The Ultra Secret by F.W. Winterbotham. Book review by Louis W. Tordella

~~SECRET~~

THE ULTRA SECRET by *F.W. Winterbothamn*, CBE. (Harper & Row, New York, 1914)

We now have available a book purporting to reveal facts about British communications intelligence successes in World War II. Same passing references are made to U.S. work in this field. If such a revelation about Allied crvptanalytic successes in yy-'W II was inevitable, it can be debated whether a professional COMINT officer would want it made by a person who knew absolutely nothing of any technical aspects of the subject (certainly true of RAF Group Captain F. W. Winterbotham) or by one possessing at least the most elementary technical knowledge. In the first instance, a Winterbotham can reveal the fact of analytic operations against the German ENIGMA while hopelessly confusing the extent of the success and the fact that other types of machines and hand systems were also involved. A person with any technical background could never have made the word ULTRA synonymous with ENIGMA decrypts. ULTRA simply was an UK/US agreed word to designate decrypts resulting from decrypts. work against any targeted high-level system.

Once reconciled to the inevitability of publication, a cryptanalyst can single out a number of interesting aspects of *The Ultra Secret*. It

increases, for instance, the depth of meaning of Churchill's famous statement "Never was so much owed by so many to so few." There actually were two "fews" involved, one of them the RAF fighter pilots and the other the "cryppies" at Bletchley Park, the site of most of the British wartime cryptanalysis. But let us not unduly distort our perspective because of the book. Cryptanalysis did not win the war either in Great Britain, in the Atlantic, in Europe, or in the Pacific. It was a weapon, one of utmost value, but still a weapon to be used either skillfully or clumsily. Both usages occurred, and many are highlighted. In the glow of crvptanalytic successes, the reader may overlook the need for the blood and the sweat and the tears of the fighting men. There was extended hard and very bloody fighting in all theatres, without whose success there would be no Free World as we know it. The fearlessness and self-sacrifice of the skilled and all-too-few RAF fighter pilots gave Britain a chance to survive. True, they were often positioned in advance and the number of them actually committed to any engagement was carefully scheduled and controlled by knowledge derived from ENIGMA (when available) and other decrypts. We should also note that the actual engagement and the fighting, once a German raid was launched, were heavily influenced by British radar which was vital both to give the precise last-minute timing and location of the raid and to provide plausible cover for the effective fighter attacks. This cover was good enough to fool the Germans and most of the English, for only a very few most senior English commanders knew of the existence of the decrypts.

Full credit must be given to Group Captain Winterbotham for the establishment and maintenance of what today we would call an SSO (Special Security Officer) system. He worked hard at it, and it was effective. I am not so sure that the comparable United States SSO system, particularly in the Pacific, was as much dependent on his energy and travel as he would have the reader believe. But he does make crystal clear the successful and necessarily extreme measures that were used to control the handling of ULTRA and, where possible, to sanitize it so that it could be used in a timely manner. He leaves no doubt that some of the brilliant tactical victories achieved by maneuver and accurate estimation of enemy intentions were made possible by looking into the ULTRA mirror which revealed key cards in enemy hands. This information may, no doubt, reduce the stature of some battlefield commanders. Some were unable to grasp the meaning of the material made available to them or unwilling to use it promptly for some reason or other. No need for me to name names in this review, for Winterbotham's book is based not on official history but on his

recollections, which are at best incomplete even if quite accurate in places.

The Ultra Secret is a prolific source of misinformation. It is absurd or wryly laughable to read that the cryptanalytic coups against the Japanese navy, e.g., the Battle of Midway, were made possible because ENIGMA machines were used by that navy. None were used for any Japanese navy traffic at any time in any area. It is equally erroneous to imply that any Japanese diplomatic communications were ever enciphered by a derivative from any version of the ENIGMA. The "purple" (diplomatic) and the "red" (naval attach6) machines were related to one another, but in no way to any German equipments.

No one of dozens I knew from Bletchley Park, either in the British party or in the sizeable American contingent, had ever heard of the "bronze goddess" or the "Eastern Goddess" or the "oracle of Bletchley" until they read this book. Winterbotham speaks of *one* decryption device, whereas in fact there were almost two hundred British devices by 1944, and more than one hundred equipments in the U.S. of a more complicated nature to deal with more sophisticated versions of the ENIGMA. All were called "BOMBES" after the Polish name for their analytic equipment, "bomba," since the Poles first achieved a cryptanalytic solution in the late 30's of one of the original (and simpler) versions of the ENIGMA. The "BOMBES" were used to set messages and not to decrypt them. Decryption was done either on replicas of the German equipments or on higher-speed cryptographic equivalents manufactured by the United Kingdom or the United States. No "goddess" or "oracle" did any speaking.

Seriously misleading inferences can be drawn from the book, e.g., that almost all German traffic was read and that all levels of traffic, including the highest level of command, were enciphered by using ENIGMA machines. In actuality a very skilled management of available COMINT resources was mandatory, for there always was more traffic to be set and decrypted than available cryptanalysts and equipment could manage. Selectivity of material and direction of effort were skillfully accomplished, as the results show. There also were several other kinds of German machines in use; the several different versions of the ENIGMA were devoted almost exclusively to operational traffic. A message from Hitler enciphered by ENIGMA is so rare as to be almost if not actually non-existent. I have heard of none such. Highest-level German Command traffic, including messages from Hitler, was enciphered in other machines apparently unknown to Winterbotham. An

occasional German commander would insist that his orders not be transmitted on the air, possibly (or probably) more because he mistrusted the setup which made cryptographic and code room personnel knowledgeable of his plans than because of any doubts about the security of the cryptography.

Another major aspect of the problem, apparently quite unknown to Winterbotham, was the difficulty of actually understanding and making operational sense out of the decrypts. This statement might be clearer if the reader were to imagine that he began to have somewhat random access to streams of technically-oriented telegrams and not to all of them in any one stream. It would take some time and intensive study and imagination to develop the background and the specialized vocabulary necessary to understand the telegraphese, the abbreviations, the specialized allusions, the references to past events and statements, etc. A very major effort had to be put into this work, and brilliant results followed. But the work involved, the competence of the intelligence analysts engaged in this area, and the many frustrations and false leads that were not allowed to hamper the flow of useful material are not even alluded to in the book.

The sizeable American contingent working side by side and around the clock with their British colleagues at Bletchley Park has been overlooked. Maybe Winterbotham never actually crossed the threshold into the working area? There is almost no mention of the German Naval ENIGMA, a more complicated equipment than the Army version, whose solution was so important in winning the battle of the Atlantic. Nowhere in Winterbotham's book is there any clear indication of the effective wartime liaison and exchange of technical personnel and data between the British and the U.S. Army and Navy COMINT organizations.

Judged from the viewpoint of today's cryptanalysts, it is most helpful that *The Ultra Secret* is the bad and incomplete book it is. His account is inaccurate in detail, and although it resembles the truth in outline, much of it is purely imaginary. Nonetheless, one seriously damaging effect the book will have is to give target communications security organizations an accurate base line from which to estimate the competence of the US/UK SIGINT organizations. The successful cryptanalysts of the ENIGMA in the 1940's as set forth in the book gives an accurate measure of competence not hitherto available in unclassified literature. Extrapolation from that information in light of the power of modern, very powerful computers may well cause several lucrative targets to have

second thoughts about their present systems and to take remedial measures. I do not believe the book should have been published, nor do I think it would have been if Group Captain Winterbotham had not hoped to usurp a prominent place in the spotlight he is using to illuminate an area that practicing COMINT personnel would prefer to have in the shadow. Without competent code clerks and communicators, the successes he details could not have occurred; his valid claim to fame is scarcely greater than theirs. In addition to alerting target Communications Security organizations to the UK/US cryptanalytic capability against a device of the complexity of the ENIGMA, *The Ultra Secret* will probably have the effect of causing someone (not me) to attempt a book in which Winterbotham's many errors are corrected and the American role adequately portrayed. Further revelations can only make steeper and rockier the road today's cryptanalysts are walking.

Louis W. Tordella

~~**SECRET**~~

Posted: May 08, 2007 08:46 AM