The Link

BULLETIN OF THE NATIONAL CRYPTOLOGIC MUSEUM FOUNDATION, INC.

VOLUME 5, NUMBER 1 Spring 2002

NATIONAL SECURITY AGENCY HALL OF HONOR

In ceremonies at the National Cryptologic Museum on 13 June, the Director, NSA, inducted six new honorees into the Hall of Honor, saluting their accomplishments – largely unknown to those outside the profession – and hailing their devotion to duty on behalf of the nation. Introduced with opening remarks by NCM Curator Jack E. Ingram, Lieutenant General Michael V. Hayden, USAF, Director, NSA, welcomed those assembled. With Dr. David A. Hatch, Director of NSA's Center for Cryptologic History, narrating, Gen. Hayden then proceeded to unveil the plaques. This year's honorees, all of whom served some portion of their professional lives at the National Security Agency, were cryptanalyst (and historian) CAPT Thomas H. Dyer (USN, Ret.); mathematician Dr. Richard A. Leibler; scientist-engineer-executive Mitford M. "Mit" Mathews, Jr.; missiles and space specialist Charles C. Tevis; research librarian and foreign operations manager Dr. Julia Ward; and Asian languages specialist Norman Wild. With the exception of Dr. Leibler, who was present, the other honors come posthumously, bestowed in the presence of family members and friends in the audience. (See article on pages 5 through 10)

The character and careers of the individuals in the NSA Hall of Honor represent the best in the American spirit and the finest traditions of government service. They represent excellence in American cryptology, as pioneers and as those who built upon the work of the earliest cryptologic leaders.

Many of their achievements have necessarily been veiled in secrecy, even today, but they have made major contributions to the security of the United States and its allies in the fields of signals intelligence and information assurance. A grateful NSA and a grateful nation now honor their achievements. They set high standards for us to follow. ■

IN THIS ISSUE

OVERVIEW

You may not have noticed, but this issue begins our fifth year of publishing *The Link.* Glancing back to Volume 1, No. 1, and scanning the quarterly issues that followed, it reflects our beginning and our coming of age as a membership support organization for the National Cryptologic Museum. I find one issue missing over that four-year period, and even its absence tells a story – how we were thrust into war against terrorism by the events of 11 September 2001, the postponement of our Annual General Membership Meeting, and the precautionary closure of the Museum for one quarter. Meanwhile, thanks to the efforts of several behind-the-scenes stalwarts, we had also developed an Internet presence with our site on the Worldwide Web.

As we continue to adjust to new realities on the Homeland Security front, our committee and project honchos are nevertheless brimming with new ideas and enthusiastic about prospects. With a crew like this, it's never a matter of pushing – it's a matter of trying to keep up! If you've checked our web site <http:/ www.nationalcryptologicmuseumfoundation.com. recently, you'll have seen some of those ideas displayed. (For those of you who haven't yet given in to computers and the Internet, highlights are noted in this issue of *The Link.*)

The new relationship of Russia to NATO as a non-voting associate is indicative of the watershed marking the old and the new. And equally indicative is the presence of a former Soviet KGB general, Oleg Kalugin, as a panelist at our 4 April program. "Who'd a-thunk it?" as one member said. We expect to see him again, with a former associate, in the future.

The Memorial Book has now been delivered for exhibition. You are encouraged to submit names of former associates, mentors, role-models – people deserving of special recognition. A donation of $100 per name covers the service and contributes to our treasury. Do remember to give the complete name if at all possible.

Our participation in Maryland's National History Day afforded an opportunity to make us, and the Museum, better known in educational circles. Thanks to Ann Caracrisit and Milt Zaslow for serving as State judges, and to Gene Becker and Julie Wetzel for representing us at the awarding of the prize in the category of cryptology.

John E. Morrison, Jr.
President

NATIONAL HISTORY DAY IN MARYLAND

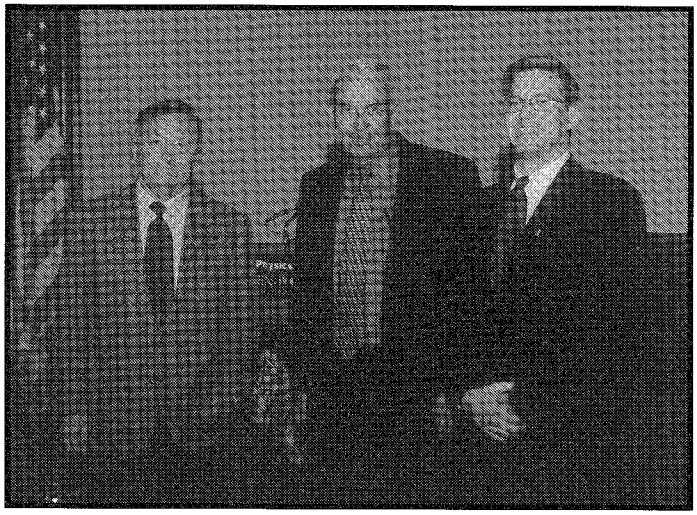
State and national testing results announced this spring reflect widespread ignorance of history among our young people. As part of an effort to correct that situation, a National History Day has been observed since 1974, with Maryland participating statewide since 1997 (although Calvert County led the way starting in 1983). More than 700,000 students are involved each year in a program that encourages research and creativity in writing, living history, exhibits, and multi-media presentations. State winners compete at the national level, held annually at the University of Maryland in College Park, Maryland. In addition to the students, teachers, advisors, and family receive recognition.

This year, acting at the recommendation of the Foundation's Program Committee (Julie Wetzel, chair), and to advance one of our objectives in cryptologic education, the NCMF

Continued on page 10

COUNTERINTELLIGENCE PROGRAM

The Foundation's rescheduled program, "Counterintelligence: A Necessary and Continuing Effort," was presented in a different venue, the Johns Hopkins University Applied Physics Laboratory



Left to Right: Oleg Kalugin, Lou Benson, John Schindler

auditorium, on 4 April 2002 from 1600-1800 hours. In form, the unclassified presentation consisted of a panel discussion, with a panel comprised of three men, Robert L. "Lou" Benson, of NSA's Office of Security, Dr. John Schindler, NSA senior staff specialist on counterintelligence, and a new-comer to NCMF events, former KGB Major General Oleg D. Kalugin. Nearly 150 were in the audience and participated in a lively and informative exchange with the panelists, followed by refreshments. The following account is by Lou Benson:

Benson introduced the program by briefly discussing problems and issues in Counterintelligence (CI) – namely, unusual sensitivity of sources and methods; privacy matters; legal aspects; and the traditional disconnect between security and CI. He then spoke about the elements and objectives of counterintelligence, giving historical examples. He emphasized that counterintelligence investigations and prosecutions are only one element of what CI is all about.

Dr. Schindler discussed the "Axis of Evil and the "'New World Disorder'." He explained the term "Counterintelligence State," a term first used to describe the Soviet Union, and which he applied to Iraq and North Korea. He described the nature of their governments and some of the major issues related to them and Iran.

Gen. Kalugin discussed his career in counterintelligence, where he served for many years in the Foreign Intelligence Chief Directorate of the KGB, eventually rising to become Chief of the Counterintelligence Directorate of that chief directorate. He talked about KGB operations to counter major terrorism within the Soviet Union in the 1940s – cases and techniques. He concluded with suggestions for strengthening U.S. counterintelligence (of which counterterrorism is a part).

JAN LEACH DEPARTS

In May, Mrs. Jan Leach, a key member of the Foundation's office staff, announced that the press of outside involvements necessitated her termination of work in the administrative support staff. In a letter of 13 May, Gen. Morrison wrote:

Your almost two years of service as a member of our front office team have been a real joy for all of us. You have made substantial contributions in many ways to the continuing success of our primary mission efforts supporting the National Cryptologic Museum. That faithful service will be long remembered with warmest gratitude.

All of us owe a debt to Jan. We join Gen. Morrison in thanking her and wishing her the very best. (We also note that he held out the prospect of calling on her for occasional help in the future.)

ROAD CONSTRUCTION

Construction has begun on the Route 32/ Canine Road "elevation" project. When completed in the fall of 2004, Route 32 will have been elevated, so that you will have to exit down from 32 to get to the Museum/NCMF office and/or NSA. But this will eliminate yet another traffic light along this heavily traveled roadway and make Museum entrance and exit safer. Effective 4 April 2002, the off-ramp from Route 295 North (Baltimore-Washington Parkway) to the Canine Road/Route 32 intersection was closed and will remain so until project completion.

There are several detour route options *from the DC area*: 1) I 95 North toward Baltimore, Exit 38-A, take Route 32 East, toward Ft. Meade, Left onto Colony 7 Road, the entrance to the Museum. 2) 295 North (Parkway) toward Baltimore, exit onto *east*bound Route 198 to Route 32 *west*bound, right onto Colony 7 Road. 3) 295 North toward Baltimore, Exit onto *west*bound Route 32, then take the ramp to *south*bound Route 295, immediately exit onto *east*bound Route 32, left onto Colony 7 Road, (This one might be the quickest, but it could make you dizzy!)

A REMINDER ON VISITING

Don't forget your NCMF membership card when visiting the Museum – it's good for a ten per cent discount on gift shop purchases. But shop employees do not have access to our membership records, so you can't just claim that you're a member. Show them your card, and all will be well. The Museum will re-open on alternate Saturdays. To be on the safe side, give them a call at (301) 688-5849 before setting out.

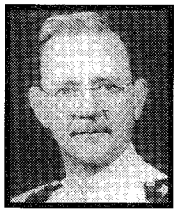
DEATH OF VIET-NAM WAR HISTORIAN

Douglas Pike passed away on 13 May 2002 at a hospital in Lubbock, Texas, following an earlier stroke. He was 77. Historian, archivist, university professor and retired Foreign Service officer Pike was a leading expert on the Viet Cong and the war in Viet-Nam. He had served in the U.S. Army Signal Corps in the Pacific during WW II. In 1960 he entered the Foreign Service and was posted to Saigon. There he began to compile what accumulated to some 7 million pages of documentation – 15,000 books, 15,000 monographs, including an unsurpassed collection of North Vietnamese documents. In 1982, he commenced publication of the quarterly, *Indochina Chronology*. He moved his collection to the Vietnam Center at Texas Tech University in 1997 and became a professor under Center director, Dr. James R. Reckner. Considered by many the successor to the late Dr. Bernard Fall as the Western expert on Viet-Nam, Professor Pike's removal from the scene weakens our ability to collate future declassified material. According to an announcement by Dr. Reckner, "It is difficult to imagine the field of Vietnam studies without Professor Douglas Pike, however, our understanding of a great many important and complex events has been greatly enhanced by his tireless efforts, his intellectual curiosity, and his unsparing integrity." There are at present no plans to resume his *Indochina Chronology*. ■

Part 2 of the text of the Enigma Bombe article by Jennifer E. Wilcox, NCM assistant curator, commencing on Page 11, continues from the previous issue. Copies of the pamphlet are available, free, at the museum.

HALL OF HONOR, 2002

Continued from page 1



Thomas H. Dyer

As the lead cryptanalyst at Station HYPO in Hawaii from 1936 to 1945, Thomas H. "Tommie" Dyer led the team that was responsible for most of the breakthroughs in reading Japanese naval communications during the war in the Pacific. After the war, he continued a brilliant career and went on to be one of the three primary cryptanalytic trainers, along with William Friedman and Lambros Callimahos, for both AFSA and NSA.

Born in Osawatomie, Kansas, in May 1902, Thomas Dyer graduated from the naval Academy in 1924. After serving tours as a radio or communications officer, he was assigned to the Department of Naval Communications' cryptanalytic organization, OP-20-G, in May 1931. There he trained under Agnes Driscoll and developed procedures for using IBM tabulators to ease the burden of sorting through the myriad possible solutions for breaking codes and ciphers. This earned him the accolade "the father of machine cyptanlysis."

In July 1936 Dyer transferred to the 14th Naval District's Fleet Radio Unit in Hawaii, soon to be called Station HYPO. During the next nine years, his accomplishments were extraordinary. In 1938, he branched out from HYPO to form the Communications Intelligence Unit in Pear Harbor, with both intercept and direction-finding stations at Heiia and Wahiawa. In early 1941, when Commander Joseph Rochefort became the officer-in-charge (OIC) of Station HYPO, Dyer remained as assistant OIC and chief cryptanalyst. Under Dyer's supervision, HYPO began contributing essential elements of information derived from the JN-25 code to Admiral Nimitz before the Battle of the Coral Sea. By 27 May 1942, HYPO had developed such a detailed picture of the Japanese plan for the occupation of Midway that Nimitz's intelligence officer was able to predict almost precisely when and where the enemy would strike. Dyer was also directly involved with the interception, decryption and subsequent intelligence information reporting which led to the shootdown and death of Fleet Admiral Isoroku Yamamoto. Dyer's work also resulted in the breaking of the Japanese merchant shipping and transport code and the main Japanese weather code.

From February 1946 to June 1949, Dyer was assigned to the Naval Security Station, Communications Support Activity in Washington, DC (precursor to the Naval Security Group) as chief of processing and technical director. In 1947 he was designated as one of the first Navy Special Duty Officers (Cryptology). Dyer was a leading member of the Navy contingent that joined the fledgling Armed Forces Security Agency (AFSA) in June 1949 and, along with Captain Laurance Safford, was in charge of all daily AFSA operations.

Later, at NSA, he established the Agency's first academic training program (college and NCS courses) for Agency employees. From October 1952 to January 1954, he was chief, NSA Far East, Tokyo. He returned to NSA Washington in February 1954 to become its first historian and remained there until his retirement from the Navy in February 1955.

Captain Dyer passed away in 1985.

Dr. Richard Leibler

Dr. Richard Leibler's contributions to mathematical practice and theory were crucial

Continued on page 6

HALL OF HONOR, 2002

Continued from page 5

to America's national security. His technical knowledge and managerial abilities helped transform an NSA-related "think tank" into an institution that kept NSA in the forefront of mathematical and cryptologic capability in the 1960s and 1970s.

Richard Leibler was born on 18 March 1914. He received his B.S. and M.A. in mathematics from Northwestern University and his Ph.D. from the University of Illinois in 1939. After a short stint in teaching, he entered the Navy in World War II – as an aviation ordnance officer, he saw action on carriers in the Iwo Jima and Okinawa invasions. After the war, he worked for the Department of the Navy and in private industry, and he spent two years at the Institute for Advanced Study at Princeton University.

Dr. Leibler came to NSA in 1953, with assignment to the Research and Development Organization. In the early years, he joined pioneer computer scientists in developing programs and practical applications for newly developed computers. Some of his theoretical work enabled NSA cryptolinguists to solve previously unexploitable Soviet espionage messages in the project codenamed VENONA. Working together, Dr. Soloman Kullback and Dr. Leibler devised a new method of measuring similarity between populations; this statistical function bears their names and is still widely used.

In 1957 Dr. Leibler became chief of the Mathematical Research Division in R&D.

In 1958 Dr. Leibler was appointed Deputy Director of the Communications Research Division (CRD) of the Institute for Defense Analysis at Princeton and became CRD's director in 1952.

CRD had been founded as an NSA-related "think tank" for mathematics and cryptology as the result of a presidential study, but initially it was given little to do by NSA.

Dr. Leibler, using knowledge and contacts gained during his years in R&D, successfully lobbied NSA for important research projects to be sent to CRD. Under his guidance, CRD successfully solved "real world" questions, and it took on the challenge of theoretical exercises in advanced mathematical problems.

The practical and theoretical work done under his direction at CRD was a crucial factor in maintaining mathematical and cryptologic excellence at NSA for at least the following two decades.

Dr. Leibler returned to NSA in 1977 to head the Office of Research in the Research and Engineering Organization, and he retired in 1980. The Exceptional Civilian Service Award presented at his retirement noted that his accomplishments were of the "highest order" and "profoundly influenced" cryptologic research for three decades.

Mitford M. Mathews, Jr.

In May 1966, Mitford M. Mathews was awarded the Department of Defense Distinguished Civilian Award, the highest honor that can be awarded a civilian employee by the Department of Defense. The award citation read, "Throughout his entire career Mr. Mathews . . . demonstrated a distinct professionalism and unique capability that had far-reaching effects." The citation succinctly summarizes the brilliant twenty-three-year cryptologic career of a man who served in many vital positions and was well known for his achievement and dedication.

Continued on page 7

HALL OF HONOR, 2002

Continued from page 6

"Mit" Mathews was born on 16 March 1922 in Alabama. He received a bachelor's degree with honors in mathematics from the University of Illinois in 1943. Upon graduation, he was commissioned in the U.S. Army, where he was assigned to the Research and Development Division from 1944 to 1946. His far-reaching engineering and scientific contributions won him the Legion of Merit.

Upon his release from the military, Mathews joined the U.S. Army Security Agency as a civilian engineer, making the transition to AFSA and NSA. He held a series of management positions in the R&D organizations, including chief of COMSEC R&D. From 1962 until his death in 1971, Mr. Mathews was assistant director for research and development (R&D).

According to his peers, Mathews turned NSA's R&D group into a premier technological organization with his management acumen and technical leadership skills. He was an active participant in all phases of research and engineering at the Agency and made major contributions within the cryptologic community in both signals intelligence and communications security. He was a "hands-on executive" whose technical advice on topics related to communications and computer science was sought by his subordinates, peers, and superiors within the intelligence community, as well as in academia and private industry. Mathews led the transition from World War II era rotor-based equipment to high-tech electronic devices and ciphony equipment. His efforts transformed the fundamental processing of radar signals from analog to digital. Extremely gifted at translating technical jargon to standard English, he was frequently sent to testify before congressional committees on both cryptanalysis and information assurance.

In 1967, he received the Exceptional Civilian Service Award, NSA's highest civilian award.

Mathews died on 19 January 1971.

Charles C. Tevis

In his thirty-two years of cryptologic service, Charles Tevis was at the forefront of advanced SIGINT activities. He specialized in collection systems and was one of the principals involved in the establishment and organization of the SIGINT Missile and Astronautics Center (SMAC) and its successor, the Defense Special Missile and Astronautics Center (DEFSMAC). His belief in the potential importance of electronic intelligence (ELINT) led to the full development of ELINT collection and processing techniques.

Mr. Tevis was born in 1921. After graduating from the College of Wooster, Mr. Tevis served in the United States Army, and he was selected for the Army's experimental program to teach students to read Japanese in thirteen weeks. After successfully completing the program, he joined the Signal Intelligence Service and was stationed at Arlington Hall Station, where he analyzed Japanese military communications.

Mr. Tevis remained in the SIGINT field following World War II. His early work included analysis of foreign technical communications. He was one of several analysts who collaborated in establishing a new reporting mechanism to provide warning of special events of high interest, which later became the basis for the establishment of SMAC. Mr. Tevis also displayed a high degree of linguistic and traffic analytic innovation in exploiting entities previously

Continued on page 8

HALL OF HONOR, 2002

Continued from page 7

considered worthless. In 1957 Mr. Tevis was awarded a fellowship to the Harvard Business School.

After helping to develop the SMAC, Mr. Tevis became a member of a select Department of Defense committee that studied the intelligence community's efforts against technical collection problems. The committee's recommendations led to the establishment of the DEFSMAC, and Mr. Tevis was appointed its first director by the Secretary of Defense in 1964.

After his success with DEFSMAC, Mr. Tevis originated the concept of a specialized collection management center, which was considered years ahead of its time. His concept later came to fruition as the Special Systems Support Center (SSSC). Mr. Tevis also served as chief of the Director's Advisory Group for ELINT and Reconnaissance (DAGER), and later as a group chief in the SIGINT Organization.

He was a member of the NSA Scientific Advisory Board (NSASAB) for eighteen years, serving on an ELINT Strategy Panel. It was largely due to his contributions and influence that the intelligence community produced detailed information about foreign high-tech weapons, which enabled the United States to devise means to counter them.

During his long career, Mr. Tevis was awarded the United States Intelligence Medal of Achievement and the NSA Exceptional Civilian Service Award. Mr. Tevis was admired and respected by all that knew him and was a mentor to many, according to former Deputy Director NSA, William Crowell. Former Secretary of Defense Dr. William Perry said of Mr. Tevis, "His brilliant mind, his insatiable curiosity and his unflagging energy led to many of the greatest intelligence achievements of [Cold War intelligence]." A relocated, modernized DEFSMAC, The Charles C. Tevis Operations Center, was dedicated in Mr. Tevis's memory in a 1998 ceremony.

After his retirement, Mr. Tevis continued to support SIGINT operations as a consultant with Ford Aerospace and TRW. Mr. Tevis died on 12 September 1994.

Dr. Julia Ward

As the founder of Central Reference, Dr. Julia Ward significantly affected the future of a key function across a wide variety of targets and problems. Her pioneering efforts to build a library of classified and unclassified resources to aid analysis greatly advanced the American cryptologic effort.

Dr. Ward was born in December 1900. She attended Bryn Mawr College, earning an Associate Bachelor's degree in 1923 and a Ph.D. in 1940. She was employed by Bryn Mawr from 1923 until she joined the cryptologic service during World War II. She held a variety of positions of increasing responsibility, culminating in Bryn Mawr's Director of Admissions and Dean of Freshmen.

During World War II, Ward joined the Signal Security Agency, the Army's cryptologic organization, and worked as a librarian in the reference section, building a collection of classified and unclassified end-product and collateral materials for use by the various analysts. By the end of World War II, she was deputy chief of this very large organization.

In October 1945 she became chief of the reference section. When Ward inherited this

Continued on page 9

HALL OF HONOR, 2002

Continued from page 8

unit, it was poorly organized, limited in scope, and focused solely on supplying collateral sources to existing customers performing analysis against established targets. Under her leadership, the section was reorganized to be responsive to the needs of new customers on new targets. Ward believed the section should be able to anticipate some of its customers' needs and to be proactive in gathering and organizing these data. Within a few years, Ward turned the reference section into a highly respected organization to which other federal agencies came for collateral information. In 1949, with the birth of the Armed Forces Security Agency, Ward was named head of the Collateral Branch, becoming the only female branch chief in the Office of Operations. She held this position through the earliest days of NSA.

While in Central Reference, Dr. Ward monitored NSA reporting to ensure Agency product maintained the highest standards of accuracy. Her vast knowledge of cryptologic targets all over the world allowed her to catch many mistakes that would have otherwise been overlooked.

About 1955, Dr. Ward, in a new direction, became deputy chief of NSA's Liaison and Foreign Operations Section. After so many years in reference, some were surprised by the change. However, she was as successful in this organization as she had been in the reference section; she was promoted to section chief by 1958 and deputy division chief by 1961.

Dr. Ward died on 18 June 1962, shortly before retirement. Her obituary in the NSA Newsletter described her as "one of the outstanding women employees of NSA, having completed many highly significant projects in the accomplishment of the agency's mission."

Norman Wild

Norman Wild was an expert in Cambodian, Chinese, Japanese, Korean, Lao, Thai, and Vietnamese. Colleagues remember not only his professional prowess but also his gentle and generous encouragement to them in their language work. He was of that rare breed: a genius who could also teach people.

Mr. Wild was born in June 1918 and grew up in New York City. In high school, he discovered that he liked to study languages and took all of the French and Spanish classes that were available. He majored in Chinese and Japanese studies at Columbia University. Wild earned both his B.A. and M.A. degrees in Chinese and Japanese from Columbia University in 1939 and 1941, respectively.

Wild joined the army in 1944 and was recruited by the Signal Security Agency (later the Army Security Agency (ASA)). After language training, he was stationed at Arlington Hall. At first, supervisors were perplexed at Wild's behavior. He was able to complete his weekly language tasks in one day. For the remained of the week, Wild assisted his colleagues with their analytic tasks. He remained a natural mentor and teacher throughout his career. After a two-year stint in the army, Wild became a civilian employee at ASA, and stayed with the organization as it evolved into the Armed Forces Security Agency and finally NSA.

Norman Wild has been described by his colleagues and by Agency seniors as "a book breaker with intuitive genius"; "an individual who was most helpful to colleagues as they transitioned to working with new languages to meet the changing needs of the agency"; and "the most competent and impressive linguist

Continued on page 10

HALL OF HONOR, 2002

Continued from page 9

ever." The following two examples justify these accolades.

Early in the Korean War, while working in a special analysis unit, Wild and two colleagues studied Chinese plaintext messages over a period of months. This team concluded that a series of messages that seemed innocuous actually suggested that Chinese troops were being centralized and prepared to enter the Korean War. Wild was lauded as a linchpin for this analytic discovery. The Chinese did enter the Korean War on 25 November 1950.

Mr. Wild's most significant and lasting achievement was his work with the Chinese-English Translation (CETA) Group's Chinese-English General Dictionary project. CETA was an ambitious project. A number of U.S. government agencies, private enterprises, and academic institutions collaborated over several decades to produce perhaps the most comprehensive and up-to-date Chinese-English dictionary ever published. Linguists had to collate an enormous general and technical vocabulary from numerous sources into a single resource. Wild played a pivotal role in selecting, translating, editing, and correcting thousand of vocabulary entries for inclusion in the dictionary. He was personally responsible for no less than a fourth of the approximately 212,000 entries! Today, this dictionary continues to be the single most widely used Chinese-English resource by the intelligence community.

In 1970 the Agency recognized Wild's achievements by presenting him its highest honor, the Exceptional Civilian Service Award. After thirty-six years of government service, Norman Wild retired in 1980. His spectacular achievements continued to influence and inspire the language community. He died in 1996.

NATIONAL HISTORY DAY IN MARYLAND

Continued from page 2

became a supporter, suggesting research topics in cryptology, and offering a special prize ($100 and a plaque) for winners. Foundation officials Ann Caracristi and Milt Zaslow volunteered to serve as judges.

Some 10,000 Maryland middle and high school students (representing public, private, and parochial schools statewide) and 200 teachers are involved in this year-long program, conducted since 1999 under the umbrella of the Maryland Humanities Council. Two Junior Group papers emerged from regional competitions this year – John Jung of Ellicott Mills Middle School, Howard County (Toni Richardson, Teacher) had selected the subject, *Did the Navaho Code Talkers Alter the Outcome of World War II?* and Ashleigh Chambers, St. Peter's School, Charles County (Kathleen Cooke, Teacher) produced *Solving the Enigma: British and American Codebreakers Cripple Axis War Efforts in World War II.* A Junior Group Exhibit, *The Secrets Within Quilts,* was offered by Sharonda Land and Tiara Williams, Chinquapin Middle School. Baltimore City (Chanta Booker, Teacher). There were no entries in our field of interest at the Senior Level.

Ashleigh Chambers' *Solving the Enigma* was adjudged winner and received the Foundation's prize in an awards ceremony at the University of Baltimore on 27 April. Presentation on behalf of the NCMF was by Gene Becker and Julie Wetzel. We are encouraged by this new initiative and plan to expand on the experience for the next year.

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE

Jennifer E. Wilcox

PART 2

Britain Builds the Bombe

Britain, like Poland, began hiring mathematicians to work in their Government Code and Cipher School (GC&CS). Alan Turing and Gordon Welchman, both mathematicians from Cambridge University, joined the GC&CS at the outbreak of hostilities with Germany. In early September 1939, the mathematicians reported to the new home of GC&CS, a Victorian manor in Bletchley, England, known as Bletchley Park (BP). They received a briefing on the work of the Polish Cipher Bureau and the Polish mathematicians. Turing and Welchman individually began thinking of ways to more quickly solve the German Enigma messages. They would both play a crucial role in the development of the cryptanalytic machine.

Alan Turing
(Courtesy of King's College Library, Cambridge, UK)

Alan Turing realized that the solution did not lie in creating a machine that replicated sixty Enigmas. The Polish Bomba searched for matches in indicators. Once already the Germans had changed how indicators were used, throwing the Poles back into the darkness until new Zygalski sheets could be cut. The Germans could easily change the indicators again. Turing began thinking about a machine that worked, not with the indicators, but with assumed text. By using text that cryptanalysts assumed appeared in the message, the machine would not be dependent on the indicators.

Like the Polish Bomba, the machine Turing conceived would also run through all the possible settings. Rotors and wires would simulate a series of Enigma rotors and pass an electrical current from one rotor to the next. However, rather than looking for the one correct rotor setting abased on the indicators, as the Bomba did, Turings' would look for all the rotor settings that allowed the cipher to match the assumed plain text. Or, more correctly, it searched all the settings and disregarded those that were incorrect. For example, if the assumed letter was "G" and the corresponding cipher letter was "L," Turing's test register ignored any results that did not allow the electrical current to pass from "G" to "L." By disproving thousands of rotor settings, those left were possible correct settings.

While Turing developed plans for his cryptanalytic machine, Gordon Welchman also thought about the Enigma problem. Though GC&CS assigned him to work in traffic analysis, a field that involves the externals of a message and not the message itself,[5] he contemplated ways to break Enigma messages more easily. On his own, he reinvented the series of perforated sheets that Henryk Zygalski had developed for the Poles. Poland had turned this achievement over to Britain at the same time as the Bomba, and BP was already creating new sheets for five rotors.[6]

Undeterred, Welchman began working on another complication on the Enigma, the plugboard. Because the plugboard uses a cable to connect one letter to another, it automatically connects the second letter back with the first. If A is plugged into E, E is plugged into A. Knowing this, Welchman designed a board that connected each letter with every other letter. The wires created a pattern of diagonal lines. He created a "diagonal board."

Gordon Welchman showed his design to Alan Turing, who agreed it would greatly enhance his machine. Although simple in design, combined with Turing's test registers, the number of possible rotor settings decreased from thousands to only a few. Analysts could easily test these few solutions on an Enigma duplicate or analog.

Turing and Welchman took the design to Harold "Doc" Keen, an engineer at British

Continued on page 12

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE

PART 2

Continued from page 11

Tabulating Machines (BTM), who was in charge of actually building the machines the mathematicians conceived. Work had already begun on Turing's machine, but upon seeing Welchman's diagonal board and realizing its implications, Doc re-engineered the cryptanalytic machine. Turning the mathematicians' conceptions into working machines took extensive engineering experience. Fortunately, "Doc" was able to combine both men's thoughts into an integrated, workable machine.

Harold "Doc" Keen Engineer at BTM of British Bombe
(Courtesy: John Keen (son) and John Harper, British Bombe Rebuild Project Manager, Bletchley Trust)

It took months to design and build the cryptanalytic machines. It wasn't until August 1940 that the first operational machines arrived at Bletchley park. Initially, each Bombe took six weeks to construct, but later BTM completed one Bombe each week. The completely redesigned Polish machine also received a slight name change from the Polish "Bomba" to the French spelling, Bombe.[7]

The British manufacturing company BTM built most of the approximately 210 Bombes used in England throughout the war. Although the machines changed and improved during the five years of production, the basic Bombes weighed one ton and stood six and a half feet high, seven feet long, and two feet wide. Each of the basic machines had thirty-six sets of three rotors. Within each set, the top drum represented the leftmost, or slowest, rotor on the German Enigma; the middle corresponded to the German's center rotor; and the bottom Bombe drum represented the Enigma's rightmost, or fastest, rotor.

The British Bombes worked through rotor settings in the opposite direction of the Enigma. Since the Bombe needed to try every combination of rotor settings, it didn't matter from which direction this was accomplished. Even though it represented the slowest moving Enigma rotor, the top Bombe drum spun the fastest at 50.4 rpm.[8] In the instant that each position made contact, an electrical current tried to complete a path through each of the test registers and the diagonal board. Most could not complete the path correctly and were discarded. Those that did complete the path caused the machines to stop.

Members of the Women's Royal Naval Service, Wrens, operated the machines, and when the machine found a "stop" the operator wrote down the rotor settings. She then reactivated the Bombe enabling it to search for any other possible solutions within that wheel order. Another Wren tested the stop on a checking machine and passed the result to a cryptanalyst in another building. When the cryptanalysts found the one correct setting, they notified the Wrens to stop work on that message and move on to the next. It took ten minutes for the Wrens to change the wheel order for the next run and an additional thirty-five to fifty minutes to set up the connections and rotor positions.[9]

By the time the British Bombes arrived at Bletchley Park, cryptanalysts had already made breaks into the German Air Force and Army Enigma systems, allowing the Bombes to routinely find the message's settings. The German Navy Enigma was much more difficult to read. The German Air Force and, to a lesser degree, the German Army, were so sure of the imbedded security of the Enigma itself that they were lax in their communication security measures. The German Navy, however, complicated their system with strict enforcement of communication security practices and the addition of three more rotors to the collection. The Navy now had eight rotors from which to select the three used in the Enigma each day. Without knowing the wiring of the Navy's additional rotors, Britain could read very few German naval messages.

Because the Polish cryptanalysts had briefly

Continued on page 13

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE
PART 2

Continued from page 12

been in occupied France, the British considered them suspect. Therefore, GC&CS did not turn to Marian Rejewski for help concerning the new rotors' wiring. The equation he developed in the 1930s could have retrieved the wiring as it had the originals. But without his assistance, Bletchley Park could have made no significant breaks into their enemy's secret naval messages. Due in part to the Allies' lack of knowledge of German naval intentions, the *Kriegsmarine* submarines ruled the Atlantic shipping lanes.

Britain depended heavily on U.S. supplies crossing the Atlantic. Although the U.S. claimed neutrality, it sold material and supplies to Britain and provided escorts for their convoys. Germany planned to destroy this supply line and cripple Great Britain. Their most destructive weapons in the Battle of the Atlantic were the German submarines, known as U-boats. For twenty-one months, as the cryptanalysts at Bletchley Park desperately tried to make breaks into the naval Enigma messages, the U-boat wolf packs decimated Allied shipping convoys.

Admiral Doenitz, commander of the U-boat fleet, operated his submarines in a coordinated strategic plan. The U-boats patrolled the ocean in search of their prey. Once they spotted a convoy, the subs alerted their forces by way of Enigma-enciphered radio messages. Other U-boats were sent to assist in the assault. Like a pack of wolves, the U-boats attacked the supply ships sending many of them to the bottom of the ocean. Had Bletchley Park been able to read the messages sent to and from the U-boats, they could have alerted the convoys. But without prior knowledge of the attacks, the ships were all but helpless. A German victory in the Atlantic loomed over the Allies before Britain finally got the break it needed.

The inability to read the Navy Enigma messages finally ended in May 1941 when Britain captured the German submarine U-110 with its encryption equipment intact. U-boat commander Fritz-Julius Lemp, fearing that the sub was sinking rapidly and that it was about to be rammed, ordered his crew to abandon ship. The radioroom crew, believing they were in great peril of drowning and obeying the order to abandon, did not destroy the Enigma or codebooks before donning their life vests and jumping overboard.

With the German submarine crew treading water in the cold Atlantic, the British ship *Bulldog* sent a boarding party to the U-110. They found a treasure trove of secrets. The boarding party collected all books, charts, logs, and other important documents and equipment. Among the captured material were codebooks, instructions, and key lists for several different German Navy and submarine codes. It also included an Enigma machine with the daily settings in place and each of the eight rotors.

Representatives arriving from Bletchley were astonished at the find. They photographed the most important documents and boxed everything up for shipment to BP. Within days BP would be reading the German Navy messages again.

Britain had at last acquired the missing rotors. With the rotors and the keys through June, Bletchley didn't even need the Bombes in order to read the messages. But those two months would pass quickly, and the Bombes needed to be ready when the keys ran out. BP began wiring drums for the Bombes to match the wiring of the three new rotors.

Fortunately, Admiral Doenitz did not realize that the U-110's Enigma rotors and other vital communications information were now in the hands of the Allies. Had he known, he certainly would have changed the system. The U-110 was boarded in sight of some of the survivors, so Britain went to great lengths to convince them that the submarine sank before it could be boarded. Word got back to Admiral Doenitz that the code was safe.

From June 1941 through the summer, BP read the U-boats' *Heimisch* or home waters coded messages at the same time as the Germans themselves. Admiral Doenitz used the

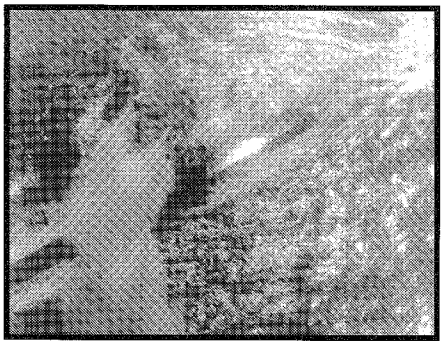
Continued on page 14

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE
PART 2

Continued from page 13

home waters code to command his forces. With foreknowledge of a U-boat's location, the Allies could take steps to avoid the wolf packs or send bombers for an Allied attack.

Admiral Doenitz noticed this change in his submarine forces' ability to sink the supply convoys. Before the spring of 1941, German attacks sank a majority of Allied shipping tonnage. Then, almost suddenly, it was the attacker who became the prey. Despite the assurances he received concerning the U-110, Admiral Doenitz suspected the Allies could read his fleet's Enigma messages. When he asked German High Command of this possibility, they assured him that the Enigma could not be broken. They proposed other reasons as to why his U-boats were less effective, including Allied direction finding capabilities (called Huff Duff by the British), aerial reconnaissance, or even a German traitor. In truth, even when the Navy Enigma messages could not be read, British direction finding combined with traffic analysis did have substantial successes.



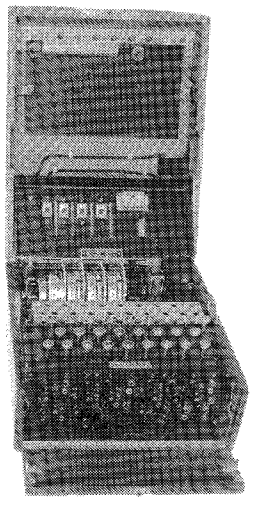
German U-boat U-117 under attack by U.S. aircraft in the central Atlantic, 7 August 1943. the boat was eventually sunk.

Certainly the Germans' faith in the Enigma was not unfounded because of the astronomical mathematical possibilities. However, to encourage this unquestioned confidence, Britain went to great lengths to disguise how Enigma information, known as Ultra, had been obtained. The British took no action based on Ultra without first providing the Germans with a deceptive reason for the actions taken. Most commonly, British aircraft flew a reconnaissance mission over an area that Ultra had shown to be significant. When the Allies subsequently attacked that area, the Germans believed their forces had been spotted by the aircraft, not given away by Enigma.

Admiral Doenitz, however, was not satisfied. He intended to change the U-boat Enigma machines. He could not radically alter the machine itself as it had to continue to work with the rest of the German Navy. His change added a thin fourth rotor between the leftmost rotor and the reflecting plate. When necessary, the rotor could be set in a straight-through position, enabling it to act as a three-rotor machine.

Bletchley Park learned of the impending change from decrypts and captured material, but until it was actually implemented there was little they could do to prepare. Fortunately, the Germans made an error. In December 1941, before the change had been made official, a U-boat sent a message using the four-rotor machine. To compound the mistake, the same message was retransmitted using only three rotors. From this seemingly innocuous error, the cryptanalysts at BP determined the wiring of the fourth rotor.

In February 1942 Admiral Doenitz officially changed the Enigma machines on his U-boats. Despite recovering the wiring to the fourth rotor, Bletchley Park had a lot of work ahead of them. In addition to changing the machine, the *Kriegsmarine* also instituted a new code, which Britain referred to as "Shark." BP now had two obstacles: break Shark and redesign the Bombe. The cryptanalytic Bombe developed by Alan Turing, Gordon Welchman, and "Doc" Keen found the rotor settings for a three-rotor machine. It could not find the settings for four rotors. Once again German submarine messages were indecipherable. Admiral Doenitz' U-boats began again to successfully prowl the waters of the Atlantic.



Four-rotor Enigma

SOLVING THE ENIGMA: HISTORY OF THE CRYPTANALYTIC BOMBE

PART 2 FOOTNOTES

Starting on page 11

⑤- Traffic analysts look at information outside of the actual message text such as the unenciphered headers prior to the message, time of transmission, and the frequency used. With this type of information, traffic analysts can reconstruct an enemy's communication network and hierarchy.

⑥- Britain called their sheets "Jeffreys sheets" after John Jeffrey, who was in charge of manufacturing the stacks of perforated papers.

⑦- Some people, not knowing the Bombe's Polish history, suggested that the name for the British Bombe came from the sound the machines made as they ticked their way through the possible rotor settings, like an old time-bomb ticking. However, Gordon Welchman, in his book *The Hut Six Story* (McGraw-Hill, 1982, 77), says, "Our bombes [the British versions] were said to make a noise like a battery of knitting needles." U.S. Navy Wave Veronica Mackey Hulick, who operated the American cryptanalytic Bombes, agreed that "the noise from the Bombe was like thousands of clacking knitting needles." However, CDR McDonald, a Bombe watch officer, doesn't recall a clicking sound, but remembers it made a lot of loud noise.

⑧- Because there were several different models used throughout the war, the speed of the machine varied depending on the model. This speed (50.4 rpm) refers to the British 39-point machine. (Correspondence to the author from John Harper, Bombe Rebuild Project Manager, Bletchley Park Trust. 12 February 2000.)

⑨- Leo Rosen and William Friedman, "Cryptanalysis of German Army & German Air Force ENIGMA Traffic" SSA (report on) "E" Operations of the GCCS at Bletchley Park, 1945, 59. (NARA Record Group 457; File #3620.)

FOR THE BOOKSHELF

A sudden surge in relevant books causes us to pause and want to send up a red flare for help in review and recommendation. They seem to fall into the following categories – VENONA, Enigma, Bletchley Park, and Varied. A casual glance at the shelves of Border's showed that *Codebreakers: The Inside Story of Bletchley Park*, by the late Sir Harry Hinsley and Alan Stripp (two names that bespeak authority), published in 1993 and, in paperback, 1994 is available in a 2001 paperback reissue from Oxford University Press. It comprises some thirty essays by – for the most part – people who "were there." The quality of writing and the contents are excellent, deserving of a place on your shelf. (But, in all fairness to those with limited budgets, we should take note of *Action This Day*, a 543-page tome edited by Ralph Erskine and Michael Smith. NCMF member Lou Kruh, reviewing this 2001 publication in the April 2002 issue of Cryptologia, calls it "absolutely the best book ever written about codebreaking at Bletchley Park (BP).")

While the newly released movie, *Windtalkers*, was a bit of a disappointment according to some who have seen it, a more serious, technically detailed account may be found in Sally McClain's 1994 *Navajo Weapon: The Navaho Code Talkers*, re-issued in 2001 by Rio Nuevo Publishers of Tucson, Arizona. Ms. McClain (a "Navy brat") never loses her respect for the accomplishment of these Navaho Marines. Her research brought her to the Center for Cryptologic History and the NCM, where she was pleased to see her appreciation of the Navaho echoed in exhibits and attitudes.

Finally, an English translation of Rudolf Kippenhahn's 1999 *Verschlüsselte Botschaften* is available in an Overlook Press (Woodstock, NY) paperback of 2000 under the English title, *Code Breaking: A History and Exploration.* (One can almost hear Elizebeth Friedman saying, "Cipher, my dear, not code.") Quibbles aside, the text deals mainly with ciphers, although "code breaking" is treated, mainly in the case of the Zimmermann telegram and the *Magdeburg* German naval codebook of 1914. Clear, concise writing makes this a pleasure to read. It is as up-to-date as PGP and privacy concerns, the use of PCs and the Internet; it would serve as an excellent introduction for a student in high school "on up." ■

Join the National Cryptologic Museum Foundation

ANNUAL MEMBERSHIP APPLICATION

❑ Please begin/renew my membership in the Foundation

- ❑ $25 Sustainer
- ❑ $100 Contributor
- ❑ $250 Supporter
- ❑ $500 Donor
- ❑ $1,000 Sponsor
- ❑ $5,000 Patron
- ❑ $10,000 Benefactor

The Foundation is certified as a non-profit organization by the I.R.S.

Name _____

Address _____

City _____

State _____ Zip _____

Phone _____ E-Mail _____

Date _____

Please make your check payable to:

The National Cryptologic Museum Foundation

The National Cryptologic Museum Foundation, Inc.

FOUNDATION TELEPHONE:
(301) 688-5436 & 5437
Fax (301) 688-5619
email: cryptmf@aol.com
http://www.
nationalcryptologicmuseumfoundation.com

MUSEUM TELEPHONE:
(301) 688-5849

MUSEUM HOURS:
Monday - Friday - 9:00 a.m. - 4:00 p.m.
Saturday - 10:00 a.m. - 2:00 p.m.

RETURN SERVICE REQUESTED

The National Cryptologic Museum Foundation, Inc.
P. O. Box 1682
Ft. George G. Meade, Maryland 20755-9998

NONPROFIT
U.S. POSTAGE
PAID
FORT MEADE, MD
PERMIT NO. 43