

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

# THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

~~TOP SECRET//COMINT//X1~~

## (U)Cryptologic Almanac 50<sup>th</sup> Anniversary Series

### (U)The Last Days of the Enigma

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

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

(U) Volumes have been written about the value of the Enigma decrypts during WWII and the extreme measures taken to protect the successes. Movies have been made depicting the extraordinary efforts taken to acquire new Enigma machines and the keys used. The most popular undertakings were the efforts to 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 of Enigma did not cease in a bunker in Berlin in 1945. It lingered on to an insignificant demise in 1955. The East Germans continued to use the Enigma equipment, but its role diminished, until by the early 1950s they were using it only in Berlin.

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

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

(~~TS//SI~~) The content of the communications carried on GCPB 00101 could be described as mundane at best. It contained fire damage reports, state of readiness of various fire stations and police reports, mostly regarding insignificant arrests. This was not the exciting content produced during WWII, yet the priority given to intercepting this traffic was extremely high. People working on the traffic analytic aspects of the problem and those continuing the efforts to read the messages could not understand why the mundane content of the messages would warrant the high priority afforded this target in the mid-1950s. Obviously those in the hierarchy at that time knew, 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 any reflection or knowledge on the part of the East Germans of the tunnel's construction and activities.<sup>1</sup> Police and fire reports might just provide such information and hence the high priority given to GCPB 00101. Little did we know at that time that the noted British traitor, George Blake from MI-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 German cryptanalytic 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 on the bombe. These menus were short passages of text, which he suspected were in the encrypted message. The menus were run on the bombe and, if the guess were correct, the bombe would yield the setting for that message so that it and other messages could be read.

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

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

---

<sup>1</sup> (~~TS//SI~~) The Berlin tunnel scheme was an elaborate undertaking to dig a tunnel from West Berlin to East Berlin and tap communications cables. Construction began in 1954 and was completed in 1955. It yielded enormous amounts of traffic before it was terminated in 1956 upon discovery by the East Germans.

Almanac 50<sup>th</sup> Anniversary Series

Content Owner: Feedback

Web POC: Feedback

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

~~TOP SECRET//COMINT//X1~~

~~DERIVED FROM: NSA/CSS MANUAL 123-2  
DATED: 24 FEB 1998  
DECLASSIFY ON: RT~~