Raising the Intelligence Bar Far, Far Too High: The Bombes and the U-Boat War

INTRODUCTION

Once upon a time not too long ago historians wrote about America's code breaking past with awe and, in some cases, near reverence.[1] However, historians have recently become sharply critical of America's codebreakers and the nation's communications eavesdroppers. They, as well as contemporary commentators, have faulted the National Security Agency and its predecessors for a long string of failures. Not predicting the onset of the Korean War, not providing convincing warnings of the attempted seizure of the Suez Canal, failing to read high-level Soviet code systems during critical years of the Cold War, not identifying Soviet missile shipments to Cuba, and 'illegally' eavesdropping on innocent Americans are a few of the items on the expanding lists. The critics direct their most intense criticisms at the alleged recent crypto failures of what they picture as the overly bureaucratic and internally insecure post-1990 National Security Agency that emerged from its Dark Ages of the 1950s and 1960s to become a giant with thousands of employees and budgets in the billions of dollars. NSA's new judges have expected the agency to able to warn of the 9/11 attack, to provide the information necessary for the capture of terrorists such Osama Bin Laden, and, to do it all without endangering civil liberties.[2]

Behind the criticisms lie historical benchmarks used as standards to evaluate the National Security Agency of the 1950s to the present. The most frequently applied standard is a Golden Age of achievements by America's codebreakers during World War II. Recently, Matthew Aid has added accomplishments during the immediate post World War II years. He drew a scenario of a handful of beleaguered postwar cryptologists solving major Soviet encryption systems while also beginning to read the seemingly unbreakable one-time-pad Venona encrypted messages about Soviet espionage during the 1930s and 1940s.[3]

Especially important to setting a standard of achievement for the Twenty-first Century is the accepted history of successes against the German's World War II "Shark" Atlantic submarine Enigma-based encoded communications system. In its outlines, the American Shark story is near miraculous. According to it, in 1942, after England's codebreakers were stymied, a few graduate students from the Massachusetts Institute of Technology, and a shop-floor experienced engineer at the National Cash Register Company in Ohio, trumped the British and hurriedly built a machine, the four-wheel Bombe, that cracked open the German submariner's Enigma system. Moreover, according to the story, the American Navy cobbled together in a few months the hundreds of people needed to turn the Bombe's output into useful intelligence. Significantly, the navy pictured the results as spectacular: the American effort prevented more German Atlantic onslaughts, albeit with some aid from the British codebreakers.[4]

The inherited Shark chronicle is more than the product of popular imagination or patriotic cultural memory. The American intelligence community has supported it since the outlines of the Bombe-Ultra Secret story were first revealed. In fact, the American Navy's official classified histories written in the 1940s and early 1950s laid the foundations for it.[5]

Although the National Security Agency might have responded to its recent detractors by citing such things as its amazing Cold War successes in monitoring Soviet missile capabilities, its public releases have continued to focus on World War II's achievements like the Shark - Bombe stories and, to a degree, the Venona struggle.[6] Putting the spotlight on the 1940s is partly a result of having to protect "methods and sources" connected to more recent times. Revealing recent triumphs might endanger on-going work and methods and, perhaps, people.

As well, Freedom of Information Act legal mandates usually allow the release to the public of NSA's sensitive archival materials only from the beginnings of American radio eavesdropping in the early Twentieth Century to the end of the war against the Axis powers.

However, there are other reasons for spotlighting the achievements of the era of World War II. For one, the American communications-intelligence agencies of the late 1930s and early 1940s were small and had identifiable leaders who could assume heroic roles. It was a time of human-scale code breaking. As well as the Shark adventure, the army's charismatic William Freidman and his handful of young mathematician apprentices conquered Japan's advanced diplomatic Purple cipher machine while the navy's badly injured Agnes Driscoll and her small team of devoted helpers unraveled Japan's high-level naval codes. In addition, a similarly beleaguered army group solved an 'unsolvable' German one-time-pad system while a tiny band in the American Coast Guard penetrated the Swiss Navy's Enigma.[7]

Drama, almost pathos, was important to the great stories. All the achievements came at great personal cost. Friedman and some navy code men[8] had emotional breakdowns because of stress. Driscoll worked despite intense physical pain; the navy's Joseph Wenger had a collapse because of the pressures; and, the American Bombe's designer, Joe Desch, had to retreat to weeks of calming isolation on a friend's farm to compensate for the ethical conflicts he endured because of his devising machines that 'killed'.[9] Such sacrifices were not wasted. There undoubtedly were American heroes and heroic achievements during the 1930s and World War II; and, the work of the men and women codebreakers made major contributions to winning the war, as well as helping to shape immediate postwar defense policies.

However, in some instances, historians have exaggerated the achievements and, as a consequence, many observers have underestimated the difficulties of modern cipher breaking and signals intelligence. As a result, the Golden Age interpretation has backfired. It has worked against the American codebreakers and communications-interceptors of today. It would be extremely difficult for them to provide satisfactory answers if they were asked: How could so few in the 1930s and 1940s have done so much with so little when you have done so little with so much?

This article, based on new analyses of primary documents and data, demonstrates that in one critical episode, the American's code breaking Battle of the Atlantic, the Golden Age benchmark is untenable. The histories of the American Navy's World War II Atlantic crypto-accomplishments have unintentionally raised the intelligence 'achievement bar' far, far too high. Admittedly, there were then few people and resources, but not as much was accomplished as commonly thought—there could not have been. Successful intelligence gathering then, as well as now, was a tough, on-going, and resource-hungry activity and there have never been overnight miracles. The inherited views of the building of the American Bombes and of the military consequences of reading Shark during World War II are examples of unintended myth-making.

The Atlantic Problem Ignored, Then Sidetracked

The United States Navy's small radio intelligence branch, OP20G, and its code breaking staff had paid little attention to German naval problems during the 1930s. Japan was its target. It was not until the last years of the decade that the beginnings of an intercept capability were established; and it was only in late 1940 that a team was put together under the ailing chief cryptanalyst Agnes Driscoll to attempt to understand and decode the German naval traffic that was finally (but partially) being picked-up by the navy's few listening stations. At the time, there had been no critical American captures of documents about the German systems and there was no knowledge of, or cooperation with, the British codebreakers despite America's growing support of England's convoys on the Atlantic.[10] The small American team began its work 'flying-blind' with only a rudimentary knowledge of a very simple and non-military version of the Enigma device, thinking that might be what the German Navy was using to encrypt its messages. Importantly, Driscoll and her helpers had few insights into the German's messaging procedures. Even after the British informed the Americans of the complex nature of the Enigma encryption machine used by the German Navy, the optimistic, and perhaps hubris-filled, American group assumed that traditional types of attacks, ones that that had worked on other rotor-based enciphering systems, would soon be capable of penetrating the Atlantic Enigma.[11] Central to such traditional methods was a "catalog-crib" attack. Driscoll believed that after statistical analyses of messages revealed the nature of the encryption wheels used in the German naval Enigma her team could identify all the inner workings of the Atlantic machine. After that, she could compile a book-form model of the machine's cycles and settings. Using that set of books and a commonly used short crib-word in a message (a suspected word) analysts could trace through to the possible choices of the encryption wheels and their settings for any transmissions. Then, they could use a paper imitation of the machine to decrypt the intercepted messages.[12]

After a year's work on the problem, there was little or no thought of advanced technology being required or helpful, although at the time the American Navy's OP20G was involved in a program to develop advanced machines for other code and cipher problems.[13] Significantly, after deeper but reluctant collaboration with Britain's codebreakers began in early 1941, and when England's cryptanalysis started sharing what they knew about the German systems, Driscoll stood by her paper-catalog approach.[14] She and her superior Laurance Safford were so committed to an independent American solution that in the summer of 1941 Driscoll turned-down an offer of all the details of England's newest and vital electro-mechanical machines, the Enigma-cracking Bombes; and, she hesitated about employing other methods used by Britain's top naval code breaker Alan Turing.[15] Driscoll did not even want the British to send her one of their Bombes, she just wanted a copy of a working naval Enigma machine so that she could complete her catalog and put into operation a unique American solution that did not require complex 'cribs', captures of documents, or expensive machinery. She claimed that with just twenty-five people, and her "catalog" method she could find Atlantic Enigma settings within two days.

That singular commitment to a purely American solution, one that was to be free of the need for captured documents and near impossible-to-find long 'cribs', continued through 1941 and much of 1942 despite warnings about its weaknesses from experts such as Alan Turing.[16] Her stubbornness meant that Driscoll spent almost a year on what became a relatively unimportant method. Her catalog attack could not be the basis for a full assault on the naval Enigma. Nevertheless, Driscoll's laboriously hand-built catalog grew to almost one million pages bound in 17,200 volumes.[17] She remained so sure of her approach that the navy had to prod her team into thinking about automating the laborious searching required by her method.[18]

Although the British sent much additional technical information and methodological advice, the Driscoll catalog was not ready to contribute in any way in early 1942 when the German U-boats were rampaging through Atlantic convoys, even sinking freighters in sight of the American coast and when the Allies feared the British Bombe attack had permanently failed. Later, after more years of additional work, including many modifications to meet changes in the Shark Enigma, the labor-intensive catalog proved of secondary worth. It was helpful as only one method of speeding the last stage of the identification of the settings of the naval encryption device. Although the British accepted America's help in building its own huge catalog, the British Bombes soon proved themselves a necessity for unraveling the Enigma settings.

Driscoll and her group may have gloated and uttered a 'we-told-you-so' when a change in the Enigma system and communications procedures used by the Atlantic U-boats (the newest Shark system) made the British 'Enigma blind' for the first ten months of 1942.[19] Their existing type of Bombes could not then overcome the changes and they could not keep supplying the American navy with intercept information about the disposition of enemy forces on the Atlantic. The allies had to rely on the still underdeveloped American and British radio direction-finding systems[20] and the bits and pieces coming from England's ability to read some secondary U-boat and other naval systems. None of that was sufficient and there was a deep sense of anxiety among many in the American Navy. The continuing recriminations about OP20G's failure to warn of the surprise Japanese attack on Pearl Harbor in December 1941, and a wrenching and emotionally draining reorganization and re-shuffling of the top leadership in the American Navy's crypto-agency worsened the situation.[21]

In 1942, OP20G's leadership was under great pressure, something that complicated the relationship with the more experienced British codebreakers. Emotions ran high and there were misunderstandings. Unfounded accusations against the British caused severe strains. A first contention was that England had withheld information vital the Driscoll's work.[22] Later, there was a claim that the British were intent on preventing America from developing its own version of a Bombe for Shark, despite England's seeming inability to fulfill its pledge to build enough of their advanced Four Wheel Bombes that were needed to allow re-entry into the post-1941 U-boat Shark encryption system.[23]

Troubles Building the American Bombe

High Hopes

With the reshuffling of people in Washington in early 1942, OP20G took a friendlier approach to the British.[24] In addition, 'G's' new administrators faced-up to the lack of progress by Driscoll's team. They assigned her an advisor while establishing a separate group that was to explore the possible development and use of an American version of the Bombe. Soon, it and other new groups necessary for the Bombe's cryptology began taking full charge of the American side of the U-boat problem. They sidelined Agnes Driscoll. As well, the British were now completely willing to show and share all with the Americans and to allow them to do research on a new anti-Shark Bombe. The British were ready to give the Americans free-reign as long as they did not try to establish their own independent attack on the system, one that might prove a security danger to the British efforts against Axis army and air force, as well as navy, targets. They also informed the Americans that their own technicians had made some breakthroughs and would soon have a sufficient number of the new Bombes, enough to handle the Shark problem.

So, in late spring 1942, the American Navy decided to send another team to England to find out more about the Bombes and Atlantic-related cryptanalytic methods. In addition, although the navy allowed Driscoll to continue-on with her catalog building,[25] it added a small group of bright young mathematically trained reservists to OP20G's new research section in Washington.[26] One of their assignments was to proceed with an exploration of the possibilities of a radically new version of the Bombe, one based purely on electronics. Although not experienced codebreakers, they and others in the section also investigated additional alternatives to the British Bombe methods. That included a search for an attack based upon advanced 'statistical' methods (and allied machines), that did not require the hard-to-find 'cribs'.

However, the search for a new and purely American 'statistical' method for the Shark problem stalled. As well, the politically sensitive research-only agreement with the British did not last long. Lingering distrust among OP20G's old-guard towards the navy's historic competitor, England, and the continuing inability of the British to speedily read any Shark messages, moved OP20G towards developing its own operational, not just research, Bombe. By late spring 1942, the navy launched an initiative to develop the first American version, one based on the cutting-edge electronics the young engineers had been exploring. A group of graduate students from MIT was shifted from working on their long-term project for special machines for Japanese and diplomatic targets. Then, an experienced electrical engineer at the National Cash Register Company in Dayton, Ohio, who had been helping with the manufacture of those devices, agreed to begin to explore the practical manufacturing requirements for an American Bombe to defeat Shark.[27]

By early summer 1942, the navy approved tentative production plans. A large building in Dayton became the secret and highly guarded preserve of the American Bombe design team. Soon, the Dayton engineer, Joseph Desch, concluded that the more tried-and-true electro-mechanical technologies, and established British methods, were the only viable options. Although the British continued to pass on all the technical details of their machines and techniques, they were quite unhappy when they learned that the Americans were moving towards breaking the research-only pledge. In turn, the resurgence of U-boat successes against the Atlantic convoys severely frightened the Americans.[28]

Then, in September 1942, the American navy's code men asked for a vast amount of money as they made some very grand promises: 'give us $26,000,000 (2009 dollars) and by January 1943 we will begin delivering one new advanced Bombe each day'. By the end of the year, they pledged, there would be one Bombe for each Shark wheel combination. Some 360 of the giant machines would allow reading the U-boat messages within a few hours, as precious time would not have to be wasted changing the basic setups of the machines needed to find each day's primary Enigma settings.[29]

Despite a caution in the American proposal stating the Bombe attack was so fragile that a change in German procedures would emasculate it and that a new pure and undefeatable "statistical" attack did need to be developed, the navy granted OP20G the funds. There was one request the navy did not fulfill, however. OP20G had asked for a large contingent of sailors to run the Bombes once they were in operation. The navy's hierarchy replied that it would only allocate a few engineers and told OP20G to plan on using personnel from the navy's new female branch, the WAVES.[30]

Using information on the British Bombes forwarded from England to Washington and then to Dayton, Joe Desch honed his unique tentative design.[31] He hired subcontractors; set up a super-secure manufacturing center in one of his company's isolated buildings; and the navy explored establishing a Bombe-intelligence operations center in an old summer-camp and amusement park on a river near Dayton. He then asked the navy to plan to have the few sailors who would maintain and operate the machines sent to him before January so they could be trained and ready as soon as the devices started to roll-off the assembly line as 1943 began.[32]

The British reluctantly, but graciously, acquiesced to the Dayton project, even sending Alan Turing to give advice, while hoping the Americans would not launch an uncontrolled

Atlantic crypto-attack once the machines were ready.[33] Meanwhile, in Washington, navy men began learning how to deal with the German messages, readying themselves for a possible full American effort against the Shark system, and preparing to help the British if-and-when they regained a reliable foothold against the U-boat traffic, hopefully one that was not fully dependent on mistakes by the Germans.

However, the men at OP20G believed they could trump the seemingly stalled British Bombe effort and save the convoy system from the coming spring 1943 onslaught. They hoped to make-up for the debacle at Pearl Harbor; for the navy's failures against the devastating U-boat attacks along the American coast in early 1942; and, for the millions of tons of shipping that were lost in the Atlantic during the rest of the year. In addition, they hoped their new Enigma accomplishments would allow more than the diversion of convoys away for U-boat locations—finally, the Allies could go on the offensive against the German undersea fleet.

There was a chance that an American crypto-Golden Age was to begin. However, it did not. The intelligence battle was difficult then, just as it is today. Much devoted effort by intelligent people and a great deal of money failed to produce a crypto-miracle in the early 1940s.

Goals Set to High, A Bombe Too Late

To great frustration and embarrassment, the project in Dayton became mired-down in technical problems; no "Analytical Machine #10" device was anywhere close to being ready at the beginning of 1943, nor in the spring as the Allies' Atlantic convoys endured horrible months. England's optimism about overcoming its difficulties with its two different new four-wheel Bombe designs did not provide much solace to the American Navy. Then, hearing that functional first models of each of England's versions were near completion, and, later, that England had already made some significant inroads into Shark without them, was not an ego-satisfying bit of information to the American Bombe team.[34] Nevertheless, the navy pressed ahead, giving even more money and highest-priority resources to the men in Dayton.[35]

The money was not enough. In March 1943, Desch's crew had just two breadboard models of their Bombe. In May, only two rather primitive test models were ready. Learning that England's newest devices were again having unexpected problems saved some engineering pride in Dayton. However, Britain's frustrations created greater pressures on Desch and his men to surmount their many technical difficulties. When the Americans learned that a new German communications procedure that eliminated sending some Shark messages on a 'readable' system would probably end Britain's tenuous early 1943 hold on the submarine system within a short time, the situation became tense.[36]

Besides the technical problems, the Dayton project had to contend with irritating bureaucratic tangles, personnel problems, and security issues. The navy's engineering and business division demanded more annoying accountability. Dayton's civilian engineers' complained about working overtime, the National Cash Register company was irked by navy interference in its plant, and its managers complained that it was unnecessarily losing income because of the navy's 'non-profit' work. There were personality based tensions, especially between the chief civilian engineer (Joseph Desch) and the navy's on-site supervisor who, for various reasons (including worries about Desch's German relatives), was living in the back bedroom of Desch's small home. Desch became frustrated and emotional, at times jumping on tables and yelling at his staff to work 'harder and smarter'. Desch and his team's members were irritated when they frequently had to modify his initial design as they discovered engineering weaknesses or received new demands from Washington. In turn, the navy became angry as the original estimates of how long it would take to run a Shark problem on Desch's Bombes proved overly optimistic. Frictions mounted as suppliers delivered parts that did not meet specifications.

Personnel problems continued. The navy discovered that one of the female WAVES assigned to the project had hidden her pregnancy. That left the government in a quandary: what should be done with a woman who had a baby, who had broken WAVE regulations about reporting possible pregnancies before enlisting, who could no longer be housed at the super-secret facility, and who knew of one of the nation's most sensitive projects? The woman was discharged without punishment and with only a hope that she would not talk about what she had seen and heard.[37] There were more problems with the new women's corps. Two dozen WAVES decided to marry while on the project although that posed the risk of additional pregnancies. One WAVE committed a crypto-sin when she brought both an original version of a test message and its decryption out of the secure area. That endangered the secrecy of the project. Several of the women proved "too nervous" to be able to be allowed to continue to operate the Bombes and they had to be found new jobs that kept them within the confines of the project.[38] There were 'men problems', as well. At times, the Marine Guards in Dayton and Washington became a bit too trigger-happy.

A graver security issue arose a year after the scrape with the unwed mother. It had the potential to alienate the British and end its growing intelligence cooperation. It also pitted American civil liberties and issues of gender equality against the needs of national security. The serious problem was with a civilian male and, unlike the WAVES' breach of regulations; the navy dealt with it very quickly, and very, very harshly. When the authorities found that a young man who was working as an engineer in one of the most secret Bombe development rooms in Dayton had contacted German diplomats before the United States formally entered the war, and to have the addresses of German agents written on cards in his car, the navy acted swiftly, perhaps too swiftly. Even though the German 'agents' had long-ago left America, the navy's officials panicked. The naïve, ill educated and lower-class young man found himself hastily convicted of "theft", sent to prison, and secretly confined in isolation with a sentence that was to last for at least the duration of the war. His prison's warden feared for the sanity of the young man from the hills of Kentucky under such conditions. The government did not yield to his pleas, however. It was well after the war ended when the government paroled him and put him under constant surveillance to ensure that he would never reveal what he had learned about the Bombes and the Ultra Secret. His release came about only because of intense lobbying by his similarly young and ill-educated wife and because of protests about his unfair conviction and treatment by a future Justice of the United States Supreme Court.[39]

Another serious security threat was kept as or more hush-hush. The British discovered that in August of 1943, just as the Bombes came into operation, a man of Swiss descent who was high-up in the American Navy Department told a Swiss Diplomat that the Allies were reading the German's most secret naval messages. The diplomat was also an informant for the Nazis. England's deep and long-standing fears about American security seemed justified. What action the American's took against the Swiss-American remains a closely guarded secret, even today.[40]

Is This the End of the American Bombe or Was It Just Too Late?

The problems and delays in Dayton and England in early 1943 almost led to the cancellation of the American Bombe project. The American higher-ups were poised to rely on radio direction finding, the analysis of U-boat transmission patterns, and on the British to produce enough other

Shark related intelligence to prevent another replay of the convoy slaughters in the Atlantic. Of importance to the Allies' relationship, the Americans were thinking of waging an all-out sea and air attack on the U-boats despite possible risks to all of England's anti-Enigma achievements, whether naval or military.

Then, there was a reversal as the navy 'brass' was persuaded to allow the Dayton project to continue to live. The crypto-men in Ohio persisted in their labors believing they and their Bombes, not Britain's, would win the Battle of the Atlantic.

They needed faith in themselves: The first American production Bombes did not appear until August 1943, some two months after the first of the British machines began its initial runs. Although the first true Shark-breaking by the Americans was on June 22, it was for a May 31 message and the Dayton-Washington codebreakers had to use hand methods and a test machine. There were few other American 'breaks' for the next ninety days.[41]

Of historical significance, the first tentative American success in late June came almost two months after the great slaughter of U-boats during the decisive convoy battles of May 1943. Those battles, such as that over the safety of convoy ONS5, led to a major withdrawal of the Germans from the Northern Atlantic for several months, and, to a major change in U-boat deployment and communications strategies.

Desch and his team had some comfort, however. The first of the original batch of eighteen British Bombes had reliability issues and only three were consistently in operation during the next few months. Meanwhile, the Dayton factory began producing a reliable Bombe a day and did so for the remainder of 1943 until it fulfilled the revised requirement of less than ninety machines. The Americas had fourteen in operation in September, forty-two by the end of November. After the end of 1943, there was some further Bombe building in America and in England. By the end of the war, the United States had some 117 'four-wheel' Bombes and the British had the equivalent of ninety-four of them in operation.[42]

However, machines were not all of what was required to overcome the Shark challenge. After August 1943, despite the flow of American Bombes, the American crypto-organization necessary for turning Enigma settings into useful intelligence required additional months of training.

Moreover, there was something much more important to the Shark story. The first American Bombes arrived well after another decisive battle against the U-boats during the critical months of June through August 1943. May was not the only horrible month for the German Atlantic submariners, despite a paucity of American or British Bombes and a near absence of Shark intelligence. The Allies, with almost no help from Enigma-breaking, made additional and crucial in-roads against the Atlantic submarine menace during the summer of 1943.

What Shark and the American Bombes Did Not and Could Not Do

There was not a Bombe 'Miracle in Dayton' and there was not a Shark-breaking miracle in Washington's intelligence center. Although England and America conquered the Atlantic Enigma by the end of 1943, consistently reading Shark did not lead to the level of radio-intelligence achievement alluded to by the American Navy in its histories of the submarine battles of World War II. What the American, and British, Bombes and their allied methods yielded was far, far less than the implied claim that some seventy percent of all American Atlantic U-boat sinkings (kills) were due to "communications-intelligence" (by implication, reading Shark).[43] More important, new analyses of the American Navy's own records underscore the fact that reading secret messages is only one part of creating useful information or waging an effective military campaign. During the entire war, there were only two months, and in one area of the Atlantic, that looked like a crypto Golden Age. Moreover, that short and limited period was a British, not an American 'Age', and it came late in the war.

The Records

The American Navy's radio intelligence division, OP20G, kept meticulous records of the decryptions of Shark and of the relationship of Shark messages to Allied attacks on Germany's submarines. The records, yield both a general statistical series and a more specific one. One of the record collections, available at the National Archives in College Park, Maryland, gives the dates and times of each day's work against the settings of the submarine Enigma, and reveals whether the British or the American code breaking centers first made a successful attack. From this first series, the "German Cipher Key Logs" one can tell how many days, even hours, it was before the British or Americans discovered a day's 'keys'.[44] Once the daily basic 'keys' were found it was a relatively easy task to unravel the other settings and then read all the Shark messages for the day.

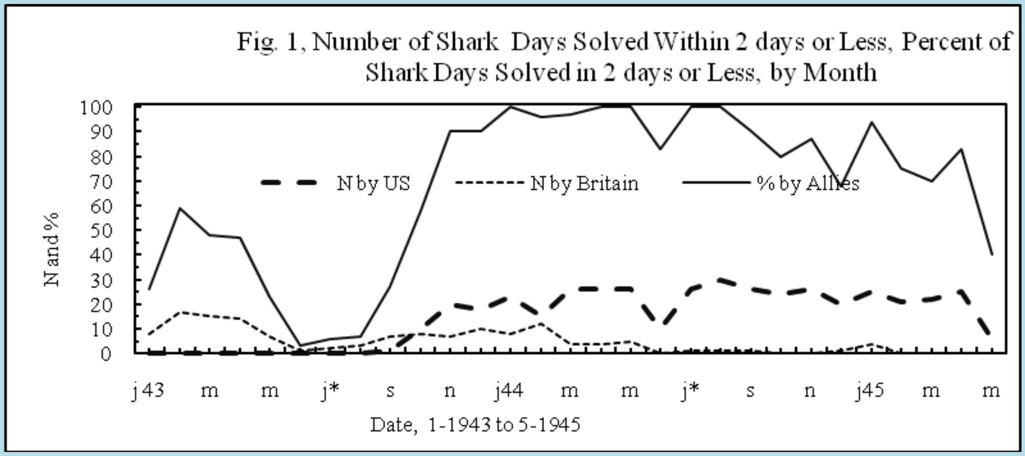
The Americans also kept a detailed account of the Allies' interactions with each German submarine, which were up-dated with post-war information on the U-boats, including the characteristics of the decrypted messages for each U-boat.[45] The strangely named, "Orange Translation" collection, when combined with lists of submarines active in the Atlantic, allows the creation of a rather detailed picture of the impact of Shark decrypts.[46]

The American Bombes and Shark-breaking

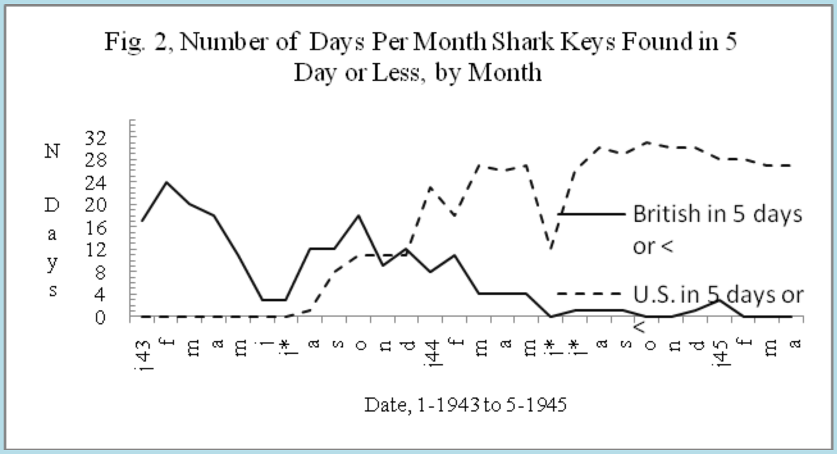
The American Four Wheel Bombes and those of the British did make a difference, but it took some time. During the first four months of 1943, captures of documents and serious German procedural mistakes had allowed rather consistent Shark-breaking. After that, there were four Dark Months. Then, the new Bombes became vital and effective. Whether measured by the number of days per month that the major 'keys' to the Shark Enigma were found within the time period the allies saw as most valuable, two days or less (Operational Time), or within five days or less, the Bombes that appeared in late summer 1943 began to have an impact .

After the frightening blackout months of late May through August, there was a constant rise in the percentage of daily Shark keys discovered by the collaborating British and Americans. However, it was not until October that the recovery percentage equaled that of early 1943. Then, by the beginning of 1944, the combined American and British centers reached a near 100% two-day or less discovery rate. That success was partially due to the Germans typically using the same major Shark settings, the ones the British and Americans designed the Bombes to uncover, for two days in a row. For much of the war, the special settings for the Limpet (officer) Shark messages were in force for days at a time, as many as five.

However, to the surprise and disappointment of the Americans, their Shark contribution did not become dominant until November 1943. The following graphs, which show the Shark-breaking results in both absolute numbers and percent of key-days per month, demonstrate that it took much longer than the American planners had hoped to be able to muster the machines and train the crypto-force needed to fight Shark. England's Bletchley Park continued to be the first to find the Shark keys within two days for close to twenty percent of the time until February 1944, and England continued to play a role in dealing with the more difficult "five day" message settings for the same period.



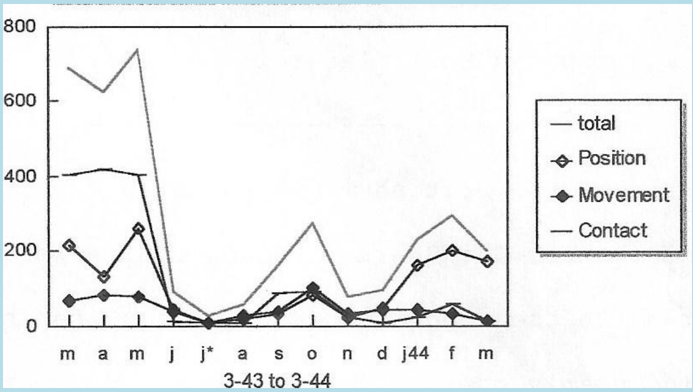
(Figure 1, Number and Percent of Days Shark Broken Within "Operational" Two Days or Less[47])



(Figure 2 Number of Days Per Month Shark Keys Found Within Five Days or Less, By British and By U.S., 1943-1945)

The late arrival of the Bombes, improvements in Germany's Shark security practices, and an alteration of German strategy for the deployment of the U-boats, led to a bleak intelligence summer of 1943 for the Allies. Besides the failure to find the Shark keys, the numbers and value of the kind of messages that made Shark-breaking important plummeted after May, with only brief but important resurgences. Each of the three types that gave the location of U-boats declined. Some messages reported contact with Allied ships; some reported a German submarine's present location. The most valuable for the Americans, who wanted to take aggressive action, were "movement" messages. They gave future locations of the German forces, thus allowing the Allies to position their navies and air forces for 'hunting' attacks as well as to divert or protect convoys.

Fig. 3, Number of Decrypted Messages Giving U-boat Present or Future Location



(Figure 3 Number of Decrypted Location Messages, By Type, March-1943 to March-1944[48])

Shark-breaking and the Battle of the Atlantic

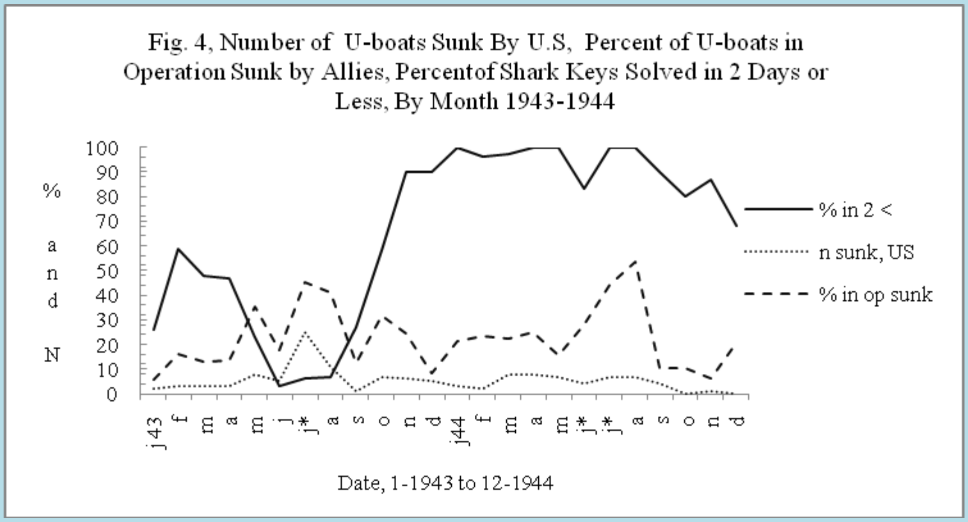
Although the Bombes could have become relatively useless if the Germans made other significant changes in their encryption devices or related procedures, the ability to find quickly the settings for the regular Shark and special Limpet messages remained amazingly high from late 1943 through remainder of the war. The successes continued despite, among other challenges, declines in the number of any of the types of messages that allowed the allies to find the probable words in messages (cribs) needed for the set-ups for the Bombes.

However, reading the submarine traffic did not necessarily mean success in the battle for the Atlantic.

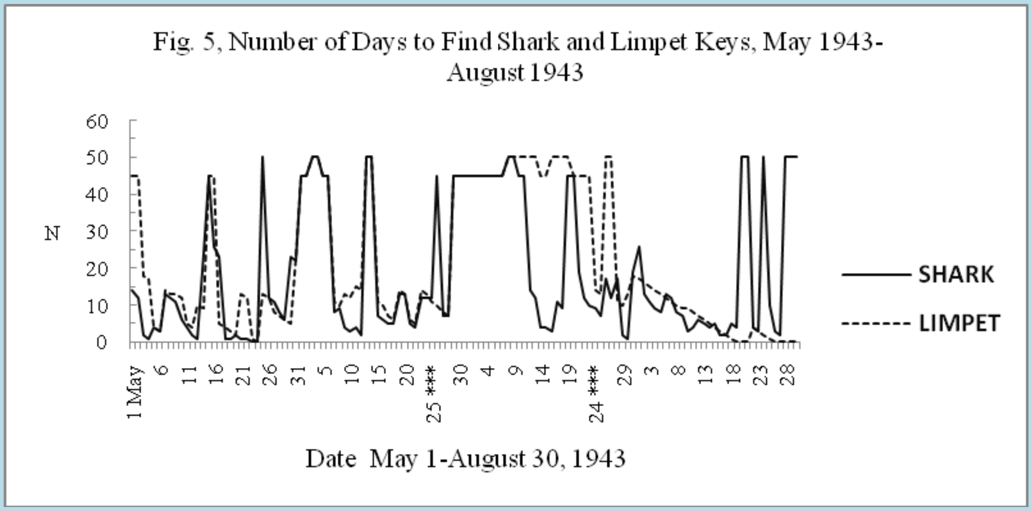
The General Statistics

Using the indicators of success chosen by the United States Navy, the number of U-boats sunk and the percentage of U-boats in operation sunk, yields challenging results. Except for some periods when there were few U-boats in operational status (and excluding from consideration the last few months of the war when the Allies were sinking U-boats in their pens or when the boats were entering the heavily patrolled Bay of Biscay) there was little consistent positive relationship between the general statistics for Shark-reading, 1943 to 1945, and U-boat kills.[49]

Because of the reduced number of U-boats and their deployments, beginning in 1945, if not by summer 1944, even the American navy's analysts found it very difficult to state whether Shark intercepts had a clear relationship to sinkings. Therefore, this study focuses upon the connections from 1943 to the end of 1944. Note that the conclusions about the Shark-sinkings relationship hold whether ones uses the U. Navy's estimates of the number U-boats in operation per month or those of independent scholars.[50]



(Figure 4, Percent of U-boats In Operation Sunk by Allied Forces, Number Sunk by U.S. Forces (Official U.S. History) . And % of Shark Keys Solved Within Two Days or Less, January 1943 to December 1944)



(Figure 5, Number of Calendar Days to Find Shark and Limpet Keys. May 1 to August 30, 1943)

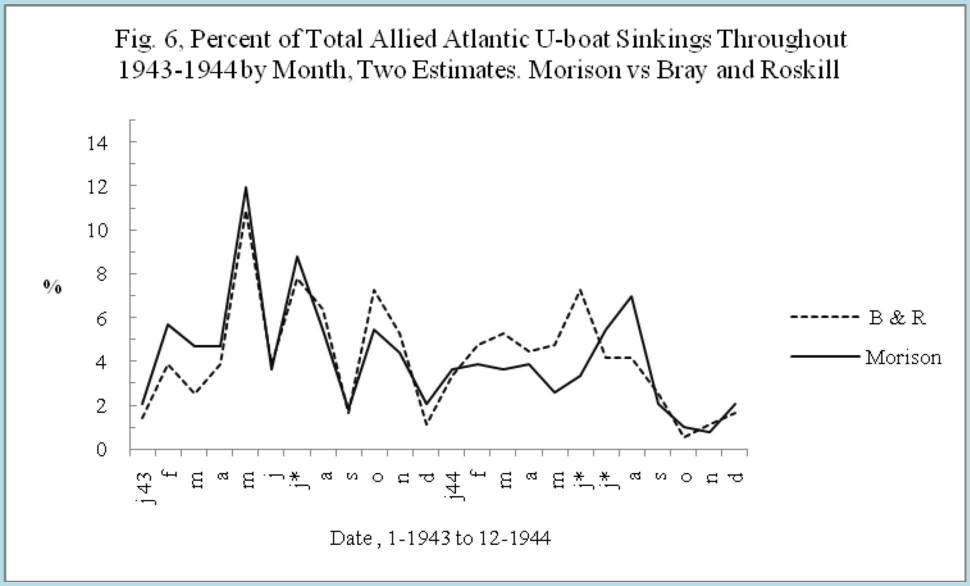
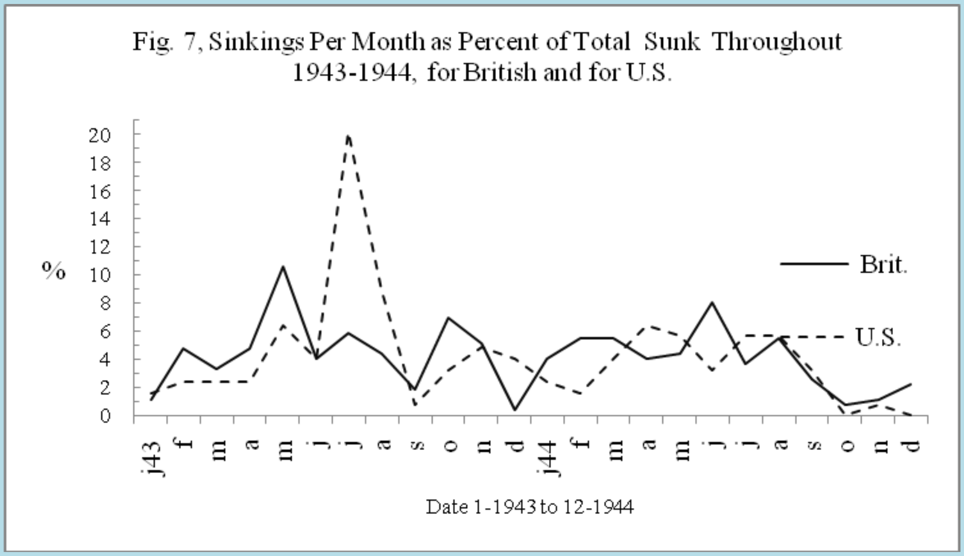


Fig. 6, Percent of Total Allied Atlantic U-boat Sinkings Throughout 1943-1944 by Month, Two Estimates. Morison vs Bray and Roskill

(Figure 6, Each Month’s Percent of Total Atlantic U-boat Sinkings During 1943-1944, Two Estimates)[51]

Most surprising, and, if they had known, perhaps disappointing to America’s Bombe engineers, the highest rate of U-boat kills came during the frustrating code breaking Dark Days of the summer of 1943. Despite a small number of inexplicable successes during those summer months, there were very, very few days when Shark or Limpet were solved within the ‘operational periods’.[52]

Yet, during the three Darkest Shark-reading months of summer 1943, the United States Navy made approximately one-third of all its U-boat kills of the entire war. Combined with Britain’s great successes, the period was one with sinking rates sometimes reaching over forty percent. The United State Navy claimed forty-one ‘kills’ in the blackout months of June, July and August, with twenty-five of those occurring in July alone. The British sunk thirty-nine with an additional twenty-nine in May, which was also a relatively poor intelligence month. Significant for the Atlantic struggle, the Allies sunk some nine of the critically important German refueling submarines during the three summer months.[53] They were the unique U-boats that allowed the fighting German submarines to stay at sea for elongated periods. Their sinking left the Germans with only three of those special boats, or less than one-third of their usual supply fleet.



(Figure 7, U-boat Sinkings Per Month as Percent of Total U-boats Sunk in Atlantic During 1943-1944, for the British and for the United States)

In contrast to the evidence from the German Cipher Key Logs, which fail to show impressive Shark-breaking in the period, the American Navy's historians claimed that the summer of 1943 was a communications intelligence (CI) triumph. They gave CI credit for sixty-nine percent of the American submarine 'kills' during the ninety days.[54]

Evidence other than the Cipher Key Logs reveal that Shark-breaking played a small role during summer 1943, even during the famed campaign by America's carrier aircraft near the Azores. That June campaign disrupted a large German submarine attack. Ralph Erskine has described it in detail, stressing the fact that the critical Shark message did not include a clear indication of the area where the U-boats would be operating.[55] The other evidence about Shark-breaking in the period comes from those poorly named "Orange Translations" files that contain a record for each German submarine. The information includes the specifics about each Shark message related to the boat as well as the date, time, and place of attacks on each submarine. The series reveal that while a May 24 Shark Limpet message that ordered sixteen submarines to a future attack position was near miraculously read by the British on the same day the Germans transmitted it, its reading did not lead to a significant number of sinkings.

The "At Risk" Test and the Summer of 1943

The U.S. Navy employed its At Risk criteria to judge the impact of reading Shark messages that gave a U-boat's present or future location. If the Allies attacked or sunk a U-boat during the At Risk period, no matter what other information the Allies gained about the submarine, the United States Navy gave the Shark message the credit. At Risk is a quite generous measure. It does not take into account the impact of other signals intelligence and improved anti-submarine technologies. It gave Shark-breaking a great advantage. The navy's analysts calculated At Risk by subtracting the date of decryption from the date of the location given in the message and adding five days to that. For example, if the British or Americans decrypted a message on May 23 that gave a location date of May 24, then the submarine would be At Risk for six days. If a message was intercepted on June 1, decrypted on June 4 and had a location date of June 10, then the boat would be At Risk for eleven days, or until June 15th.

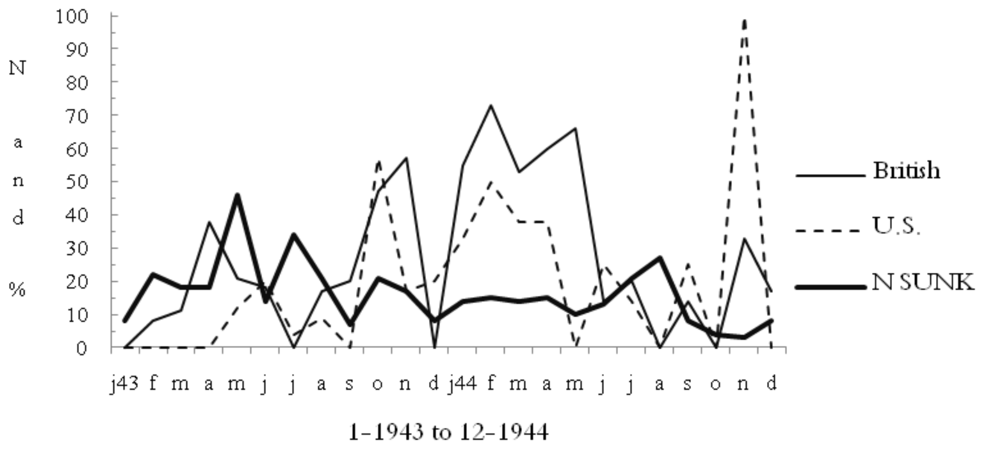
An analysis using the At Risk criteria of the Navy's 'Orange' records for the submarine battles during the summer 1943 yields a far different view of Shark's contribution than do the summary statistics the Navy gave about the role of Communications Intelligence. Navy histories gave estimates of a credit to CI of sixty percent for the five American sinkings in June and sixty and ninety percent credits, respectively, for the some twenty-five in July and eleven in August. In comparison, At Risk Shark-breaking accounted for only ten percent (no matter which estimate of total 'kills' is used) during the three summer months and about half of those American Shark related sinkings came within a one day At Risk period. The one-day At Risk period suggests that American air and naval forces were already close to the U-boats.

During the particularly critical June battle off the Azores, Shark deserves At Risk credit for only one American submarine kill. Furthermore, of the nine critically important refueling submarines sunk by the Allies during the summer, only one was an At-Risk casualty. A similar overall At Risk percentage marked the British experience during June, July, and August. The At Risk analysis suggests the American Navy included the contributions of direction finding and perhaps radar in its definition of Communications Intelligence.

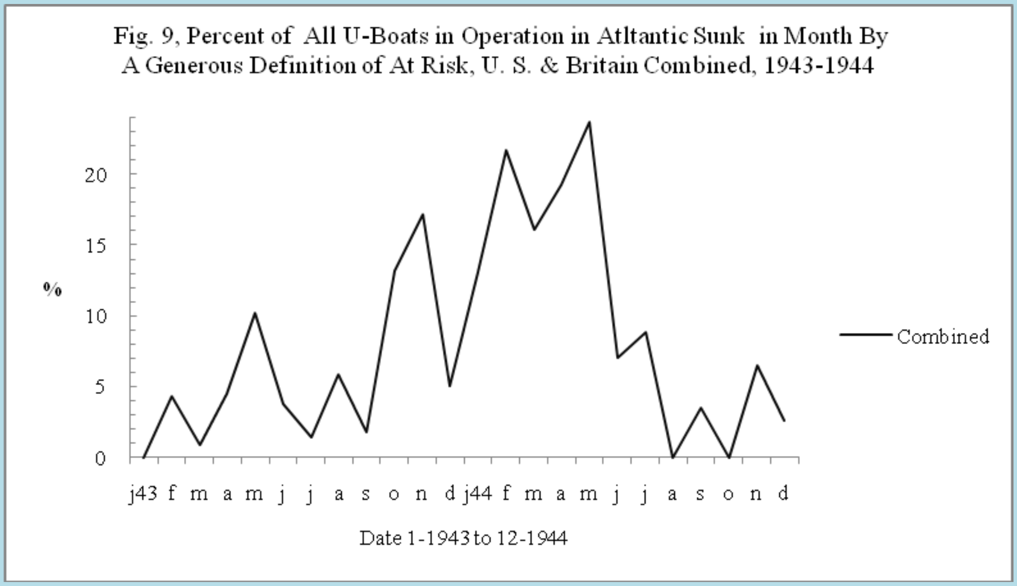
At Risk and the Remainder of the U-boat Battle, Even Britain's

A trace through the At Risk records for all of 1943 and 1944 does show some months when Shark contributed at rates approaching the American Navy's estimates of the role of all types of Communications Intelligence. In October and November 1943, when the Germans were sending many location-movement messages, both the Americans and the British used Shark for almost fifty percent of their U-boat kills. During early 1944, British At Risk rates reached seventy percent and remained high for several months. That came despite eliminating the many only "partial" credits the British gave to Shark messages. However, it was not until November that even the British attacks showed signs of active hunting. Until then, most sinkings occurred within one day of the decryption of a message about a U-boat. That many of their kills were in already heavily patrolled areas suggests the sinkings might have resulted without the decrypted location messages. The rates are impressive, nevertheless.

Fig. 8, Percent of British and U.S. Sinkings in Month by At Risk and Number of Allied Sinkings, 1-1943 to 12-1944

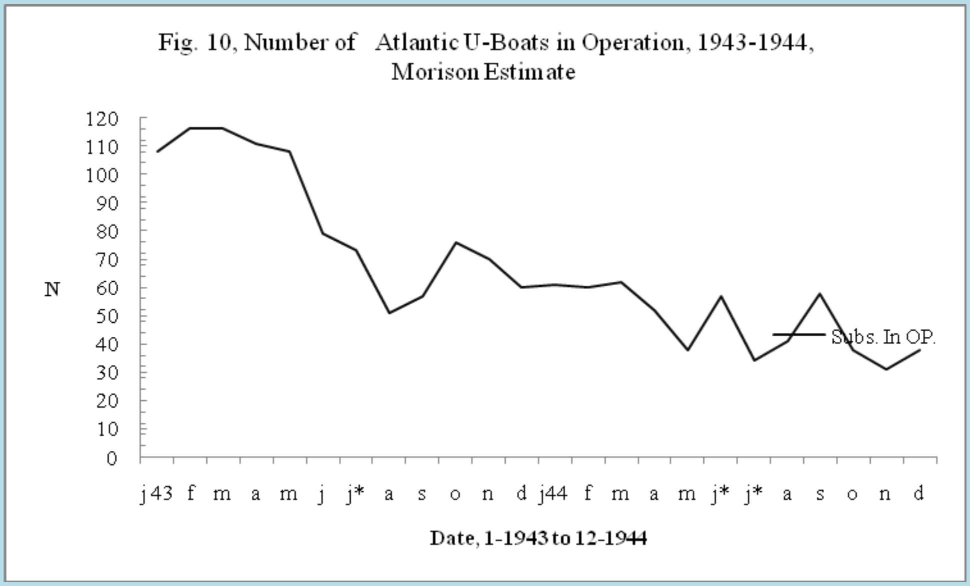


(Figure 8, Percent of British and American Atlantic U-boat Sinkings Per Month Due to At Risk Shark Messages, and Number of U-boats Sunk by Allies, 1943-1944)

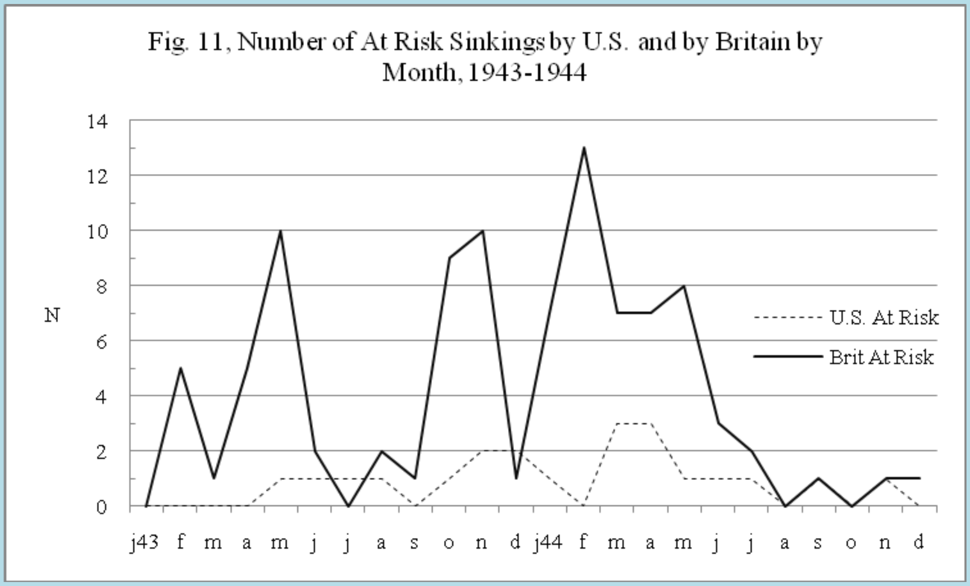


(Figure 9, Percent of All Atlantic U-boats Sunk In Month by the Allies (Combined) 1943-1944, Generous Definition of At Risk Influence)

The American At Risk percentages during the first months of 1944 are also impressive. However, the absolute number of U-boats sunk by the United States' forces and by the British reduces the impact of Shark during those months. Whether using earlier or more recent estimates of the size of the U-boat fleet, the low number of U-boats in operation diminishes the importance of Shark during early 1944. There were relatively few submarines in operation and, numerically, Shark-breaking helped to sink few in 1944.



(Figure 10, Number of Atlantic U-boats in Operation, 1943-1944, Morison estimate)



(Figure 11, Number of At Risk U-Boat Sinkings by the United States and by Britain, 1943-1944)

Estimates of the impact of Shark-reading by various periods, as well as for all of 1943 and 1944, show that it did, at times, play an important role.[56] But, it was not as great as the navy historians implied. Furthermore, the estimates are generous, and not only because of the extra five days in the determination of the At Risk period. Even the conservative estimates of Britain's percent of sinkings when U-boats were At Risk include many sinkings in densely patrolled areas where Shark identifications may have been redundant or unnecessary. Therefore, the following percentages of all sinkings due to Shark-reading should be interpreted as upper-boundaries. The generous overall 'upper boundary' for estimates of the contribution of the American and British Bombes for the post summer-1943 months when the new Bombes began to appear is thirty-nine percent of U-boat sinkings.

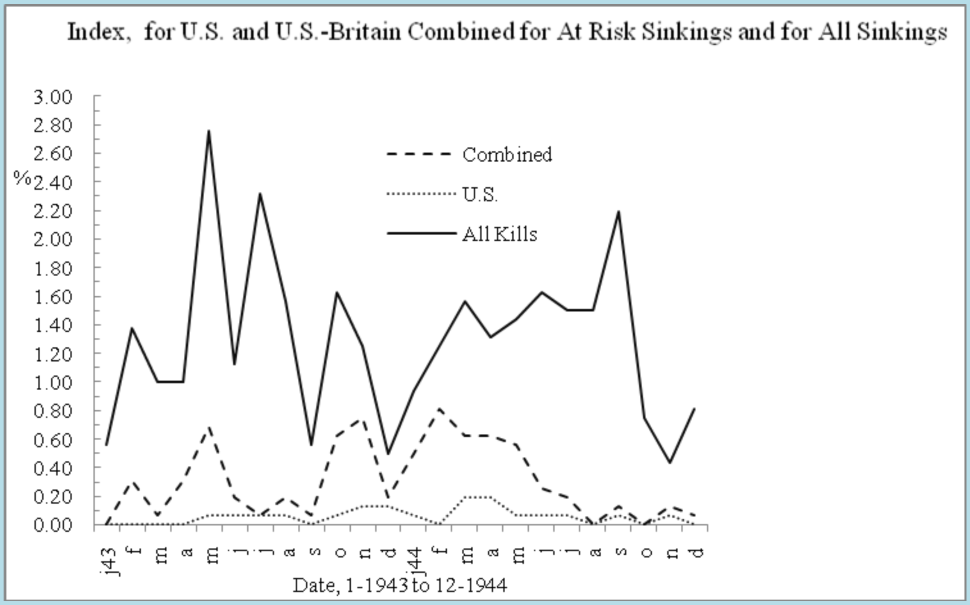
Table 1, Estimates of Percent **of** U-boat Sinkings by At Risk, Various Periods, For U.S, Britain, and Combined

Date	**U.S.**[57]	**Britain**[58]	**U.S. & Britain**[59]
1-1943 to 5-1943	11	19	26
1-1943 to 7-1943	6	16	17
6-1943 to 7-1943	11	7	9
8-1943 to 12-1944	22	34	39
1-1943 to 12-1944	17	27	32

(Table 1, Estimates of At Risk Sinkings as Percent of All U-boat Sinkings)

An Index

Those percentages should be placed in context to allow a more sensitive evaluation. To obtain a sense of the relative contribution of Shark-reading over time the monthly percent of At Risk sinkings can be weighted by the percent of U-boats in operation per month that were sunk[60]. Doing so creates a monthly index of Sharks' importance over the two critical years, 1943 and 1944. Not surprisingly, the sparse Shark-reading months of May and summer 1943 have the higher index scores for all sinkings (At Risk or otherwise) with the post-Normandy invasion months being next in importance. As for Shark At Risk kills, the high point for combined Allied efforts came in May and then, October and November 1943. For the American Navy alone, they came in the same months. However, even during those great Shark-reading months only a tiny percent of the two years' submarines ever in operation were sunk by Allied At Risk action. Thus, while three percent of the U-boats in operation throughout 1943 and 1944 were sunk by all means in May 1943, only a bit more than one-half of one percent were sunk in any At Risk period by either the United State' or Britain's forces. For the United States, its At Risk percentage peaked at approximately two-tenths of a percent in early 1944.



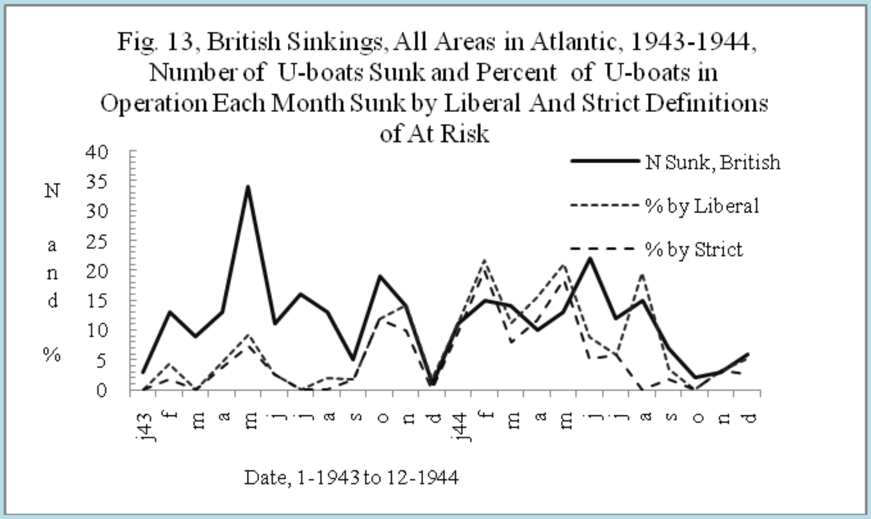
(Figure 12, Index of Relative Monthly Contribution of At Risk and All U-boat Sinkings, 1943-1944)

A Brief Golden Age In One Place and For One Country

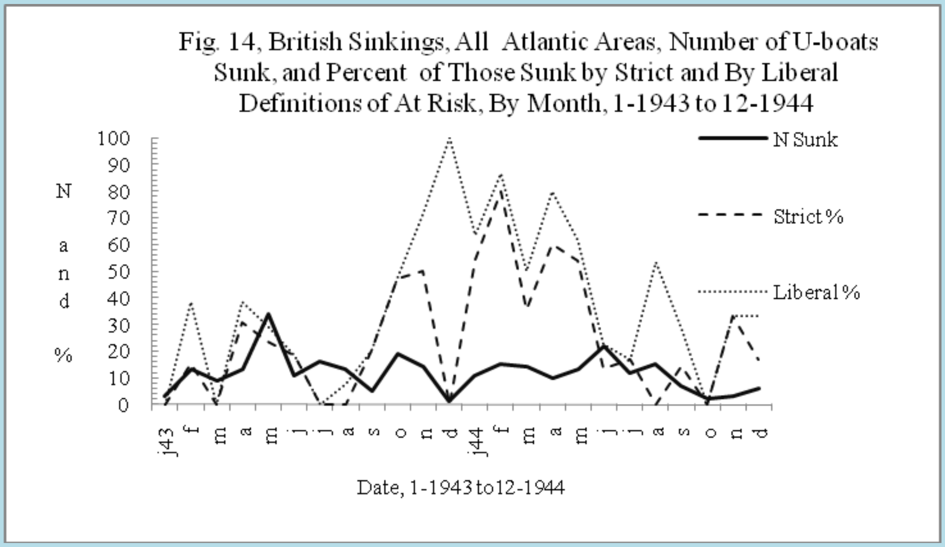
If there was a Bombe/Shark-breaking Golden Age, it was a brief one and it was British. It was only in two areas patrolled by the Empire's forces, and during two, perhaps three months in early 1944, that the sinking rates due to Bombe Shark-At Risk location messages approached the United States Navy's stated rates for Communications Intelligence related U-boat sinkings in the Atlantic. In addition, those successful Bombe months were ones in which the number of U-boats in operation had greatly diminished since the spring 1943 convoy onslaughts. And, in only two of the months did the U-boat sinkings appear to have been the result of days of ‘hunting’ rather than encounters with packs already near convoys and their escorts. Proximity to in-place escorts and air cover allowed the Allied attacks to be successful within one day or less after the decryption of a Shark location message and suggest that At Risk messages were not the exclusive cause of a submarine’s demise.

Other qualifications help place the Britain’s Golden Age in perspective. Did a Bombe Shark message play a direct or indirect (partial) role in a U-boat’s sinking? The British ‘Orange’ records were more detailed than those for the American’s U-boat histories. They indicated that many of the Bombe related U-boat At Risk sinkings were only partially due to Shark-breaking. ‘Partial’ influence seems to have been when a U-boat’s location was known by other means, or when the message was about a pack already identified rather than a particular boat, or when the message yielded only general information about an enemy submarine. Significantly, the ‘Orange’ records and other histories concerning British U-boat attacks in the Atlantic emphasized that after the Allied invasion of Europe, Shark messages concerning the U-boats in the Bay of Biscay and the English Channel were generally superfluous. Because the areas were so heavily patrolled, and because of the stereotyped nature of the U-boat transmissions concerning their entry or exit from their bases, Shark was redundant. Therefore, in many instances two estimates are presented below for the British At Risk experience. One, tagged as “Liberal”(or “Both”) includes instances of direct and partial Shark-breaking influence. The other “Strict’ includes only sinkings through a direct impact on U-boat hunting.

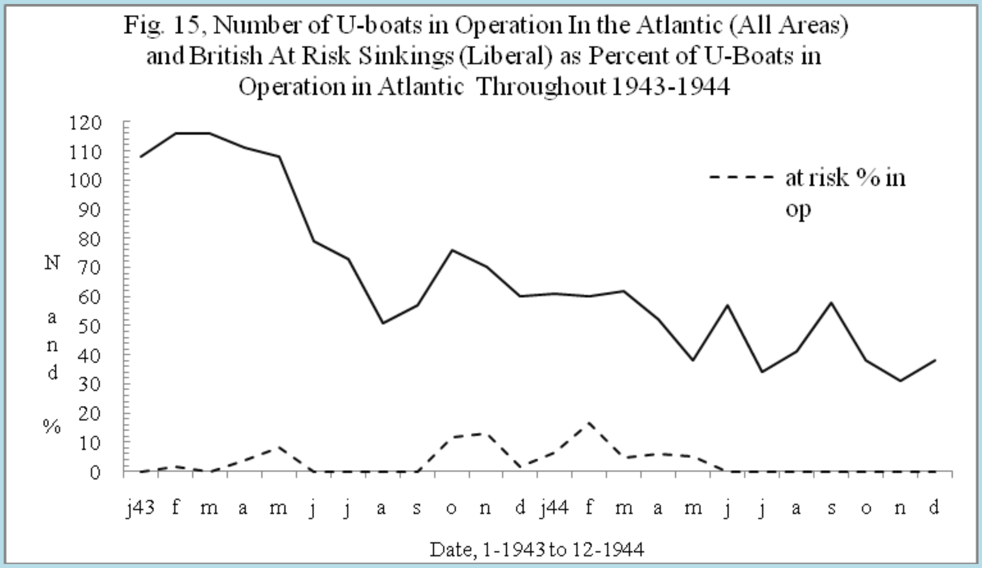
Both estimates reveal a significant Shark-breaking contribution, especially in the North Atlantic and the Arctic. However, for the British sub hunters in the Atlantic during 1943 and 1944, the At Risk sinkings in May 1943, before the Bombes became operational, contributed almost as much to the war effort as those of October and November 1943 and February 1944.



(Figure 13, British Sinkings, All Atlantic Areas, Number Sunk and % of U-boats in Operation Sunk by At Risk, (Strict and Liberal) **)**



(Figure 14, British Sinkings All Atlantic Areas, Number of U-boats Sunk and Percent if Those Sunk by At Risk (Strict and Liberal), By Month, 1943-1944)



(Figure 15, Number of U-boats in Operation In the Atlantic and British At Risk Sinkings (Liberal) As Percent of U-boats in Operation in Atlantic Throughout 1943-1944)

The North Atlantic

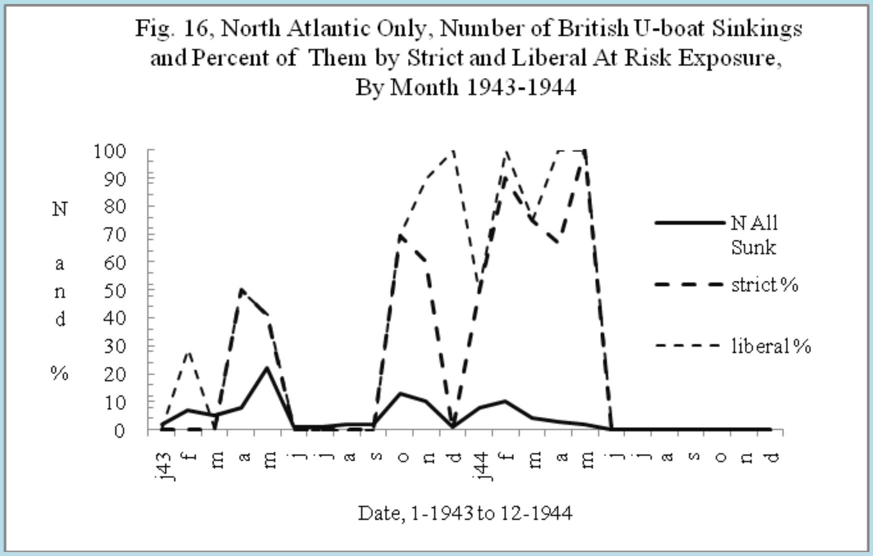
Shark-breaking played a special role in the areas that were two of the major Allied convoy routes, the North Atlantic and the Arctic.

Table 2, British At Risk Sinkings

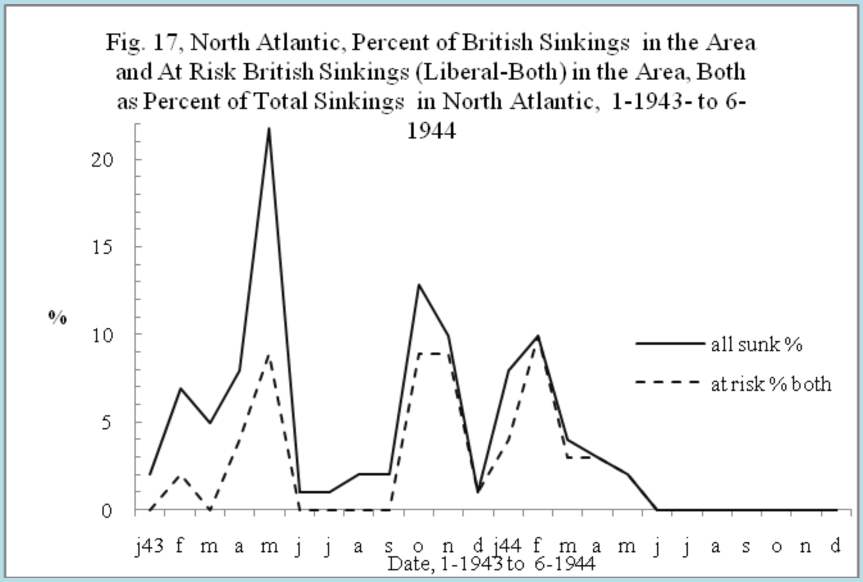
AREA	**% By Sunk At Risk (Liberal) 1943-1944**[61]
North Atlantic	47
Channel	20
Bay of Biscay	5
Arctic	53
All Other Atlantic	15
Combined	30

(Table 2, Percent of U-boat Sinkings by British by At Risk, by Area 1943-1944)

After the summer of 1943, with the return of U-boats to the North Atlantic, the At Risk percentages rose above those of April and May 1943. In February, the rate approached eighty percent. Significantly, during that month, as had been the case in November, the sinkings were not the result of attacks within one day or less of the decryption of messages. However, when those rates are weighted by the percent of total sinkings for 1943 and the first half of 1944, the contributions of those two months were at levels of about those of spring 1943.



(Figure 1, North Atlantic Only, Number of British U-boat Sinkings, and % By Strict and Liberal At Risk Exposures)



(Figure 17 , North Atlantic, Percent of British Sinkings in the Area and At Risk British Sinkings (Liberal-Both) in the Area, Both as Percent of Total Sinkings in North Atlantic, 1-1943- to 6-1944

Caveats and Conclusions

There have been suggestions that Shark-breaking could have played a greater role in the Battle of the Atlantic if the Allied commands had allowed their navies to use all the decrypted location messages to launch attacks. They were prevented from doing so, it has been asserted, in order to avoid German suspicions that their most precious code system had been compromised. The British demanded that no Shark-based attacks be allowed until the Germans were made to think conventional air or sea forces had spotted the U-boats. We may never know how much of a role such limitations played in the Shark story because of the impossible task of checking though all messages and all orders for attacks against U-boats and correlating that with available Allied forces. However, there are hints that a ban against Shark attacks was neither absolute nor necessary. The May and October 1943 confrontations, the wholesale attacks against the refueling submarines in the summer of 1943, the American campaign in the Azores, the U-boat slaughter in the Bay of Biscay, and the February 1944 battle in the North Atlantic suggest that Shark-breaking was not always underused.

Whatever the amount of restraint in exploiting Shark-breaking, At Risk sinking rates are useful and informative in evaluating code breaking's contributions. Yet, they are only partial reflections of the importance of cryptanalysis during World War II's anti-submarine and other military intelligence battles. An attack on one of a pack of U-boats could disrupt a campaign against a convoy. Knowledge of new U-boat technologies and countermeasures came from reading the Enigma messages. Grand strategies were gleaned from the intercepted messages. A convoy diverted away from a U-boat attack because of an intercept saved lives and valuable resources and the use of the American as well as British Bombes on German army and air force problems provided much valuable information.[62]

That said, the At Risk rates and history of the American Bombe-Shark project yield a helpful new and more realistic benchmark for judging the accomplishments of later crypto and communications intelligence efforts.

[1] Kahn, David. c1996, *The Codebreakers : the Story of Secret Writing*, (Rev. and updated ed.). New York : Scribner; National Security Agency, Center for Cryptologic History. 1992. *The Friedman Legacy [microform] : a tribute to William and Elizebeth Friedman* . Fort George G. Meade, MD, The Center; Lewin, Ronald. c1982. *The American Magic: Codes, Ciphers, and the Defeat of Japan*. New York: Farrar Straus Giroux; Bamford, James. c1982. *The Puzzle Palace: a Report on America's Most Secret Agency* New York, N.Y., U.S.A.: Penguin Books.

[2] *Bamford, James, 2002. Body of Secrets: Anatomy of the Ultra-secret National Security Agency* **.** New York: Anchor Book*s*; Alvarez**,** *David. 2000. Secret Messagse***:** ***C****odebreaking an****d*** *American Diplomacy, 1930-1945***.** Lawrence, KS; Bamford**,** *James 2008*. The Shadow Factory: the **U**ltra-secret NSA from 9/11 to the **E**avesdropping on America**.** New York :Doubleday*;* Bamford, James. *2005.* A Pretext for War: 9/11, Iraq, and the Abuse of America's Intelligence **A**gencies**.** New York: Anchor Books; Hanyok, Robert. 2002**.** *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975***.** Ft. Meade, Maryland: Center for Cryptologic History, and**,** http://fas.org/irp/nsa/spartans/aftermath; Hanyok, Robert J. c2000. "Skunks, Bogies, Silent Hounds and the Flying Fish : SIGINT and the Gulf of Tonkin Mystery, 2-4 August 1964, *Cryptologic Quarterly*, 20, #1 (Winter 2000-Spring 2001): p.8, Nov. 2005, NSA Gulf of Tonkin document release.

[3] Aid, Matthew. 2009. *The Secret Sentry: the* ***U****ntold* ***H****istory of the National Security Agency***.** New York: Bloomsbury Press; Johnson, Thomas R. c1995**.** *American Cryptology During the Cold War, 1945-1989*, Ft. Mead Maryland, National Security Agency, Center for Cryptologic History, 4 vols., circa. 1995-1998; redacted FOIA-released version of vols. 1-3 as of 2007, available on the internet at:
http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-1.pdf :
http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/NSA-2.pdf;
http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-3.pdf;http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-4.pdf;
http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-5.pdf;
http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-6.pdf .
(the fourth volume is expected to be released soon)

[4] Debrosse, James. http://www.daytondailynews.com/project/content/project/enigma/enigma_index.html.Ohio History, http://www.ohiomag.com/ME2/dirmod.asp?sid=&nm=Events&type=Publishing&mod=Publications%3A%3AArticle&mid=0D549927D9364573812B50822D4B2BD4&tier=4&id=B80A1A989FC64669BC4B3C2C0B35F65; The Center for Cryptologic History. nd. *The Bombe: Prelude to Modern Cryptanalysis*. Fort George G. Meade, Maryland.

[5] Some of the more important official reviews are: NARA RG457, Box 112, SRH368, "Evaluation of the Role of Decryption Intelligence in the Operational Phase of the Battle of the Atlantic'; NARA RG457, Box 112, SRH367, "A Preliminary Analysis of the Role of Decryption Intelligence in the Operational Phase of the Battle of the Atlantic; RG457 HCC Box 583 NR 1427 CBKH18 1886A 19450000 APPENDICES TO OP-20-G HISTORY OF THE U-BOAT WAR IN THE ATLANTIC, WWII; RG38, CNSG Library, SRH336 and 337 Boxes 66 and 583, Submarine Attacks and E Traffic**;** NARA RG38 Crane Library, Box 108 5750/99, 'Historical Review of Communications Intelligence WWII', 1945'; NARA RG457, Box 43, SRH142, Commander Jerry C. Russell, USN, Ultra and the Campaign Against the U-boats in World War II; RG38 CNSG Library box 183 , SRH 024, Battle of the Atlantic, vol III-IV; NARA RG457 SRH142 Box 43, 'Ultra and the Campaign Against the U-boats'; NARA RG38 CNSG Library Box 182 SRH02, 5750/433 ' Battle of the Atlantic; NARA RG457 Box 5, SRH008, 'Battle of the Atlantic'; NARA RG38 Crane Library Box 104, American Cryptanalysis of German Naval Systems, 7-7-1944 R. B. Ely Lt. Commander.

[6] Center for Cryptologic History. 2002. *Solving the Enigma: History of the Cryptanalytic Bombe*. Fort George G. Meade, Md.: National Security Agency; Benson. Robert L., 2001. *The Venona Story*, Fort George G. Meade, Md. : National Security Agency, Center for Cryptologic History.

[7] On Mrs. Friedman and her small Coast Guard group's attack on the Swiss Enigma, NARA RG457 HCC, NR1737, Box 705, "Enigma Conferences'.

[8] NARA RG38 CNSG Library, Box 175 1200/2, Civilian Personnel, '5 September 1940, to Granat, Safford Recommends ex-employee who had nervous breakdowns, mentions a suicide'.

[9] James Debrosse. 2004. *The Secret In Building 26: The Untold Story of America's Ultra War Against the U-boat Enigma Codes*, New York: Random House.

[10] NARA RG38 CNSG Library Box 104, 5750/91; 'Driscoll and two assistants assigned to German Problem, 9-0ct-1940; NARA RG38 CNSG Library, Box 66 ,'German Cipher Problem' nd.. For a more detailed history of the 1940 American anti-Enigma effort, see, Colin Burke, 'Agnes Meyer Driscoll v the Enigma And the Bombe', unpub. essay, 2007

[11] RG38 Crane Library Box 66 5750/772 'German Cipher Problem: II Attempted Solution by Analytical Mathematical Methods'; NARA RG38 Crane, RIP, Box 168, '7-6-43, The Catalogue and Its Use'; NARA RG457 HCC Box 1009 ACC11289 CBNM78, 'Cryptanalysis of the Yellow Machine' (US Army) which also mentions a possible "statistical" attack; NARA RG38 Inactive Stations, Box 65 5750/750, Enigma Catalog for Commercial Wired Wheels, 1943 (U.S. Navy); TNA PRO HW 14/129, June 2, 1945, 'Destruction of Catalogs'; NSA FOIA Oral History Interview NSA-OH-14-83 with Howard Campaigne by Robert D. Farley, 19 June 83. On earlier U.S. Navy and Coast Guard attacks on Enigma machines, NARA RG457 HCC Box 705, "Enigma Conferences"; On the U.S Army's codebreakers and the use of a catalog attack against Japanese machine, NARA RG457 HCC NR2804, Box 950, "Eggs Catalog".

[12] On the beginnings of Driscoll's "E' work with a small team in October 1940, U/S Naval Historical Center, Operational Archives, SRH355, " Naval Security Group History to World War II. Part I."

[13] NARA RG38 CNSG Library Box 7 2500/78, 14 Nov 1941. 'Driscoll Problem Not That Important'; NSA FOIA, 5 Nov. 1941, Memorandum for OP-20-A, Report of Conference, re 'Professor Howard'; NARA RG38 CNSG Library Box 7 2500/78, 'Analytical Machines'; RG38 Crane Library 2500/78 box 171 CNSG Analytical Macinery, 18 Sept. 1936-6 Jan. 1942.

[14] Erskine, Ralph. 2000. "What Did the Sinkov Mission Receive from Bletchley Park?", *Cryptologia, 24 #2 (*April). Pp. 97-109.

[15] For an outline of Driscoll's decisions in 1941 and citations to them see, James Debrosse. 2004. *The Secret In Building 26: The Untold Story of America's Ultra War Against the U-boat Enigma Codes*, New York: Random House; TNA PRO HW 14/45, August 18, 1941. "List of Driscoll questions to GCCS re E and its solution'; TNA PRO HW 14/45 August 18, 1941, Denniston, "Interrupted Conference with Commander Safford'; TNA PRO HW 14/45, 46 , 'Denniston Reports'; TNA PRO HW 14/45 December 12. 1941, to Denniston, 'Driscoll short cut method failed, only 5 people on her work'; TNA PRO HW 14/45, December 12 , 1941, ' to Denniston, Driscoll group still frustrated, want more information on Enigma and any codebooks, especially short signals'; On the long history of the navy's reluctance to share intelligence secrets with the British see, Robert L. Benson, "The Origins of British Communications Intelligence Co-operation, 1940-1941," http://www.nsa.gov/public_info/_files/cryptologic_spe.trum/origin_us_british.pdf. Safford had long distrusted British intentions, had protested against the early 1941 sharing of secrets and machines, and felt that the Roosevelt administration had weakened the American Navy's intelligence capability against Japan by sending scarce resources to England. See for example, Dundas P. Tucker (Laurance F. Safford). 1982. "Rhapsody in Purple,"

Cryptologia, 6 #3, 193-228. Safford's interpretation of the events of 1941 flowed into later official histories, such as: NARA RG 457 HCC, NR4384, Box 705, "History of the Bombe Project, 24, April, 1944, and NARA RG38 CNSG Library, Box 104, 5720/205, "American Cryptanalysis of the German Naval Enigma, 7 July 1944," and, into later histories by skilled historians such Stephen Budiansky and Lee A. Gladwin . Although the major frictions between the two nation's intelligence groups eased during 1942 and 1943, even the British had less than fond memories of the relationships in 1941 and early 1942. See, for example, TNA PRO HW 3/93, Eric Jones' Comments on Nigel DeGrey's Official History, November 23, 1948. See, also, NSA Cryptologic Almanac 50th Anniversary Series, "Madame X: Agnes Driscoll in Twilight, The Last Years of the Career of Agnes Driscoll, 1941-1957, NSA FOIA 2010 release #52567.

[16] Ralph Erskine, Colin Burke, and Philip Marks. 2004. "Memorandum to OP2-20-G on Naval Enigma (c; 1940)", in Jack Copeland (ed*), The Essential Turing,* Oxford, Clarendon, pp. 341-352.

[17] OP20G, GYA, RIP 425 History of OP20GYA1 Provided by Ralph Erskine; The American Attack on the German Naval Ciphers, CNO, October 1944; 7 July 1944, American Cryptanalysis of German Naval Systems, R. B. Ely Lt. Commander, USNR, Supplied by Robert Hanyok; NARA RG38 CNSG Library Box 5750/205 Box 117 and RG38 Crane Library, Box 104, 'Turing's letter and critique of Driscoll methods'.

[18] NSA FOIA Report on Meeting With Prof. Howard, 11-1-1941. At the end of 1942 the navy began a project to build the Hypo film-based machine to automate the catalog search. This HYPO machine was not delivered until October 1943 and then it was used not for a catalog but a more purely "statistical" attack. The navy built a version of a similar "statistical" attack into a Bombe device, the Bulldozer, which was in operation in June 1945. An introduction to the history of these machines is found in Lee Gladwin. 2007. "Bulldozer: A Cribless Rapid Analytical Machine (RAM) Solution for Enigma and Its Variations," *Cryptologia*, 31 #4, pp. 305-315. Technical descriptions of the HYPO and Bulldozer machines and their allied crypta-methodologies may be found in NARA RG38 R.I.P., RIPs 401, 601, and 605 #5, and documents such as NARA RG457 HCC, Box 600, 'HYPO'.

[19] Erskine, Ralph. 1999. "Kriegsmarine Short Signal Systems: and How Bletchley Park Exploited Them," *Cryptologia*, 23 # 1 (January), 65-97.

[20] Bray, Jeffrey (ed). 1994. *Ultra in the Atlantic*, Vol IV, Laguna Hills, California: Aegean Park Press . p. 207, shows that during early 1943 the median distance between a U-boat's location and a df 'fix' was over 100 miles. However, the 'fixes' became more accurate over time with fifty miles becoming the median distance in mid-1944. See also, NARA RG38 CNSG Library, Box 67, 'DF and the Submarine War', and. RG38 CNSG Library box 67 5750/783 'Analysis of the Effect of D/F Against The U-boats'. For other evaluations of direction finding during the early 1940s see, Ralph Erskine. 2004. "Shore High Frequency Direction-Finding in the Battle of the Atlantic: An Undervalued Intelligence Asset," *The Journal of Intelligence History*, 4 # 2, pp. 1-32, and, 1987, "U-boats, homing signals and HFDF," *Intelligences and National Security*, 2 #2, 324-330.

[21] NARA RG38 CNSG Library, Box 114, 'Safford on Reorganization of OP20G, 1942'.

[22] TNA PRO HW 14/45 December 1, 1941, 'To Washington CXG 105., ' Mrs. Driscoll has been sent all but an E machine, British co-operating on all systems'; TNA PRO HW 14/45, August 18, 1941. "List of Driscoll questions to GCCS re E and its solution'; NARA RG38, J. N. Wenger. Memorandum for Op-20-G, 13, May, 1944 'British Had Supplied Us With Needed Information on Enigma in 1941'; Kahn, David. 2002. "Britain Reveals it Bombe to America: From the Archives," *Cryptologia* ,26 # 2, (April), 124-128. TNA PRO HW 14/91, 4-11-43 November 4 1943 Commander Travis, OP20G Bombe Policy; TNA PRO HW 14/45 March 3 1941, 'Weeks pledge of secrecy'; TNA PRO HW 14/45 August 5, 1941, 're British - U. S. cryptologic relations'; TNA PRO HW 14/45 December 5, 1941, From Denniston. 'Explains lack of capture recent codebooks, states Britain has told OP20G all, and awaits Mrs. Driscoll information on her work'; TNA PRO HW 14/8, November 5, 1940 'DNI says request for US-British exchange of cryptographic systems came from British and U.S. Navy has no people to send;

[23] NARA RG457 HCC Box 705, NR 1736/7 'Bombe History and Enigma Conferences; NARA RG457 HCC Box 705, Bombe History folder; NARA RG38 CNSG Library, Box 117, 5750/205, 'Various on history of Bombe

project and British-OP-20-G relations; NARA RG457 Box 1124 Acc 17640, OP20G, 'History of the Bombe Project, 30 May, 1944; RG457 HCC Box 705, 35701 CBLH17, 24 April 1944; RG457 HCC Box 705, 35701 CBLH17, 24 April 1944.

[24] TNA PRO HW14/16, Feb. 15, 1942, On Britain's approval of the replacement of Safford. On the easing of tensions in general, Ralph Erskine, 1999, "The Holden Agreement on Naval Sigint: The First BRUSA," *Intelligence and National Security*, 14 # 2 (Summer), pp. 187-197.

[25] NARA RG38 Crane CNSG Library 5750/441 Box 183, Bombe Correspondence, July 16, Eachus Report to OP20 on Two-way flow in British GCCS Bombe; NARA RG38 Crane CNSG Library 5750/441 Box 183, Bombe Correspondence, August 6, September 18, and October 29 1942.

[26] NARA RG38, Crane Library, Box 115, On GYA.

[27] NSA FOIA, RAM File, April 25, 1942, 'Description of proposed U.S. Bombe'.

[28] NARA RG38 CNSG Library, Box 183 Bombe Correspondence; NSA FOIA, September 4, 1942, Wenger to Eachus, 'Electronics infeasible will pattern our Bombe on British.; NSA FOIA , September 23, 1942, Engstrom to Desch, 'Your plan for Bombe approved'.

[29] NSA FOIA, OP20G,, Wenger, 'Cryptanalysis of the German Cipher Machine, Sept. 3, 1942'.

[30] NSA FOIA, "Memorandum for OP-20, Establishment of OP-20-G activities at Dayton, Ohio," by J.N. Wenger, nd. (Re WAVES)

[31] NSA, FOIA, Desch, Joseph, "Memo of Present Plans for an Electromechanical Analytical Machine, September 14, 1942', also, http://cryptocellar.web.cern.ch/cryptocellar/USBombe/desch.pdf.

[32] NSA FOIA 10-23-1942, Desch to Washington.

[33] NSA FOIA, January 5, 1943, Engstrom to Meader, 're Turing visit and report and need to keep Bombe design flexible'. Gladwin, Lee A. 2001. "Visit to National Cash Register Corporation of Dayton, Ohio", *Cryptologia*, 30 # 1 (January), pp. 1-16. . See also, Gladwin's article on Alan Turing's critique of Driscoll's crib-catalog attack, *Cryptologia*, XXVII #1 (January 2003), pp. 50- and the update to that in, Ralph Erskine, Colin Burke, and Philip Marks. 2004. "Memorandum to OP2-20-G on Naval Enigma (c; 1940)", in Jack Copeland (ed), *The Essential Turing*, Oxford, Clarendon, pp. 341-352.

[34] NARA RG38 Crane CNSG Library 5750/44, Box 183, Bombe Correspondence 12-28-42, Travis Reports first Run of GCC's High Speed Bombe' but also reports possible changes in Enigma may call for changes to Bombes'

[35] NARA RG38 CNSG Library, Box 183.

[36] NARA RG38 Crane CNSG Library 5750/441 Box 183, Bombe Correspondence, June 3, 1943, 'GCCS informs OP20G of critical need for four wheel Bombes due short signal problem.

[37] NSA FOIA, Enciphered Telegraphic Link, Washington OP20G, Dayton NCR, 9-28-43 Dayton to Washington, 'Quillan pregnant'; NSA FOIA, Enciphered Telegraphic Link, Washington OP20G, Dayton NCR, 9-14-43 Dayton to Washington, WAVE cracks doing shortruns';

[38] NSA FOIA, Enciphered Telegraphic Link, Washington OP20G, Dayton NCR, 8-31-43 Dayton to Washington, 'WAVE Breaks Security'; NSA FOIA, Enciphered Telegraphic Link, Washington OP20G, Dayton NCR, 11-30-43 Dayton to Washington, 'Two WAVES unsuited for this work'; NARA RG38, CNSG Library, 1040/4, CNSG, General Personnel, ' Examples of WAVE letters, permissions and complaints by Washington D. C. residents'.

[39] NARA RG38 CNSG Library, Box 180, 3222/180, 'Secret teletype to Stone, re Montgomery'; FOIA releases from, FBI, ONI, Dept. of Justice.

[40] NARA RG457, HCC, Box 1729, August 10, 1943, 'Swiss American Reveals Allied Codebreaking.'

[41]

RG38 CNSG Library, Boxes 111-113, OP-20-GM-1-c-3 War Diaries, May-June 1'943; NSA RG457 HCC Box 620-1 NR 1665 CBKJ17 7465A 19410200 GERMAN KEY LOGS (FEB 41 - MAY 45).

[42] TNA PRO HW 3/93, 'Number and types of Bombes'. The major British Four-wheel Bombe could run two problems at once. That was in contrast to the American's single menu Bombe. Given the relative speeds and numbers of the two types, the British thus had the equivalent of 94 American Four-wheel Bombes.

[43] Bray, Jeffrey (ed.). 1994. *Ultra in the Atlantic*, 3 vols., Laguna Hills , California, Agean Park Press. Bray also listed 93 CI kills by American forces which equals 70% of all US sinkings during the war

[44] NSA RG457 HCC Box 620 NR 1665 CBKJ17 7465A 19410200 GERMAN KEY LOGS (FEB 41 - MAY 45) . NARA RG38 Crane Library Box 65, "Evaluation of the Role of Decryption Intelligence in the Operational Phase of the Battle of the Atlantic", has an analysis apparently using the file of original messages with a breakdown for each day by type of location messages -- but for only one year." The study for this article was made independently of the "Evaluation" report but the tallies proved equivalent. The Evaluation study is also in RG 457, Box 112 as SRH 368.

[45] The series includes a complete history of each German U-boat and its fate, from its launching through the end of the war. The nature of the records suggests that any allied claim of a sinking was checked against the later history of a U-boat. The nature of the records for the U-boats attacked or sunk by the Americans differs in some respects from those for British attacks and sinking, although they are in the same series. The British records are more detailed. They contain comments that differentiate between direct or full influence by Shark decrypts and partial influence. To allow comparison of the American and British records, two different estimates of Shark's British influence were compiled. The generous (Liberal) one combines the full and partial Shark-U-boat kills. The other (Strict) is for the fully-influenced kills only. The attacks and sinkings classified as 'partial' by the British seem to be those in which the location of a U-boat was already known through other means or that, for example ,there was not specific message about a U-boat although other messages had location data about other U-boats in the same pack.

[46] NARA RG38, Records of the Office of the Chief of Naval Intelligence (CNO). Records of the Naval Security Group (NSG) Central Repository Crane, Indiana, Boxes 96- ; Jeffrey Bray. (ed.). 1994. *Ultra in the Atlantic*, 3 vols., Laguna Hills, California: Agean Park Press.; David Syrett (ed.).1998. *The Battle of the Atlantic and Signals Intelligence, U-boat Situations and Trends, 1941-1945* Aldershot: Ashgate; and, David Syrett (ed.). 2002. *The Battle of the Atlantic and Signals Intelligence: U-boat Tracking Papers, 1941-1047*, Ashgate. For the Navy Records Society*;* Roy Conyers Nesbit. 2008. Ultra *Versus U-boats: Enigma Decrypts in the National Archives*, Barnesly, England, Pen and Sword; *David Syret. 1994, The Defeat of the German U-boats*, Columbia, South Carolina: University of South Carolina Press; *Captain S. W. Roskill, 1960. The Navy at War, 1939-1945* London: Collins; and, Samuel Eliot Morrison, *History of United States Naval Operations in World War II, 1st ed., 1947-1962*. Of these sources, Jeffery Bray's was judged as the most complete. NARA RG38 Crane Library Box 5,

"Evaluation of the Role of Decryption Intelligence in the Operational Phase of the Battle of the Atlantic", had analyses of what seems to be the data from the Orange files, but for only the summer of 1943..

[47] Bray, op. cit., Vol VI, p. 20, gives estimates similar to those derived from the German Cipher Key Logs.

[48] Bray's, op. cit., analysis of number of location, movement, and contact messages decrypted in the OP20G "evaluation" report also showed significant declines after May 1943, but with a temporary resurgence of "movement" messages in October 1943 as the U-boats reentered the North Atlantic convoy routes.

[49] The general data do suggest two brief periods of Shark success when key finding, the number and types of location messages, policies leading to aggressive Allied hunting-killing, and improved anti-submarine technologies came together in October-November 1943 and February 1944. However, the sinking rates during those months were still below the rates for the Dark Summer period; and, the high rates were confined to the area of the North Atlantic under British control..

[50] Bray's, op. cit., estimates, Vol. VI. p.2, and Roskill, op. cit., show some differences from those of Morison, but the trends are the same.

[51] Experts such as Bray, op cit., have revised the original estimates of sinkings by the Americans as in Morison, op. cit., but the differences are relatively slight and have little relevance to the theses in this article.

[52] Analysis of the summer 1943's cipher breaking yields 32 instances of two day or less decrypts that gave a U boat's location. But, most were from a May 24 message, five were from August nineteenth, and four were from July thirtieth messages. So, only three days during the some 3 to four months account for almost all 'locations'. See, NARA RG38 Crane Library Box 65, "Evaluation of the Role of Decryption Intelligence in the Operational Phase of the Battle of the Atlantic.

[53] On the refueling fleet, Bray. op. cit., Vol II, p. 83; NARA RG38 WWII Action Reports, 'Task Group 21.13, 'Bouge'.

[54] On the CI estimate see: NARA RG457, Box 112, SRH368, "Evaluation of the Role of Decryption Intelligence in the Operational Phase of the Battle of the Atlantic'. This and other sources give very high percentages to Shark for CVE attacks during summer 1943. However SRH368 also shows that of 62 At Risk incidents only 9 subs were attacked and for 92 instances of some location messages only 9 were attacked,

[55] Erskine, Ralph. 1995. "Ultra And Some U. S. Navy Carrier Operations." *Cryptologia*, 19 #1, (January), pp. 81-86.

[56] The U.S. records included an "indirect" influence of Shark location messages, The U.S. "indirect" was not defined as well as was the "partial influence" of the British. "Indirect" was defined as having a decrypted location message for a U-boat but its sinking occurring anytime (stress, anytime) beyond the At Risk limits. As a percentage of all sinkings, indirect was slightly more than 40% 1943-1945, 60% for 1943, 20% for 1944, and 30% in 1945. As with the American's "direct" influence, the "indirect" measure did not control for other factors.

[57] Using the analysis of Bray's list, op. cit., of 93 CI sinkings by the U.S. forces as the base, the estimate of At Risk U.S. sinkings, adjusted for out-of-Atlantic sinkings for 1943-1944 was 16% of the 133 total. Note that SRH 009 states there were 63 'direct' U.S. Ultra sinkings and some 30 indirect overall during the war.

[58] The Strict definition of At Risk was used for the British estimates in this column, the liberal (both strict and partial At Risk kills estimates were : 194 3= 29%, 1944 = 49%, 1943 & 1944 = 38%, 1-43 to 7-43 = 22%, 6-5 to 7-43 = 7% and 8-43 to 12-44 = 47%.

[59] For this combined estimate the liberal (both strict and partial) for At Risk influence for British sinkings was used.

[60] The index was computed by: (n of each month's u-boats in operation / sum of u-boats in operation 1943-1944) * (percent of u-boats in operation each month sunk while At Risk).

[61] Statistics complied from Roskill's, op. cit., lists and using his definition of areas.

[62] Meigs, Montgomery C. 1990, *Slide Rules and Submarines: American Scientists and Subsurface Warfare in World War II*, Washington D.C.: National Defense University Press..