Naval War College Review

Volume 41
Number 4 *Autumn*

Article 12

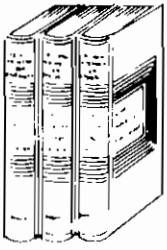
1988

Enigma. How the German Machine Cipher Was Broken, and how It Was Read by the Allies in World War II

George Kraus
U.S. Navy

Wladyslaw Kozaczuk

PROFESSIONAL READING



A book reviewer occupies a position of special responsibility and trust. He is to summarize, set in context, describe strengths, and point out weaknesses. As a surrogate for us all, he assumes a heavy obligation which it is his duty to discharge with reason and consistency.

Admiral H.G. Rickover

Commander George Kraus, U.S. Navy

Kozaczuk, Wladyslaw. *Enigma. How the German Machine Cipher Was Broken, and how It Was Read by the Allies in World War II*, ed. and trans. Christopher Kasparek. Frederick, Md.: Univ. Publications of America, Inc., 1984. 348pp. $24

A large and growing number of books and articles regarding the cryptologic effort by the Allies that resulted in the breaking of the German Enigma machine cipher system in World War II are available to the interested reader. In addition to *The Ultra Secret* by F.W. Winterbotham (1974), which provided for most readers the first intimation of the nature and scale of the success of this effort, books by and about many of the participants have been published, and a number of studies on the use and impact of the actual decrypted traffic on the war's course and outcome are available. A short list of the best of these works to date is appended at the end of this review. While the earliest books and articles were often somewhat sketchy, if not outright misleading, many of the more recent works have benefited from the larger body of declassified material that continues to appear and from more serious scholarly attention to these sources. Nonetheless, the work of reconstructing what really happened and answering the question of whom to credit or blame continues apace. In that regard, and for its impact on World War II, *Enigma* by Wladyslaw Kozaczuk is essential reading for the student of cryptology.

In the fall of 1932, three young mathematicians began work in the Cipher Bureau in the general staff building in Warsaw, Poland. During the next

four months, these men, Marian Rejewski, Henry Zygalski, and Jerzy Rozycki, were able to break the German Enigma machine cipher. From this initial success in January 1933, they continued to read the Enigma traffic through the end of 1939. The Germans' many changes over that period were followed successfully by these men at a time when they were the only existing cryptologic element having such success.

In order to solve the complex unknowns of the changing keys used by the Germans, the Poles evolved the basic tools that were later elaborated and enlarged upon by the British at Bletchley Park (Government Code and Cipher School) to perform the same functions for the remainder of the war. In January and July 1939, the Polish met with the British and French in Paris and Warsaw respectively, and the tripartite collaboration dedicated to the breaking of Enigma was arranged. These meetings were set in motion by Major Gustave Bertrand, Chief of French Radio Intelligence, who had maintained an ongoing collaboration with the Polish since late 1932. The British were reluctant participants, apparently believing that there was little to be gained from such a meeting, though they were not reading Enigma traffic at that time. As Kozaczuk notes, the British ". . . had not been in touch with the Polish cryptologists and did not imagine that they could have any achievements in regard to Enigma." Though little was accomplished in January, the Polish General Staff consented to make available to the Allies in July 1939 the methods and devices developed to read Enigma. The British and French each received a Polish-built duplicate Enigma machine and chapter and verse on techniques of solving the keys. In addition to the reconstruction of the Enigma machine itself, the Polish had developed an electromechanical device designated the "Bomba" (later to be rechristened "Bombe" in its elaborated British version), an aggregate based on six Polish Enigmas that tested all the possible rotor positions to yield the daily keys. They had also worked out a method using specially perforated paper sheets to break the double-enciphered individual message keys. These techniques were also provided to the British and French.

The perceptive reader who is familiar with the Enigma literature will no doubt realize that the reconstructed machine with the details of its internal design and layout complete, including the description of additional rotors that were added to increase the keying complexity, was of paramount importance to the British cryptologic effort. The details of the decryption techniques employed, the "Bomba," and the perforated sheets used to break key were equally invaluable. In fact, though these techniques were later elaborated in both sophistication and scale, they formed the basis of virtually all the Enigma work at Bletchley Park. Thus, a careful reading of this book demonstrates that the Polish solved Enigma and provided the solution and everything that went with it to the British. The enormous and sustained effort, organization, and talent that enabled the denizens of Bletchley Park

to read Enigma traffic thereafter is not demeaned by the acknowledgement of the true extent of the Polish contribution. The author uses personal accounts and documentary sources in Polish, English, French, and German to make his case and includes a detailed set of appendices, including one (Appendix E) by Marian Rejewski that describes the mathematical solution of the Enigma cipher. A reader of the major available works regarding Enigma at Bletchley will be forgiven for not having discovered the true extent of this Polish contribution earlier because the Polish connection generally has been treated in cursory and contradictory fashion.

Although this book is an interesting and necessary addition to the literature about the Second World War, it is flawed. The work is choppy and somewhat disjointed, partly because so much of the story has been put into the copious documentation that follows every chapter, resulting in the requirement to swing back and forth between the details of the cryptologic effort and the grander sweep of wartime developments. It may be that this is the result of a less than perfect translation, but, on the whole, it is only an occasional annoyance. In contrast, the decision to place the more detailed mathematical descriptions of the assault on Enigma in appendices is applauded. This permits reading through the narrative and getting the essential chronology, while those interested in the detailed mathematical treatment can consider Rejewski's solution at their leisure.

Unfortunately, the author makes several errors of fact (of the sort he criticizes in other books that discuss the Polish contribution). For example, he repeats the story of Churchill's decision not to evacuate Coventry despite having been warned of impending attack by decrypted Enigma traffic (p. 167). Though he does note that this tale is disputed, he leaves the reader with the impression that it is at least plausible. The accurate, detailed description of this incident in R.V. Jones' *The Wizard War* shows that it was, in fact, impossible. On page 187 the author asserts that it has now ". . . become clear that the decisive factor in Germany's loss of the Battle of Britain may well have been Allied mastery of Enigma," rather than Britain's use of radar. Once again, I would recommend referring to R.V. Jones for a more balanced view of the defeat of the Luftwaffe attacks. He shows rather clearly the interaction of intelligence, provided from all sources, with the operational employment of air defenses crucially controlled by radar. In the otherwise fairly accurate chapter on "Enigma at Sea" (chapter 14), the author relates an account of the *Bismarck* affair that is neither as complete nor as accurate as the detailed discussion he quotes from Patrick Beesly's *Very Special Intelligence* (chapter 5). Winterbotham, who is extensively quoted, is an unreliable source since much of his book is based on memory and he was not involved in the analysis process. Beesly's account is by far the more balanced and accurate.

The author also engages in an almost Soviet-style aggrandizement of history with his description of the Polish destroyer that "finally located and pinned down" the *Bismarck* (chapter 14, footnote 9). The battleship had been damaged by air attack and her fate was already clear due to her jammed rudder that precluded escape. The Polish ship was one of five destroyers under the command of Captain Philip Vian, RN, that maintained contact with the *Bismarck* until the converging British battleships arrived.

Nevertheless, though imperfect, *Enigma* is an important book about the specialized area of cryptology during World War II. It highlights the critical role of the small but talented band of Polish patriots who were able to hand a most critical advantage to their allies, even as their own country was being overrun by the Germans and Soviets. David Kahn has characterized the breaking of the Enigma machine cipher as one of the greatest intelligence feats of all time, "an accomplishment that, during World War II, determined the fate of thousands." Judged in that light, Churchill's paean to the "few" of the RAF to whom "so many owed so much" after the Battle of Britain, could well be expanded to include these "few" Polish mathematicians.

The following short list includes some of the best books available regarding the business of cryptology during World War II and the use of its product:

Hinsley, F. H. et al. *British Intelligence in the Second World War.* London: Her Majesty's Stationery Office, 1979-84. 3v.

The "official" version of events and certainly the most comprehensive intelligence history published anywhere.

Beesly, Patrick. *Very Special Intelligence.* Garden City, N.Y.: Doubleday, 1977.

This is one of the very best descriptions of the creation of an "all-source" intelligence center focusing on the naval war, with the detail that Donald McLachlan could not include regarding Ultra in his earlier, but still valuable book, *Room 39.* Also see Beesly's:

Very Special Admiral: The Life of Admiral J. H. Godfrey CB. London: Hamish Hamilton Ltd., 1980.

Bertrand, Gustave. *Enigma: ou la plus grande enigma de la guerre.* Paris: Plon, 1973.

General Bertrand's book actually predates the publication of *The Ultra Secret* in the United States and includes many of the same revelations. It also is much more explicit regarding the role of the Polish in breaking Enigma than most subsequent accounts. Nonetheless, Bertrand tends to overstate his role, and the book should be read with care.

Calvocoressi, Peter. *Top Secret Ultra*. New York: Pantheon, 1980.

A short but very useful look at Bletchley by an insider. It includes the most complete and accurate account previously available regarding the role of the Polish cryptographers (chapter 2). The appended note on the Ultra documents released as of its publication (pp. 115-117) is quite useful to the researcher.

Jones, R. V. *The Wizard War*. New York: Coward, McCann & GeoGhegan, 1978.

The best book on the difficult process of intelligence analysis by one of its foremost practitioners. R. V. Jones virtually invented scientific and technical intelligence as a discipline while serving in the British Air Ministry in World War II. His account of some of the most significant intelligence coups of the war are told in both an entertaining and educational way. Certainly one of the single best books on the intelligence business.

Kahn, David. *The Codebreakers*. New York: Macmillan, 1967.

This book predates most of the revelations regarding Ultra and Enigma, focusing on the U.S. efforts against the Japanese. It is, however, a *tour de force* regarding the history of cryptography for the serious student of the game and for the professional intelligence and military officer.

Lewin, Ronald. *The American Magic*. New York: Farrar, Straus & Giroux, 1982.

Lewin, Ronald. *Ultra Goes to War*. New York: McGraw-Hill, 1978.

These two books are among the best currently available regarding the use of Ultra information in pursuing the war effort. Also highlighted is the effectiveness of the disparate commanders in using the often unique insight given them by Ultra.

Parrish, Thomas. *The Ultra Americans: The U.S. Role in Breaking the Nazi Codes*. Briarcliff Manor, N.Y.: Stein and Day, 1986.

A useful insight into the development of U.S. signals intelligence in World War II and the participation of U.S. personnel at Bletchley. Parrish lists Kozaczuk's book in the bibliography and refers briefly, but accurately, to the Polish role (see for example, pp. 50-51 and 112-115).

Welchman, Gordon. *The Hut 6 Story*. New York: McGraw-Hill, 1982.

Another book about the details of the decryption business from a veteran of Bletchley Park. This is both an entertaining and insightful look at cryptological problems and at the personalities of the players, and is most accurate when Welchman sticks to the activities with which he was personally involved. He does, however, include some material of dubious

accuracy. See, for example, his rehashing of a story from William Stevenson's *A Man Called Intrepid* (p. 13), a flawed tale from a flawed and notoriously inaccurate book.

■

Lieutenant Commander Sam J. Tangredi, U.S. Navy

Topitsch, Ernst. *Stalin's War*, trans. A. Taylor and B. E. Taylor. New York: St. Martin's, 1987. 160pp. $19.95

Subtitled *A Radical New Theory of the Origins of the Second World War*, *Stalin's War* is not just another revisionist interpretation of an often-told story. It is undoubtedly the boldest revision yet attempted, representing an authentically novel approach to answering history's greatest enigma: what were Adolf Hitler's strategic goals in launching an apparently suicidal war against all other world powers?

Previous efforts to answer this question have focused on the role of Hitler as architect of the war and ultimate world decision maker. There are various shadings of explanation: Hitler was a psychotic, he miscalculated the character of the Allies, he was a military genius who overextended his forces, he was goaded by the capitalists, etc., etc.

Yet, all the varying interpretations agree on the central role of this one man, although some revisionist writers have passed small bits of conspiratorial guilt on to others—to an uncompromising Churchill or bellicose Roosevelt. But, by consensus, it is still Hitler's war; written, directed, produced, and starring the Reichsführer, who—most fortunately—loses control of the production in the end, although only after the Continent is laid to waste and whole ethnic groups destroyed. However, despite the consensus on the focal point, the question still seems to defy a definitive explanation—what did Hitler really want?

To answer the question, Professor Topitsch inverts it. As a starting point, he posits that it is impossible to determine what Hitler wanted because the Führer did not know what he wanted. Beyond "his twin obsessions" of *Lebensraum* in the East and Teutonic racial superiority, Hitler did no coherent planning and had only the vaguest strategic aims. Controlling the world was grandiose even from a Nazi perspective, and Hitler was often heard to proclaim his regrets at the multifront conflict resulting from continual blitzkrieg.

Concluding that Hitler started a war that was never in his strategic interests (since he had already achieved his immediate aims in the West, without war), Topitsch is forced to tackle the question from the opposite direction and ask: in whose strategic interest was the war that pit Germany against the democracies? While not attempting to deny Hitler's personal