Naval War College Review

Volume 40
Number 2 *Spring*

Article 19

1987

Machine Cryptography and Modern Cryptanalysis

James S. O'Brasky

Cipher Deavours

Louis Kruh

dedicated secret service organization that did its part in World War II in the face of overwhelming odds. Foot describes the circumstances, political turbulence, and decisions that went into the creation of the super secret SOE and guided its operations throughout its existence. He explores in detail the ways agents were recruited, trained, equipped, and controlled. The people that made up the SOE were ordinary people of uncommon valor from all walks of military and civilian life.

An agent had to live by his wits in an environment where even the slightest unconscious mistake could result in discovery and capture. Capture often meant imprisonment, torture, and death. Some agents "sold out" to the enemy, some held out valiantly until their deaths, and a few were able to maintain such a convincing cover story that they were released without it being discovered who they really were. Some operations succeeded, some failed, and some simply survived bureaucratic bungling. SOE experienced the same turmoils, rivalries, and suspicions that unconventional organizations cloaked in secrecy experience today.

The author strives to give the reader an appreciation of the dangers, frustrations, and triumphs experienced by this small group of brave volunteers. He also atrempts to give broad insight into the creation and functioning of this fascinating organization that, in a way, is a forefather of today's covert intelligence agencies.

DAVID C. RESING
Commander, U.S. Navy

Deavours, Cipher and Kruh, Louis. *Machine Cryptography and Modern Cryptanalysis*. Dedham, Mass.: Artech Hse., Inc., 1985. 256pp. $56

Communications intelligence and code breaking have become such standard features of World War II historical analysis that the contemporary reader may be forgiven for assuming that this body of information was generally known shortly after the war's conclusion. In fact, the first allusion to the penetration of the German Enigma system appeared in the 1968 book, *The Philby Conspiracy*, and the full magnitude of this accomplishment did not become apparent until F. W. Winterbotham's book, *The Ultra Secret* was published in 1974. A number of books have been published since that time dealing with the military, political, and organizational aspects and the implications of these revelations.

The breaking of machine cyphers is first and foremost a scientific and intellectual achievement of the highest magnitude. In this book the authors have provided the technical reading public with a singular service; namely, a guided tour through one of the last great intellectual achievements executed by a single human mind or through a small team effort. Messrs. Deavours and Kruh have reconstructed and presented a highly readable form, the procedures which decoded the five princi al mechanical and electromechanical code machine families. These procedures are presented in a step-by-step manner so that the interested reader can, with patience and

diligence, solve these machine cyphers himself. At each step, the mathematical justification is presented. In many cases, the authors have consulted primary sources in the development of their solutions. Such sources are technical papers of the actual participants and where possible, the actual principals have been interviewed.

Machine Crytography and Modern Cryptanalysis is clearly a book for a special audience of scientists, engineers, applied mathematicians and of course, "cypher fanatics." While a knowledge of group theory and statistics is extremely helpful, the general reader can very profitably read this work, given concentration and patience.

For the general reader and the specialist this work provides a number of valuable insights:

- Simultaneous invention of methods, procedures and even hardware is a common occurrence even in a secret environment;
- Superiority in applied mathematics and science and at least a local environment of free expression and technical honesty are the enabling conditions for great technical achievement in general and cryptological breakthroughs in particular. The survival of one's nation can turn on the result;
- Secrecy is a necessary environment which must be creatively managed if interactions between secret developments are to be fully integrated, e.g., cryptanalysis and cypher machine development; and
- As activities grow and require industrial style organization, programs become managed by people who often do not have the depth of understanding of the technical issues which govern their programs. The bureaucratic imperative becomes operative, often with tragic results. The failure of the German and Japanese cypher systems can be laid fundamentally to such causes.

The specialist reader will find certain editorial mistakes in this book somewhat disturbing. This reviewer noticed several. In retrospect however, corrupted text is a constant in cryptanalysis. To Messrs. Deavours and Kruh, "very nicely done."

JAMES S. O'BRASKY
Naval War College

Krepinevich, Andrew F. *The Army and Vietnam*. Baltimore: The Johns Hopkins University Press, 1986. 318pp. $26.50

Andrew Krepinevich is an Army major currently assigned to the Office of the Secretary of Defense. This book is an outgrowth of his doctoral dissertation and, as its title states, stresses the Army's role in the Second Indochina War.

The central question the author seeks to answer is how an army of the "most powerful nation in the world" failed to defeat the smaller force of a lightly armed opposition. At the outset he hypothesizes his answer: "The United States Army was neither trained nor organized to fight effectively in an insurgency conflict environment."