

## INTELLIGENCE IN RECENT PUBLIC LITERATURE

### Cryptology

THE CODEBREAKERS: The Story of Secret Writing. By *David Kahn*. (New York: Macmillan. 1967. 1164 pp. \$14.95.)

The journalist-author of this massive, richly informative, and eminently readable book has been an amateur cryptologist since 1943, when he was thirteen, and for many years President of the American Cryptogram Association. He has largely succeeded in the undertaking set forth in his preface, to write a serious history of cryptology—the development of the various methods of making and breaking codes and ciphers and how these have affected human events—using primary sources wherever possible and not fictionalizing or exaggerating the influence of cryptologic successes, although “codebreaking is the most important form of secret intelligence in the world today.” Certain deficiencies from an unqualified success of the work will be noted at the end of this review.

The preface is followed by a helpful few pages on the vocabulary of cryptology, and then the reader is launched into the 965 pages of main text.

The opening chapter, “One Day of Magic,” is a dramatic presentation of the role of cryptology in connection with the attack on Pearl Harbor. The story begins with Herbert O. Yardley’s cryptologic section of military intelligence in World War I and “Black Chamber” of the 1920s. The events of the period between the wars are woven into a coherent narrative leading to the American success in breaking Japanese codes as war came closer. Kahn tells what was done, how it was done, and what the effect of those achievements was on the “day of infamy.” The lengthy cast of people cited in these 67 pages is widely varied and generally pertinent. The standout star is William F. Friedman, “the world’s greatest cryptologist,” in his role in the attack on the Purple crypto-system of the Japanese.

The real conclusion to this chapter appears early in “Notes to Text,” which occupy 156 pages at the back of the book. In the first few of these pages Kahn gives a cogent summary of his views on the responsibility for the Pearl Harbor disaster, paralleling closely such authoritative and well-reasoned opinions as those of the congressional investigative committee, Roberta Wohlstetter, and Samuel E. Morison.

After this dramatic opening the reader is treated to a pageant of cryptography through the centuries, beginning with the earliest known deliberate transformation of a writing about 1900 B.C., found in the tomb of Khnumhotep II. Cryptographic developments of the ensuing 3,000 years are traced through India, Mesopotamia, Babylonia, and Assyria, in Greek and Roman writings, in Persia, Egypt, Anglo-Saxon Britain, and Scandinavia.

To this point the story is simply of cryptography, the rendering of a message unintelligible by some transformation of the plain text. The cryptanalysis side of cryptology begins with the Arabs, who in the seventh century were the first to discover and record methods of analyzing the frequency and juxtaposition of letters. The author describes with examples and anecdotes the developments from this beginning to the sudden rise of secret writing with the Renaissance in western civilization and the work of Geoffrey Chaucer and Roger Bacon. Thirty centuries is a long period to cover in some thirty pages of text, but seven pages of notes on this chapter indicate that Kahn has rather thoroughly plowed the field.

Next the spread of political cryptography is pursued from rudimentary beginnings in the early 13th century through Venice, Rome, the Vatican, the secular principalities of Italy, and throughout Europe. The growth of cryptology paces evenly the flowering of modern diplomacy. Kahn's examples range from the well to the little known and from the simple to the recondite in each period and stage of development.

The development of the modern system of polyalphabetic substitution, described in a chapter called "On the Origin of a Species," began in the 17th century with the work of four amateurs who adopted a mixed alphabet, the principle of letter-by-letter encipherment, and an easily changed key. A further improvement came in the use of grilles and tableaux to govern the enciphered sequence. These successes were not achieved without pitfalls and pratfalls, which Kahn recounts with clarity and gaiety, including an example of Casanova's use of cryptanalysis as a key to seduction.

In spite of the advance to polyalphabetic substitution, the nomenclators system of cryptography first developed for Pope Clement II in the late 14th century continued to flourish in Europe. Kahn at-

tributes its continued use to a legend of unbreakability nourished by writings of inferior cryptologists, whose books

... have a certain air of unreality about them. There is good reason for this. The authors borrowed their knowledge from earlier volumes and puffed it out with their own hypothesizing, which seems never to have been deflated by contact with the bruising actuality of solving cryptograms that they themselves had not made up. The literature of cryptology was all theory and no practice.

"The Era of the Black Chambers" begins with the work of "France's first full-time cryptologist: the great Antoine Rossignol," under Richelieu, Louis XIII and XIV, and Mazarin. Kahn goes on to describe the almost unbelievably efficient *Gebirne Kabinets-Kanzlei* of Vienna in the 18th century, and in England the work of John Wallis for William and Mary and later of Edward Willes and his descendants, who dominated the English field for nearly a century.

Across the Atlantic cryptology was making its way informally into the life of the American colonies. In 1775 the solution of a monoalphabetic substitution cipher showed George Washington that a Boston Tory was sending military information to British commander Gage. James Lovell, of the Continental Congress, may be called the father of American cryptanalysis for his prompt solutions of some intercepted redecoat cryptograms. There was cryptographic involvement in the case of Benedict Arnold and later that of Aaron Burr. Thomas Jefferson invented a "wheel cypher," far and away the most advanced of its day, but he seems to have filed and forgotten it. It was rediscovered among his papers in the Library of Congress in 1922, the year the U.S. Army adopted an almost identical device invented independently.

Kahn stresses how telegraphy made cryptography what it is today, principally by creating a new instrument for war—the signal communications that enabled commanders for the first time in history to exert instantaneous and continuous control over great masses of men spread over large areas. The telegraph broke the 450-year reign of the nomenclator and brought acceptance of the need for polyalphabetic substitution—the adoption of which was, however, followed shortly by its solution. The role of ciphers in the Civil War and postwar politics is described in a brief chapter called "Crises of the Union."

Of cryptologic events before World War I perhaps the most sensational involvement occurred in the Dreyfus case, which was not finally closed until 1906. Less than a decade later the war engulfed most of

the principal nations of the world, and communications—now by radio as well as cable—took on a new importance. British and French cryptology had an early lead; Germany had no cryptanalysts on the Western Front for the first two years of the war. In the United States, Hitt's *Manual for the Solution of Military Ciphers*, selling for thirty-five cents, served as the textbook to train cryptanalysts of the American Expeditionary Forces.

In "A War of Intercepts" Kahn covers the episodes of the war in which cryptology was involved, that of the Zimmermann telegram being the outstanding one. This war "marks the great turning point in the history of cryptology." From an infant science it had become big business. Radio made all the difference, but cryptanalysis had matured, too.

"Two Americans" are introduced in chapter 12—Herbert O. Yardley, who "owes his fame less to what he did than to what he said—and to the sensational way in which he said it," and William Frederick Friedman, "uncontestably the greatest," whose eminence is due "most emphatically to what he did." Of the latter:

His theoretical studies, which revolutionized the science, were matched by his actual solutions, which astounded it. Both are complemented by his peripheral contributions. He straightened out the tangled web of cipher systems and introduced a clarifying terminology for his arrangement. Words he coined gleam upon more than one page of today's dictionaries. His textbooks have trained thousands. His historical articles have shed light in little-known corners of the study, and the Shakespeare book has done much to quash one major area of a perennial literary nuisance. Singlehandedly, he made his country preeminent in his field.

The work of private individuals and corporations in developing new machines and new aspects of cryptology in the period between the wars is told in convincing and sometimes intimate detail in the chapter entitled "Secrecy for Sale." The principal names are Vernam, Hebern, and Hagelin. Kahn seems to have something of an obsession for his belief that "the armed forces had adopted the rotor principle from Hebern and used it without just compensation in hundreds of thousands of high-security machines in World War II and in the cold war."

Kahn missed, incidentally, an interesting anecdote about the testing of the Hebern machine at the Navy building. There were continuing electrical problems—fuses blowing and solenoids burning out—although other tests which the Director of Naval Communications had suggested be carried out at his home on Kalorama Road gave no such trouble. It was finally discovered that the Navy building was

still using direct current in 1926, while the Kalorama Road neighborhood was provided with AC power.

The cryptography of World War II is delineated in four chapters covering 136 pages. Numerous anecdotes and episodes and some epic stories are interestingly told, many in good perspective. It is clear that Kahn found several ready European sources of information about allied, enemy, and neutral cryptology in the war. The detail sometimes appears exhaustive. The sources he names are never the top experts, for the most part entirely unknown; and his narratives consequently depend upon surface and low-level detail. But the stories are well told.

The one great exception to his European coverage is Britain, and the gap shows. Probably British cryptologists, under the constraints of their Official Secrets Acts, are less likely to talk than those from countries with less severe protective laws. In any case, Kahn has stated that he excised from his text at the request of the Defense Department the material he had on British cryptologic activities.

In narrating events of the Pacific war Kahn sometimes violates his prefatory promise not to credit cryptanalysis unduly, or at least he fails to credit other factors. After telling, dramatically and in detail, the story of the interception and death of Admiral Isoroku Yamamoto, for example, he concludes, "Cryptanalysis had given America the equivalent of a major victory," thus ignoring his own reminder that "Knowledge alone is not power. To have any effect it must be linked to physical force."

A chapter of 62 pages devoted to the history and structure of the National Security Agency tells of publicized successes and failures in which it has been involved. Descriptions of scandals and defections, most notably that of Martin and Mitchell, are derived from news accounts and lead to an endorsement for Congressional surveillance of intelligence agencies. This chapter reports on military communications generally, along with those of the Department of State and other parts of the government, including the hot line to Moscow. Most of the material is based upon news releases, news accounts, and speculation. Kahn seeks to validate the latter by a sedate notice in his "Notes to Text" that he has used "the word 'probably' or the verb 'may' to indicate that the statement is my own supposition"—rather too inconspicuous flags of warning, it seems to this reviewer.

The book's last section is a collection of heterogeneous addenda that can be taken or left. There is a psychoanalytic treatment of

cryptology in which cryptanalysis is equated with voyeurism and it is implied "that cryptography may come ultimately from the infantile sexual pleasure that Freud says children obtain from the muscle tension of retaining the feces." There is a catch-all chapter discussing miscellaneous motives, purposes, and media for cryptologic activity. "Runrunners, Businessmen, and Makers of Nonsecret Codes" offers well-told stories about these subjects and introduces a lady code expert of the war against rumrunners in the prohibition era--Mrs. William F. Friedman. There is a collection of historical oddities, the most intriguing of which is probably the still unsolved Voynich manuscript. The problem of Roger Bacon and the Shakespeare writings is treated not uninterestingly. Finally we go way out with paracryptology to "Ancestral Voices" and "Messages from Outer Space."

In sum, this reviewer learned a lot from *The Codebreakers*, found many parts and sections to be of great interest, and considers it a monumental work. The shortcomings I mentioned above derive from a careless and somewhat cavalier attitude toward factual detail in matters not strictly cryptologic. One detail is the meaning of the word interview. A number of the people whom the author "interviewed" told me they had no idea their conversations with him were related to the writing or publication of a book. One man assured me that his "interview" consisted of a 15-minute telephone conversation devoted mostly to reasons why Kahn should not try to write about this subject.

As to historical detail: there are anachronisms in military rank; a 5'8" commander is called "tall"; Ellis M. Zacharias is mistakenly treated as a cryptanalyst; the "Manchu laws" requiring the rotation of Army officers to the field are foolishly applied to the Navy; Vladivostok is cited as having a U.S. legation when there was never more than a consulate there; the distance from Navy building to State is called 8 or 10 blocks; the United States is said to have had in World War II 1,350 days of conflict, three too many; Yamamoto is said to have lost two fingers of his right, rather than left, hand; Magic is given as the source of a report on Japanese shipping which actually came from ONI agents along the Chinese coast; a Japanese ship is misnamed; it is claimed that the creation of the USAFFE command was a "direct" result of intercept information about German pressures on the Japanese.

As this review was nearing completion I had occasion to talk with Kahn and mentioned some of these errors; he brushed them aside as too

minute to be concerned about. It is more understandable that his lack of experience in any kind of wartime office leads to some gaucheries and misinterpretations of the relationships among offices, functions, people, and intelligence reports; nowhere were organizational arrangements so precise and neat as he describes them.

Roger Pincau