel rescued from Corregidor in the Philippines. The listening post there had been established well before the war. When, in April of 1942, it became obvious that the Philippines would fall to the Japanese, the Navy evacuated the small radio intelligence detachment by submarine to Java and then to Australia where, in cooperation with the Australian radio intelligence effort, they supported MacArthur.

One cannot discuss signals intelligence in the Southwest Pacific without some examination of the theater commander, General Douglas MacArthur. Brilliant, imaginative, and personally brave (he had won two Distinguished Service Crosses and seven Silver Stars in World War I), he was also vain to a fault, did not like information that contradicted his already formed opinions, and surrounded himself with sycophants. Indeed, at one meeting when MacArthur disagreed with General Marshall and began with the words, "My staff says," General Marshall exploded with the statement, "You don't have a staff, General, you have a court."

Such was the case of his intelligence officer, Colonel Charles Willoughby. Intensely loyal to his chief, he was just as opinionated and resentful of "interference." He also had the distressing tendency to produce intelligence based on what MacArthur wanted to hear.

MacArthur also avoided integrating his signals intelligence assets. He kept the Army signals intelligence unit under his own control and refused to combine it with the Naval sigint unit, which remained subordinate to the Navy. Coordination between the two was bedeviled by Army-Navy friction which grew, rather than diminished, as the years went by.

Nonetheless, SIGINT continued to provide superb information to commanders. At Tarawa, for example, SIGINT provided precise information on enemy order of battle, their logistical status, and many other details, although it could not inform assault troops the exact outline of the enemy defense and the Marines still had to take the island one pillbox at a time.

The decision to attack Kwajalein was a direct consequence of Ultra information. Shocked by the casualties at Tarawa, Nimitz' staff was unanimous in recommending attacks on Kwajalein's outlying islands prior to an assault on Kwajalein itself. Ultra had informed Nimitz, however, that the Japanese, in anticipation of such a move, had shifted forces from Kwajalein to those same outlying islands. He

thus overruled the strong objections of Halsey and Turner and named Kwajalein as his objective. It was taken in a few days with less than 2,000 casualties.

As the war went on, the cryptanalysists had more and more success. From March, 1943 through early 1944, the Japanese Army code was gradually broken and more and more traffic could be read. The Japanese Empire, so quickly expanded in early 1942 was clearly on the verge of extinction.

Sinking the Japanese Merchant Fleet

The enormous expansion of the Japanese empire in 1942 over the vast Pacific meant that maintenance of that empire would be highly dependant on the ability of its merchant fleet to resupply and reinforce its far flung garrisons. For the American submarine fleet, this meant a plethora of targets. Yet, in the first year of the war, the American submarine fleet proved unable to hurt severely the Japanese merchant fleet. Some American commanders proved insufficiently aggressive. Pre-war training had not accurately portrayed what experience showed to be actual tactical situations, and some American commanders proved slow to adapt. The ineffectiveness of American torpedoes, and the lengthy period it took to convince the Bureau of Ordnance that they were faulty and to get the design corrected was scandalous. Finally, the Japanese merchant ship code remained unbroken until 1943.

Then, in that year, everything came together. Commanders had learned their trade or been replaced, new torpedoes had reached the fleet, and the Japanese had been forced to adopt the convoy system. Japanese convoy procedures required substantial use of radio communications, including daily position reports, which could now be read by the Americans, and this information began to be passed to the submarine fleet, despite the fact that such information pointed directly to SIGINT sources. Submarine commanders found they received not only the number of ships in a given convoy, and often their names and cargos and number and type of escorts, but even the convoy's exact noon position for some or all of its voyage.

By 1944, American submarines had been equipped with both radar and new torpedoes, and their attacks became so effective that despair began to infect the Japanese. As their empire contracted, so it became easier for the submarines to find and finish their enemy. The Japanese had to abandon most of their convoy routes and leave thousands of soldiers on bypassed islands where they slowly starved. On the home islands, oil stocks had been cut ninety per cent. Japan, which had started the war with some six million tons of merchant

shipping, saw nearly five million at the bottom of the ocean by the end of the war.

Support to the China-Burma-India Theater

The Navy had established a listening post in China well before the war, specifically in Shanghai, and when war came to the United States, its efforts expanded many-fold. Beginning with a weather service established in Japanese held territory, it expanded into the provision of coastal intelligence. China provided guerrilla forces to protect the Americans.

In 1943, the two governments established the Sino-American Cooperative Organization (SACO) which set up weather, communications, and intelligence stations from Indo-China to the Gobi Desert, concentrating on the area along the China Coast behind Japanese lines of communication. Besides supporting the American submarine campaign, they also provided critical information to the 14th Air Force.

SACO rapidly branched out into direct combat operations as the Chinese guerillas, with American training and logistical support, attacked Japanese columns, lines of communications, and logistical points all over their areas of operations.

End Game in the Pacific

As Nimitz drove on the Japanese in the center, so MacArthur drove from the south. There, the Japanese base of Rabaul stood defiant. But from the Ultra intercepts, it was obvious that Rabaul's condition was grave, and by early March, 1944, it was no longer worth the blood and treasure necessary to take it. Therefore, Marshall and the Joint Chiefs ordered MacArthur to bypass it and establish a forward base at Hollandia.

To planners examining Hollandia, it seemed obvious that the area around the airstrip and harbor would be the heaviest defended, but Ultra revealed that the Japanese had decided to stand nearer MacArthur's lines. Thus MacArthur decided to feint where the enemy expected him and to move directly on Hollandia.

The capture of Hollandia resulted in the cut off of some 18,000 Japanese troops, but the Japanese resolved to fight rather than give in. Ultra now provided the date and details of the Japanese attack, including the locations of the Army command post and rear echelons. The attacks were broken with the loss of 9,000 Japanese killed.

As the days followed, SIGINT began to provide more and more information. When the Japanese began to shift troops from China to New Guinea, Ultra told when and where to attack. In the "Great

Marianas Turkey Shoot," an American fluent in Japanese listened in on the Japanese Master Pilot and gave real time intelligence to American air controllers. When the attack on the Pelieus took place, commanders and staffs knew all the details of the garrison on the main and outlying islands.

By this time, Ultra was just one, if the most important, of intelligence sources, and it was the integration of information gained from captured document, aerial photography, direction finding, traffic analysis, and prisoner interrogation, as well as Ultra, that provided the intelligence picture. By summer of 1944, when the planning for the invasion of the Philippines was underway, the Japanese Order of Battle was scrutinized by the Army staff, in Washington by the Military Intelligence Service, and at Pearl by the Joint Intelligence Center.

No convoy could sail without the Americans knowing its content and destination, nor could any large military unit keep its moves secret. When MacArthur issued his final invasion plan, the location, strengths, and condition of the troops of the 224,000 troops of the Japanese Fourteenth Army in the Philippines were known with some precision.

But despite MacArthur's superb use of Ultra on the strategic level, his headquarters proved less than that in giving the information to commanders on the scene. When Admiral Mitchner brought his carriers down to provide additional air cover for the Hollandia operation, he found it impossible to pry from Army channels information of Japanese strength. In the Philippines, General Eichelberger, perhaps MacArthur's best field commander, kept himself informed on Ultra by using Navy sources. In short, MacArthur's staff mirrored MacArthur's concern with control and the assignment of credit. MacArthur's genius made up for these faults, but the same could not be said for his staff.

Ultra and other SIGINT continued to provide information as the Army and Marines drove toward the home islands. The final contribution of Ultra in the Pacific dealt with the decision to use the Atomic Bomb. Separating Army from Navy contributions here is almost impossible. Both services intercepted and translated a great deal of traffic, and it was the combined use that gave allied commanders, including the President, insight into the Japanese mind.

American intelligence soon knew several things. It knew that the air offensive against Japan had not impaired morale to the point that it would accept the Allied terms, for the Army was clearly preparing for a fight to the finish. Intelligence derived from Japanese Army intercepts indicated some thirty-six divisions and over two million

men readying themselves for the final battle. Decrypts of diplomatic traffic showed that the Russians were not about to help Japan reach a negotiated peace. In retrospect, the decision to drop the bomb seems inevitable.

Conclusions

That Magic and Ultra made a vast contribution to victory in the Pacific is beyond dispute. But some caveats remain. All the decrypts and other signals intelligence could provide was information. It still took courage and skill on the part of the soldiers, sailors, and marines, and the leadership of Nimitz, Spruance, Halsey, Turner, and yes, MacArthur to win the battles and the war. Further, the war demonstrated the necessity of joint operations. The lingering animosity that predated the war between the Army and Navy had, particularly in MacArthur's headquarters, made military operations less efficient and probably cost the lives of some American servicemen. Any post war SIGINT organization would have to take this into account.

The Battle of the Atlantic

The war in the European theater differed greatly from that in the Pacific for it was primarily a land war in which control of the seas, while necessary for an Allied victory, would not in itself lead to the defeat of Germany. In the Atlantic there would be no great carrier battles, nor major fleet engagements. Nor could signals intelligence be as quite as vital as in the Pacific, for other forms of communication were available to the Germans, such as land line, which were not susceptible to intercept. While the Germans depended on radio during much of the war, particulary in Russia, as they were forced back, they increased utilization of land line communication, and decryption became less productive.

Further, other intelligence gathering assets, such as aerial photography and agents, could be better employed on the Continent that in the vast reaches of the Pacific, so signals intelligence was bound to be of somewhat less overall value that it was in the early days of the Pacific war. This is not to denigrate the importance of decryption in the West, simply to put it into perspective. It was still a vital tool.

The Germans, unlike the Japanese, did not use a code. Instead they relied on a cipher machine, known as Enigma. Using three rotors and a patch board, it was capable of some three hundred million possible combinations. In the days before computers, the Germans felt their machine secure. It was not. Beginning in 1940, the British,

building on earlier Polish and French analysis, had begun to read at least some Enigma signals, labeling the result "Ultra."

In one area, Ultra was essential, and that was the war against the U-boats. Far at sea, no land lines were available to them, and their "wolf-pack" tactics depended on control from land. And in the spring of 1942, the U-boats were running wild.

The British had already lost eight million tons of shipping. Now it was America's turn.

Hitler's declaration of war against the United States was quickly followed by Operation Drumbeat in which Admiral Donitz sent his U-boats against the huge numbers of American ships operating off the East Coast of the United States.

The U. S. Navy, traumatized by the losses at Pearl Harbor, and with its attention riveted on the Pacific, was slow to react. From January to April, U. S. merchant shipping losses off the east coast averaged 100,000 tons per month. The United States Navy, after much prodding by the British, took corrective action, blacking out coastal cities and adopting the convoy system. However, their most important action was the close cooperation established between the two navies. The Americans quickly set up an Atlantic Section, Operational Intelligence. Its Chief, Commander K. A. Knowles was soon in London consulting with his British counterpart. The British kept the American continuously informed throughout the war, and daily exchanged Ultra information. The two tracking rooms even had a direct signal link on which the chiefs and their deputies could communicate.

But the heart of the operation was the ability to read German submarine traffic, the "Hydra" cipher, and this had been lost when the German submarines in the Atlantic adopted a new cipher, "Tryton," in February of 1942. Although other ciphers, particularly Hydra, which still indicated when submarines left or returned from patrol, and "Tetis," used in the Baltic, continued to be read, and provided much information on the strategic level, tactical messages from submarines in the Atlantic were now a mystery.

To make matters worse, the Germans had broken the "BAMS" (British and Allied Merchant Shipping) code. By the end of the year, the allies had lost an additional eight millions tons of shipping in the Atlantic. In retrospect, there is little question why the German submariners called this period "the happy time."

Despite the allied inability to read the Tryton cipher, they were not without signal intelligence. As mentioned above, Hydra and Tetis continued to provide important information, and, thanks to Commander Laurence Safford's work before the U. S. entry into the

war, the United States Navy possessed a string of high frequency direction finders along the Atlantic Coast. Stations reported their bearings to the control center in Maryland which sent them on to the naval signals intelligence station at Nebraska Avenue where Commander Knight McMahon and his staff processed them, turned them into fixes, and sent the result on to the Intelligence Section's Atlantic Division.

The system could react with incredible speed. On the morning of July 30, 1942, U-158 went on the air to report to Donitz that he had nothing to report (Donitz encouraged his commanders to communicate and thus their communications discipline was very poor). The signal was heard by four DF stations and flashed to McMahon. Within minutes, McMahon had the U-158's position. Within a few more, this information had reached Lt. Richard E. Schreder, a naval aviator in the air flying an anti-submarine patrol out of Bermuda. Ten miles from the reported location he found the sub loafing on the surface and sunk it with a depth bomb onto its superstructure as it tried to dive away.

The system got even better as the war went on. In 1944, DF readings and the resultant harassment by American ships vectored to her position kept the U-66 from its rendezvous with a resupply submarine. When it reported its plight in a burst transmission of less than fifteen seconds, a remarkable twenty-six different stations got its bearing. Three hours later, the sub was spotted visually by an American plane, and a hour later sunk by an American ship.

Although DF provided great assistance, it was fortunate that in December, 1942, months of effort enabled the allies to make their first inroads into the Tryton cipher. Not only did this allow the allies to read German U-boat tactical communications, it also gave the first overt indications that the Germans were reading the BAMS code. But it took until June before new code books could be distributed, and in the meantime, the German assault continued.

The opening months of 1943 were a savage time. After a decline in January, German sinking of allied shipping began to climb once again. In March, by reading BAMS, Donitz was able to send forty U-boats against two convoys. Slaughter resulted with over fifty ships lost. On top of this, on March 8th, the Germans had ordered the activation of the new Enigma machines with four rotors each. The fate of Britain hung in the balance.

Then, in only a few weeks, the tide turned. The new 10cm radar sets came on-line against which the Germans had no warning system. Escort carriers were quickly sent to the Atlantic, and long range aircraft patrols reinforced, as was Coastal Command. and the escorts

improved their capabilities remarkably. Perhaps most importantly, the four rotor system proved remarkably easy to crack and Ultra flowed again. With Ultra providing both Donitz' orders to the wolf packs and their responses, the other weapons in the allied arsenal could be used most effectively. At the end of March, the allies despaired, but by May, it was the German submarine fleet which withdrew, shattered and licking its wounds. Over fifty of its boats had been sunk. Never again would allied communication with Britain be in danger.

THE NATIONAL SECURITY AGENCY

With the Japanese surrender, the huge signals intelligence force that the United States had built up during the war faced major reductions. Best placed to withstand the cuts was the Army for the Navy had given up all interest in anything but specifically naval traffic and codes during the war in order to concentrate on the defeat of Japan. The Army was loathe to readmit the Navy into what it now considered its business. Nonetheless, the two services worked out a compromise.

Coordination between the two services dated back before the war, but that had largely been the result of the personal relationships established by the few Army and Navy officers who were interested in the arcane field. Formal efforts at coordination were somewhat erratic until 1944 when an informal Army-Navy Intelligence Coordinating Committee was established, This became the formal Army-Navy Communications Intelligence Board in March of 1945.

Other agencies sought admission. The State Department had established its own office to handle the flow of cryptologic intelligence into the department, so in December of 1945, it joined and its name was added to the title. Next to join was the FBI and the new Central Intelligence Agency, followed by the newly organized separate Air Force. The expanded group was known as the United States Communications Intelligence Board (USCIB).

On July 1, 1948, the USCIB promulgated the first charter for the communications intelligence community. Although the charter, National Security Council Intelligence Direction No. 9, did provide a basic framework, it proved a flawed instrument. Its most important flaw was that it required the unanimous consent of its twelve members (two from each agency represented) for any decision, and that it was specifically prohibited from interfering in the internal working of each communications intelligence agency.

Thus, the USCIB was little more than a clearing house for information, and the communications intelligence community was as fractionalized as it had ever been. The Army was generally in favor of some consolidation since it still controlled the bulk of the communications intelligence assets, had the most experience with its non-military aspects, and could therefore expect to dominate such an organization. The Navy, for the same reason, was opposed, as was the newly independent Air Force that wished only to be left alone to set up its own network of listening posts.

In August, 1948, the Secretary of Defense, James V. Forrestal, created a board, under the Chairmanship of Rear Admiral Earl

Everett Stone, then Director of Naval Communications, to study the matter. Made up of representatives of the three services, the Stone board could not reach agreement and submitted a divided report, the Army favoring consolidation, and the Air Force and Navy opposed.

Forrestal's successor, Louis A. Johnson, brought in General Joseph McNarney to resolve the problem. McNarney compromised with a plan that called for a merger, but left the three services' communications intelligence organizations intact. On May 20, 1949, Secretary Johnson issued a directive that established the Armed Forces Security Agency (AFSA) and its governing board, the Armed Forces Security Agency Council (AFSAC) made up of the service representatives from the old USCIB plus an additional member from each service. The appointment of the Director brought total membership to ten. Nothing much had changed. The three services dominated the AFSAC, and the AFSAC required unanimous agreement to do anything important. The services continued to go their own ways.

All this could have been tolerated if the intelligence product had been satisfactory, but it was not. The largest problem was the disconnect between the USCIB target list, and the service agencies responsible for collection. Although the USCIB could and did decide on targets, and provide those targets to the AFSA, targets identified were overly broad and did not convert intelligence needs into clear communications intelligence targets. This failure was highlighted by the outbreak of the Korean war, for despite the fact that the CIA considered Korea the fifth most volatile area of the world, this was not communicated to AFSA through the USCIB's intelligence requirements list.

The Establishment of NSA

The Korean war brought major changes to AFSA. Targeting improved, and the Agency more than doubled in size. However, AFSA spent most of the early days of the war, when intelligence was vitally needed, playing catch up. Disappointment over its performance led President Truman to establish another committee, this time chaired by George A. Brownell, to find a fix for AFSA's problems.

The Brownell Committee interviewed forty-three witnesses and dove deeper into the secret world of communications intelligence than had ever been done before. In its report, issued on June 13, 1952, the committee blamed the services and the Joint Chiefs for the mess, and specifically damned the unanimity rule of AFSAC. Its proposals for a fix were complicated but effective. It proposed taking the agency away from the Joint Chiefs, and giving it to Secretary of Defense. It increased the authority of the director of the AFSA and abolished the AFSAC while increasing the power of the USCIB, but revoking the rule of unanimity. Further, the new USCIB would not include service representatives but would be composed of one member each from Defense, State, and the FBI, the Director of the AFSA, and the Chairman of the Joint Intelligence Committee of the JCS. A vote of four of the five members would be binding, but any dissenting member could file an appeal to a Special Committee whose determination would be final.

The recommendations placed far greater authority in the hands of the Director of AFSA who now had the authority to manage the collection effort. It also broke the strangle hold of the services on communications intelligence and permitted civilian users, such as State and the FBI, to have a say.

On October 24, 1952, President Truman signed a directive that incorporated the Brownell Committee's recommendations, with one major exception. In accordance with its new orientation, the organization had a new name, the National Security Agency.

Both Rochefort and Safford lived to see their fascination with codes and ciphers provide not only the successes of the war, but also to see the organizations that became the National Security Agency. Today the Navy cryptologic community is part of both the Navy and the National Security Agency. The huge NSA complex sprawls across the grounds at Fort Meade, Maryland, and its operations, personnel, and budget are known only to those who need to know. Yet it traces its ancestry back directly to the few pencil and paper cryptanalysts who labored in the twenties and thirties to prepare for

a war that might never come. Perhaps their true epitaph might be, "They also serve who stand and think."