CRYPTOLOGIA
2023, VOL. 47, NO. 3, 205–226
https://doi.org/10.1080/01611194.2021.1998808

Taylor & Francis
Taylor & Francis Group

The Codebreakers war: David Kahn, Macmillan, the government, and the making of a cryptologic history masterpiece

David Sherman

Independent scholar

ABSTRACT

David Kahn's *The Codebreakers,* published in 1967, is the first modern comprehensive history of cryptology. Based on extensive research, including interviews with former government cryptologists in the United States and Europe, Kahn's volume blazed a trail that numerous historians would follow. It also attracted the attention of intelligence officials in Washington and London, who sought to excise or edit passages in the book. In one of these, Kahn made but agreed to remove a claim that during World War II the Allies had broken the supposedly invulnerable Enigma, a feat that would remain secret until the following decade.

KEYWORDS

David Kahn; Enigma machine; Government Communications Headquarters (GCHQ); National Security Agency (NSA)

Introduction

The Russian novelist Fyodor Dostoevsky is often – wrongly – claimed to have uttered one of the most famous dictums about one writer's influence on others. "We all," the apocryphal saying goes, "came out from under Gogol's *Overcoat*." Leaving aside its dubious attribution to Dostoevsky, this claim about an earlier Russian writer – Nikolai Gogol – and his story of how a lowly government clerk is driven mad by his quest for a stylish new jacket does capture a certain aspect of Gogol's impact on authors who followed him and the psychological realism of much Russian nineteenth century fiction.

Shifting to the early twenty-first century and another field, one might well wonder whether something similar could be said of David Kahn and his influence on the writing of cryptologic history. Might all those who today write the story of cryptanalysis and cryptography rightly trace the origins of their work to Kahn's *The Codebreakers*, first published in 1967? Are they in Kahn's debt for making their work possible? In a narrow sense, the answer is almost certainly "No." Some eminent intelligence historians presumably have not read Kahn's book, at least not in its 1000-page

CONTACT David Sherman ✉ djshermansk@hotmail.com

entirety. Speaking more broadly, however, a reasonable case can be made that *The Codebreakers* marks a starting point, perhaps *the* starting point, for subsequent efforts. Reading through the numerous books and articles on the subject that have appeared in the years since Kahn's work, one rarely encounters references to earlier studies. *The Codebreakers*, moreover, not only proved that it was possible to write the history of cryptology. It showed how it could be written despite the walls of secrecy that governments erect around it.

This is not to say that Kahn did not have to deal with secrecy while researching and writing his book. He did, especially when attempting to gain access to key documents and insights from current and former government officials. Perhaps even more notably, the government shaped three sections of the published text of *The Codebreakers* in significant ways. All three demonstrated Kahn's resourcefulness as a researcher. All three also were deemed enough of a threat in London and Washington for the American authorities to approach Kahn's publisher, Macmillan, and ask that they be deleted. Most notably, in one of the three passages, Kahn reached but refrained from publishing a conclusion that would remain secret for another decade: the British breaking of the German Enigma machine during World War II.

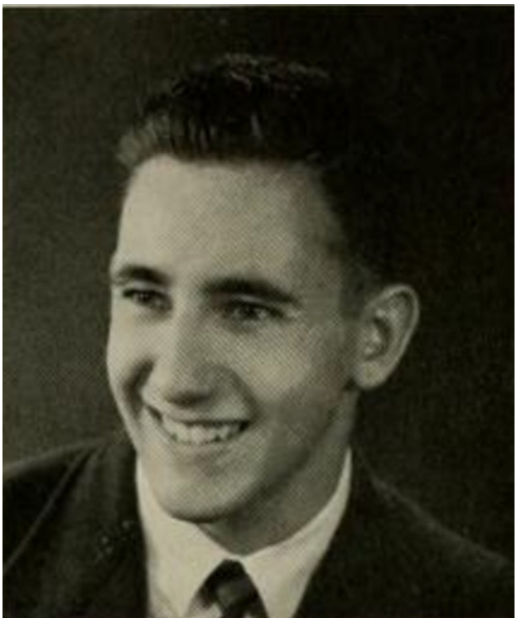
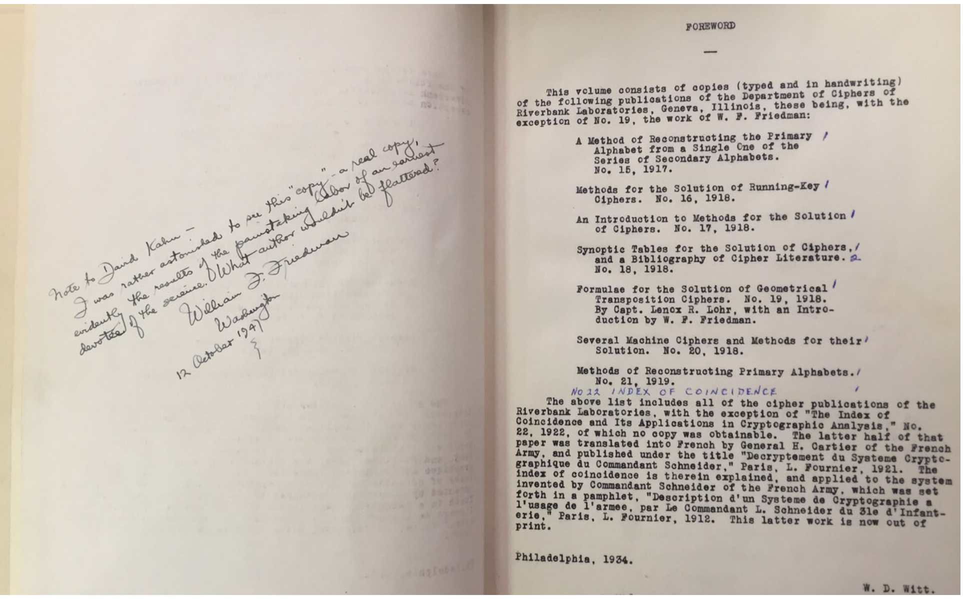


Figure 1. David Kahn in 1951 (Bucknell University).

Kahn before *The Codebreakers*

David Kahn was born in 1930 in New York City to Jesse Kahn, a Hungarian immigrant who had come to the United States as a child and became an attorney, and his wife Florence. While attending high school during World War II, Kahn read Fletcher Pratt's *Secret and Urgent*, a popular history of codes and ciphers.[1] After encountering Pratt's book, Kahn would later say, he "was hooked."[2] He joined the American Cryptogram Association (ACA), a group of amateur enthusiasts, and began assembling a collection of books and papers that he ultimately donated to the National Cryptologic Museum.



Note to David Kahn —
I was rather astonished to see this "copy" - a real copy,
evidently the results of the painstaking labor of an earnest
devotee of the science. What author wouldn't be flattered?
William F. Friedman
Washington
12 October 1947

FOREWORD

—

This volume consists of copies (typed and in handwriting) of the following publications of the Department of Ciphers of Riverbank Laboratories, Geneva, Illinois, these being, with the exception of No. 19, the work of W. F. Friedman:

A Method of Reconstructing the Primary Alphabet from a Single One of the Series of Secondary Alphabets. No. 15, 1917.

Methods for the Solution of Running-Key Ciphers. No. 16, 1918.

An Introduction to Methods for the Solution of Ciphers. No. 17, 1918.

Synoptic Tables for the Solution of Ciphers, and a Bibliography of Cipher Literature. 2 No. 18, 1918.

Formulae for the Solution of Geometrical Transposition Ciphers. No. 19, 1918. By Capt. Lenox R. Lohr, with an Introduction by W. F. Friedman.

Several Machine Ciphers and Methods for their Solution. No. 20, 1918.

Methods of Reconstructing Primary Alphabets. No. 21, 1919.

NO 22 INDEX OF COINCIDENCE

The above list includes all of the cipher publications of the Riverbank Laboratories, with the exception of "The Index of Coincidence and Its Applications in Cryptographic Analysis," No. 22, 1922, of which no copy was obtainable. The latter half of that paper was translated into French by General H. Cartier of the French Army, and published under the title "Decryptement du Systeme Cryptographique du Commandant Schneider," Paris, L. Fournier, 1921. The index of coincidence is therein explained, and applied to the system invented by Commandant Schneider of the French Army, which was set forth in a pamphlet, "Description d'un Systeme de Cryptographie a l'usage de l'armee, par Le Commandant L. Schneider du 31e d'Infanterie," Paris, L. Fournier, 1912. This latter work is now out of print.

Philadelphia, 1934.

W. D. Witt.

Figure 2. Friedman Inscription (National Cryptologic Museum).

One of the earliest items that Kahn obtained for his collection was a series of essays on codebreaking that pioneer American cryptologist William Friedman had written during and after World War I for Riverbank Laboratories, a research institution outside Chicago. Kahn used money received from his parents for his high school graduation to acquire typewritten copies of Friedman's "Riverbank Publications" and in September 1947, just before leaving home for college at Bucknell, wrote to Friedman asking that Friedman sign them. Friedman obliged, substituting for Kahn's

[1] Fletcher Pratt, *Secret and Urgent: The Story of Codes and Ciphers* (Garden City, NY: Blue Ribbon Books, 1939).

[2] David Kahn, "How *The Codebreakers* Was Written," in Kahn, *Kahn on Codes: Secrets of the New Cryptology* (New York: Macmillan, 1983), 18. Reprinted from *The Bucknell Alumnus* (November 1967).

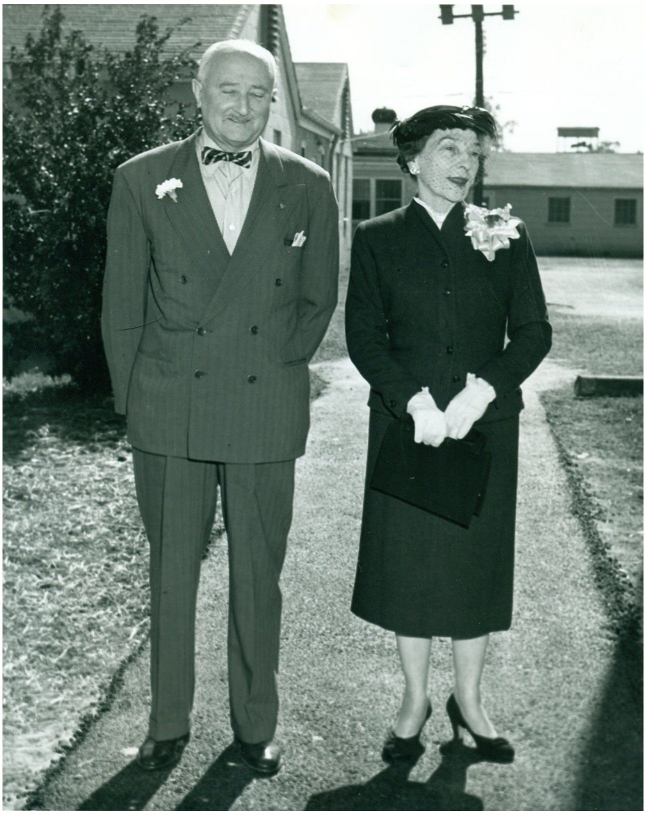


Figure 3. William and Elizabeth Friedman in 1955 (George C. Marshall Foundation).

typescripts a set of signed copies of the originals that Friedman provided from his personal collection. Kahn was overjoyed by Friedman's gift. The two corresponded into the 1960s, when Friedman's declining health led his wife Elizebeth to insist Kahn stop writing.[3]

Graduating from Bucknell in 1951, Kahn applied for a position with the Armed Forces Security Agency, which had been formed from the military's World War II codebreaking efforts and within a year would become the National Security Agency (NSA). Without much explanation, aside from saying that "we have been unable to assist you in locating a position for which you qualify," AFSA personnel chief Gertrude Kirtland retuned Kahn's application in the hope that he might be able to find other

[3] Letters from Kahn to William Friedman, September 1, 1947, September 30, 1947, October 16, 1947, and December 2, 1947; and from Friedman to Kahn, September 18, 1947, and October 14, 1947. William F. Friedman Collection, George C. Marshall Foundation, Lexington, VA (GCMF/WFFC), Correspondence Files, Box 5, Folder 10. Friedman was not the only cryptologist the young Kahn contacted in the late 1940s. In 1949, Parker Hitt inscribed Kahn's copy of his *Manual for the Solution of Military Ciphers*. Letter from Kahn to Hitt, November 19, 1962. David Kahn Collection, National Cryptologic Museum, Fort George G. Meade, MD, Box 56/Folder 9. See also Betsy Rohaly Smoot, *Parker Hitt: Father of American Military Cryptology*, forthcoming from the University of Kentucky Press.

employment.[4] One wonders how the writing of cryptologic history might have unfolded had Kahn become a government codebreaker instead of an author (Figures 1–6).

Kahn's interactions with NSA during the 1950s did not end with his unsuccessful application for employment. By 1954, Kahn had become President of the New York Cipher Society, a small group of ACA members who met monthly to discuss common interests. In December of that year, Kahn sent a statement from the Society entitled "To Improve Our Cryptologic Defenses" to President Eisenhower, NSA Director Ralph Canine, the *New York Times*, and others.[5] Keying off a recent analysis by the American Association for the Advancement of Science that argued government efforts to classify basic research undermined both security and science,[6] Kahn argued that excessive secrecy similarly prevented the scientific community from discussing and refining cryptology and thereby benefit the national interest. Responding on behalf of the government, an aide to Secretary of Defense Charles Wilson sought to assure Kahn that it recognized the challenges of balancing national security with free scientific inquiry and decided to classify scientific information only after thorough and thoughtful deliberation. Kahn wrote back that, while he agreed with the need to protect the government's most sensitive activities, its efforts to restrict more general public discussion of cryptology were excessive. Otherwise, however, Kahn had little choice but to let the matter drop.[7]

Following his unsuccessful attempt to join AFSA, Kahn worked for a time as a freelance journalist and was hired by the Long Island newspaper *Newsday*. Starting in 1954, he published several articles on cryptology. He seems to have started thinking about writing a book in the late 1950s. Initially, Kahn conceived of what became *The Codebreakers* as a primer on how to make and break codes and ciphers, prefaced by a brief historical introduction. One can find traces of this original concept in published editions of *The Codebreakers*.

Kahn began his book project in earnest in November 1960, after he got what was arguably his "big break" by publishing an article on cryptology in the *New York Times Sunday Magazine*. Written following the defection to the Soviet Union earlier that year by two employees of the National Security Agency, William Martin and Bernon Mitchell, Kahn's article

[4] Letter from Gertrude Kirtland to Kahn, December 4, 1951. Kahn Collection, Box 4, Folder A.

[5] William F. Friedman Collection of Official Papers, National Security Agency, Fort George G. Meade MD, Item A66773. Available online at: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_368/41755619079477.pdf.

[6] Board of Directors of the American Association for the Advancement of Science, "Strengthening the Basis of National Security," *Science*, Vol 20, No. 3128 (December 19, 1954), 957–59.

[7] Undated letter from G.B. Erskine to Kahn; Letter from Kahn to Erskine, February 6, 1955, Kahn Collection, Box 136, Folder 47.

recapped the history of codes and ciphers from the Bible to the Cold War. In eight short paragraphs, he also provided more information about NSA than even the most well-read *Times* subscribers probably had ever encountered. Kahn also was quite positive about the impact of NSA's codebreaking activities. "There is always the chance," he wrote, "that a seemingly meaningless group of letters may someday spell victory or defeat in the cold war."[8]

Work on the book begins

When Kahn arrived at work the day after the *Times* article appeared, he found messages from three publishers asking if he would consider writing a book. Doubleday and Berkeley were two that expressed interest, but Kahn was more impressed by the advance offered by Macmillan as well as its proposed royalties of ten percent for the first 7,500 copies sold and fifteen percent thereafter. A few weeks later, he signed a contract with Macmillan. His working title was *The Romance of Cryptology*.[9]

Having begun the research for the book that would become *The Codebreakers*, Kahn stumbled into another tussle with the government, this one involving NSA. In 1962, the now retired Friedman passed an essay that Kahn had written on the definitions of cryptologic terms in Webster's dictionary to the editor of NSA's *Technical Journal*, an in-house publication featuring both classified and unclassified articles. The editor, Paul Friedman, wrote enthusiastically to Kahn, praising the essay as "a valuable contribution to the cryptologic literature, not only for its content but for its presentation as well." Two months after Friedman's initial reply, however, Kahn received a second, terse letter indicating that the article was no longer considered "suitable material for publication in the Journal." An increasingly tense exchange of letters and phone calls ensued between Kahn and veteran cryptologist (and Friedman protégé) Frank Rowlett, then a personal assistant to NSA Director Gordon Blake. Kahn believed that NSA's reversal of its original decision to publish his manuscript reflected the agency's unwillingness to consider the expertise of outsiders. Rowlett argued that, to the contrary, a further review had indicated lacked sufficient technical merit to interest an NSA audience. Kahn went so far as to appeal

[8] David Kahn, "Lgcn Otuu Wllwqh Wl Etfown," *New York Times Sunday Magazine*, November 13, 1960. The title is Kahn's encipherment of a fictitious message "They Will Attack at Midway."

[9] Kahn, "How *The Codebreakers* Was Written," 18; Letters from Kahn to Peter V. Ritner, January 24, 1961; and from Kahn to Frances Goldin, January 26, 1961. Kahn Collection, Box 58, Folder 2. Ritner was Kahn's editor at Macmillan. Goldin was employed by Jeanne Hale, Kahn's literary agent.

Figure 4. Thomas Dyer (National Security Agency).

to Secretary of Defense Robert McNamara for assistance in forcing NSA to publish his piece, to no avail. [10]

Kahn initially thought that the book he was writing for Macmillan might take a year or two to finish. This proved to be wildly optimistic, by almost four years. Kahn had underestimated the amount of archival material available and kept turning up items that he thought had to be included in his book. The 150 pages of footnotes in the finished work are one indication of the scope and scale of Kahn's research. The voluminous files for the book in his personal papers are another. By late 1961, Kahn knew that he could not possibly produce a finished draft by the spring of the following year. That deadline was extended to early 1963, when Kahn provided several chapters to his editor at Macmillan, Peter Ritner. "These chapters come off perfectly," Ritner wrote. Ritner added that, while admitting he was not expert, "it looks to me as if you are writing the book on cryptanalysis in the English language."[11] Nevertheless, throughout the remainder of 1963 and most of 1964, Kahn repeatedly asked Macmillan to extend the deadline for his submitting a completed manuscript.

Another of Kahn's major sources – interviews with prominent cryptologists – was the source of his first conflict with the government that dealt specifically with *The Codebreakers*. While Kahn's requests to speak with current NSA officials were rebuffed, he succeeded in interviewing dozens of

[10] Letters from Paul Friedman to Kahn, July 18 and September 14, 1962; letters from Kahn to Frank Rowlett, September 26, October 12, October 29, and November 18, 1962; letters from Rowlett to Kahn, October 8, October 19, and November 15, 1962; letter from Kahn to Secretary of Defense Robert McNamara, May 7, 1963; and letter from John E. Carland, May 24, 1963. Kahn Collection, Box 114, Folder 14.

[11] Letter from Ritner to Kahn, May 9, 1963. Kahn Collection, Box 58, Folder 2.

individuals in the United States and Europe about their work from World War I through World War II. Two were retired U.S. Navy officers Thomas Dyer and Wesley Wright, who had been involved in breaking Japanese naval codes during World War II. These interviews were conducted with the Navy's permission. Its somewhat grudging acquiescence came after New York Senator Jacob Javits called the Pentagon on Kahn's behalf to urge that the interviews be granted.[12]

Kahn conducted these sessions in 1963. In its letter to Kahn authorizing them, the Navy indicated that its permission was contingent on its subsequent review of the substance Kahn gleaned from them. "I will be awaiting receipt of your copy," an official from the Navy's informed Kahn, referring to whatever notes Kahn took during the interviews and anything he subsequently wrote about them. The Navy officer also insisted that both Dyer and Wright be able to review these.[13] Kahn resisted turning over his notes, arguing that Dyer and Wright assured him that they had not divulged anything sensitive. Strictly speaking, this assertion was not accurate. Specifically, Wright wrote to Kahn after his interview asking that Kahn not publish what Wright had said about the joint work that American and British codebreakers in the Pacific had performed against Japan's World War II codes. Having this appear in print, Wright worried, "might conceivably get people in difficulty."[14]

The Navy pushed back. "All interviews are on an unclassified basis," it explained to Kahn. "These were scheduled on the basis of a review, since the officers concerned are not in a position to know what is presently unclassified."[15] In response, Kahn repeated his claim – somewhat disingenuously – that both Dyer and Wright had affirmed that no review of the notes would be necessary as they had not discussed classified materials. However, having noted that "the negotiations regarding my material seem to have reached the approximate level of complexity of the disarmament conferences in Geneva," Kahn turned the notes over to the Navy in early 1964. Kahn reminded the Navy, however, that the Pentagon's top public affairs officer, Assistant Secretary Arthur Sylvester, had said only Kahn's notes would require review, not any conclusions he subsequently drew

[12] Memorandum for United States Intelligence Board Members, April 1, 1964. Kahn Collection, Box 26, Folder 18.

[13] Letter from Lt. F.X. Steele to Kahn, December 11, 1963, Kahn Collection, Box 58, Folder 2.

[14] Letter from Wright to Kahn, December 19, 1963. Vera Filby Collection, National Cryptologic Museum, Fort George G. Meade MD, Box 35, Folder 11.

[15] Letter from Lieutenant Commander David M. Cooney to Kahn, December 31, 1963. Kahn Collection, Box 58, Folder 2. Cooney was the head of a Navy Department Office whose responsibilities included review of proposed books and magazine articles.

from them in his book. Kahn also claimed the right to add material from "non-official sources," which he argued the Navy had no right to control.[16]

The government was divided on whether the notes were classified. The Navy argued they were. In contrast, NSA found the notes contained nothing that had not appeared already in print elsewhere. This conclusion presumably included a judgment by NSA that the wartime codebreaking relationship between the United States and the United Kingdom which had given Wright pause was in fact not classified.[17]

Looking at Kahn's notes today, it is not obvious what was of such concern to the Navy, other than perhaps the claim about joint British-American codebreaking efforts.[18] It simply may have opposed drawing any attention to intelligence matters, especially in the considerable detail that Kahn seemed to be amassing. It also might have been, as Kahn himself suggested at the time, that the Navy simply was insufficiently familiar with just how much information on World War II codebreaking had made its way into the public domain.[19] Regardless, for the time being the Pentagon pursued the matter further. A year later, however, it wrote to Macmillan to emphasize that the Navy had determined Kahn's notes contained classified information. It also inquired about the status of his manuscript.[20]

Pursuing the Anglo-American connection

Kahn made a significant effort to unearth how successful the United States and the United Kingdom had been against Axis codes during World War II and how closely they had worked together to achieve whatever successes they had attained. In 1963, Kahn wrote twice to Winston Churchill in an attempt to obtain the former British Prime Minister's views on the significance of codebreaking during the Second World War. Kahn had read the discussion of American decrypts of Japanese diplomatic cables prior to Pearl Harbor in Churchill's *The Second World War*, and argued that that his "overall appraisal of cryptanalysis" would offer Kahn's readers a unique perspective on the conflict. Not surprisingly, Churchill refused on each

[16] Letter from Kahn to Cooney, January 4, 1964. Kahn Collection, Box 58, Folder 2.

[17] "The Code-Breakers, by David Kahn," undated, signed memorandum. Kahn Collection, Box 26, Folder 18.

[18] Kahn Interview with Thomas H. Dyer, December 12, 1963. Filby Collection, Box 35, Folder 12. Kahn Interview with Wesley A. Wright, December 12, 1963. Filby Collection, Box 35, Folder 11.

[19] Letter from Kahn to Cooney, January 4, 1964. Kahn Collection, Box 58, Folder 2.

[20] Letter from Lieutenant Colonel C. V. Glines, USAF to Lee C. Deighton, April 8, 1965. Kahn Collection, Box 58, Folder 2.

occasion, with his private secretaries writing to Kahn that "it is not possible for him to contribute any information that would be of help to you."[21]

Around the time Kahn wrote to Churchill, he became aware that Bletchley Park, a small estate north of London, had played a role in British codebreaking during the war. Writing to the head of the local government for Bletchley in 1964, Kahn claimed that "the British code-breaking bureau" had been located there, that it appeared to have been "a rather large establishment," and that "its accomplishments played … no small role in helping the Allies defeat Hitler." Specifically, Kahn sought information on when Bletchley Park had been built and it condition before the war, as well as "when the government's cryptologic effort arrived and whether any buildings were temporarily erected." The local authorities referred Kahn's inquiry to an office of the Royal Mail that had moved to Bletchley Park after the war. Its representative sent Kahn a pamphlet on the site's prewar history while also noting that "as you say … the wartime history of the Park is extremely interesting but is covered by a security ban, but I can tell you that a very large number of people worked here during that time in the same buildings we now use for our training purposes."[22]

Conflicts and controversies

A more serious battle between Kahn and the government, waged largely through Macmillan rather than directly between the two sides, erupted in early 1965 as he was nearing completion of the manuscript for *The Codebreakers*. This dispute also triggered a series of spats between Kahn and Macmillan itself. We know about these in part though Kahn's correspondence with his agent and with Macmillan. Equally important, in the 1990s Kahn filed a Freedom of Information Act request with NSA and received almost 100 pages of materials, some redacted, related to the government's review of his manuscript. These are preserved among Kahn's papers at the National Cryptologic Museum.[23]

Having read Kahn's finished draft, Macmillan's attorneys believed that, given the sensitive nature of cryptology generally, the publisher had little choice but to submit it to the government for review. Otherwise, they

[21] Letter from Kahn to Churchill, February 27, 1963. Kahn Collection, Box 56, Folder 7. Letter from Morris Graham to Kahn, March 7, 1963. Kahn Collection, Box 56, Folder 6. Letter from Doreen Pugh to Kahn, January 4, 1964, Box 56 Folder 20. Churchill's comments on the American success against Japanese diplomatic messages, which had been disclosed in 1946 at Congressional hearings on the Pearl Harbor attack, are contained in the third volume of his history of the Second World War II. See Winston S. Churchill, *The Grand Alliance* (Boston: Houghton Mifflin, 1950), 532-3.

[22] Letters from Kahn to Chairman, Bletchley Urban Council, May 20, 1964; and from D.B. Low to Kahn, June 4, 1964. Kahn Collection, Box 56, Folder 20.

[23] Correspondence and Memoranda Related to NSA Prepublication Review of *The Codebreakers*. Kahn Collection, Box 26, Folder 18.

argued, Macmillan risked legal action in the event that it unknowingly published classified information. Accordingly, and without Kahn's knowledge or permission, sometime in the summer of 1965 Macmillan provided the Pentagon with the two chapters it thought had some chance of being of concern to Washington. These were the book's opening section, on Pearl Harbor, and a later one dealing with subsequent American efforts against Japanese cryptographic systems, most notably a decisive breakthrough against the main Japanese fleet code, JN-25, prior to the Battle of Midway.[24]

Kahn was upset when he heard Macmillan had shared part of his draft with the government, but relieved to learn that these chapters posed no problems. He was appalled, however, when he was told that Macmillan's own attorneys were recommending that a third chapter, one dealing with NSA, be removed in its entirety without even being sent to Washington for review. Kahn pushed back, arguing that he already had "excluded from my copy all references that might endanger national security." He also made a First Amendment argument that providing the Pentagon with any more chapters from the book would compromise his scholarly integrity.[25]

Macmillan, however, was adamant. "It is part of our publishing responsibility to you, not to speak of ourselves and our shareholders," Kahn's editor Peter Ritner told him, "to choose the ground on which to fight a battle." Accordingly, when Kahn finished his manuscript in a few months, Macmillan intended to send it to the government in full. "Vetting and preparing are not the same as surrendering," Ritner noted. "But we must know what we are getting into."[26]

Macmillan forward Kahn's completed manuscript to the Pentagon on 4 March 1966.[27] Writing in late May on behalf of a group of intelligence and defense officials who had reviewed it, NSA Director Marshall Carter concluded that while there was no individual piece of information that the government could claim was classified, Kahn's comprehensive narrative of codebreaking could lead foreign adversaries to conclude that sensitive communications they thought were secure were in fact not, leading them to adopt more sophisticated encryption systems. Kahn's book, Carter noted, also might damage American relationships with friendly nations, which might conclude the United States was an untrustworthy partner that could not protect its secrets. The Navy, perhaps recalling its earlier encounter

[24] NSA completed its review of the two chapters forwarded by Macmillan in July 1965. Memorandum by NSA Director Marshall Carter, July 16, 1965. Kahn Collection, Box 26, Folder 18.

[25] Letter from Kahn to Ritner, November 24, 1965. Kahn Collection, Box 58, Folder 2.

[26] Letter from Ritner to Kahn, December 1, 1965. Kahn Collection, Box 58, Folder 2.

[27] NSA Memorandum, "The Code-Breakers by David Kahn." Apparently dictated by NSA Director Marshall Carter on 14 July 1966. Kahn Collection, Box 26, Folder 18.

with Kahn, was particularly adamant "that every effort should be made to prevent the publication and circulation of the book."[28]

As NSA and other American intelligence agencies were completing their review of Kahn's manuscript, the situation they faced became more complicated. Although NSA was finding nothing that was classified or not otherwise already in the public domain, the British – with whom NSA had shared the manuscript due to their now almost 30-year-old codebreaking relationship – raised serious concerns. Initially, London appears to have wanted Washington to prevent Kahn's book being published in any form, a position that may have been communicated in a letter that Bernard Burrows, chair of the Joint Intelligence Committee, sent to Director of Central Intelligence Richard Helms in the summer of 1966. Ultimately, perhaps persuaded by the Americans that suppressing the entire book was not possibly, the British focused on three passages that they wanted deleted. These dealt with Britain's Government Communications Headquarters, or GCHQ; the vulnerability of cryptography used by various nations in the developing world; and the readability of Germany's World War II systems, specifically the Enigma.[29]

The British concerns placed NSA in a difficult position. On the one hand, it wanted to honor the British request that it ensure these three passages from Kahn's manuscript were excised. On the other, drawing attention to them also risked having to disclose additional information to Macmillan. It also might prompt Kahn to complain publicly that the government wanted to censor his book. Some at NSA, particularly Frank Rowlett, also suspected Kahn possessed a considerable amount of sensitive information that he had not included in his manuscript. Pressing Kahn to remove the three sections might tempt him to release this information. Senior NSA officials also admitted to not being sufficiently well-versed in which details about codebreaking were already in the public domain, or at least not enough to be certain that Kahn could not produce something showing the information the British were seeking to protect had in fact already been released.[30]

In mid-July 1966, acting at the suggestion of Director of Central Intelligence Richard Helms and with the approval of Secretary of Defense Robert McNamara, Carter went to New York to meet with Macmillan executive Lee Deighton, Kahn's editor Peter Ritner, and an attorney that the company retained to handle sensitive business matters. Carter attended alone,

[28] Memorandum from Marshall Carter to United States Signal Intelligence Board Members, May 31, 1966. Kahn Collection, Box 26, Folder 18.

[29] "The Code-Breakers, by David Kahn," undated, signed memorandum; memorandum drafted by Marshall Carter for Director of Central Intelligence Richard Helms to Secretary of Defense Robert McNamara,, July 8, 1966; memorandum from Denis Greenhill to Helms, November 11, 1966. Kahn Collection, Box 26, Folder 18.

[30] The concerns of senior NSA officials, including Carter, about approaching Macmillan or Kahn about these concerns are reflected in a lengthy summary of a conversation among them that appears to have taken place sometime in June 1966. Kahn Collection, Box 26, Folder 18.

without his aides or an NSA attorney. Macmillan agreed not to create a memorandum on the meeting for its files; Carter later briefed NSA senior leaders on the session. The transcript of their conversation was obtained by Kahn in the 1990s under a Freedom of Information Act request.[31]

Carter learned that Macmillan itself faced a dilemma, albeit one different from that confronting NSA. Deighton, Ritner, and their attorney informed Carter than they had told Kahn his book either had to be cleared by the Defense Department or be based on information that Kahn could prove was already in the public domain. However, Macmillan also had a reputation to protect and could not be perceived as "censoring" the book. It also had to consider that Kahn almost certainly would sue if changes were made to his manuscript without his permission, an action Macmillan's contract with him explicitly forbade. At the same time, the company noted that Kahn likely would be amenable to small textual changes requested by the government. It also said that, were the government to insist on cuts over Kahn's objections for reasons of national security, it was willing to make them but would need to provide supporting information to provide to a judge in the event of a lawsuit. "If you are prepared to support us in case the author sues," Carter summarized Macmillan's leaders as saying, "then we are prepared to go down that line to help."[32]

Carter did not say so at the meeting, but he was not interested in such a strategy as it would require the government to disclose even more information than was in Kahn's manuscript. Accordingly, he suggested that the matter could be quietly resolved if Kahn made changes to three passages in the book. These were those the British found objectionable. The government would drop any other objections, including any insistence that the chapter on NSA be removed entirely, although as a formality it would continue to say that publication of the book was not in the national interest. Macmillan agreed to support this course of action.

Three contested passages

Kahn was in Paris during the summer of 1966. After Carter's visit to New York, Macmillan contacted him and indicated there were the three passages that the government wanted him to remove, although like Macmillan he presumably was not told that it was London and not Washington that objected to them.[33] Kahn agreed to two of the redactions in their entirety. In the third

[31] Record of Carter Conversation with Staff, probably mid-July 1966. Kahn Collection, Box 26, Folder 18.

[32] Record of Carter Conversation with Staff, probably mid-July 1966. Kahn Collection, Box 26, Folder 18

[33] Oral History Interview with Marshall S. Carter, October 3, 1988, National Security Agency, Fort George G. Meade, MD, 301. Available at https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/oral-history-interviews/NSA-OH-15-88-Carter.pdf .

instance, he deleted a considerable amount of text but somehow was able to retain enough of what he had written that he came closer to revealing arguably the greatest intelligence secret from World War II – the British decryption of Germany's Enigma machine – than any previous author had. The so-called "Ultra Secret" would remain hidden from public view for another decade, but Kahn had taken an important step on the path to its ultimate disclosure.

The first section that the British objected to consists of three paragraphs on GCHQ.[34] They described GCHQ's position in the British Government; its senior leaders; and its relationships with NSA, Canada, and Australia. The section also noted that GCHQ and NSA, working through liaison officers, provided each other with the results of their separate work on foreign codes and ciphers. They also were said to occasionally agree on divisions of effort where one focused on certain countries and the other on other nations. Kahn correctly placed GCHQ within the Foreign Office, while noting that it "apparently handles strategic cryptanalysis for the military" as well. He also listed several of GCHQ's Directors and a few of its leading analysts. Regarding John Tiltman, for example, Kahn related that he was "perhaps England's outstanding expert in the field" and noted, accurately, that he had worked at NSA for "the last few years."[35]

London presumably flagged this section because, as of the mid-1960s, it was resisting any public discussion of the organization. Kahn argued that he had based these paragraphs solely on openly available information. It is not possible to verify this claim, as Kahn's annotations do not appear in the galleys for *The Codebreakers* but only in the published book. He may have received some insights from individuals in the United Kingdom or the United States familiar with GCHQ's operations who believed what they were telling Kahn was innocuous. Regardless of where he obtained the information for the three paragraphs, however, he agreed to delete them. In the published book, there is a single sentence noting GCHQ's existence. Interestingly, while in the galleys for *The Codebreakers* Kahn correctly

[34] James Bamford, whose account of NSA's interactions with Macmillan and Kahn regarding *The Codebreakers* is generally correct, errs when he identifies the section on GCHQ as the sole redaction. Bamford's version, contained in his *The Puzzle Palace: Inside the National Security Agency*, mostly relies on an interview with Carter and as well as on papers that Carter had deposited at the George C. Marshall Research Library. However, Bamford also came across a sheet in Friedman's personal papers containing the three paragraphs and a handwritten note dated February 4, 1968, that stated, "This contains the only paragraphs which were deleted from Kahn's ms. at the request of GCHQ authorities." Friedman presumably obtained this information from one of several British friends, possibly Tiltman. GCMF/WFFC, Box 5, Folder 1. Bamford claimed, correctly, that Kahn's endnotes to the deleted section on GCHQ survived in the published version of *The Codebreakers*. However, these notes refer to biographical directories of government officials in the United Kingdom and are not otherwise illuminating.

[35] Galley proofs for *The Codebreakers*, Kahn Collection, 249-249A. Tiltman's biography for his NSA Hall of Honor induction (https://www.nsa.gov/About-Us/Current-Leadership/Article-View/Article/1622415/brigadier-john-tiltman/) indicates that he was a consultant at NSA from 1964 to 1980.

identified it as the Government Communications Headquarters, the published book substituted "General" for "Government."[36]

The second section that concerned the British dealt with the codes used by newly independent nations in Africa.

> Easiest to solve are those of some of the newly emerging countries of Africa. One of these actually used a ten-alphabet mixed polyalphabetic for several years after it received its independence in the late 1950s. These new countries often get their cryptographic instruction, and sometimes their equipment as well, from the older countries with which they are affiliated, as nations like Ivory Coast, Upper Volta, and Chad are with France. This is dangerous to them, since the parent country usually gives them its cast-off equipment and tends to make sure that it will be able solve their cryptograms. Some of the other new countries simply go to Hagelin [Boris Hagelin, founder of the Swiss firm Crypto AG] and buy an installation of his machines. Usually their handling of their systems leaves a great deal to be desired – which is, after all, only to be expected, since they usually have little knowledge of any governmental functioning, much less the recondite one of cryptography. The United Nations, interestingly enough, has relied on the one-time pad virtually since its creation. Its peace force in the Congo in 1960, which was formed of contingents from 28 nations, likewise employed the one-time pad, as well as cipher machines. [37]

A decade later, Kahn claimed that Britain had sent some of the German Enigma machines it had collected at the end of World War Two to its former colonies. "Presumably," he wrote in 1974, "if she [Britain] could read Enigma messages in 1940, she could do so in 1950."[38] Many of the recipients, Kahn added, had replaced their purportedly donated Enigmas with more modern machines. There is little if any evidence to support Kahn's claims.

The prepublication review file that Kahn obtained from NSA in the 1990s does not indicate the specific objections that the British had raised to this section, nor why it apparently did not concern NSA to the same degree. It seems likely, however, that London would have been concerned by the inference that, like France, it had supplied antiquated cryptanalytic machinery to its former colonial subjects and therefore could break their supposedly secure communications with ease. The British also may have been worried by any suggestion that operators in the developing world did not know how to use more modern technology correctly, thus rendering any enciphered messages they sent more liable to be successfully broken. Finally, the British might have resisted any discussion of specific encryption systems such as mixed-alphabet ciphers or one-time pads. Whatever the case may have been, having

[36] David Kahn, *The Codebreakers* (New York: Macmillan, 1967), 730.

[37] Galley proofs for *The Codebreakers,* Kahn Collection, 265–6. Letter from Kahn to Ritner, September 1, 1966, Kahn Collection, Box 58, Folder 2. Memorandum of Conversation with Lieutenant General Marshall Carter, Director NSA, Kahn Collection, Box 26, Folder 18. "The Code-Breakers, by David Kahn," Kahn Collection, Box 26, Folder 18.

[38] David Kahn, "The Ultra Secret" (review of eponymous book by F.W. Winterbotham), *The New York Times Book Review*, December 29, 1974, 5.

heard from Macmillan that Washington was concerned about this section but not knowing it actually was London that had objected, Kahn deleted it. It does not appear in *The Codebreakers* as published.[39]

The third section in Kahn's draft for *The Codebreakers* that London found problematic is the most interesting. While researching his book in the early 1960s, Kahn apparently learned that the Allies had broken Germany's supposedly invulnerable Enigma. Kahn's draft section on this success, specifically against the version of the Enigma used by Germany's submarine force, read as follows:

> The main U-boat cryptosystem appears to have been the Enigma. Each machine was supplied with ten rotors, the encipherer selected for use three at a time according to keys listed in a book. The United States not only broke this cipher originally, but – in one of the finest cryptanalytic achievements of the war – kept solving U-boat intercepts on a current basis… By January of 1943 they were reading [German Admiral and U-Boat force commander Karl] Donitz's messages directing his wolf packs to Allied convoys. This enabled the convoys to change course radically and so avoid the U-boats. In May they read Donitz signal ordering his submarines to retire temporarily from the convoy route for rest and regrouping. A year later the cryptanalysts had grown so expert, and worked so fast, that when *U-516* was ordered to rendezvous with a 'milk cow' (supply submarine) at Grid Reference D, it arrived to find no milk cow – but an American bomber directly overhead. And in dozens of other cases, the solutions gave anti-submarine forces entrée into wolf pack and supply meetings.[40]

At the time, very little in the public domain even hinted at the possibility of this success, and any claim to that effect rightly would have been labeled highly speculative or even groundless. While still in draft, the first two volumes of Churchill's history of the Second World War had contained some clear references to information derived from the breaking of Enigma, but these were rigorously removed before they appeared in print.[41] One of the few references to German cryptography during the war came in 1957 when American Admiral Daniel Gallery published a memoir of the June 1944 capture of the German submarine U-505. Gallery claimed, accurately, that his force had taken "current code books, the cipher machine, and hundreds of dispatches with the code version on one side and the German translation on the other." "We read the operational traffic between U-Boat headquarters and the submarines for the rest of the war," Gallery continued, a success that "may have had something to do with the sinking of nearly three hundred U-Boats in the next eleven months."[42] Gallery's claims were

[39] Kahn, *The Codebreakers*, 727.

[40] Galley proofs for *The Codebreakers*, 199.

[41] Christopher Moran, *Classified: Secrecy and the State in Modern Britain* (Cambridge: Cambridge University Press, 2013), 262-263.

[42] Daniel V. Gallery, *We Captured a U-Boat* (London: Sidgwick and Jackson, 1957), 243-4.

repeated, albeit in less detail, several years later by Ladislas Farago in his book *The Tenth Fleet*.[43] Kahn was aware of both Gallery's and Farago's accounts, and included them in *The Codebreakers*.

Kahn caveated his draft by saying that the U-Boat operation system that had been broken "appears to have been Enigma," leaving open a small window of doubt. He also erred on some points. The variant of Enigma used by the German Navy used four rotors, not three, after a new model was introduced in early 1942, rendering it unreadable for several months, and the maximum number of rotors for the system available to a code clerk was eight, not ten. More notably, while the Americans benefited from intelligence derived from Enigma messages, and provided and operated some of the "bombe" machines used in their decipherment, British codebreakers at Bletchley Park achieved the successful cryptanalysis of the system.

That said, in his draft Kahn came closer to revealing the "Ultra Secret" than any other author would for another decade. In the mid-1960s, however, the British success against the Enigma remained a closely guarded secret, and it is not surprising that London wanted this section removed. More intriguing is why Kahn came to believe that it was the Enigma that had been broken, how he obtained specific details on the way German operators used it during World War II, and where he learned about the intelligence the Allies obtained from decrypting it.

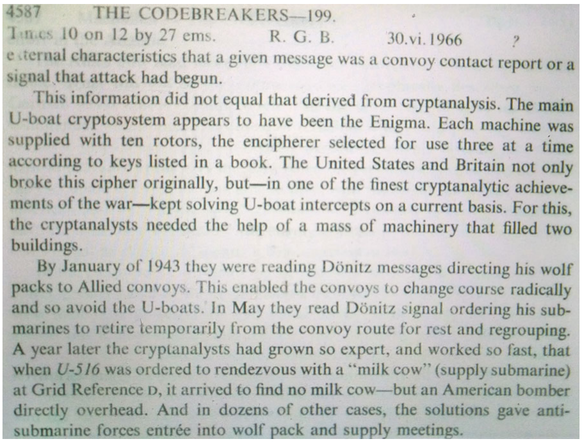
Kahn had concluded by March 1965 that the Enigma had been broken, as his preparatory notes for a telephone interview with John Tiltman that month indicate than he planned to ask whether the "US Navy's solution of the U-Boat Enigma helped by Admiralty?" Tiltman refused to tell Kahn anything, about Enigma or any other subject. Tiltman could not "say anything at all about anything," Kahn noted. "Does not want any publicity."[44] Subsequently, however, Tiltman was willing to speak with Kahn about the Voynich Manuscript, a Renaissance manuscript with a text that was impenetrable then and remains so today.[45]

Tiltman may have remained silent, but it seems highly likely that Kahn obtained his information about the Enigma from one or more of the other individuals he interviewed. Given his mistaken claim that "the United States not only broke this cipher originally … but kept solving U-boat

[43] Ladislas Farago, *The Tenth Fleet* (New York: Ivan Obolensky, 1962), 270.

[44] Kahn, Notes of Interview with John Tiltman, March 18, 1965, Kahn Collection, Box 61, Folder 37.

[45] "Brigadier John Tiltman: A Giant Among Cryptanalysts," (Fort George G. Meade, MD: National Security Agency/Center for Cryptologic History, 2007), 60. Available at: https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/misc/tiltman.pdf. It has been claimed that Tiltman approached Kahn at the request of GCHQ to ask that Kahn remove any reference to the agency in his manuscript. The author has yet to find any documentary evidence that this is the case. Friedman claimed that Tiltman's role was to persuade GCHQ to speak with Macmillan's London office about the book. GCMF/WFFC, Correspondence Files, Box 5, Folder 1.



4587 THE CODEBREAKERS—199.
Times 10 on 12 by 27 ems. R. G. B. 30.vi.1966 ?

external characteristics that a given message was a convoy contact report or a signal that attack had begun.

This information did not equal that derived from cryptanalysis. The main U-boat cryptosystem appears to have been the Enigma. Each machine was supplied with ten rotors, the encipherer selected for use three at a time according to keys listed in a book. The United States and Britain not only broke this cipher originally, but—in one of the finest cryptanalytic achievements of the war—kept solving U-boat intercepts on a current basis. For this, the cryptanalysts needed the help of a mass of machinery that filled two buildings.

By January of 1943 they were reading Dönitz messages directing his wolf packs to Allied convoys. This enabled the convoys to change course radically and so avoid the U-boats. In May they read Dönitz signal ordering his submarines to retire temporarily from the convoy route for rest and regrouping. A year later the cryptanalysts had grown so expert, and worked so fast, that when *U-516* was ordered to rendezvous with a "milk cow" (supply submarine) at Grid Reference D, it arrived to find no milk cow—but an American bomber directly overhead. And in dozens of other cases, the solutions gave antisubmarine forces entrée into wolf pack and supply meetings.

Figure 5. Enigma Redaction (National Cryptologic Museum).

intercepts on a current basis" and his less significant errors in explaining how the Enigma's rotor system worked, it appears probable that Kahn's source was someone not directly involved in the day-to-day cryptanalysis of the system. His generally correct statements about U-Boat movements and resupply operations suggest a more likely source was someone with regular access to intelligence regarding such activities. His conclusion that the United States had broken Enigma point toward the likelihood that his source was American, perhaps a retired naval officer. It is equally plausible, of course, that Kahn learned at least part of the Ultra Secret from a British source. Less likely, it seems, it could have been speculation based on something he heard from one of his German contacts.

Regardless of who disclosed the Ultra Secret to Kahn or the fact that Kahn erred when explaining some details, he agreed to the government's request and deleted the two paragraphs. Strangely, however, the published book retains a statement that starting in 1943 the Allies were able to read an unnamed code used for U-boat operations in near-real time and, while the remaining narrative focuses mostly on Allied captures of German cryptographic equipment and materials, attributes their success to earlier feats of cryptanalysis. As published, *The Codebreakers* also claimed in a separate section that the Soviets had broken Enigma.[46] Assessing this confused situation today, one is tempted to conclude that the British simply wanted to avoid any suggestion that they had solved Enigma. Alternatively, however, Kahn may have made a significant enough deletion for Macmillian to conclude that he had given the government what it wanted and to opt not to submit the changed manuscript for a second review.

[46] Kahn, *The Codebreakers*, 506 and 649.

What the publisher missed, on this interpretation, were the tantalizing hints that Kahn managed to retain.

Denouement

There was one final twist in the history of *The Codebreakers* before it was published, and it came just before the book's appearance in print. When making final corrections to the galleys for the book in early 1967, Kahn added a sentence to the preface indicating that the Pentagon had reviewed it prior to publication. "At the publisher's insistence," he wrote, "the manuscript was submitted to the Department of Defense, at whose suggestion I have made a few minor changes."[47] The Pentagon objected, noting that it had only raised concerns about the book and never said anything about giving it any sort of imprimatur. NSA, fearful of doing anything that gave Kahn credibility or boosting the book's sales, was particularly adamant on this point.

When Macmillan acceded to the government's request to remove Kahn's statement about clearance, Kahn – feeling that his reputation and integrity as an author was at stake – threatened legal action to stop its publication unless the company put the sentence he had included about government review and clearance back in. Macmillan, at this point clearly tired of Kahn's behavior and simply wanting the book out, in turn threatened to proceed to publish it regardless of whatever Kahn did. In the end, however, tempers cooled and Kahn was persuaded that simply stating that the book had been submitted to the government for review would suffice, especially as it would be hard for the government to object to such an inconclusive statement that was moot on the question of whether the book had been cleared. It appears in the book as published.[48]

Conclusion

David Kahn was not the first author to tangle with a government over a book dealing with intelligence, nor would he be the last. Authors, literary agents, publishers, and government officials have accumulated a half-century of experience dealing with one another. Given the ever-increasing number of books and articles published each year in the field, one presumes that more than a few major publishing houses and literary agencies now have branches or individuals who specialize in shepherding such

[47] Letter from Kahn to Ritner, September 1, 1966. Kahn Collection, Box 58, Folder 2.

[48] Letters from Kahn to Ritner, February 26, 1967; from Ritner to Kahn, March 3, 1967; and from Kahn to Ritner, March 18, 1967. Kahn Collection, Box 58, Folder 2.

material into print and dealing with what is probably an equally large number of government counterparts concerned with its appearing.

The story of how *The Codebreakers* made its way into print, like that of any similar book, is unique, with its own specific issues, actors, and outcome. That said, there are a number of general observations that can be made about the interactions between the government, the publisher, and the author which may have relevance to analogous situations today

Each participant acted rationally. It would be difficult to construe the actions of Kahn, Macmillan, or the government as anything other than reasonable. Kahn had invested years, often apparently working full time, to produce what he almost certainly thought was the book that would establish his reputation as an author. Macmillan likely judged it had a volume that would sell well, although over time it may have started to have some doubts in that regard given its burgeoning length. As for the government, it never had encountered the possibility that someone would write such a comprehensive study of codebreaking. It is not surprising that it saw Kahn's book as a threat.

While Kahn, Macmillan, and the government all acted to defend their respective interests, each also made an effort – albeit at times a halting one – to respect the interests of the others. At times, Kahn may have found the government's positions absurd – possibly because he had a superior knowledge of what information about cryptology already was in the public domain – but in the end he agreed to its request that he remove certain information from his manuscript. Similarly, he initially resisted pressure not to disclose that the government had reviewed his manuscript, but ultimately compromised. Much the same can be said of the government. It may have been outraged by the possibility of such a comprehensive story of cryptology appearing in print, but it also came to understand the exceptional amount of information that Kahn's research has amassed from public sources and that, at best, it could protect only a few pieces of information that it deemed most sensitive. As for Macmillan, it successfully defended its investment and reputation while at the same time protecting both Kahn's rights as an author and the government's national security interests.

Finally, viewed from the perspective of hindsight, the final outcome seems almost inevitable. As their negotiations evolved, moreover, Kahn, Macmillan, and the government may have come to view the outcome in this way. It also is difficult to imagine how, once Kahn had completed *The Codebreakers*, it could not have been published more or less how he had written it. He had done his research, and had gathered the bulk of his information from open if not particularly well-known sources. As for the remainder, it came from his background as a journalist and his methodical interviews with an impressive number of sources in Europe and the United

Figure 6. David Kahn in 2010 (National Security Agency).

States. How much classified information these sources might have inadvertently shared is anyone's guess. The question was whether the government could prove this, and with one possible exception – the breaking of Enigma – the government decided it could not, at least not without revealing even more information.

Historians of cryptology are fortunate that the story of *The Codebreakers* unfolded in the fashion that it did. Had it not, another tenacious, resourceful individual presumably would have replicated Kahn's achievement eventually, most likely in the years following the 1974 disclosure of Britain's Enigma success and its impact on the course of World War II. That scholar – or like Kahn, for that matter, journalist – would have had several advantages that Kahn lacked. The amount of primary source material would have been increasing significantly and regularly. Access to it would have been generally easier, and participants in key historical events more willing to share their memories. All of which, of course, makes *The Codebreakers* that much more impressive as an accomplishment. It also leaves all who write today on cryptologic history significantly in its author's debt.

Disclosure statement

No potential conflict of interest was reported by the author.

About the author

David Sherman retired from the National Security Agency in 2017. He thanks Jeffrey Kozak and Melissa Davis of the George C. Marshall Foundation, Rene Stein and Robert Simpson of the National Cryptologic Museum, Tony Comer, Robert Hanyok, and Betsy Rohaly Smoot for their assistance during preparation of this article.

Bibliography

Archival Collections

Vera Filby Collection. National Cryptologic Museum, Fort George G. Meade, MD.

David Kahn Collection. National Cryptologic Museum, Fort George G. Meade, MD.

William F. Friedman Collection of Official Papers. National Security Agency, Fort George G. Meade, MD.

William F. Friedman Collection. George C. Marshall Foundation, Lexington, Virginia.

Books and Articles

Bamford, J. 1982. *The puzzle palace: Inside the National Security Agency*. Boston: Houghton Mifflin.

Farago, L. 1962. *The tenth fleet*. New York: Ivan Obolensky.

Gallery, D. V. 1957. *We captured a U-boat*. London: Sidgwick and Jackson.

Kahn, D. 1967. *The codebreakers*. New York: Macmillan.

Kahn, D. 1983. How *The Codebreakers* was written. In *Kahn on codes: Secrets of the new cryptology*, ed. D. Kahn. New York: Macmillan.

Kahn, D. 1960. Lgcn Otuu Wllwqh Wl Etfown. *New York Times Sunday Magazine*, 13 November.

Kahn, D. 1974. The ultra secret. *The New York Times Book Review*, 29 December.

Moran, C. 2013. *Classified: Secrecy and the state in Modern Britain*. Cambridge: Cambridge University Press.

Oral History Interview with Marshall S. Carter, October 3, 1988. National Security Agency, Fort George G. Meade, MD.

Pratt, F. 1939. *Secret and urgent: The story of codes and ciphers*. Garden City, NY: Blue Ribbon Books.