UNCLASSIFIED

DAILY ENTERPRISE

(U) HISTORY TODAY - March 30, 2016

FROM: CCH
Run Date(s): 03/30/2016

(U) **A look back at WW II: double-encrypted Enigma messages**

(U) *"Until June 1943, a rather ridiculous situation existed that both sides were decrypting at least some of their opponent's signals without being aware that they themselves were being subjected to exactly the same form of eavesdropping."*
--- Patrick Beesly
Deputy Chief of the Admiralty's Submarine Plotting Room during WW II.

(U) During World War II Allied codebreakers recognized the link between speedy communication and successful German attacks against Allied convoys bringing supplies to the warfront. In U-boat warfare, communication was a major part of German military order; U-boats were not allowed to deviate from orders without asking (and receiving) permission from *Befehlshaber der U-boote* (BdU), the Head of the U-boat Arm. Although communications between the U-boats and BdU were short burst transmissions, communication was frequent and covered every aspect of U-boat disposition and attack. Studying U-boat communications allowed the Allied Admiralty Tracking Room to understand the U-boat problem, to the point that they could eventually predict the locations of U-boat wolf packs* with great accuracy.

(U) These tactics were used *against* the Allies. Allied communication was just as plentiful, and the security of convoys was closely linked to the encryption of their communication systems. Just as allied codebreakers eventually broke three-wheel, and later, four-wheel Enigma traffic, Axis codebreakers broke many codes pertaining to Atlantic convoys. Just as breaking Enigma traffic led to rooting out the locations of U-boat wolf-packs, breaking Allied convoy codes revealed the travel routes of convoys.

(U) One of the last Allied ciphers broken by Axis codebreakers, was Naval Cipher #3. The cipher was combined cipher, so-called because it combined a four-digit book code with a subtractor table (which acted as a layer of encipherment). Most codes at the time used additive rather than subtractor tables, but at the time, the British favored using subtractor tables due to their complexity. The subtractor table was changed every 10 days to maintain security. Despite these measures taken by the British, the German codebreaking unit B-Dienst figured out the basic methodology and was able to read a good portion of Allied messages.

(U) Some historians believe that cracking this cipher allowed BdU to know the whereabouts of Allied convoys 10-20 hours before the convoys received their orders. In February 1943 the Germans used intelligence from this cipher to plan and implement a successful attack against Allied convoy ON.166.

(U) Convoy ON.166 eventually reached its destination but incurred substantial losses (14 freighters sunk, 262 killed or drowned). To make matters worse, this cryptologic break coincided with the introduction of the fourth-rotor on U-boat ENIGMA cypher machines. The introduction of the fourth rotor meant that the Allies no longer had advance warning of waiting wolf packs. The wolf packs also seemed to be waiting for the convoys every time they changed directions.

(b)(3)-P.L. 86-36

[redacted]

(U) Lacking ENIGMA traffic to analyze, the Atlantic section of Op-20-G, the U.S. Navy’s cryptologic unit, reviewed tracking reports of U-boat patrols. Op-20-G analysts became suspicious when they realized that U-boats were switching their lanes of patrol within 30 minutes of each Allied convoy reroute. The Op-20-G analysts suspected a compromise to Naval Cipher #3 and requested an investigation.

(U) The investigators were unable to prove whether the Germans had broken Naval Cipher #3 and/or had obtained their intelligence elsewhere. Sure, B-Dienst had cracked previous Naval Ciphers 1, 2, and 4, but the Germans had intelligence coming from P.O.W. interrogations as well as sympathetic agents reporting Allied military movements. It was also possible that the compromise happened internally; U.S. Navy-British Naval communications were complex, repetitious and no one in authority knew how many times any particular message had been sent, by whom, and on what communication system. There was a general reluctance to refit the entire Allied communication system with an expensive new cipher, so Naval Cipher #3 remained in use.

(U) Admiral Karl Doenitz, commander of the German submarine fleet, congratulating some of his successful U-boat crews.

(U) By May 1943, the tide had turned. A new cryptanalytic *bombe* was able to break 4-rotor ENIGMA traffic and yielded proof of cipher compromise in the form of three Offizier messages.** Analysis of these messages found that three U-boat networks had received guidance so specific it had to have come from an Allied crypto compromise. Like the February attack, U-boats were given position coordinates and attack instructions, which they used to attack convoys HX 237 and SC 129. The difference was this time investigators could tie the intelligence to a specific source. Naval Cipher #3 had been used in all dispatches concerning convoys in the Atlantic.

(U) After obtaining access to the Navy’s 10th Fleet Convoy and Routing files, Allied investigators were able to look at suspected convoy messages and cross-check that information against Italian Naval Counter Intelligence interrogations. These interrogations provided the missing link: the Germans and Italians had cooperated in an attack on the Naval Cipher #3, aided by a copy of the basic codebook that they obtained covertly. This discovery eventually led to German understanding of the specific enciphering tables used to encrypt the message.

(U) Once the Atlantic section’s investigation was complete, the evidence was submitted to COMINCH (Commander in Chief of the U.S. Navy). After pushing the UK for a new cipher, the final book-based cipher used during the war was rolled out: Naval Cipher #5.

* (U) Wolf packs was a term used to describe a German U-boat naval warfare tactic used against Allied convoys in the Battle of the Atlantic during WW II. If an Allied convoy was located by a patrolling U-boat, the U-boat would alert its command BdU. BdU would then order other U-boats nearby to converge and attack the convoy.

** (U) Offizier messages were double-encrypted enigma messages. They were created on the U-boat enigmas, but used a special set of Offizier Stecker (plugboard settings) which were reserved for officer communications. They were then enciphered with the daily key. These messages were the only place investigators were able to find evidence that Naval Cipher #3 had been compromised.

(U) To discuss historical topics with interesting folks, visit the Center for Cryptologic History's blog, History Rocks ("go history rocks").
(U) Have a question or comment on History Today? Contact us at DL cch or [redacted]

(b)(3)-P.L. 86-36

[redacted]

Information Ow[redacted]
Page Publisher [redacted]
Last Modified: [redacted]
Last Reviewed: March 30, 2016

~~DERIVED FROM: NSA/CSSM 1-52, DATED: 20180110, DECLASSIFY ON: 20430110~~

UNCLASSIFIED

(b)(3)-P.L. 86-36

[redacted]