Cryptologic Quarterly

2023-02 • Vol. 41

Center for Cryptologic History

Cryptologic Quarterly

Publisher: Center for Cryptologic History
Chief: John A. Tokar
Executive Editor: Jennie Reinhardt
Associate Editors:
Kristina Crowe, Laura Redcay

Editorial Policy. *Cryptologic Quarterly* is the professional journal for the National Security Agency/Central Security Service. Its mission is to advance knowledge of all aspects of cryptology by serving as a forum for issues related to cryptologic theory, doctrine, operations, management, and history. The primary audience for *Cryptologic Quarterly* is NSA/CSS professionals, but *CQ* is also distributed to personnel in other United States intelligence organizations as well as cleared personnel in other federal agencies and departments.

Cryptologic Quarterly is published by the Center for Cryptologic History, NSA/CSS. The publication is designed as a working aid and is not subject to receipt, control, or accountability.

Contacts. Please address questions or comments to Editor, *CQ*, at history@nsa.gov.

Copies of *Cryptologic Quarterly* can be obtained by sending an email to history@nsa.gov.

Cover: World War II cryptolinguist Elizabeth Boba and husband Imre at Radio Free Europe, around 1954. Photograph courtesy of the Boba family. Article on page 3.

Contents

2023-02 • Volume 41

(U) The Editor's View

Human Stories All

Now that I have reached the latter part of my publishing career, I am finally noticing that the kernel of even the most technical and complex writings is the same: the authors' response to the circumstances of their lives. Events wonderful and awful, exhilarating and dismaying happen to everyone. Learning how others have responded is compelling because that knowledge can inform how we will react in our own lives.

If you have already arrived at this insight, you'll quickly grasp the thread running through this issue of *Cryptologic Quarterly*!

Biographical stories of course focus on the choices individuals made as they were shaped by their families, eras, and locales. But don't math and technology stories also boil down to humans' efforts to make sense of—and sometimes mold—the swirl of nature and humanity surrounding them? This collection of articles is a case in point.

* * * * * * *

Elizabeth Boba met and married her life partner in the 1950s, worked as a university administrative assistant, and became a grandmother: a seemingly traditional life for her time and position in her world. Fortunately for us, however, she wrote down for her family descriptions of her military service during World War II, which began with the US Army Signal Corps at Arlington Hall Station and went on to include the decoding of Japanese and Soviet Bloc communications! Even luckier for the historical record, her family shared her memoir with the Center for Cryptologic History. Boba lived to be 100. I think you will enjoy reading the astonishing details she recorded.

How does someone driven by an interest in science and business reveal his responses to life circumstances? Edward Hebern invented a cryptographic machine; he desperately needed it to be a commercial success for his family's financial stability. The machine was indeed built—one is on display in the National Cryptologic Museum in Maryland—yet historian David Kahn described Hebern's story as ultimately "tragic, unjust, and

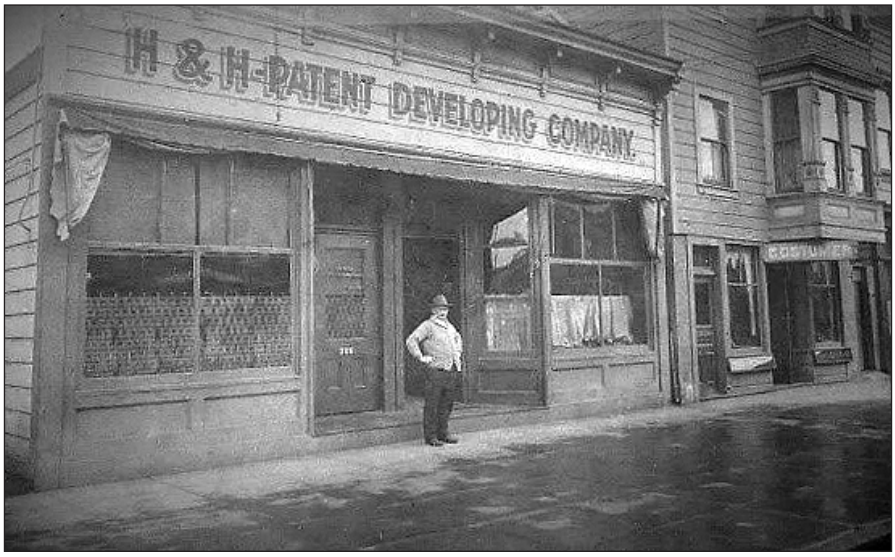
pathetic." Although his efforts led to the development of better US military cryptographic machines, playing a key role in protecting important US communications during World War II, Hebern likely never knew about those successes. The article on his "cryptographic odyssey" lays out the oscillations of his story.

Rob Bonney's article on probabilistic failure theory—statistical mathematics—might seem a complete departure from the others: perhaps fine within such a math-robust agency as NSA but possibly too technical for most readers. Yet don't we all weigh "the risks of taking risks" multiple times daily and conclude, as Bonney did, that we "… *must* be very reliably safe from day to day if we are to realize a long and happy life"? See if his exploration of risk taking does, after all, pertain to your experience!

An expert on historic military operations, Max Hastings in his book *The Secret War: Spies, Ciphers, and Guerrillas, 1939-1945* turned his focus on intelligence in World War II. How did wartime decision-makers use, or fail to use, the intelligence provided to them? The NSA historian describes the strengths (and a few shortcomings) of the book.

Enjoy the varied humanity in these collected articles!

Jennie Reinhardt
Executive Editor



In an effort to steer his destiny, Edward Hebern founded a patent company. Shown here is the Oakland, California, establishment in the early 20th century. Article begins on page 9.

My Experiences during World War II

Elizabeth H. Boba (Oma)

Introduction

On December 21, 2020, Elizabeth Herndon Hudson Boba passed away at the age of 100. Her life had been as full as it had been long. In the 1950s she moved to Munich, Germany, where she worked for Radio Free Europe. There she met and married Polish-Hungarian refugee Imre Boba, and there their two daughters were born. The Bobas later moved to Seattle, where Imre taught history at the University of Washington while Elizabeth worked as an administrative assistant in the Classics Department. In the ensuing decades Elizabeth enjoyed frequent return trips to Europe, continued her lifelong interest in music, and kept up with a wide network of friends and family, including two grandchildren.

But there had been more to her life story. In 1943 Elizabeth had left graduate school and joined the work of the US Army Signal Corps at Arlington Hall Station in Virginia. Before the year was out, she was applying her musician's analytical intuition as part of the large-scale effort to decode Japanese communications. She stayed on for several years after World War II, extending her expertise to Soviet Bloc targets.

In January 2021 Elizabeth's family contacted the Center for Cryptologic History to offer Elizabeth's memoir—written to share with her family—of the war years and her time at Arlington Hall Station. We found her account informative, compelling, and impeccably written. We reprint it here so that our readers may also enjoy this first-hand account from a previously unheralded Arlington Hall cryptolinguist.

Brenda McIntire, CCH historian

Figure 1. A work center at Arlington Hall Station. Mrs. Boba's daughters have identified her as sitting three rows back, on the right. Arlington Hall Photograph Collection, nsa.gov

There has been quite a lot of attention given lately (2007) to the events of the Second World War. I think that up to now it has been difficult to talk about [the war]. Which seems strange to say—there have been a lot of books, films, programs, discussions, etc., about aspects of it, but there is still something deep that changed those who lived through it. And yet, life went on—more easily in the United States but gradually in other parts of the world. Perhaps it is because the Second World War introduced many new methods of communication—we seemed to awaken to the situations in many faraway places. At any rate, I thought perhaps you would like to know what I was doing during that period.

1. September 1939

What strikes me now as I think about the period leading up to the war is how little news we had—especially about events in Europe. News

reached us mainly through newspapers; there were not many radios in homes. We got our first radio—a little thing about the size of a shoebox—in 1934. I don't remember how much news was broadcast, but I am quite sure it was very little. When a sensational event happened, newsboys shouted it out on the street and newspapers published "extras."

I was a junior in college in the fall of 1939, and after two years at Illinois College in Jacksonville (where my father was college president), I transferred to Sweet Briar College in Virginia (where my father had been a history professor). My whole family took me by car to Sweet Briar, stopping to visit relatives along the way. We also stopped for a day or two in New York City to visit the World's Fair that was in progress. While we were there, a German steamship (I believe the name was *Europa*) weighed anchor unexpectedly and sailed out of the harbor. I am not sure of the exact date, but it was publicized as the result of the outbreak of hostilities in Europe: Hitler had invaded Poland on September 1, 1939.

As a student at Sweet Briar, I lived in a dormitory and became engrossed in my studies and in student life. I didn't have a radio in my room; in fact, I don't remember where I got any news—or if I did very regularly. I heard that one of the students had listened to a short wave broadcast of a Hitler speech, but I never heard any details. I was studying English history, Shakespeare, Chaucer, Greek, philosophy, and counterpoint, and taking piano lessons.

Recently, I have been reading William Shirer's *Berlin Diary: The Journal of a Foreign Correspondent, 1934-1941*. Shirer was a journalist stationed in Berlin during the late 1930s and the year 1940. He did from Berlin what Edward R. Murrow did from London—nightly broadcasts to the United States, in Shirer's case all of five minutes! And his script was censored by Nazi authorities. He often resorted to American slang in order to get the true situation across.… It is no wonder that Americans did not know very much about the war in Europe.

2. December 7, 1941: Pearl Harbor

After graduating from Sweet Briar College in June 1941, I returned to Jacksonville and lived at home while taking postgraduate (fifth year) classes locally. During my senior year at Sweet Briar, I made up my mind that the one thing I wanted to study was music. I had had a number of years of piano lessons and I had sung in a variety of church choirs and local choruses, but I wanted to learn more about the technical side of music. I knew it was late to begin a new course of study, but that was my ambition—aside from getting married and having a family. So I enrolled in the local music department, which was actually part of the other college in town: MacMurray College for Women. In summer 1941 I started organ lessons, continued piano lessons, and took a course in music theory, continuing all of these during the 1941-42 school year. (I also took a two-week course in beginning typing at the local business school, because—believe it or not—I only used the hunt-and-peck system for typing all through college!)

On Sunday afternoon, December 7, 1941, as I remember, I was alone listening to the New York Philharmonic concert over the radio. By that time, we had acquired a very nice Philco combination radio and phonograph. At some point, the concert was interrupted by an announcement that Pearl Harbor had been attacked by Japanese planes! I knew this was a really big event, but I did not feel frightened or worried. Hawaii was far away, and it was impossible to know what might happen afterward. I am not sure whether any others of the family were in the house at that time—I think my mother was resting upstairs. I don't even remember whether the concert came back on. But events moved swiftly after that.

3. My Part in the War Effort: 1943-1945

I completed my music courses for spring and summer 1942, applied for graduate school at the University of Michigan, Ann Arbor, and was accepted to their MA program. At Ann Arbor, I lived in a dormitory and took some wonderful music courses, particularly a course in medieval music. The music department was located in a tower! We moved from class to class by elevator. I also took some organ lessons, but the professor discouraged me from continuing. I wasn't up to graduate school level in organ.

Ann Arbor was a neat place to live in the fall. The snow arrived by Thanksgiving, and I had a lot of fun attending the football games. The war in Europe seemed far away, and even when I was at home for Christmas, I didn't feel very much moved by it. My father, however, in his position as administrator of a college, received all sorts of recruiting notices for various war jobs. And, recalling the situation during World War I, he felt that everyone should do his part for the war effort—and in situations such as WWI and WWII, one certainly should. He heard about jobs in Washington working with maps, and he also heard about the need for persons with language ability to work near Washington for the Signal Corps. Persons with mathematical skill and/or foreign language skill were sought. So the upshot was that I left Ann Arbor at the end of the first semester and went to Arlington, VA, for a job at Arlington Hall.

Arlington Hall was a [former] boarding school for girls, which had been commandeered by the Army Security Agency for their work on codes [cryptography and cryptanalysis]. The main building, a colonial brick building, was used for offices, and one or two two-story temporary buildings were put up for the operations. The whole campus was converted into an army post, complete with barracks, bugle calls, mess halls, etc. A number of army recruits with high IQs were made second lieutenants overnight and housed in Quonset huts on the grounds. They took delight in annoying their sergeant by lolling on their bunks studying their Sanskrit or Japanese and refusing to obey orders.

But the bulk of the personnel were civilian recruits from the ranks of college faculty and other professional posts. One of the first persons I met was my favorite junior high school English teacher from Lynchburg, VA. All personnel were placed in the training school until they received their security clearance. It took about six weeks for me, although I was kept on as an instructor for a total of about six months. During this time, I got together with a former college friend (I knew she was there) and together we rented a flat with two other girls. It was the upper floor of a private home within walking distance of the [post]. And two years later, our landlady offered us a whole house even closer to the [post], which was a great joy to all of us. The rent was $100 a month—divided among four girls. That does not sound like much, but you have to realize that my beginning salary at Arlington Hall was $1,640 per year (later raised to $1,820)!

Finally, I was assigned to an operations unit—the section that was working on intercepted radio messages between Japanese military attachés and their headquarters in Tokyo. We occupied one whole wing (second floor) of a temporary building—a huge room with windows on both sides and rows and rows of long tables, with an aisle in the middle. The section was administered by a civilian and an army captain, but the work was supervised by a few "brains" (e.g., a math professor, a classics professor, etc.). They directed the rest of us, who sat at [those] long tables and [processed] by hand what nowadays would be done in a flash by a computer. (Remember, that was in the 1940s!) Every new radio message was broken down by its parts and filed on little slips of paper (different colors) in file drawers. When enough of

the key was solved, a message was overlapped with messages using the same key; we clerks worked with dictionaries and common guesswork to figure out what the missing codewords were. There were two former missionaries (Seventh Day Adventist) who spoke Japanese and who assisted us in our work.

Japanese, as you know, is built up with digraphs, for the most part, e.g., Hi-ro-shi-ma or O-sa-ka, etc. And instead of prepositions, they use postpositions: -wa denotes the subject of the sentence (if I remember correctly) and -no denotes a noun after a preposition. Then, they had special digraphs to stand for numbers: AK equaled one, BL equaled two, etc. In short, the whole square (the alphabet each way) was used to make up words. [I thought] it was really not a very sophisticated code or cipher arrangement, and the Japanese continued using the same code and keys for a long time. But all of a sudden—one day—one of the experts stood up at the front of the room and solemnly tore a big worksheet into little bits: the Japanese had changed their codebook!

After that, our work changed quite a bit. At one point, part of the big room was cordoned off and some mysterious machine was set up. It made a clicking noise and produced long endless strips of yellow tape with perforations in it. You will probably guess that it was a very early stage of a … computer! But it was very "hush, hush" and was referred to only as "Zimmie's machine' for the woman [possibly Wilma Zimmerman Davis] who was entrusted to run it. This was probably in 1944 or 1945.

Keeping up with the news was much easier in those days, of course, but we still got it mostly from the radio. And we didn't really follow the progress of our troops very carefully. The US/British invasion of Europe was expected all through the spring of 1944, but I was really taken by surprise when it happened on June 6. My daily routine was to get up at 6 a.m. and turn on the radio to a local station that brought a half-hour of classical music at that time. The morning of June 6, I was so angry: there wasn't any music at all, and it was only after I calmed down that I listened more carefully and realized that the invasion had begun!

Figure 2. Elizabeth Hudson in Munich, around 1952. Photograph courtesy of Boba family

4. Continuation of Cryptography Work, 1945-1948

With the end of hostilities between the United States and Japan, the work at Arlington Hall turned to the Soviet threat. I was assigned to work on one of the Soviet codes, in preparation

for which I was given a five-day, 40-hour, crash course in Russian. It sounds like an impossible assignment, which of course it was in the strict sense of the word, but I found that it was very exhilarating: The instructor taught us the Russian alphabet and went right on into the main grammatical elements. We learned that Russian nouns have six cases (if memory serves me right), that there are three numbers (singular, dual, and plural), and that there are 32 letters in the Russian alphabet. The similarity between Russian and Greek letters was helpful: written Russian was actually based on Greek. No attempt was made to teach us to speak Russian, of course, and even though we were given tutorials later in reading excerpts of Russian fiction, I for one never mastered the language that way.

In 1947, however, I began to think that I should develop my Russian to qualify for what seemed to be a market for Russian-trained employees of various kinds. With this in mind—and to get a break from the grind in Arlington, I attended Columbia University Summer School in New York City. I took two courses and learned a little—but really not very much. It was an interesting experience, however, including a trip with the Russkii Kruzhok (Russian Circle) to the estate of the Countess Tolstoi, daughter of the author, who was offering a refuge for many Russian refugees on her estate called Reed Farm. We sat on the lawn and ate our lunch, and the countess came by and spoke with us. There was a Russian Orthodox Church on the grounds; as it was Sunday, we looked in on a service in progress.

I returned to my job in Arlington after the course was over, but by May 1948 I was thinking seriously of doing something else. My parents were also urging me to come back home, and so I did in May or June. As part of the formality of [separating] from the service, I was sworn to secrecy about anything having to do with the work at Arlington Hall, and I kept my promise for a number of years. In the early 1960s, however, when we were living in Seattle, I discovered a book or two expressly about the US cryptographic work during World War II in the Northeast Branch Seattle Library! It was written by a well-known cryptographer, [William] Friedman, who along with [Herbert] Yardley really got US cryptanalysis up and running. So, I decided I could finally talk about my experiences!!

Let us hope that such an upheaval as World War II never happens in the world again!

Oma/E.H.B.

From Hebern to SIGABA and Beyond—A Cryptographic Odyssey

Patrick Bomgardner

Meet Edward Hugh Hebern

If you've ever read David Kahn's *The Codebreakers*, or visited the National Cryptologic Museum, or just have an interest in cryptologic history, then it's a good bet that you've heard of Edward Hugh Hebern. It's also a good bet that you may not know his whole story.

Born on April 23, 1869, in Streator, Illinois, Hebern grew up in the Soldiers' Orphan Home in Bloomington. He worked on a farm, but eventually made his way to California where he worked a timber claim that he subsequently sold to a sawmill. Hebern later became a carpenter, building and selling homes in Fresno.[1] He did nothing of cryptologic significance until he was in his early 40s.

The details are sketchy, but Hebern's widow Ellie told Kahn that he developed his interest in cryptography while incarcerated from 1907 to 1909 in San Quentin State Prison, convicted of stealing a horse. Cryptologic pioneer William Friedman once asked Hebern if he was guilty of the charge, to which Hebern replied, "The jury thought so."[2] After reading about some American government codes that had been broken, he became determined to figure out a more secure way to encrypt messages.[3]

Upon his release from prison, Hebern married

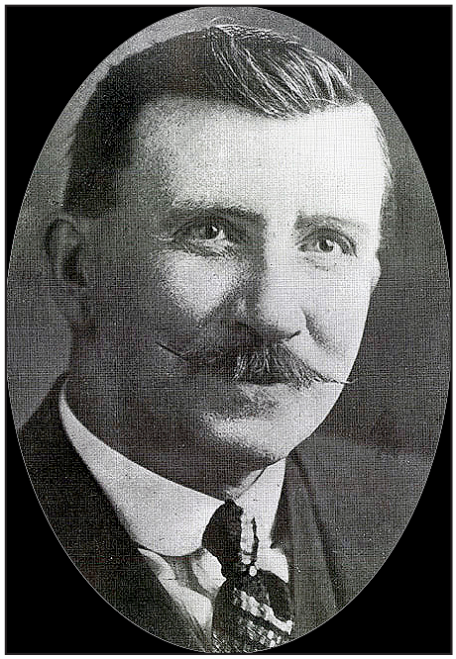


Figure 1. Edward Hugh Hebern, n.d., *Collection of the Center for Cryptologic History*

Ellie and incorporated the H & H Patent Developing Company with Fred Hoffman in Oakland, California (figure 2). Between 1912 and 1915, H & H patented a few devices, including one for reading coded messages embedded on the faces of checks using perforations and another attachment

Figure 2. H & H Patent Developing Company, n.d., *Collection of the Center for Cryptologic History*

designed to turn an ordinary typewriter into a cipher machine.[4] I found no evidence that either was a big seller.

Cryptography Gets a Charge

It wasn't until 1915 that Hebern randomly wired two electric typewriters together so that depressing a key on the plaintext typewriter would produce a cipher-text output on the other. The result was an unsophisticated monoalphabetic substitution, but it was the germ of the idea for Hebern's most significant invention—the wired rotor (figure 3).[5]

Simply put, a wired rotor is a disk made from nonconducting material with 26 interconnected, equally spaced contact studs on each face. The studs are connected by a wire so that an elec-

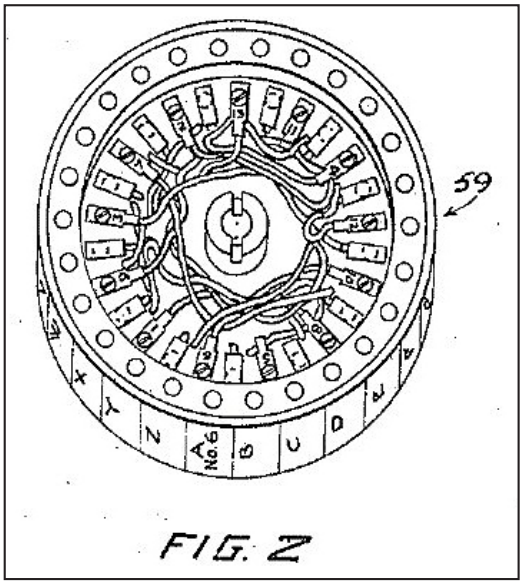


Figure 3. Wired rotor drawing, 1921, US Patent 1,510,441, *US Patent Office website*

Figure 4. Hebern Code machine at the National Cryptologic Museum, 2023, *photo taken by author*

trical current entering one side of the rotor will exit from a different position on the other side. Hebern was also the first inventor to use the "interval method" to wire his rotors in order "to produce as flat a polyalphabetic frequency distribution as possible" (figure 4).[6]

Sometime in 1917, Hebern placed a wired rotor device between the typewriters. Depressing a key sent an electrical impulse through the rotor to the other typewriter. The rotor moved once with each keystroke, producing a polyalphabetic substitution cipher. He built a working model of it in 1918 but didn't file a patent for it right away. Around the same time other inventors, including Arvid Damm, Hugo Koch, and Arthur Scherbius, independently came up with similar devices in Europe. Koch's and Scherbius's would evolve into the infamous Enigma cipher machine used by the Nazis during World War II.[7]

Have I Got an Electric Code Machine for You!

Hebern showed his machine to the US Navy commandant in San Francisco in 1921.[8] He

advertised an "unbreakable" cipher in a magazine, but Agnes Meyer—the navy's principal cryptanalyst—easily broke the sample message.[9] Her boss sent the solution to Hebern who rushed to Washington, DC, at his own expense to pitch his machine. The navy was looking for something "radically different" in terms of secure communications and was very impressed with Hebern's demonstration. While in Washington, Hebern filed his application for US Patent 1,510,441.[10]

Hebern incorporated Hebern Electric Code in Oakland in 1921—the first cipher machine company in the United States. Encouraged and assisted especially by Meyer of the navy's Code and Signal Section, and rightly believing that his wired rotor machine was the device of the future, he raised $1 million (approximately $17 million in 2023 dollars) from 2,500 shareholders, mostly in Oakland. Much like tech startups today, he had no orders or income. Regardless, in February 1922, he bought a machine works to make dies and molds.[11]

On September 21, 1922, believing that his company was on the verge of great things—even though he still had no orders for any cipher machines—Hebern broke ground on a three-story, neo-Gothic headquarters building. At a cost of around $380,000 ($6.9 million), it occupied half a square block at 829 Harrison Street in Oakland and was meant to accommodate 1,500 employees. Hebern even had a corner office with a fireplace. The building was projected to cost $250,000 ($4.3 million), but ballooned to $380,000, $100,000 ($1.7 million) of which Hebern had to mortgage (figure 5).[12]

The following February, he hired Meyer away from the US Navy to be his technical advisor for cryptologic matters and liaison with the navy (figure 6).[13]

However, on January 2, 1923, a navy board comprising Commander (CDR) Royal E. Ingersoll, CDR Russell Willson, and Lieutenant Commander (LCDR) W. W. Smith examined several Hebern devices but recommended against purchasing the machines unless improvements were made. The Secretary of the Navy approved the board's recommendation on January 18.[14]

Figure 5. The former Hebern Electric Code, Inc., building currently serves as the Asian Resource Center for Oakland, California, 2010, *Wikimedia Commons*

Anticipating that Hebern would make the necessary improvements, the Bureau of Engineering (BuEng) put $50,000 ($873,000) in its 1925 budget for the purchase of 98 Hebern machines. The stipulation was that Hebern had to "develop two electric printing cipher machines to fulfill Navy requirements" and that the "pilot models proved satisfactory."[15] Hebern Electric Code and the navy signed contract 61155 on August 5, 1924.

According to Captain Laurance Safford's 1943 naval history of the ECM Mark II, the main problems with the Hebern machines were mechanical deficiencies in the printer and power drive. The cryptographic features could be improved, but the navy decided not to give Hebern any more suggestions that could be incorporated into machines offered for sale to foreign governments. The navy planned to accept the cryptographic features as is and then modify the machines after delivery to make them more secure.[16]

Later in 1923, the US Army Signal Corps

Figure 6. Agnes Meyer Driscoll, n.d., *Collection of the Center for Cryptologic History*

purchased two "Hebern Electric Super-Code" machines for "examination and consideration relative to its suitability for use in the military service."[17]

The US Navy also requested that William Friedman, chief of the Signal Intelligence Section (SIS) in the army's Office of the Chief Signal Officer (OCSigO), conduct a cryptanalytic test of Hebern's machine based on 10 test cryptograms prepared by the navy's Code and Signal Section (figure 7).[18]

Figure 7. William Friedman and the Hebern Cipher Machine, n.d., *Collection of the Center for Cryptologic History*

Friedman found the device to be compact and rugged with a degree of secrecy comparable to the printing telegraph cipher machine developed for the army by AT&T, which in its present form was too bulky for deployment below army headquarters level. The Hebern machine was much more suitable for field use. However, he also found that it was not "absolutely indecipherable" or even "practically indecipherable,"[19] due mostly to the predictable metered stepping motion of its cipher wheels.[20]

Friedman issued his findings in an unpublished, typewritten secret document; he believed that enemy military forces might use such devices in future wars and that his analysis would be essential in the study of the intercepted messages.[21] The army didn't purchase any of Hebern's machines nor did they share Friedman's findings with Hebern. Friedman had other plans, as detailed below.

Shareholder Revolt

Meanwhile, with no money coming in, Hebern defaulted on the mortgage for the new building, so Hebern Electric Code levied a 10 percent assessment on shareholders to pay the interest. The angry shareholders prompted a 1924-1925 state investigation by Alameda County District Attorney (and future California governor and chief justice of the US Supreme Court) Earl Warren. Hebern had allegedly violated the California Securities Act by selling stock for more than its $1 par value (figure 8).[22]

Figure 8. Earl Warren, n.d., *California State Archives*

Hebern went on trial on March 1, 1926. After Caroline Gowdy testified that she bought 200 shares for $5 per share, the jury deliberated for 12 minutes before finding Hebern guilty.[23] The trial judge overturned the verdict after no one presented evidence to dispute Hebern's claim that Gowdy bought the shares privately from Hebern's brother-in-law, so neither Hebern nor the company was involved in the transaction.[24] The judge's decision was upheld on appeal and Hebern was freed, although he reportedly suffered a nervous breakdown.[25]

Nevertheless, shareholder anger and public scrutiny made it difficult for Hebern to raise capital, so Hebern Electric Code went into bankruptcy in June 1926.[26]

Undeterred, and still confident of gaining a navy contract, Hebern incorporated the International Code Machine Company in Reno, Nevada.[27] Unlike the army, the navy was still willing to work with Hebern and his new company. In January 1927 Hebern submitted a new machine to the navy for a service test. While it was cryptographically satisfactory, the navy found it unsuitable because it was so mechanically and electrically unreliable.[28] The navy also tried unsuccessfully to get Hebern either to license his patents or to sell his interest in the navy machines so that it could work with a more established firm such as Ford Instrument Company to build the machines more reliably.[29] Finally, with some advice from technicians LCDR Safford and LCDR John MacLaran at the Washington Navy Yard Radio Test Shop, Hebern managed to "perfect" his machine (figure 9).[30]

Hebern delivered two "special cipher typewriters" for $3,270 ($60,000) in March 1930 under confidential contract Nos-13798. After two months of service testing, the machines proved

Figure 9. Laurance F. Safford, n.d., *Collection of the Center for Cryptologic History*

satisfactory, so the navy ordered 31 machines for $46,500 ($851,000).[31] Hebern equipped the machines with the secret universal (or US Navy) dog action—a mechanical means for pseudo randomly stepping the cipher rotors (figure 10). Safford worked hard to make the Hebern machines a success, staking his service reputation on the effort.[32]

The Navy Pulls the Plug and the Rug

Two years later the navy bought a modified machine from Hebern for $4,300 ($96,000) under contract 25436. The Code and Signal Section requested that the army's SIS test the machine "with utmost severity." The navy provided the machine and 165 test messages that had been enciphered on it. Under Friedman's supervision, SIS junior cryptologists Frank Rowlett, Solomon Kullback, and Abraham Sinkov conducted the test and cryptanalysis. Although the new machine's method of stepping the cipher wheels was an improvement over the model analyzed by Friedman in 1923, the SIS cryptanalysts were able to figure out the machine settings and read the test messages.[33] Based on these findings, the navy decided the machine was not suitable for service use and informed Hebern they were no longer interested in it.[34]

BuEng's Bern Anderson reported to the head of Radio Division that the defects in the Hebern machines were "largely due to the failure to use or disregard of basic electrical laws and principles of design."[35] Stanford C. Hooper, director of Naval Communications (DNC) from 1928 to 1935, would years later, perhaps with some affection, refer to Hebern as a "screwdriver engineer."[36]

Around this time, the Office of Naval Operations decided to take responsibility for developing the navy cipher machine away from the Code and Signal Section—citing a lack of personnel and equipment—and give it to BuEng.[37] Anderson and Lieutenant (LT) Donald Seiler undertook the development of an in-house cipher machine—the ECM Mark I. It was heavy, bulky, and unreliable (figure 11). It took five years to work out the bugs.[38]

Seeing that the in-house development of the ECM Mark I might not bode well for Hebern's fortunes, DNC Hooper wrote to the chief of the Code and Signal Section (OP-20-G) on August 30, 1934:

> Offhand I would say the Government owes Mr. Hebern something. The course we are pursuing to obtain the machines is necessary. … Certainly we do not wish to turn Mr. Hebern away in the cold. We wish him to feel the whole Navy appreciates fully his work and contribution.[39]

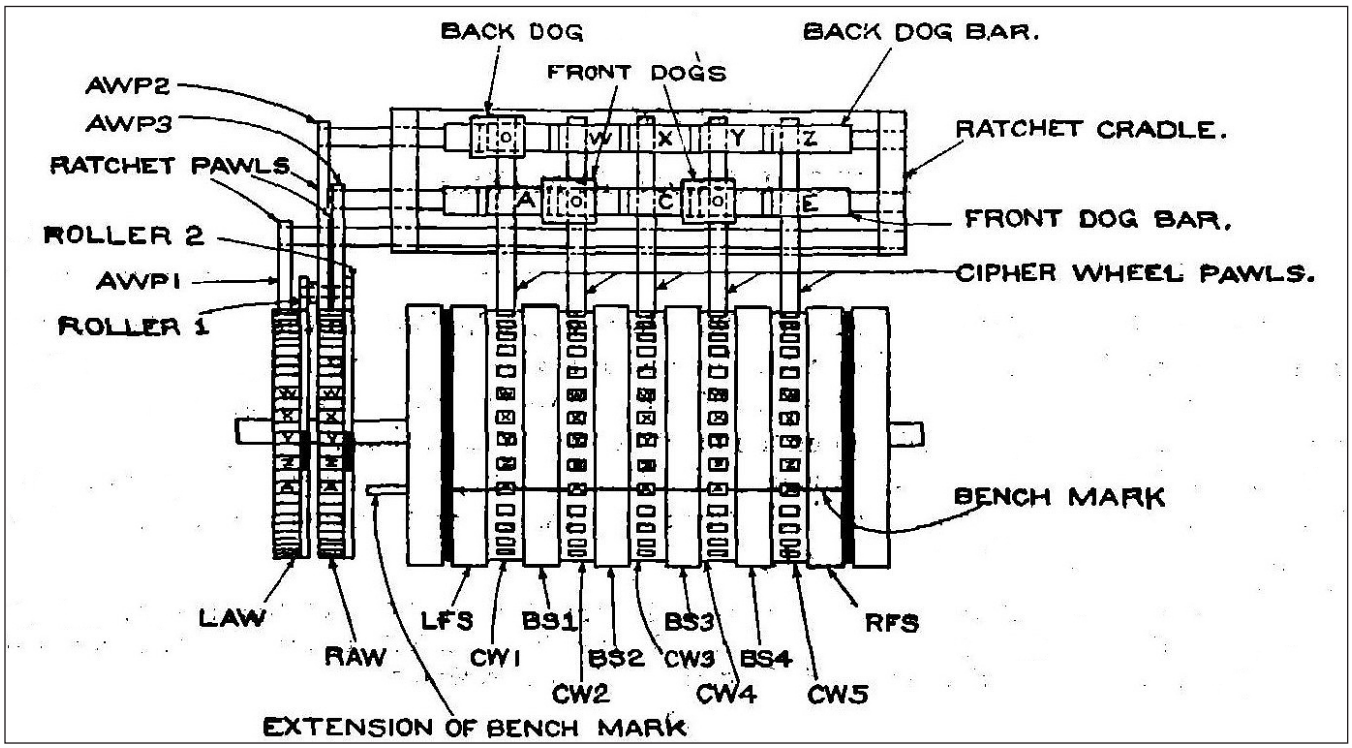


Figure 10. Universal Dog Action, 1935, schematic drawing from *Analysis of a Mechanico-Electrical Cryptograph, Part II*

Figure 11. ECM Mark I, n.d., *Collection of the Center for Cryptologic History*

Agnes Meyer (by then Meyer Driscoll), who had returned to the Code and Signal Section amidst the turmoil of Hebern's securities act investigation in 1924, also wrote a note to her Office of Naval Communications superior, CDR Howard Kingman, expressing similar sentiments about Hebern's contributions and the navy's treatment of him.[40]

Despite Hooper's and Driscoll's efforts, the incoming DNC, Rear Admiral Gilbert Rowcliff, unceremoniously cut all ties with Hebern in a very abrupt and discourteous letter. According to Safford, "They pulled the rug out from under Hebern, and were not even polite about it."[41]

Friedman Has a Better Idea

In Safford's opinion, from 1924 to 1932, the Signal Corps appeared to think that the Teletype scrambler would be a more practical machine

for army use than the Hebern cipher machine.[42] However, Friedman was trying to get OCSigO support and funding to build a cipher machine of his own design. The army had practically given up on cryptography after the end of World War I, even though the service was spending millions on developing radio communications with no means to protect it.[43]

After finding fault with the metered motion of Hebern's cipher rotors, in February 1926 Friedman came up with the idea of using an external element—Baudot code keying tape—to control rotor movement. He teamed with George A. Graham, chief engineer of the Wire Section at the Signal Corps Development Laboratories in Fort Monmouth, New Jersey, to make drawings of a single rotor machine using a keying tape. Further development of the machine was not prioritized or funded until July 1, 1930—and then only $1,500 allocated for development but given no boost in priority at the labs. Prioritization was finally raised from 19 to 6 in September 1931. Friedman and Graham filed a patent application on January 23, 1932; US Patent 2,028,772 was granted January 28, 1936.[44]

The first device that resulted from this idea—the Converter M-134-T1—was a failure (figure 12). The initial test conducted on March 24, 1932, proved the device to be very slow, enciphering only 25 letters per minute. Friedman tested a revamped model nine months later, but it was still too slow and difficult to use.[45]

Friedman abandoned the M-134-T1 in favor of "[t]he Proposed New Cryptograph," the Converter M-134-T2 (figure 13). This new device used five rotors and eventually had an integrated IBM typewriter for printing. What was the major conceptual difference between the two prototypes? Where the T1 used a random keying tape to *stop* a rotor, the T2 used random keying tape to *step* the rotors. This eliminated the fundamental flaw in Hebern's design, which was the "fixed

Figure 12. Converter M-134-T1, n.d., *Collection of the Center for Cryptologic History*

character of the successive rotatory movements of the cipher wheels."[46]

On April 12, 1933, OCSigO directed the Signal Corps Development Laboratories to develop the M-134-T2 by adding the keying tape transmitter and making other mechanical modifications to one of the Hebern machines they had purchased. The M-134-T2 passed preliminary testing on July 14, 1934, but was returned to the labs for some changes (figure 13).[47]

The labs delivered two new models for service testing in June 1936. Friedman took a device to Panama in October to conduct a long-distance field test with another device set up in the OCSigO in Washington, DC. The test was successful with the machine producing 30-35 words per minute with the "highest degree of cryptographic security."[48] Friedman filed US Patent 682,096 under secrecy order. It was the first to describe a rotor machine controlled by an externally generated key, i.e., perforated Baudot code keying tape.[49]

Despite some security-related misgivings about having its new secret converter built by a commercial firm, the US Army awarded the contract for the production model to Wallace and Tiernan Products, Inc., of Belleville, New Jersey.

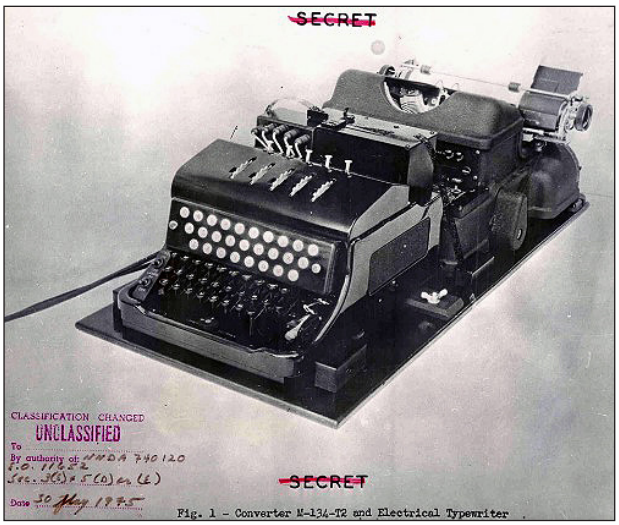


Figure 13. Converter M-134-T2, n.d., *Collection of the Center for Cryptologic History*

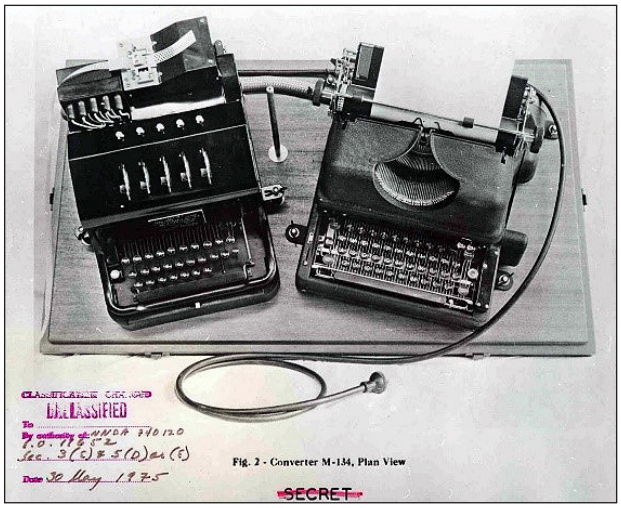


Figure 14. Converter M-134, n.d., *Collection of the Center for Cryptologic History*

The company delivered 12 Converter M-134 (figure 14) (SIGHIC) machines to the OCSigO on August 2, 1938, at a total cost of $25,620 ($555,000). Operational experience with these 12 machines led to minor changes being incorporated into the next 56 new models delivered between April 1, 1940, and December 13, 1943, which also resulted in a change of designator to Converter M-134-A (SIGMYC).[50]

Rowlett Goes a Step Beyond Friedman

Friedman assigned Frank Rowlett (figure 15) the unenviable task of producing the perforated keying tape for the M-134. Rowlett saw the inherent problems with using keying tape and thought there had to be a better way to randomly control the movement of the cipher rotors.[51] In June 1935 Rowlett came up with the concept of controlling the motion of the cipher rotors "by means of an electrical current through the circuits of a rotor maze to generate a long, irregular sequence of characters"—i.e., the Stepping Maze.[52] Rowlett managed to convince a very reluctant Friedman of the benefits of his idea, which they went on to develop together.[53] Because the M-134 had already gone into production, however, the chief signal officer (CSigO) wouldn't allow any changes.[54]

Rowlett's idea went nowhere—at least for the time being, although Friedman and Rowlett filed US Patent application 70,412 on March 23, 1936, under secrecy order.[55]

The army deployed 68 M-134/M-134-A devices around the United States and the world, but, as Rowlett had predicted, the keying tape mechanism proved to be their weakness. This mechanism on existing units was replaced in mid-1941 by Keying Unit M-229, which used Rowlett's rotor maze concept.[56]

When DNC Hooper learned that the army had used the Government Printing Office to print the findings of the SIS analysis of the Hebern machines, he considered it an egregious security breach and forbade BuEng and the OP-20-G from discussing the ECM Mark I with the SIS.[57] Despite Hooper's directive, in October 1935, then LT Joseph Wenger, assistant to the officer-in-charge of the OP-20-G (figure 16), walked across the bridge from the Navy Building to the

Figure 15. Frank Rowlett, n.d., *Collection of the Center for Cryptologic History*

Figure 16. Joseph Wenger, n.d., *Collection of the Center for Cryptologic History*

Munitions Building for a general discussion about cipher machines with Friedman. Wenger was dissatisfied with the ECM Mark I and asked if the SIS "had any good ideas" along those lines.[58]

At first Friedman told Wenger he was not at liberty to discuss any new developments, but he eventually secured permission from the CSigO to share his and Rowlett's idea with Wenger. After a series of meetings and discussions, the navy told Friedman and Rowlett they had no interest in their idea at the time.[59]

Eureka!

That all changed in the winter of 1936-1937, when Wenger showed CDR Safford, the new officer-in-charge of OP-20-G, a paper signed by Wenger, Friedman, and Rowlett that diagrammed "the means by which electric control of an ECM could be achieved through an ECM maze." Safford immediately realized that electric control gave them the answer to many of their unsolved problems and had to be incorporated in the navy's ECM Mark II machine.[60]

In January 1940 the navy offered the ECM Mark II to the War Department for joint army-navy use. At a meeting on February 3, 1940, with DNC Rear Admiral Leigh Noyes, CSigO Major General Joseph Mauborgne, Friedman, and others, Safford acknowledged to Friedman the navy's use of his and Rowlett's invention (figure 17).[61]

Friedman and Rowlett examined the changes that CDR Safford and LT Seiler had made to their original Stepping Maze design. They subsequently decided to retain the "index maze" instead of a plug board, but rejected dividing the Stepping Maze, and changed the proposed step-

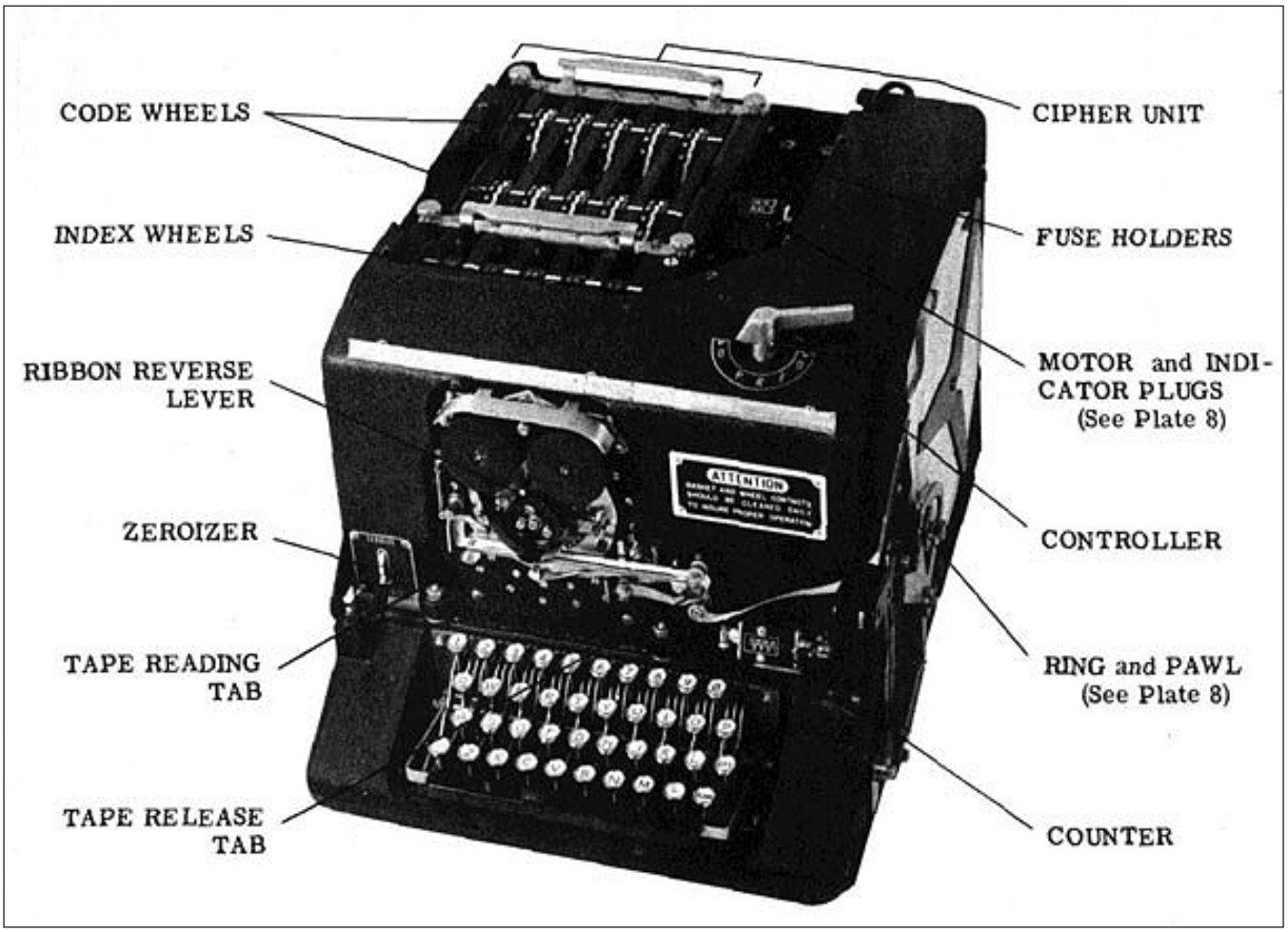


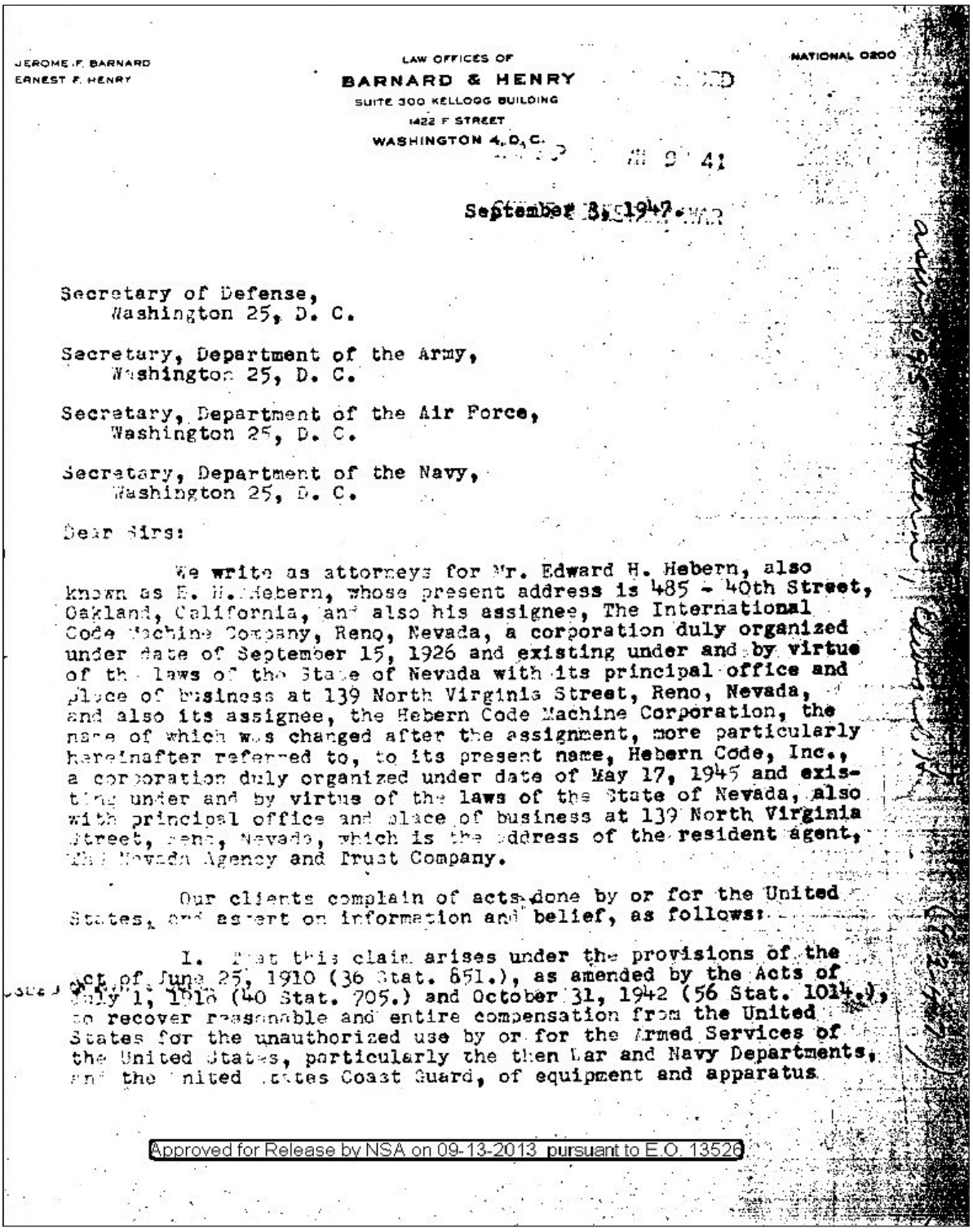
Figure 17. SIGABA/ECM Mark II, n.d., *Collection of the Center for Cryptologic History*

ping order. With those changes, the ECM Mark II was deemed satisfactory and accepted by the army. The joint army-navy SIGABA/ECM Mark II system manufactured by the Teletype Corporation went operational on August 1, 1941[62]—just months before the Japanese attack on Pearl Harbor—and was used throughout World War II. Unlike the more renowned Enigma, the SIGABA was never broken by the enemy.

Hebern Files a Complaint

On March 4, 1946, after the war was over, Hebern wrote to now Captain (CAPT) Safford seeking an endorsement for his new "Commercial" machine, which he had developed from the 31 navy machines but without the secret universal dog action.[63] After careful consideration, Safford decided not to reply.[64]

On September 3, 1947, Hebern's attorneys filed a complaint (figure 18) with the Secretaries of Defense, the Army, the Air Force, and the Navy claiming the US government's infringement of five patents: 1,683,072 (Super Code Machine); 1,861,857 (Universal Dogs); 2,267,196 (Remote Control System); 2,269,341 (Message Transmission Device); and 2,373,890 (New Code Wheel).



JEROME F. BARNARD
ERNEST F. HENRY

LAW OFFICES OF
BARNARD & HENRY
SUITE 300 KELLOGG BUILDING
1422 F STREET
WASHINGTON 4, D. C.

NATIONAL 0200

SEP 9 '47

September 8, 1947.

Secretary of Defense,
Washington 25, D. C.

Secretary, Department of the Army,
Washington 25, D. C.

Secretary, Department of the Air Force,
Washington 25, D. C.

Secretary, Department of the Navy,
Washington 25, D. C.

Dear Sirs:

We write as attorneys for Mr. Edward H. Hebern, also known as E. H. Hebern, whose present address is 485 - 40th Street, Oakland, California, and also his assignee, The International Code Machine Company, Reno, Nevada, a corporation duly organized under date of September 15, 1926 and existing under and by virtue of the laws of the State of Nevada with its principal office and place of business at 139 North Virginia Street, Reno, Nevada, and also its assignee, the Hebern Code Machine Corporation, the name of which was changed after the assignment, more particularly hereinafter referred to, to its present name, Hebern Code, Inc., a corporation duly organized under date of May 17, 1945 and existing under and by virtue of the laws of the State of Nevada, also with principal office and place of business at 139 North Virginia Street, Reno, Nevada, which is the address of the resident agent, The Nevada Agency and Trust Company.

Our clients complain of acts done by or for the United States, and assert on information and belief, as follows:

I. That this claim arises under the provisions of the Act of June 25, 1910 (36 Stat. 851.), as amended by the Acts of July 1, 1918 (40 Stat. 705.) and October 31, 1942 (56 Stat. 1014.), to recover reasonable and entire compensation from the United States for the unauthorized use by or for the Armed Services of the United States, particularly the then War and Navy Departments, and the United States Coast Guard, of equipment and apparatus

Figure 18. Letterhead for Hebern's original complaint against the government, 1947, *NSA Archives*

The complaint also claimed that the Navy Department had Hebern sign an agreement not to disclose the vital features of the 31 machines he sold the navy for five years with assurances that the Hebern Company would be given all contracts for future machines. He asked for $50 million ($685 million) in compensation, only because he was unable to determine—because of wartime conditions—the exact extent to which the government had used his patents without compensation.[65]

While the government dragged its feet in replying to his complaint, Hebern died of a heart attack at age 82 while lifting a heavy box on February 10, 1952.[66]

Nevertheless, the government continued its investigation into Hebern's claims. On September 8, 1952, Hebern's lawyers met with representatives from the navy, air force, Armed Forces Security Agency, Army Signal Corps, and Army Judge Advocate General (JAG) to take a statement from former DNC Hooper (figure 19). Hooper remained sympathetic to Hebern's case, stating, "I feel it my duty to both the service and Hebern that something proper be done about it. Too bad the old gentleman died before settlement was finally made."[67] Hooper also tried to read into the record the memo he'd written to the chief of OP-20-G back in 1934, but the JAG would not let him continue, fearing it would prejudice the government's case.[68]

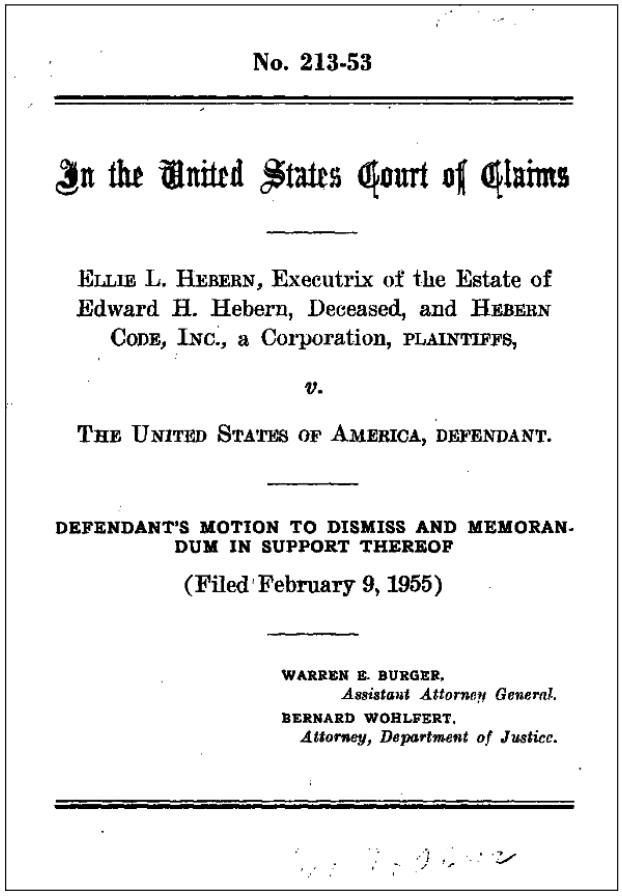
Despite Hooper's advocacy, the government completely rejected Hebern's claims on January 22, 1953,[69] even though there was enough evidence the government had actually infringed Hebern's US Patents 1,683,073 and 1,861,857. (According to their calculations, they were only liable for between $15,000 [172,000] and $60,000 [$687,000]. The amounts represented 1-4 percent of $1.5 million [$17 million] worth of navy contracts for cipher machines.)[70]

On May 19, 1953, Ellie Hebern, as executrix of her late husband's estate, and Hebern Code, Inc., filed a petition to the US Court of Claims seeking $50 million ($572 million) from the US government for infringing six of Hebern's patents. This petition added the 1924 US Patent 1,510,441 (Electric Coding Machine) to the five patents noted in Hebern's original complaint.[71]

Figure 19. Stanford C. Hooper, former DCN, n.d., *Collection of the Center for Cryptologic History*

Let's Just Settle This

On June 10, 1955, the court granted the government's motion to dismiss (figure 20) on most points because: the statute under which the plaintiffs were suing was not retroactive; US Patents 1,510,441 and 1,683,073 had expired; neither party could find evidence of the implied contract or secrecy agreement claimed in the original complaint; recovery with respect to the other patents (three of which had already been determined irrelevant to the case) were limited to between May 19, 1947, and May 19, 1953; and US Patent 1,861,857 had expired on June 7, 1949, so the only applicable timeframe was May 19, 1947, to June 7, 1949.[72]



No. 213-53

In the United States Court of Claims

ELLIE L. HEBERN, Executrix of the Estate of Edward H. Hebern, Deceased, and HEBERN CODE, INC., a Corporation, PLAINTIFFS,

v.

THE UNITED STATES OF AMERICA, DEFENDANT.

DEFENDANT'S MOTION TO DISMISS AND MEMORANDUM IN SUPPORT THEREOF

(Filed February 9, 1955)

WARREN E. BURGER,
Assistant Attorney General.
BERNARD WOHLFERT,
Attorney, Department of Justice.

Figure 20. Cover page of US government's motion to dismiss case No. 213-53 1955, *NSA Archives*

The plaintiffs now faced the reality of a severely limited case—one that depended on the government providing accurate information about the numbers and value of cipher machines it produced using concepts from the one remaining patent during a timeframe that didn't include the prewar or war years. Not surprisingly, they finally offered to settle for $48,000 ($508,000) on January 16, 1958.[73]

The government, however, wasn't finished. At the direction of NSA Director Lieutenant General John Samford, USAF, Deputy Director Howard Engstrom, and Director of Research and Development Solomon Kullback, NSA's Patent Attorney Henry B. Stauffer recommended to the US Army JAG that the government should settle the Hebern case since it was likely the navy had infringed some patents and "in view of the general doubts as to the outcome which nearly always exist in litigated cases." However, Stauffer made it clear that NSA would make "no recommendation as to an exact figure at which compromise should be attempted."[74]

Given the uncertainties of prevailing in court and the possibility that it would have to reveal cryptographic secrets at trial, the government counteroffered a settlement of $30,000 ($317,000), which the plaintiffs accepted on May 23, 1958. Judgment for the plaintiff in that amount was awarded by the court on June 4, 1958.[75]

Somewhat ironically, in 1956 a grateful Congress had awarded $100,000 ($1.1 million) to William Friedman for his contribution to SIGABA and for other cryptologic achievements. Two years later a similar sum was granted to Laurance Safford for his World War II cryptographic work, and in 1964 Frank Rowlett received his own $100,000 ($986,000) cash award.[76]

Where Credit Is Due

While Friedman and Rowlett received the lion's share of accolades for World War II cryptography, Hebern's contributions were acknowledged and appreciated—if not equivalently compensated—by the army and navy. Shortly after the navy stopped doing business with Hebern, Agnes Meyer Driscoll observed:

> While I know little of patent affairs, it seems to me that, after allowing for refinements, the Department's model [ECM Mark I] achieves substantially the same result in substantially the same way as the Hebern model.[77]

The Army Security Agency said this in its *History of the Converter M-134-C* (SIGABA):

> The history of Converter M-134-C necessitates following two important cryptographic principles through a rather intricate development. The first of these principles is encipherment by means of an electric current passing through a series of cipher wheels or rotors. The second of these principles is concerned with how these enciphering rotors step.[78]
>
> Edward H. Hebern invented the type of rotor which is used in many rapid, electrical, rotor cryptographs of the Army and Navy. Use of such rotors in cascade (or encipherment by means of electrical current going through a rotor maze) is, as has been pointed out previously, one of the two basic principles of Converter M-134-C. This principle was reduced to practical means by Edward H. Hebern. Whether anyone else independently conceived and patented the same practical means (namely, that which has become known as the Hebern-type rotor) for use of this principle is for the courts to decide. Regardless of their decision, however, it was Hebern's machine which first brought the physical embodiment of this principle to the attention of the Army and Navy in a form so practical that it has never been abandoned.[79]

In his 1943 *Naval History of Invention and Development of the Mark II ECM*, CAPT Safford summed up Hebern's story this way:

> Hebern has never received adequate recompense for his part in the development of the Electric Cipher Machine. He is the original inventor. He brought his machine to the attention of the Navy Department, built numerous models, and by his perseverance developed it to the point where it almost became a practical machine. Hebern organized three or four different companies, which went bankrupt in turn. He lived in poverty, and during much of this period was supported by his wife who ran a boarding house. Hebern was put in jail by irate stockholders and would have been much better off personally if he had not invented the ECM or had not had any dealings with the Navy Department.[80]

A Loyal American

Hebern didn't appear bitter about his treatment by the government. When asked if there had been an agreement between Hebern and the navy about keeping Hebern's inventions secret, Hooper said, "Yes, absolutely. He voluntarily didn't tell anybody, he was very loyal. He felt just like a good old sergeant, he was proud to keep this thing a secret and work for us. He spent every nickel he had in development."[81]

David Kahn wrote to Hebern in 1946 asking where he might buy or rent one of Hebern's machines. Hebern packed one up and sent it to the cryptologically curious teenager with a note:

> Any suggestion you may make for the improvement of the cipher system will be greatly appreciated. As a loyal American, my whole effort for years has been to perfect a cipher system that would give our Government the advantage over other nations in having a secure means of communications when the need is vital.[82]

Kahn devoted four pages of *The Codebreakers* to Hebern's story, but out of respect and gratitude for Ellie granting him an interview in 1963, Kahn

never mentioned that Hebern had spent time in San Quentin for stealing a horse.[83] That information, however, had been made broadly known when the prosecutor brought it up at Hebern's 1926 trial.[84]

Like Hooper and Safford, Kahn decried the government's treatment of Hebern. "His story," said Kahn, "tragic, unjust, and pathetic, does his country no honor."[85]

Edward Hugh Hebern never saw the SIGABA/ECM Mark II, nor is it likely he had a complete picture of the crucial role he played in protecting vital US communications during World War II. Some giants of modern cryptology like Meyer Driscoll and Friedman knew how important Hebern's contributions were—and now so do you.

Patrick Bomgardner is a Standby Active Reserve (SAR) employee in the Center for Cryptologic History. After a varied 41-year NSA career, he retired in September 2018 as chief of the Information Security and Classification Division.

Notes

1. Glenn Zorpette, "The Edison of Secret Codes," *Invention and Technology Magazine* 10, issue 1 (Summer 1994), https://www.inventionandtech.com/content/summer-1994-1.
2. William F. Friedman, "SCAMP V Lecture, History of the Invention and Development of Cipher Devices and Cipher Machines," 1958, 22, Document Reference ID A38378, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/lectures-speeches/FOLDER_024/42037759107657.pdf.
3. Zorpette, "The Edison of Secret Codes."
4. David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: Macmillan, 1967), 415. (See also: E. H. Hebern, Machine for Interpreting Code Messages, US Patent 1,135,452 filed March 11, 1912 and issued April 13, 1915; and E. H. Hebern and F. Hoffman, Cryptographic Attachment for Type Writing Machines, US Patent 1,123,734 filed September 6, 1912 and issued January 5, 1915, US Patent and Trademark Office website, https://ppubs.uspto.gov/pubwebapp/static/pages/ppubsbasic.html.
5. Kahn, *Codebreakers*, 415.
6. Cipher A. Deavours and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis* (Dedham, MA: Artech House, 1985), 4-5.
7. Deavours and Kruh, *Machine Cryptography*, 5.
8. Memorandum of Conference on 8 September 1952 in Office of the Judge Advocate General re: *Hebern v. United States*, NSA Archives, Accession 16886N, Document Reference ID A183468.
9. Kahn, *Codebreakers*, 415.
10. Kahn, *Codebreakers*, 416.
11. Kahn, *Codebreakers*, 417.
12. Kahn, *Codebreakers*, 417.
13. Kahn, *Codebreakers*, 417.
14. Laurance F. Safford, "History of Invention and Development of the Mark II ECM," October 30, 1943, NSA Archives, Accession 17455, Document Reference ID A2141770.
15. Safford, "History of Mark II ECM," 9.
16. Safford, "History of Mark II ECM," 12.
17. William F. Friedman, "Analysis of a Mechanico-Electrical Cryptograph, Part 1" (Washington,

DC: Government Printing Office, 1934), 1, NSA Archives, Accession 48854, Document Reference ID A2810694.
18. Safford, "History of Mark II ECM," 19.
19. Friedman, "Analysis of a Mechanico-Electrical Cryptograph," 1.
20. Friedman, "Analysis of a Mechanico-Electrical Cryptograph," 2.
21. Friedman, "Analysis of a Mechanico-Electrical Cryptograph," 2.
22. Kahn, *Codebreakers*, 418.
23. Kahn, *Codebreakers*, 419.
24. *People v. Hebern*, 84 Cal. App. 661 (Cal. Ct. App. 1927), https://casetext.com/case/people-v-hebern.
25. "History of Hebern C. M.," date unknown, NSA Archives, Accession 9952N, Document Reference ID A55287.
26. Kahn, *Codebreakers*, 419.
27. Kahn, *Codebreakers*, 419.
28. "History of Hebern C. M."
29. "History of Hebern C. M."
30. "History of Hebern C. M."
31. "History of Hebern C. M."
32. "History of Hebern C. M."
33. Safford, "History of Mark II ECM," 19.
34. Safford, "History of Mark II ECM," 11.
35. Bern Anderson, Memorandum for Head of Radio Division, "Summary of Development of Hebern Cipher Machine," August 3, 1932, NSA Archives, Accession 9952N, Document Reference ID A55277.
36. Memorandum of Conference on 8 September 1952.
37. Safford, "History of Mark II ECM," 13-14.
38. Safford, "History of Mark II ECM," 18.
39. S. C. Hooper, Memorandum to the Chief of OP-20-G, August 30, 1934, NSA Archives, Accession 9952N, Document Reference ID A55270.
40. Agnes Meyer Driscoll, Memorandum for Commander Kingman, "Observations on the History and Development of the HEBERN MACHINE," August 29, 1934, NSA Archives, Accession 9952N, Document Reference ID A55270.
41. Memorandum of Conference on 8 September 1952.
42. Safford, "History of Mark II ECM," 22.
43. "History of Converter M-134-C," Volume 1, Army Security Agency, undated, 28, Document Reference ID A533328, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_123/41768449080756.pdf.
44. "History of Converter M-134-C," Volume 1, 26-27.
45. "History of Converter M-134-C," Volume 1, 31-34.
46. "History of Converter M-134-C," Volume 1, 34, 43, 47-48.
47. "History of Converter M-134-C," Volume 1, 51-52.
48. "History of Converter M-134-C," Volume 1, 55.
49. "History of Converter M-134-C," Volume 1, 56.
50. "History of Converter M-134-C," Volume 2, Army Security Agency, undated, 7, Document Reference ID A523186, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_123/41768399080751.pdf.
51. Timothy J. Mucklow, *The SIGABA/ECM II Cipher Machine: A Beautiful Idea* (Ft. Meade, MD: Center for Cryptologic History, 2015), 7-9.
52. Safford, "History of Mark II ECM," 23.
53. Mucklow, *The SIGABA/ECM II Cipher Machine*, 10-12.
54. Safford, "History of Mark II ECM," 23.
55. "History of Converter M-134-C," Volume 2, 26.
56. "History of Converter M-134-C," Volume 2, 27.
57. Safford, "History of Mark II ECM," 21.
58. Safford, "History of Mark II ECM," 24.
59. Safford, "History of Mark II ECM," 24-25.
60. Safford, "History of Mark II ECM," 25-26.
61. Safford, "History of Mark II ECM," 26-27.
62. Safford, "History of Mark II ECM," 28-31.
63. E. H. Hebern, letter to L. F. Safford, Captain USN, "Re: Improved Hebern Cipher System Machine," March 4, 1946, NSA Archives, Accession 9952N, Document Reference ID A55208.
64. Memorandum of Conference on 8 September 1952.
65. Letter from the Law Offices of Barnard and Henry to the Secretaries of Defense, the Army, the Air Force, and the Navy, September 3, 1947, Document

Reference ID A273701, https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/patent-equipment/FOLDER_116/41763369080250.pdf.

66. Kahn, *Codebreakers*, 420.
67. Memorandum of Conference on 8 September 1952.
68. H. E. Galleher, Chief, Claims Branch, Patents Division, Judge Advocate General's Office, US Army, Memorandum for the File, Subject: Conference with Claimants Attorneys Hebern Code, Inc.–Infringement Claim, September 9, 1952, NSA Archives, Accession 16886N, Document Reference ID A183376.
69. *Hebern v. United States*, 132 F. Supp. 451, 132 Ct. Cl. 344 (Ct. Cl. 1955).
70. Memorandum Relative to Hebern Infringement Suit, Unsigned, Undated, NSA Archives, Accession 16886N, Document Reference ID A183134.
71. *Hebern v. United States*.
72. *Hebern v. United States*.
73. Letter from the Law Offices of Ernest F. Henry to Honorable George Cochran Doub, Assistant Attorney General, re: *Hebern v. United States*, NSA Archives, Accession 16886N, Document Reference ID A183601.
74. Henry B. Stauffer, NSA Patent Attorney, Memorandum (Serial: PAT-010) to the Chief, Patents Division, Judge Advocate General, Department of the Army, Subject: *Hebern v. United States*, February 28, 1958, NSA Archives, Accession 16891N, Document Reference ID A184263.
75. *Hebern v. United States*.
76. Mucklow, *The SIGABA/ECM II Cipher Machine*, 26-27.
77. Driscoll, memorandum.
78. "History of Converter M-134-C," Volume 1, 1-2.
79. "History of Converter M-134-C," Volume 1, 24.
80. Safford, "History of Mark II ECM," 12.
81. Memorandum of Conference on 8 September 1952.
82. Zorpette, "The Edison of Secret Codes."
83. Zorpette, "The Edison of Secret Codes."
84. "History of Hebern C. M."
85. Kahn, *Codebreakers,* 420.

The Risks of Taking Risks
or, What Every High School Student and NSA'er Should Know About Taking Chances

Rob Bonney

Taking a risk for thrills: bungee jumping in India, 2023. Wikimedia/Aniketrana8321

Introduction

Risk-taking is inevitable; there is no existence without risk. Yet a long happy lifetime, for a person or piece of equipment, comes in part from intelligent risk management. This article presents some consequences of taking risks that may be a little surprising and that may motivate the reader to think a little more about risks. Then an analysis of risk is offered, leading to quantitative ways to manage it.

Some Examples of Risk Taking

Consider acts that are done every day that involve risk. Examples include driving to work, flying in an airplane, or even skydiving and bungee jumping. A more compelling example to some might be real-life tests of the efficacy of birth control pills. We clearly are not willing to live riskless lives, but we seldom think quantitatively about the risks we take.

Suppose that one identically performs a particular act many times and that any individual failure causes a global and permanent failure. This is a "weakest-link" scenario—so named because the failure of any link of a chain causes the entire chain to fail. While weakest-link theory (WLT) will be applied below to analyze probabilistic failure in a fairly general way, here a simple example will suffice to concentrate attention on risk taking.

Let the probability of failure for any individual act (or test) be small: 1 out of N, where N is large (say 100 or so). Yet let there also be many tests of this act; for now, let there be N tests. What

is the global failure probability? It is easy to calculate: since not one failure can be tolerated, the global success probability is simply the N^{th} power of the individual success probability:

$$S = 1 - F = s^N = \left(\frac{N-1}{N}\right)^N \qquad (1)$$

where S and F are the global success and failure probabilities, respectively, and s is the success probability of the individual test. The value of F is easily found for any N and can be plotted versus N as shown in figure 1.

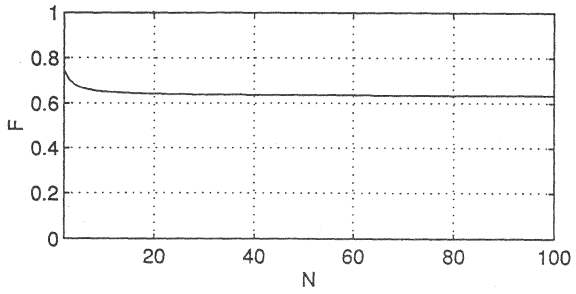


Figure 1. Failure probability for *N* trials at 1/*N* failure rate

A result that may be surprising to some is that attempting an act that has a 99 percent success rate leads to a global failure rate of 63 percent if 100 attempts are made! *Failure is more likely than success.*

The global failure rate for this particular case is not very sensitive to the value of N. For $N = 2$, for example, it is easy to calculate that the failure rate is 75 percent; as N grows large, the rate drops to about 63 percent. Left for the reader to demonstrate is the relation of this last figure (in the limit of $N \to \infty$) to the number e.

This means that success rates for possibly fatal acts (such as driving a car on I-95) must be *very* close to 1 if such acts are performed often. For the example above with $N = 100$, an individual success rate of 0.99 (2 nines) is inadequate; the more nines, the better.

Now consider how the global success rate changes if the number of trials is different from N, where N still characterizes failure probability for one trial. For example, if $N = 1{,}000$ and 100 trials are made, the global success rate is about 90 percent, and if $N = 10{,}000$ for 100 trials, the rate is 99 percent. Essentially, a factor of 10 in N for a fixed number of trials adds a 9 to the global success rate. It is easy to write relations similar to Equation 1 to extract this result, using a series expansion and the fact that (for the cases when N significantly exceeds the number of trials) global failure probability is small.

This example serves notice that understanding risk-taking is important. It can mean life or death to a person *or* to an Agency operation. The following sections present a quantitative approach to regulating risk.

A disclaimer: While some of the perspectives in this article may be novel, there is no question that the basic material, especially in the very next section, is well known to reliability engineers. The author asks their patience.

Weakest-Link Theory

We will consider the simple case where any failure is "fatal," in which case so-called weakest-link theory (WLT) applies.

Consider a situation in which global failure results from any single failure within a large number of consecutive trials. Good examples are the failure of a chain with many links of finite strength or the possibility of having a fatal auto accident during one of many trips. Start with a discrete model, which can then pass to a continuous one. Suppose many consecutive trials are made, indexed by i. The probability of failure after the i^{th} trial F_i is

$$F_i = F_{i-1} + (1 - F_i)n(\tau_i)(\tau_i - \tau_{i-1}) \qquad (2)$$

where $n(\tau_i)(\tau_i - \tau_{i-1})$ is the marginal failure probability associated with an increase of the underlying property τ from trial to trial, and $(1 - F_i)$ is the probability of success up to that point. For example, $\Delta\tau = T_i - T_{i-1}$ might represent an added length of chain or an additional time spent driving.

Transforming the discrete relation into a differential equation gives

$$\frac{dF}{d\tau} = (1 - F)n(\tau). \qquad (3)$$

This equation is solved by hauling out an ordinary differential equation (ODE) text and trying the solution

$$F = Ce^{Q(\tau)} + A \qquad (4)$$

where C, Q, and A must be determined. This is done by applying the following boundary condition:

$$F = 0 \text{ for } \tau = 0 \qquad (5)$$

$$\text{assuming } \int^0 n(\tau)\mathrm{d}_\tau = 0, \qquad (6)$$

yielding

$$F(\tau) = 1 - e^{-\int^\tau n(\lambda)\mathrm{d}\lambda}, \qquad (7)$$

where λ is a dummy variable of integration. This expression is the main result of WLT and can also be written as

$$1 - F = e^{-N(\tau)} \qquad (8)$$

where

$$N(\tau) = \int^\tau n(\lambda)\mathrm{d}\lambda \qquad (9)$$

is a cumulative risk function.

Note that neither n nor N is a probability density function (pdf) since neither integrates to unity. The quantities n and N are measures of the likelihood of encountering failure conditions as the trials progress, and it is very likely that N will grow without bound with increasing τ. The derivative of F, on the other hand, is a pdf, giving the probability that (say) a chain of length τ will fail under some specified load.

Now consider the case when global failure probability is very low: $F << 1$. Then the exponent is small and an expansion is accurate: $e^{-\varepsilon} \approx 1 - \varepsilon$, so that F can be rewritten as

$$F = \int^\tau n(\lambda)\mathrm{d}\lambda = N(\tau). \qquad (10)$$

This expression links the local and global failure probabilities in the regime where F is small, as is often the case.

Now let us consider special cases. To make the arguments easier to follow, assume that τ represents time; from here on, we will use the variable τ instead and speak of times (though we could just as well use lengths or a number of other scale variables).

Consider the case where $n(t)$ is a constant n (that is, a time shift does not matter): then the expression for F becomes

$$F = n \cdot t. \qquad (11)$$

To evaluate n, assume that F achieves some acceptably low value F_0 after some long lifetime T. Then $n = F_0/T$ and thus

$$F = \frac{F_0}{T}\, t. \qquad (12)$$

Thus F linearly approaches the acceptable lifetime value of F_0.

Now consider the failure probability associated with any small time slice Δt. Since any slice

is as good as another for constant n, we can take $t = \Delta t$ (the first slice) and write

$$F(\Delta t) = F_0 \frac{\Delta t}{T}. \quad (13)$$

This says that the failure probability within a small time slice decreases with that duration, and it is scaled by an acceptable baseline failure rate over a long lifetime.

This behavior is similar to noise behavior in circuits. Consider noise measurement using a spectrum analyzer. As resolution bandwidth is decreased, the noise level drops; measured noise depends on the measurement bandwidth. That is why equivalent noise voltages and currents are often specified in such units nV / √Hz or pA / √Hz. Here, as a resolution *time* is decreased (vice bandwidth, for noise), the incremental failure probability also drops. Just as noise is spread over bandwidth, failure probability is spread over time (or a similar scale quantity such as length of a chain). It is interesting to note that if time t is the variable of interest, n has units of Hz.

If the probability of "surviving," whatever that may mean, over a long lifetime is high, then the probability of surviving for a short interval is vastly higher. For example, if an individual has a probability of 0.9 of surviving for fifty years, that same person has a probability of 0.999995 of surviving any single day! Every factor of 10 in time reduction adds a 9 to the survival probability—so survival probabilities for very short times are very high.

It is good that we and our deployed systems are so likely to live to see tomorrow. But the better lesson is that we *must* be very reliably safe from day to day if we are to realize a long and happy life.

Conclusion

This article presents some simple notions of probabilistic failure theory to analyze the management of risk. The essential message is that failure probabilities must be *very* low over short times, if a reasonably low failure rate is to be maintained over a long lifetime. It is probable that many people who take risks do not appreciate the consequences of regularly taking seemingly small risks.

Editor's note. This article is reprinted from a 1996 *Cryptologic Quarterly* (vol. 15, no. 4).

Rob Bonney joined NSA in 1986 and was assigned to the Research organization. He then moved to an office focused on special programs in 1992 where he was a senior electronic engineer. When this article was originally published, Bonney was working as a visiting scientist at the Massachusetts Institute of Technology. He held a PhD in electrophysics from the University of Maryland, an MS in engineering science from the California Institute of Technology, and a BS in electrical engineering from Tulane University. He was a member of the Institute of Electrical and Electronics Engineers and was a National Science Foundation doctoral fellow. Bonney passed away in 2005.

Intelligence in World War II: A Scorecard

Max Hastings
The Secret War: Spies, Ciphers, and Guerrillas, 1939-1945
New York: Harper Collins, 2016, 672 pages

Review by David A. Hatch

Max Hastings, a prolific author on military topics, particularly World War II and the Korean War, has not emphasized intelligence matters in his books and has only occasionally in his military narratives discussed intelligence that resulted in action. His strength always was a clear explanation of how military operations were planned and how they unfolded in actuality.

In his 2016 book *The Secret War: Spies, Ciphers, and Guerrillas, 1939-1945*, Hastings turns his considerable narrative ability exclusively to the study of intelligence in World War II. Despite his preference for narrative rather than analysis, the book still has value for professional readers (specifically intelligence producers and consumers) but with some caveats.

One recurring problem in doing intelligence history has always been connecting the intelligence produced with the actions it provoked. For cryptologic history especially, there has been adequate but still incomplete data on how many wartime decision-makers used (or didn't!) the decrypts provided to them. For the period after World War II, however, all too often there was copious information about the production of signals intelligence (SIGINT), but precious little about what happened to it (or because of it) once it went over the transom to the decision-makers.

Hastings has taken advantage of the cottage industry of writings about World War II intelligence over the last four or five decades, including memoirs and the massive declassification of documents. His range of coverage includes all the major combatants in the war, and some minor ones, although he spends less time discussing Japan and Italy.

Hastings takes a jaundiced view of most intelligence activities in World War II, although he praises the SIGINT highly, particularly from mid-war to the end of hostilities. Despite this high regard, he takes a measured although generally positive view of ULTRA, the British-led effort to decrypt high-grade cipher systems.

He is particularly critical about the quality of intelligence activities prior to the war. Hastings frequently suggests that intelligence failures during this time resulted in poor policies under which decision-makers led their countries closer to and then into war. Many prewar leaders had no appreciation for intelligence and often ignored important intelligence information that conflicted with the policies they wanted to pursue. Even mil-

itary leaders, who might be expected to appreciate the need for intelligence as a discipline, did not support it; in fact, in many countries, including the United States, officers who aimed for high rank avoided intelligence assignments.

Per Hastings's analysis, intelligence agencies around the world, almost without exception, were inefficient and ineffective. For most, because intelligence was not honored in their government, much of the staff was mediocre and the appointed leadership more interested in gaining political favor than in "telling truth to power." Many intelligence leaders had no vision of what kind of information might be needed, so they concentrated on collecting facts. Too often, they had little skill at analysis and harvesting the meaning from these facts that might be important to their country's security and welfare.

Some countries did excel in certain aspects of intelligence collection. For example, in the USSR, the intelligence services were the best in the world in human intelligence, both traditional spying and recruiting informants in other countries. Balancing this out, however, was the fact that top intelligence chiefs feared giving Josef Stalin, the Soviet dictator, any reports containing information he did not want to read or hear.

Some countries improved dramatically because of the experience of war. This is certainly true of the United States and Great Britain, which recognized that intelligence, effectively produced and used, was a necessary tool to overcoming the great reversals that they had suffered at the beginning of the war. They also realized the key point that good intelligence production and analysis had to be developed and nurtured; nothing worth having would just fall into their laps.

The Axis nations never came to this realization, to their peril.

The book principally covers British, American, German, and Soviet intelligence, and concentrates on the war in Europe. Hastings occasionally mentions Japanese intelligence but with few details. In an early chapter, he notes that the Japanese did well in tactical collection focused on specific topics, such as gathering data about Pearl Harbor, then cites several examples of poor intelligence management later in the war. He dismisses the subject overall by saying, "The Japanese made less effective use of intelligence than any other warring power between 1942 and 1945."

Hastings writes very frankly about the individuals involved in intelligence activities. He points out their limitations and does not hesitate to name those he considers below par or to say when they caused problems rather than solved them. This includes welcome evaluations of famous figures. For example, he describes Stewart Menzies, prewar and wartime head of Britain's MI-6, as a man well out of his depth, but who had the support of the country's top leadership because he brought them the invaluable ULTRA decrypts.

In another example Hastings reappraises one of the most misunderstood figures in World War II intelligence history, Admiral Wilhelm Canaris, the German intelligence chief. Canaris in retrospect has been hailed as a natural leader in clandestine activities and praised for his anti-Nazi work behind the scenes. Hastings clearly shows that Canaris was simply a bureaucrat promoted beyond his level of competence; his quarrel was not with Nazism but with the crudities of Hitler himself and the way the Nazi dictator was changing traditional German life.

A constant theme in this book is the obvious but seldom stated fact that even in humankind's most terrible war, in which the differentiation between good and evil was particularly clear, there was no cessation of political infighting, turf battles, and egoism in favor of lockstep marching toward victory. Hastings reinforces this concept with many examples of petty behavior, ill-advised appointments, tolerance of second-rate officials

in responsible positions, and actions taken to secure and maintain a personal or bureaucratic advantage rather than self-sacrifice in the midst of total war.

This is nowhere better illustrated than in the United States at the outset of our participation in the war. President Franklin Roosevelt decided to establish a federal organization for intelligence, the Office of Strategic Services (OSS). This was opposed by the military, and when they could not prevent the rise of the OSS, they restricted its access. In addition, J. Edgar Hoover sought to ensure that the OSS did not intrude on the FBI's role in counterintelligence in the Western Hemisphere, frequently bad-mouthing the OSS and its director. Still further, Hoover struggled bureaucratically against Nelson Rockefeller, who had been appointed the Coordinator of Inter-American Affairs and was perceived as a threat to FBI dominance of action in South America.

The same kind of internecine struggles happened in most of the belligerents in the war, on both sides. In fact, many countries could have had a fairly vigorous war within their own borders, even before they confronted an external enemy.

Along the way, Hastings cites a few examples of human intelligence (HUMINT) that had a strong impact on the war, but he argues that it was mostly ineffective. Throughout the book, Hastings credits the role of SIGINT, although his discussion of production difficulties and occasional poor use of decrypts is a welcome dose of reality to the myths about ULTRA that abound in many military histories.

Hastings's narrative of SIGINT's role and effect before and during the Battle of Midway is good professional reading for intelligence personnel, but he goes on to make a rather curious judgment: "[SIGINT] contributed to some 1942-43 naval battles, but achieved maturity only in 1944-45, and even then never influenced a single action as dramatically as it had done at Midway." Well, yeah! It is hard to compare anything to the best, most effective use of intelligence in one of the most important battles in world history. (And, as Hastings himself points out, after Midway, the Japanese Navy, while dangerous in individual instances, was never again an effective threat to overall US military power in the Pacific.)

He also makes the important point that decision-makers in World War II who had access to ULTRA tended to over-rely on it. The failure to give proper weight to non-SIGINT data allowed the last German offensive, the Ardennes Campaign, to come as a surprise.

Like many of us who practice history, Hastings lets stories dominate his points and conclusions—but, fortunately, they usually are great stories. To the detriment of the book, however, Hastings uses a broad definition of *intelligence*, one that includes deception, covert operations, and paramilitary action. Thus, his narrative contains large sections about support to the resistance in Nazi-occupied Europe and irregular military operations elsewhere, particularly in the Soviet Union. Some of these details should be included in a book on intelligence, since agencies like Britain's MI-6 and the American OSS had responsibility for both information collection/analysis and for secret operations behind enemy lines.

Having said that, even though the stories Hastings shares about covert and resistance operations are fascinating (such as Soviet partisan operations and the French resistance), I feel that much of this material should have been relegated to a separate book dealing only with paramilitary operations.

Although his narrative talent often is a great asset, particularly in a book of this heft, Hastings often gets bogged down in unnecessary details and trivia. For example, he devotes a chapter to the Munchausen-esque tale of a failed British commando as told by the man himself. The man's actions, whatever they truly were, had absolutely

no effect on the war effort, and even in his own time his story was dismissed as delusional. Perhaps some might call it a morality story about an intelligence operation gone wrong; others might call it a waste of reading time.

Hastings has important points to make about the failures and successes of information warfare in World War II, and the reasons for both; these important insights should not be diluted, even for exciting or tragic stories.

Throughout, Hastings explains how intelligence was important to decisions and actions, or seeks to explain why it was not. He concludes with two factors he considers absolutely essential to making intelligence effective:

- First, a leader who understands and nurtures intelligence, and is willing to take action on it. Hastings singles out British Prime Minister Winston Churchill as the only major figure in World War II on any side that fits this description.
- Second, the power to take advantage of intelligence data. He cites many examples in the last six months of the war, when German intelligence gained good data on US operations (partly through American carelessness) but no longer had the military power to take advantage of the opportunities.

Despite unevenness of coverage and a tendency to discuss diversions at length, *The Secret War* has plenty of insights from which intelligence producers and consumers alike can benefit.

David Hatch is technical director of the Center for Cryptologic History (CCH) and is also the NSA Historian. He has worked in the CCH since 1990. From October 1988 to February 1990, he was a legislative staff officer in the NSA Legislative Affairs Office. Previously, he served as a congressional fellow. He earned a BA degree in East Asian languages and literature and an MA in East Asian studies, both from Indiana University at Bloomington, and holds a PhD in international relations from American University.

Recent releases from the Center for Cryptologic History

To request your free copy, email history@nsa.gov.