A Global Forum for Naval Historical Scholarship

International Journal of Naval History

Volume 1 Number 1 April 2002

German vs. Allied Codebreakers in the Battle of the Atlantic

Stephen Budiansky

In mid-November 1941, Admiral Karl Dönitz, the Nazi commander of U-boats, noted in his war log his puzzlement over the repeated failures of German submarines to find and sink Allied convoys in the Atlantic. “Accident does not fall on the same side every time,” he insisted; it just could not be a coincidence that the Allies always seemed to choose a course that steered clear of his waiting submarines. There had been other suspicious events, too. Notably, in late September a British submarine had suddenly appeared and made an unsuccessful attack on three U-boats at a rendezvous off the Cape Verde Islands. It seemed to stretch credulity that a British submarine just happened along at this remote spot. Maybe, Dönitz speculated, the British had a new, secret kind of radar. Maybe the British were locating the U-boats with direction-finding fixes on their radio signals. Yet none of these possible explanations seemed quite right.

On the other hand, the one theory that *could* fully account for what was happening in the waters of the North Atlantic was inconceivable. Of this the Admiral was quite certain: The British could not possibly have broken the German Navy’s coded signals that were sent to and from the U-boats using the ultra-secret Enigma cipher machine. “This possibility is continuously checked by the Naval War Staff,” Dönitz wrote, “and regarded as out of the question.” The number of possible combinations that a code breaker would have to try each day in the hopes of hitting on the correct day’s setting of the Enigma machine was astronomical; it was a number on the order of a million million million million.

And yet the fact remained that each time Dönitz would deploy his U-boats to new positions, the Allied convoys would divert their courses around them. In June 1941, U-boats had sunk 310,000 tons of shipping. But in the months that followed the German success rate plummeted—to a quarter of that in July, a fifth of that in August. Dönitz felt in his bones that somehow the Allies were getting inside information.

* * *

One of the things about the code war behind the Battle of the Atlantic, which I think has not been fully appreciated, is that it was not merely a race to break the other side’s codes and thereby discover the enemy’s intentions—although neither side fully appreciated the fact themselves for quite a while—, it was also a race to discover that one’s *own* codes were insecure. It is a fascinating reflection on human nature just how resistant each side was to believing that its own codes were vulnerable. It took the Allies years to catch on

International Journal of Naval History

Volume 1 Number 1 April 2002

that their convoys were being found and sunk as a direct result of the insecurity of the Allied convoy codes, which the Germans had been reading on and off since fall of 1940. The Germans, for their part, *never* realized that the Enigma had been cracked. In fact in the late 1970s, when the first information about the Allied code-breaking triumphs in World War II began to filter out, Heinz Bonatz, director of the German navy's wartime code unit, the B-Dienst, declared that this was all nonsense. The British, he said, were simply incapable of *die geistige arbeit*—the "mental work"—required for such a feat. Bonatz insisted that the only times the British had ever achieved success in reading German code systems was when they had happened to obtain, by capture or theft, actual copies of German codebooks, as had happened in World War I.

Interestingly, the director of the British Admiralty's code-breaking unit during the First World War, Sir Alfred Ewing, had remarked in a public speech he gave in 1927 that one thing which had greatly aided their effort was what he called the "British reputation for stupidity," which prevented the Germans from ever suspecting that the British might haven broken their codes. History was certainly to repeat itself.

Interesting, too, was that Ewing indiscreetly revealed that throughout the war, the British had been very careful, when sending out to their own commanders' intelligence reports based on decoded intercepts, to disguise the source of that information—particularly, by attributing it to radio-direction-finding fixes, rather than to cryptanalysis. That was also a lesson the Germans failed to notice, or heed.

Documents released since those first revelations in the late 1970s have revealed how close a thing the code-breaking war was for the Allies in the Battle of the Atlantic. They also show how arguably the greatest bonanza that the British and American codebreakers reaped from breaking the German U-boat signals was that it allowed the Allies finally to discover the insecurity of their own convoy codes. That led, at the climax of the Battle of the Atlantic in late May 1943, to an urgent order to change the convoy code, and from that point on to the end of the war the Germans never broke it again.

There were also some unbelievable coincidences in this story. I still find it one of the most astonishing coincidences of the war that fate dictated repeatedly that each side's moments of success in breaking the other's codes would coincide almost precisely with a reversal of cryptanalytic fortunes on the other side. The result was that again and again each side would peer into his enemy's communications and reassuringly find no evidence that his own secret communications had been compromised. It happened in spring 1942, again in December 1942, and again in March 1943.

In March 1942, the German naval staff had conducted one of its repeated security investigations and in its report emphasized that there was nothing in Allied signals indicating the Allies were reading German Enigma transmissions. The report also

International Journal of Naval History

Volume 1 Number 1 April 2002

significantly concluded that the very fact that the British were using a code that was quite easy to break showed how unsophisticated they were about codes in general; therefore they were obviously incapable of the vastly greater cryptologic sophistication that would be required to break the complex Enigma machine. Again, the "British reputation for stupidity."

The reason the Germans found no hint of British success in reading German coded signals at this moment was, of course, that at just that moment the British were *not* having success. In retrospect, that was from the British viewpoint a small silver lining in what at the time seemed an unmitigated disaster. Beginning back in 1939 the British mathematician Alan Turing had brilliantly developed a complex sequence of mathematical techniques to break the Enigma. The challenge, however, was that breaking the Enigma was not a once-and-for-all proposition. You needed to do it every single day and on every single separate radio network the Germans operated; each day the German operators on a given network set up their machines to a different setting—a different one of those million million million million combinations. Turing's breakthrough was to see how as a matter of fundamental mathematical principle the machine was vulnerable; but there was still the Herculean daily task of applying his method to recover each day's new combination.

The key, first step to applying Turing's method was that it was necessary, each day, to be able to correctly guess at least a few of the actual words that a coded Enigma message contained. Then the codebreakers could apply Turing's mathematical procedures, recover that day's setting of the Enigma machine, and thereafter read every other message sent that same day on that particular network. Being able to come up with these correct guesses of words in a message was often the make or break part of the codebreakers' job. These bits of putative plain text were called "cribs."

The German Luftwaffe and to a lesser extent the German army were obliging enough to help the Allied codebreakers in their search for cribs by employing some terribly bad and sloppy practices, such as sending the same or virtually the same pro-forma reports day after day. There was for instance the German army unit at a remote outpost in North Africa that every day would send, at precisely the same time, a message reading "SITUATION UNCHANGED." Then one day the messages from this station abruptly ceased. The codebreakers were dismayed to learn a few days later that the British had captured this German outpost. Gordon Welchman, one of the leading British mathematicians working on Enigma, wrote a not-entirely-facetious memorandum asking if the British army would please check with him first before taking any more prisoners.

The German navy however ran a much tighter ship. Code operators were instructed to keep their messages to a bare minimum and to vary the way they wrote out familiar words and abbreviations so they would not use the same series of letters from one

International Journal of Naval History

Volume 1 Number 1 April 2002

message to the next. For example, instead of addressing signals to BDU, the abbreviation for Commander of U-boats, Enigma operators were instructed in their procedure manual to sometimes write BDUUU or any of a series of other inventive variations.

But by summer 1941 the British codebreakers had achieved their first real breakthrough and were beginning to read naval Enigma traffic. One particularly fruitful source of cribs were the routine weather reports the U-boats sent. These messages were enciphered with the Enigma machine, but they were first encoded in a shorthand form using a special weather codebook. Thanks to some codebooks captured from German weather ships and submarines in May and June 1941, the British knew how the weather code worked. And they were able to match up these weather reports sent from U-boats with subsequent synoptic weather broadcasts transmitted in a much simpler code, which they had already broken.

But then in February 1942 the Germans introduced a terrible complication—they changed the U-boat weather codebook, and almost simultaneously introduced a new Enigma machine with four coding wheels in place of three. The British were blacked out.

The next month B-Dienst broke the Allied convoy code, and Dönitz was frequently receiving decoded signals transmitted by convoys within 24 hours of their transmission. From June to November of 1942 virtually every order he sent to a U-boat group at sea was a direct response to intelligence gleaned from these decoded signals.

The Allies' dramatic capture of the new edition of the weather code book from U-559 in the Mediterranean in late October 1942—at the cost of the lives of two British sailors—finally ended the Allies' blackout. (This was the true story that was bastardized in the recent Hollywood movie, in which, among other things, the British became Americans.) By December 1942, the Allies were once again reading the U-boat Enigma signals, and again the strange and quirky hand of fate decreed that at just that moment the German codebreakers would temporarily lose their ability to read the Allied convoy code—this as a result of a routine change in codebooks.

So once again, the Allies were able to begin diverting their convoys around the waiting wolf packs. Once again, Dönitz sounded a security alarm. But once again neither side could see any direct evidence of code-breaking success on the other side, and so neither suspected that his own codes might be insecure.

By late January 1943 Dönitz was growing increasingly desperate. He wrote in his log that there could now be only two possibilities: either the Allies had somehow done the unthinkable and broken the Enigma, or —equally unthinkable—there was treason in the Germans' own ranks. The B-Dienst was feverishly working to break back into the Convoy Code and were by now reading occasional snippets. One of those snippets was

A Global Forum for Naval Historical Scholarship

International Journal of Naval History

Volume 1 Number 1 April 2002

distinctly alarming. An intercepted British signal on January 29 had warned of two U-boats at a precise latitude and longitude. The only trouble was the U-boats were not there yet. They had been *ordered* there for a rendezvous, but were still en route at the time the British warning went out. Direction-finding fixes could hardly explain that one.

Vizeadmiral Erhard Maertens, Director of Naval Communications, carried out yet another investigation. Yes, there was that odd January 29 report. But overall, Maertens concluded, the British intelligence reports were vague and "monotonous." If the enemy were actually reading German signals, Maertens insisted, their reports would be much better and more precise. And in a sort of triple logical backflip, Maertens argued that if the British were reading German signals, they surely would know from what was in the German signals that the Germans were reading British signals, and if they knew that, they surely would have immediately tightened up their own codes in response. But they had not done so, and so therefore the Enigma had not been broken. Martens titled this key chapter of his report "The Enemy is Reading Our Ciphers!?!" which I must say has a sort of perfect Colonel Klink cadence to it.

In March, for a third time fate played its impish trick. The Germans introduced yet another new weather codebook, blacking out the British codebreakers—just as the Germans' own codebreakers had caught up and began once again regularly breaking the Allied convoy code. Frantically the British codebreakers struggled to break back into the U-boat signals, and when they did on March 16 it was just hours too late to save two large convoys. The German codebreakers intercepted a series of signals from convoys HX229 and SC122 ordering course changes, and within hours, those signals were broken and in Dönitz's hands. Forty U-boats converged on the hapless convoys and it was a slaughter; 22 merchantmen and one escort were sunk, 146,000 tons in a single action.

Dönitz was jubilant, but it was to be his last hurrah. Of course, many forces were at work by spring of 1943 to turn the tide. Escorts were beefed up, new weapons such as the hedgehog depth charge thrower were introduced, Allied patrol aircraft were equipped with centimeter-wave radar, very-long-range aircraft were transferred to protect the convoys. But the climax of the Battle of the Atlantic in the late spring of 1943 also saw a climax of the code war, and the Allies' victory in this shadow war would have enormous and lasting consequences for the struggle at sea during the remaining two years of the war. In May 1943 U.S. Navy codebreakers helped crack three Enigma messages sent in the extremely difficult "officers-only" system that was used to relay intelligence to submarine commanders. All revealed that the Germans had incredibly precise knowledge of Allied convoy movements: location in latitude and longitude to a degree, speed to a tenth of knot. The U.S. Navy codebreakers immediately went to the convoy operations command and asked to see any messages the convoys had transmitted, to see if any of the Allied signals could have been the source of this German intelligence. The Navy codebreakers were summarily told that the messages were top secret and they could not

International Journal of Naval History

Volume 1 Number 1 April 2002

see them. Only after appealing directly to Admiral King was this bureaucratic door broken down. It was then instantly obvious that the Allied transmissions matched up precisely with the German intelligence reports. With this proof in hand, things happened fast. A new convoy code, Cypher No. 5, was immediately issued and ordered into effect, and that was that. The Germans never broke the convoy code again.

By summer 1943, U.S. Navy codebreakers had begun to take over the U-boat Enigma problem from the British—100 special-purpose, electromechanical code-breaking machines were being built by National Cash Register under a Navy contract, and the first ones began to come on line that summer.

With this advantage, and with their own codes now secure, the Allies' dominance of the code war was used to crushing effect. In June, July, and August 1943 the U.S. Navy carried out a series of devastating attacks at U-boat refueling rendezvous that they had advance knowledge of from Enigma signals. Within a year, the Allies had sunk 16 of the 17 tanker U-boats in the German fleet.

The Allies also used intelligence from broken Enigma signals to carry out some brilliant deception operations. The Enigma signals revealed that Dönitz incorrectly believed that the Allies had been locating his U-boats with infrared detectors; the British immediately fanned those fears by spreading double agent reports to the same effect. The Germans in response applied a new infrared-reducing paint to their boats, which actually made them *more* visible to Allied radar.

What in the end tipped the scales in the code war so heavily in the Allies' favor was not so much that they were smarter than the Germans, but that they were less cocksure. More specifically, the Allies, unlike the Germans, had always at least in principle been aware of the dangers of sending "raw" signals intelligence to their own commanders and had always made a point of watering it down or disguising its source. When they did want to send raw SIGINT to top commanders, they used an unbreakable one-time-pad code system. The Germans, supremely confident of the security of the Enigma, and especially the "officers-only" system within Enigma, did not take similar precautions.

But ultimately it came down to a fundamental asymmetry in views: The Allies correctly concluded that if they could break the Germans' codes, then the Germans might be able to break theirs. The Germans drew exactly the opposite conclusion: that if they could break the Allies' codes, then the Allies could not possibly break theirs. And that made all the difference.