(U)Cryptologic Almanac 50th Anniversary Series

(U)The Last Days of the Enigma

(U) After hearing the many intriguing success stories about theexploitation of Enigma communications (shortening WWII by at least a year,successes in the battle of the North Atlantic, support to the battle inEurope), did you ever wonder how it all ended?

(U) Use of the Enigma started modestly in the late 1920s and early 1930swith the machine being applied to commercial uses. Only the Poles, however,who were more keenly aware than most of the German threat, saw the potentialdangers of Enigma being used for military purposes. They acquired a machineand started working on ways to exploit the problem. In 1939 with the Germaninvasion of Poland, the Poles passed their knowledge to the British andFrench. The British made great progress advancing the art of breakingEnigma, and continued developing the "bombe" used in breaking the Enigmamessages. The bombe was a huge electromechanical device, which could analyzeassumed text and determine the validity of the proposed solution. The Polesconceived and built the device, and the British developed its application.The British in turn involved the U.S., which refined the bombe's use indecrypting the Enigma messages.

(U) Volumes have been written about the value of the Enigma decrypts duringWWII and the extreme measures taken to protect the successes. Movies havebeen made depicting the extraordinary efforts taken to acquire new Enigmamachines and the keys used. The most popular undertakings were the effortsto capture German submarines in order to get the cryptographic materials.

(~~TS//SI~~) At the end of WW II, contrary to what one might believe, the use ofEnigma did not cease in a bunker in Berlin in 1945. It lingered on to aninsignificant demise in 1955. The East Germans continued to use the Enigmaequipment, but its role diminished, until by the early 1950s they were usingit only in Berlin.

(~~S//SI~~) Case notations were used to identify discrete communicationsentities so that one could follow and maintain continuity on a given set ofcommunications. These designators were assigned according to a prescribedsystem. For instance, in GCPB 00101, the "GC" denoted East German, the "P"indicated Police, and the "B" meant that the mode of communications wasManual Morse. The "001" and "01" signify the number of the network and thenet within the network. In this case we have only one net and that was theEast

German police in Berlin. GCPB 00101 was the last communications networkto carry Enigma traffic, which the U.S. exploited.

(TS//SI) The content of the communications carried on GCPB 00101 could bedescribed as mundane at best. It contained fire damage reports, state ofreadiness of various fire stations and police reports, mostly regardinginsignificant arrests. This was not the exciting content produced duringWWII, yet the priority given to intercepting this traffic was extremelyhigh. People working on the traffic analytic aspects of the problem andthose continuing the efforts to read the messages could not understand whythe mundane content of the messages would warrant the high priority affordedthis target in the mid-1950s. Obviously those in the hierarchy at that timeknew, but the rest could only speculate.

(TS//SI) In retrospect it would appear that, with the famous "Berlin Tunnel"operation under way, the U.S. was most interested in knowing about anyreflection or knowledge on the part of the East Germans of the tunnel'sconstruction and activities.[1] Police and fire reports might just providesuch information and hence the high priority given to GCPB 00101. Littledid we know at that time that the noted British traitor, George Blake fromMI-6, in all probability had already had compromised the tunnel operation.

(S//SI) Then one day in 1956 Ellie Carmen Klitzke, chief of the East Germancryptanalytic section located in A Building at Arlington Hall Station,notified Preston Welch that the effort on Enigma was to be terminated.Preston was the cryptanalyst in charge of developing "menus" to be run onthe bombe. These menus were short passages of text, which he suspected werein the encrypted message. The menus were run on the bombe and, if the guesswere correct, the bombe would yield the setting for that message so that itand other messages could be read.

(U) With a modest degree of fanfare, Preston held up a package and announcedthat it contained the last menus to be run on the bombe. He handed thepackage to a cryptanalytic intern who caught the shuttle bus from ArlingtonHall Station to the Naval Security Station and delivered the menus to theNavy Waves who ran the bombe. They in turn ran the machine for the lasttime. By way of footnote, one of the last bombes used is on display at theNational Cryptologic Museum.

[(U//FOUO) William T. Kvetkas, Center for Cryptologic History, 972-2893s]

---

[1] (TS//SI) The Berlin tunnel scheme was an elaborate undertaking to dig atunnel from West Berlin to East Berlin and tap communications cables.Construction began in 1954 and was completed in 1955. It yielded enormousamounts of traffic before it was terminated in 1956 upon discovery by theEast Germans.

DOCID: 3101787

Almanac 50th Anniversary Series

Content Owner: Feedback

Web POC: Feedback

Last Modified: by nsr
Last Reviewed: February 28, 2003
Next Review: 365 days