# Cryptologic Quarterly

## NSA's Friedman Conference Center

PLUS: Vint Hill Farms Station • STONEHOUSE of East Africa

The Evolution of Signals Security • Mysteries of Linguistics

2019-01 • Vol. 38

Center for Cryptologic History

# Cryptologic Quarterly

**Publisher**: Center for Cryptologic History
**Chief:** John A. Tokar
**Executive Editor**: Pamela F. Murray
**Managing Editor**: Laura Redcay
**Associate Editor**: Jennie Reinhardt

**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 feel free to address questions or comments to Editor, *CQ*, at history@nsa.gov.

**Disclaimer.** All opinions expressed in *Cryptologic Quarterly* are those of the authors. They do not necessarily reflect the official views of the National Security Agency/Central Security Service.

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

**Cover:** "Father of American cryptology" William Friedman's retirement ceremony in the Arlington Hall Post Theater, Arlington, VA, 1955. Lieutenant General Ralph Canine is at left, Solomon Kullback is seated left, Friedman is second from right, and Director of Central Intelligence Allen Dulles is at far right. *National Security Agency Archives.* See story page 53.

# Contents

**2019-01 • Volume 38**

# History and Transparency: Two Years at a Glance!

John A. Tokar

At the start of each year, I deliberate the style and format of the calendar or portfolio I choose to accompany me each day in both my work and private lives. Unlike many other professions, at the National Security Agency/Central Security Service (NSA/CSS) we do not have the option of using our smartphones for this purpose. Some years I will just continue using the same version of calendar as the last. Early in my US Army career, I carried a pocket-sized calendar that was commercially available from an office store. I preferred its size and layout to the many government-issued varieties available. Later, I would forego a templated, preprinted calendar altogether, and just carry one of the omnipresent, lime-green, hard-sided tablets issued by the Federal Supply Service. It fit neatly in the cargo-pocket of my uniform pants, and it was virtually indestructible. That style of tablet suited me for decades, and I would either write calendar dates on the lined pages inside, or sometimes print small, 5" × 8" calendars and stick them inside for reference. This year, I am back to a larger, commercially available planner. I particularly like the "year-at-a-glance" feature inside the front cover.

Why all this talk about calendars? For one, we use them to track time, a fairly important characteristic of our chosen profession at the NSA/CSS Center for Cryptologic History (CCH). Moreover, one of the many challenges of any leader or manager is a seemingly never-ending demand from one's superiors for information: reports, metrics, and sometimes merely lists. Lists of people; lists of resources; lists of dates and meetings; lists of suspenses; and lists of accomplishments. The latter are sometimes required to track individual accomplishments, for example in support of an award nomination, performance appraisal, or promotion packet. Other times the request is for organizational information, listed in weekly, quarterly, and annual tallies.

Shortly after my arrival at CCH, one of our historians cleverly began a year-at-a-glance narrative of the many ways that CCH conducts its mission to "provide objective, meaningful historical support to the NSA/CSS leadership and workforce to enhance decision making, cryptologic knowledge, and esprit de corps." Many of those actions and activities also serve to "preserve and advance an understanding of cryptologic history for the United States Intelligence Community (IC), the Department of Defense, other government agencies, academia, and the general public." More than a simple list or calendar of events,

this running tally has proven very valuable to us, as the entire team contributes to its maturation throughout the year. It serves to remind us of where we have been, what we have done, and the impact that we are having as a federal government history program in general and on NSA/CSS in particular. Moreover, it serves as a useful tool to plot course changes and to allocate our resources against future requirements.

This issue of NSA's professional journal *Cryptologic Quarterly,* timed to precede our biennial Symposium on Cryptologic History, strives to present "two years at a glance" from CCH's perspective. My hope is that it will provide the NSA/CSS workforce, the rest of government, academia, and the general public with a deeper understanding of what we do as a federal government history program. In 2017, I wrote an article that explored how CCH provides meaningful historical support to the NSA/CSS leadership and workforce to enhance decision making, cryptologic knowledge, and esprit de corps ("What CCH Can Do for You: Make History Relevant!" *Cryptologic Quarterly* 2017-03: 1-7). In this article, I'd like to focus on transparency by providing a two-years-at-a-glance view of CCH's outreach efforts from 2017 through 2019.

**2019 Symposium on Cryptologic History**. This fall, we again will partner with the National Cryptologic Museum Foundation for our 17th Symposium on Cryptologic History, which will be held at the Johns Hopkins University Applied Physics Laboratory in Laurel, Maryland. The theme for 2019 is "From Discovery to Discourse." The symposium is an occasion for historians (and fans of cryptologic history) to gather for reflection and debate on relevant and important topics from the cryptologic past. Since 1990, our symposium has served as an opportunity to present historical discoveries found in unclassified and declassified IC records and engage in scholarly discussion about their significance. The symposium attracts hundreds of attendees and dozens of presenters from NSA, the IC, academia, and the general public from around the globe. It is the largest event of its kind, welcoming all topics relevant to the history of cryptology, signals intelligence, cybersecurity, computer technology, information assurance, and other related national security themes.

**Schorreck Lecture**. CCH also educates and informs the NSA/CSS workforce through briefings and panel presentations, often aligned with significant anniversaries in cryptologic history. The Henry F. Schorreck Memorial Lecture series has been sponsored by CCH for the past twelve years. Schorreck, former NSA historian, was a pioneer in the discipline of cryptologic history. Last year, we were fortunate enough to host Dr. Mitchell Lerner, Ohio State University professor of history and director of the Korean Studies Institute, to mark the 50th anniversary of the capture of the USS *Pueblo* by North Korea. While the primary focus of his lecture was based upon his book *The Pueblo Incident: A Spy Ship and the Failure of American Foreign Policy*, his expertise with the modern day Democratic People's Republic of Korea was the topic of many of the questions he fielded, truly emphasizing the potential impact of applied history to current operations. This year, we were extremely honored to host Mr. Tony Comer, Departmental Historian at the Government Communications Headquarters (GCHQ), NSA's counterpart in the United Kingdom, which marked its centennial in 2019. Tony's talks both inside and outside the fence were well attended. This year's Schorreck Lecture not only served to educate attendees about GCHQ's century of achievement, but more importantly it reinforced the nature of the special relationship that exists between the cryptologic communities of the United States and the United Kingdom.

The GCHQ headquarters building, Cheltenham, UK. For the 2019 Schorreck lecture, CCH hosted GCHQ historian Tony Comer. *GCHQ*

**Collaboration.** A significant portion of CCH resources and effort is directed at developing and enhancing a culture of history at NSA. One way is through the orientation program for new employees. Almost every onboarding class receives an in-depth introduction to a few key stories told at NSA's National Cryptologic Museum (NCM). When they see how their predecessors were able to change the course of world events through codemaking and codebreaking, they are better able to appreciate the importance of the careers they are about to begin. The NCM, which just celebrated its 25th anniversary, is the only museum in the IC open to the public. This enables visitors to appreciate what NSA/CSS contributes in support of our national security. While CCH and the NCM are separate organizations within NSA/CSS, we cannot fully execute our assigned missions without complete cooperation. CCH continuously provides subject matter expertise to the existing museum as well as to those designing

The National Cryptologic Museum celebrated its 25th anniversary in 2018 with a party; two attendees dressed as pioneering cryptologists Elizebeth and William Friedman. *CCH collection*

exhibits for the new Cyber Center for Education and Innovation—which will be the future home of the National Cryptologic Museum.

CCH also collaborates with US service military academies to sponsor two interns every summer. These young women and men are usually history majors, and sometimes, but not always, they are headed to military careers in the intelligence and cyberspace career fields. We assign them to a specific research topic, assist them with locating primary source material and conducting oral history interviews, and guide them toward a finished written research paper that may be published in *Cryptologic Quarterly*. We are constantly amazed by the quality of these finished papers: one US Naval Academy midshipman even won honorable mention in NSA's prestigious Cryptologic Literature Award competition in 2018.

When a CCH historian learned in early 2018 that the original Soviet wood carving of the Great Seal of the United States—a Cold War "bugging" artifact—was hanging in an obscure room in a State Department building, he coordinated a visit and photo shoot. For readers unfamiliar with the story, the Soviets presented a handmade replica of the Great Seal to the US ambassador in Moscow in 1946. The seal remained in the ambassador's residence until 1952, when an implanted KGB listening device was discovered inside the seal. (A replica of the seal is on display at the NCM.) The visit presented the opportunity for CCH to engage with State Department personnel and discuss the cryptologic significance of the artifact.

In a separate exchange in fall 2018, the State Department's Foreign Service Institute (FSI) invited CCH staff members to participate in historical outreach with local public school history teachers. The FSI is physically located at Arlington Hall Station, NSA's original home, and CCH staff enjoyed visiting the historic buildings. During the outreach event, CCH historians joined other IC historians and Ms. Liza Mundy, author of *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. This collaboration at FSI led, a few months later, to CCH inviting Mundy to participate in a Women's History Month panel presentation to the NSA workforce titled "The Women of Arlington Hall." Concurrent with this event, NSA released to the public a massive collection of previously unpublished World War II era photographs from Arlington Hall. Digitizing these photos was a mammoth undertaking involving many organizations. When the final collection of photographs (over 3,000) is available on www.nsa.gov, it will tell a visual story that will be of enduring value to the history programs of NSA and the State Department for generations.

**Sharing Subject Matter Expertise**. Another way that CCH provides outreach activities to the NSA/CSS workforce and the public is through briefings and panel presentations, often aligned with significant anniversaries in cryptologic history. CCH is more than a collection of people who share a passion for NSA/CSS's history and heritage. Our team members' career backgrounds also represent nearly every facet of the Agency's mission spectrum: intelligence analysts, linguists, cryptanalysts, cybersecurity operators, and more. A small sample of our outreach reflects the range of staff member expertise. Topics of cryptologic history presentations to the NSA/CSS workforce as well as to audiences in other venues included World War I; the Vietnam War's Tet Offensive; the 65th anniversary of NSA's founding; oral histories of men and women from as far back as the Mexican Expedition; the IC Senior Historians Panel; and external presentations to the Society for History in the Federal Government, the National


CCH participated in the release of a massive collection of previously unpublished World War II era photographs from Arlington Hall, NSA's original home. *CCH collection*

Council on Public History, the Society for Military History, the Chinese Military History Society, and the Charlotte International Cryptologic Symposium. Our historians consulted with Barry Levinson, director of *The Bit Player*, a soon-to-be released biographical documentary about Claude Shannon, the father of information theory. They also consulted with the production staff of an upcoming remake of the 1970s blockbuster film *Midway!* They were interviewed by *National Geographic* and *Slate* magazines, among others, and gave a presentation and museum tour to the staff of Atlas Obscura.

CCH's formal and informal outreach and education programs have matured in both quantity and quality over the past two years. In conjunction with the National Cryptologic School, our general and special topic cryptologic history courses remain incredibly popular with the Agency workforce. Our Civil War staff ride to Antietam National Battlefield is always wait-listed, and our debut Gettysburg staff ride met with similar demand (see photo on next page). Staff rides are open to all of our affiliates and emphasize the role of intelligence in past battles. These battlefield studies mean far more than a day away from the office, involving elaborate preparation on the part of students and instructors, and highlighting the numerous parallels with modern warfare and intelligence production.

**Cryptologic Hall of Honor.** NSA/CSS has always been, first and foremost, a collection of

CCH Staff Ride (HIST1863) at Little Round Top, Gettysburg National Battlefield. *CCH collection*

talented and dedicated people. One of the most rewarding parts of working in CCH is when we get an opportunity to honor these women and men, and to meet them and sometimes their families to acknowledge their achievements. We are able to do this in several different ways, such as the Cryptologic Hall of Honor process. One 2017 inductee to the Cryptologic Hall of Honor was Colonel Frank E. Herrelko, US Air Force, who pioneered the organization and principles of communications security (COMSEC), the predecessor of information assurance and cybersecurity. At the time of his nomination, Colonel Herrelko was 104 years old and living just outside of Philadelphia. Through his daughter, we were thrilled to learn that he might even be able to attend the formal induction ceremony. Alas, as the date approached, his health would not allow him to travel, so CCH took the ceremony to him the very next day! Colonel Herrelko's daughter had arranged through his assisted living facility to gather his closest friends, staff, and even the local press for a mini-ceremony just for him. It was such an honor to meet a man who had served in World War II, was later a protégé of Lieutenant General Ralph Canine, NSA's first director, and continued to serve NSA/CSS in uniform and as a civilian into the 1980s. Colonel Herrelko passed away in 2018 at age 105, but like the other great women and men that we honor in the Cryptologic Hall of Honor, he will never be forgotten.

**Memorializations**. In the past several years, CCH has worked in conjunction with NSA's Installations and Logistics Group to memorialize many individuals through the naming of buildings and other facilities in the NSA/CSS enterprise. CCH supported the 2018 rededication of the William and Elizebeth Friedman auditorium. It is now a world-class, high-tech conference center that hosts significant, enterprise-wide events nearly every work day. A year earlier, CCH supported the renaming of the NSA director's remodeled conference room. In that case, the Agency memorialized Ann Z. Caracristi, a former deputy director, NSA's highest civilian position. The first woman to achieve that post, Caracristi came to the cryptologic field straight from college during World War II. It is quite appropriate that a state-of-the-art meeting

space, in daily use by the highest ranking decision makers, is named for her.

Other notable memorializations CCH supported over the last two years included the ribbon-cutting and building dedication of the Colonel Alva B. Lasswell Hall, the new home of the US Marine Corps Forces Cyberspace Command (MARFORCYBER) on NSA's East Campus. Lasswell was an outstanding cryptanalyst and Japanese linguist whose contributions at Station Hypo during World War II were legendary. Just months earlier, CCH coordinated a site visit and tour of the Major General John E. Morrison, Jr., Center, also located on the new East Campus. Morrison was the driving force behind the creation of the National Security Operations Center in 1972. For both occasions, we welcomed the friends, children, grandchildren, and even great-grandchildren of these men to NSA. We were able to extol their achievements and assure their descendants that NSA is dedicated to maintaining their legacies. We do this not just for their benefit. Equally important, these facilities, and the history behind their naming, serve as daily reminders to NSA/CSS employees that the work they do is vital and can have an impact that stands for decades or longer.

Special Cryptologic Hall of Honor ceremony with (*left to right*) Chief, CCH, John Tokar; CCH historian Mark Nixon; Kathy Herrelko Easton (daughter); inductee Colonel Herrelko; Tom Easton (son-in-law); and NSA Historian David Hatch. Colonel Herrelko passed away nearly one year later at age 105. *CCH collection*

**Publications.** In any given year, CCH releases both new and updated publications to the public. Publications are revised for a number of reasons, such as the availability of new information due to declassification or to update the design to improve the reader experience. Over the past two years, CCH has updated and rereleased Dave Gaddy's translation of *Essential Matters: A History of the Cryptographic Branch of the People's Army of Viet-Nam, 1945-1975* and Sharon Maneki's *Learning from the Enemy: The GUNMAN Project.* We are in the final stages of publishing Dr. A. Ray Miller's *The Cryptographic Mathematics of Enigma*. CCH has also released a new publication, Carol B. Davis's *Candle in the Dark: COMINT and Soviet Industrial Secrets, 1946–1956,* as well as this issue of *Cryptologic Quarterly*. Please enjoy the following collection of articles and the photographs that accompany them. They represent a wide spectrum of topics from a diverse list of authors: a combination of old favorites and new offerings. Sarah Parsons pays a warm tribute to William and Elizebeth Friedman and the event space that

NSA has dedicated to their memory. Retired CCH senior historian Betsy Rohaly Smoot has assembled a photo history of Vint Hill Farms Station, once a key collection site for the US Army Security Agency, a predecessor to NSA. Mark Nixon, a CCH historian, shares a fascinating history of NSA's STONEHOUSE high-altitude communications facility in East Africa, which closed its doors in 1975. The remaining two articles are reprints from a pair of Cryptologic Hall of Honor inductees, Jack Gurin and David Boak. CCH thought the time was right to share their articles about linguistics and signals security, respectively, with a new, wider audience.

Last but not least, one of CCH's most popular publications is our annual cryptologic history calendar. It is a perennial favorite among the workforce, and we publish and distribute more than 14,000 calendars every year. Our staff scours digital and nondigital photographic records for previously undiscovered gems to include in each year's calendar. They also double-check the validity and accuracy of the historical entries. These calendars are important tools for increasing the visibility of cryptologic history and maintaining our culture of history. They are especially practical tools for those who have an interest in NSA/CSS's heritage but perhaps cannot devote the time necessary to read CCH's long-form history publications.

NSA is a government (and often industry) leader in many different fields: mathematics, linguistics, physics, engineering, and computer science to name but a few. The Agency has a rich, documented history of achievement in all of them. In each of those chosen fields, NSA introduces technical and academic rigor and applies it against a specific challenge or problem set. With healthy doses of dedication and hard work, positive outcomes are usually (but admittedly not always) achieved. Here at CCH we take a similar approach. We use established, recognized standards and methods of historical research, writing, and publication. We educate using academic practices that are both widely recognized and sometimes unorthodox. We then apply them across a wide spectrum of outreach platforms and distribution venues. Using continuous feedback from our valued internal and external customers, CCH remains committed to our overarching goal: not simply writing history for history's sake, but *applying* history that can improve current and future NSA/CSS operations, as transparently as possible.

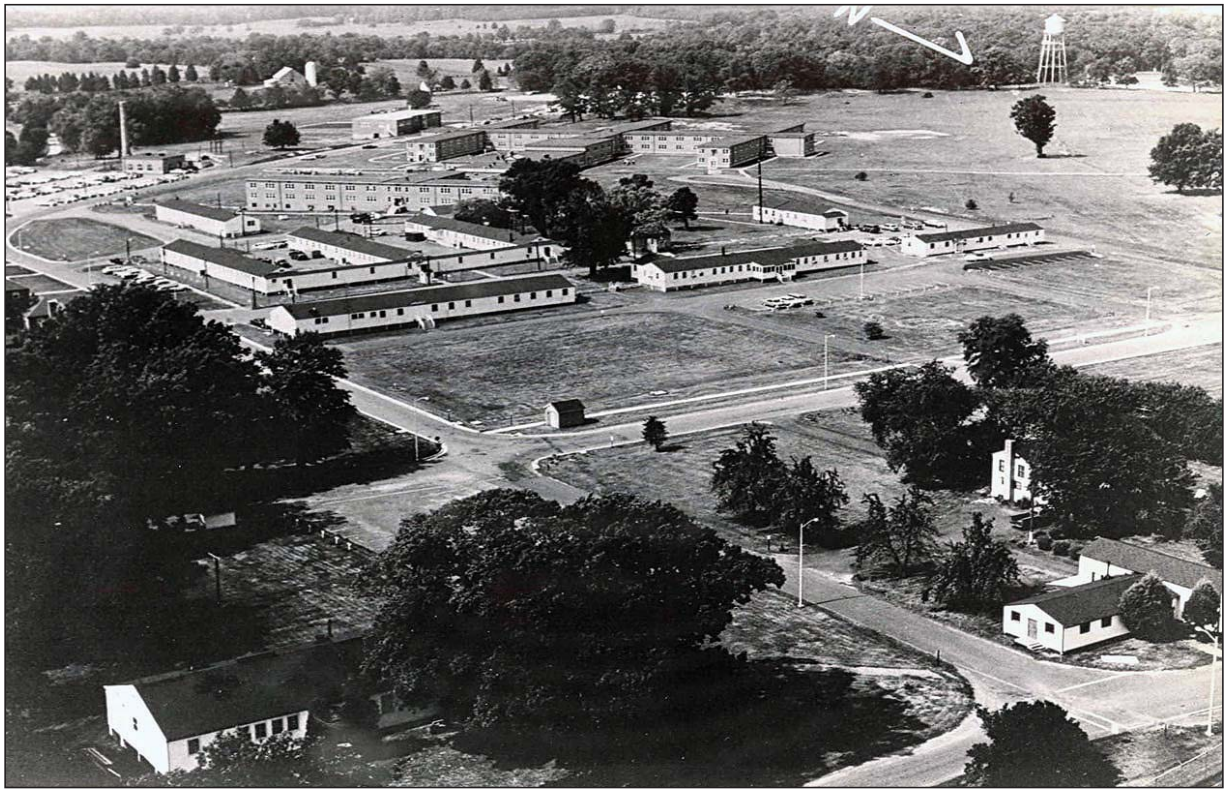
**John A. Tokar** is the Chief, NSA/CSS Center for Cryptologic History (CCH). Prior to joining CCH, he served in a variety of cyberspace planning and cybersecurity assignments in the NSA/CSS Threat Operations Center, US Cyber Command, and its predecessor organizations. He is a retired US Army officer with a background in special operations, strategic and operational planning, and logistics, to include two command assignments. He also served three years at the US Army's Center of Military History, which included a deployment to Afghanistan as US Special Operations Command's field historian, conducting oral history interviews of special operations forces and Intelligence Community personnel.

# Family Album

## Vint Hill Farms Station

Betsy Rohaly Smoot

Vint Hill, or more formally, Vint Hill Farms Station (VHFS), is a legendary place in cryptologic history, one equal in importance to Arlington Hall Station (in Virginia, home of NSA's predecessor, the Armed Forces Security Agency) for many cryptologists, particularly those who served



Aerial view of the station in 1956. Note the white silo and barn in the upper left. This barn was where the intercept operation was established in early July 1942.

The barn at Vint Hill in the 1940s, before army renovations

The Vint Hill barn, probably in the late 1940s or early 1950s

Operations shift personnel, Second Signal Service Battalion, in front of Vint Hill Station silo, World War II

in the Army Security Agency. The 721-acre site, encompassing all or parts of eleven farms in the northeast corner of Fauquier County, Virginia, was purchased by the US Army in 1942 for $127,500. The most prominent of these farms had been called "Vint Hill," named for the vineyards that covered the rolling hills in the late eighteenth century. Close to the Bull Run Mountains and only 40 miles from Washington, DC, the location was particularly well suited for radio intercept work. The area may have come to the attention of the Army's Signal Intelligence Service (SIS) because local ham radio operators were often able to listen to taxicab communications in Berlin, Germany.

In the early days of World War II, as SIS prepared to move from its Washington, DC, location to Arlington Hall, Vint Hill was chosen to be the first large signals intelligence (SIGINT) field station of the modern era. The army would establish at least nine more field stations during the war, but Vint Hill was first and carried the designator

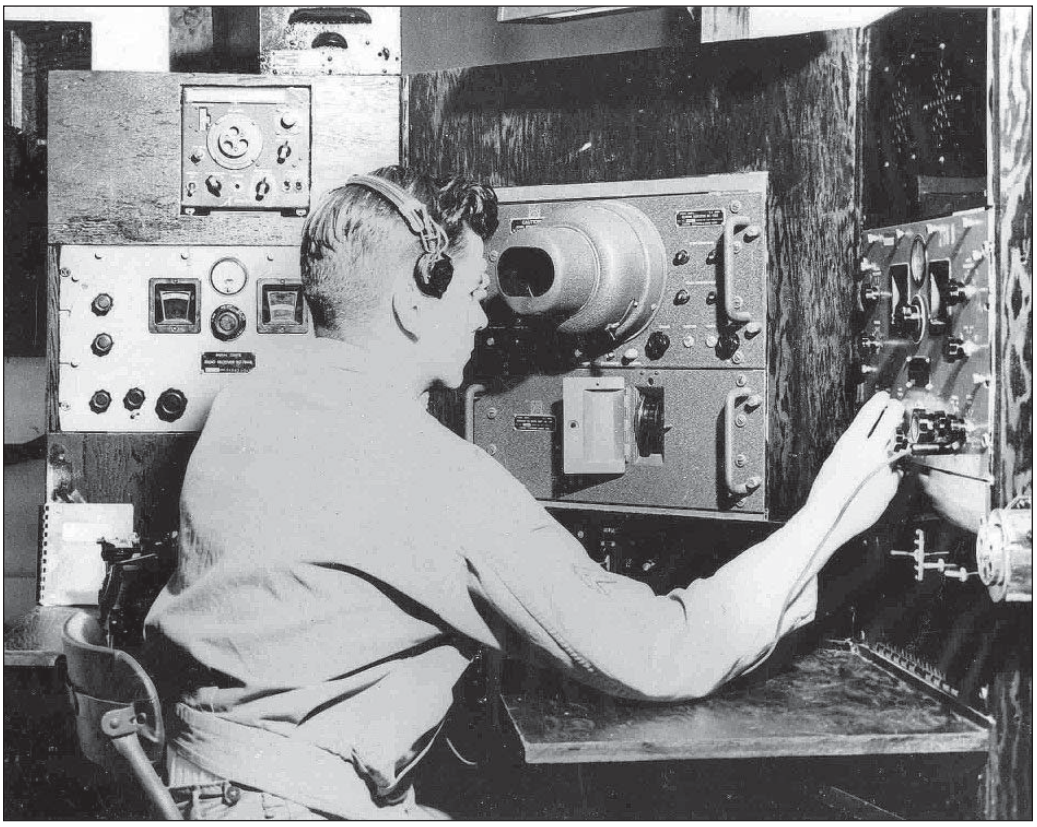
Radiotelephone intercept recording technology in use at Vint Hill Farms Station, 1945

Monitoring Station #1.[1] Various training schools were also located at Vint Hill, and many intercept operators, radio repair technicians, and linguists were trained there prior to duty overseas or at Arlington Hall.

In 1975, army intercept operations at VHFS were moved to Lackland Air Force Base in San Antonio, Texas, and were combined with an air force intercept site. A variety of other NSA and non-NSA efforts continued at VHFS until the post was closed in September 1997, a victim of the Base Realignment and Closure Commission. In recent years, Fauquier County has developed the site as a mixed-use business and residential community. The Federal Aviation Administration has a modern facility on the property. A Cold War Museum opened there in 2011.

The main farmhouse at Vint Hill, a brick two-and-half-story mansion, was built just before the Civil War by Andrew Low, an English immigrant to Virginia. In June 1942, during the army's initial construction phase at the site, the mansion was used both as an office and as sleeping quarters for the first arrivals. It was later turned into the post's officers' club and bachelor officers' quarters. Today it is the Vint Hill Inn.

The Center for Cryptologic History, the NSA Archives, and the National Archives and

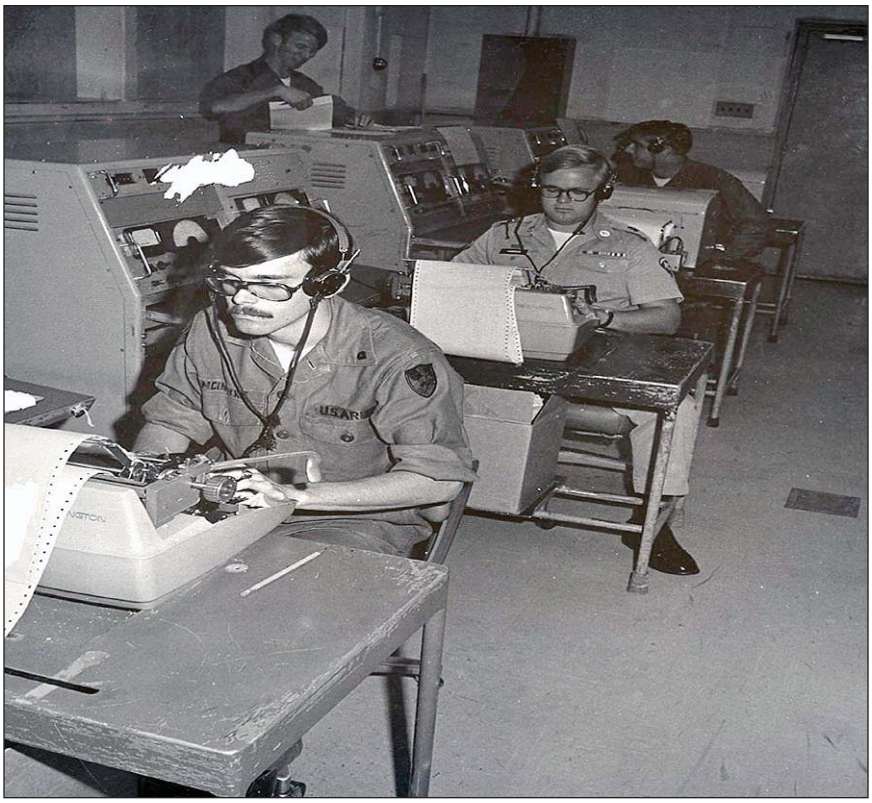


Direction finding operator at Vint Hill, World War II

A 1948 view of the radio search room, staffed by a watch chief and six operators

Vint Hill operations, undated

The barn from another angle, 1975



Intercept operations in 1974, just prior to the site's closure

Records Administration have many photographs from early US Army facilities but very few photographs from early US Navy facilities. When army and navy cryptologic operations merged into the Armed Forces Security Agency in 1949, many of the navy records appear to have been filed or archived with the Office of Naval Intelligence, the parent organization of the navy's cryptologic service.

## Note

1. While the field station would go by several names in later decades, it was given the SIGINT Activity Designator USM-1 in 1947 and carried that designator until the army intercept site was moved in 1975.

**Editor's note.** This article first appeared in a slightly different form in the Winter/Spring 2011 *Cryptologic Quarterly*. All photos are from the CCH collection.

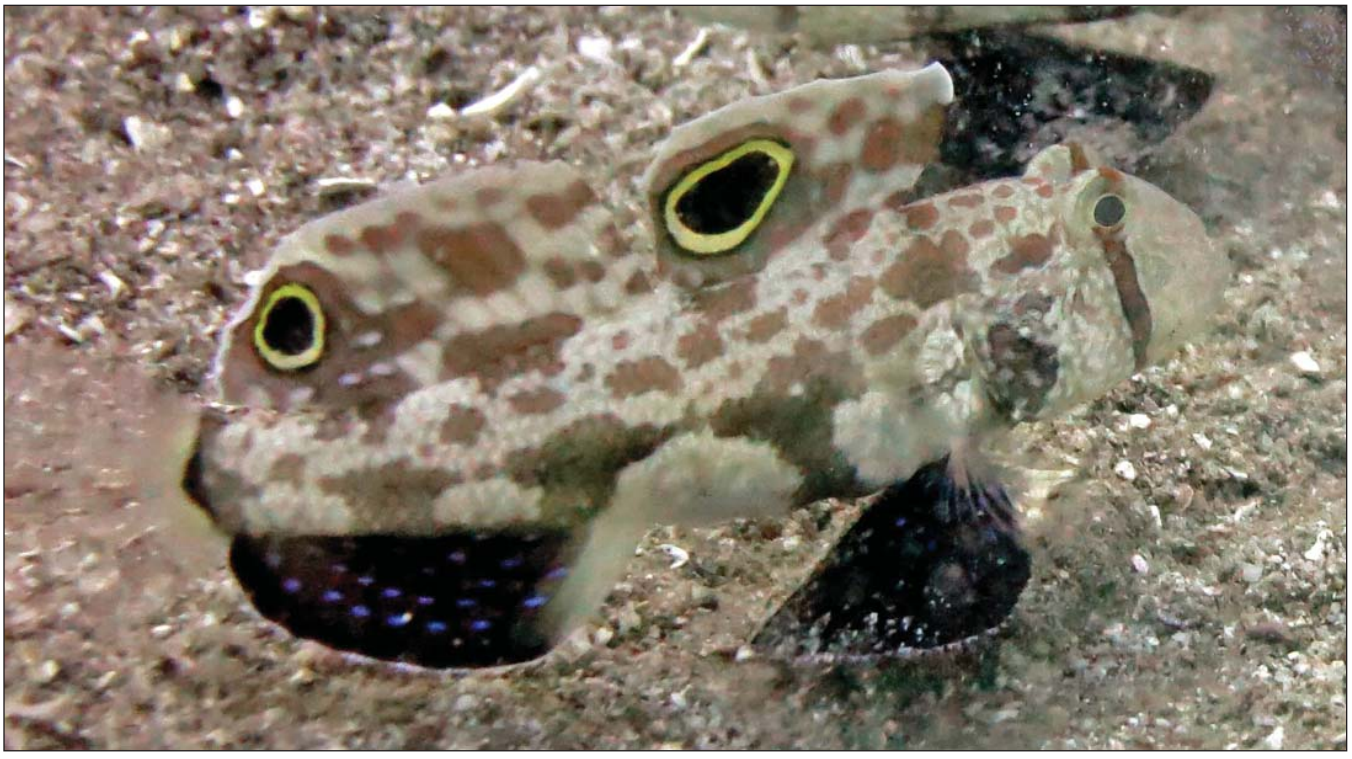
**Betsy Rohaly Smoot** came to the National Security Agency in 1983 as a traffic analyst. She has worked in analytic, staff, and managerial positions at Fort Meade and overseas. She joined the Center for Cryptologic History as a historian in October 2007. Her particular research interests included World War I, the Cold War, and terrorism. Mrs. Smoot received a BA from Mary Washington College with a double major in geography and economics and an MS in strategic intelligence from the Defense Intelligence College. She retired in 2017.

# The Evolution of Signals Security as a Counterintelligence Discipline

David G. Boak

Doubtless, adversaries—predators and prey alike—have been attempting to hide information from one another since earliest biological times. Camouflage, concealment, and deception have been used to disguise size, strength, location, and intentions since species began competing with each other and among themselves.

Deception is rampant in nature—not excepting human nature, of course. A few examples:



Deception in nature: Gobi fish have spots near their tails that look more like eyes than their real eyes do; they can evade predators by darting in an unexpected direction. *Lakshmi Sawitri, Wikimedia*

Predators and prey have evolved markings and behaviors that make them nearly indistinguishable from their surroundings.

Top to bottom: Polyphemus moth with "eye" spots; vine snake, Agumbe rainforest, India; tiger in dry grass, Todoba Andhari National Park, India

Homer Edward Price, *Wikimedia*

Vrinda Menon, *Wikimedia*

SushG, *Wikimedia*

Many fish have spots near their tails that look more like eyes than their real eyes do, surprising the striking barracuda by darting in the wrong direction. There are lepidoptera with huge eye-like wing spots suggesting an animal a thousand times their actual size. Birds feign broken wings in a diversionary tactic to lead predators away from nest sites. Threatened cats, of course, raise fur and arch backs to make themselves look larger.

Camouflage and concealment are also prevalent. Many insects, crustacea, fish, amphibians, reptiles, and so on up the chain in the animal kingdom have evolved markings and behavior patterns making them nearly indistinguishable from their surroundings. The technique applies equally to the hunter and the hunted as they seek, respectively, to ambush prey or to avoid detection. Some examples are stick insects, crabs that glue seaweed and benthic debris to their shells, fish that look like rocks, alligators like logs, and striped tigers in the tall grass.

The variety of sensors present in nature—i.e., intelligence-gathering mechanisms—is remarkable. They include audio, visual, olfactory, sensory, infrared (in the case of some pit vipers), sonic (echolocation in the case of bats), and electromagnetic (in the case of homing pigeons). Further, the sensitivity of some of these intelligence collectors is extraordinary.

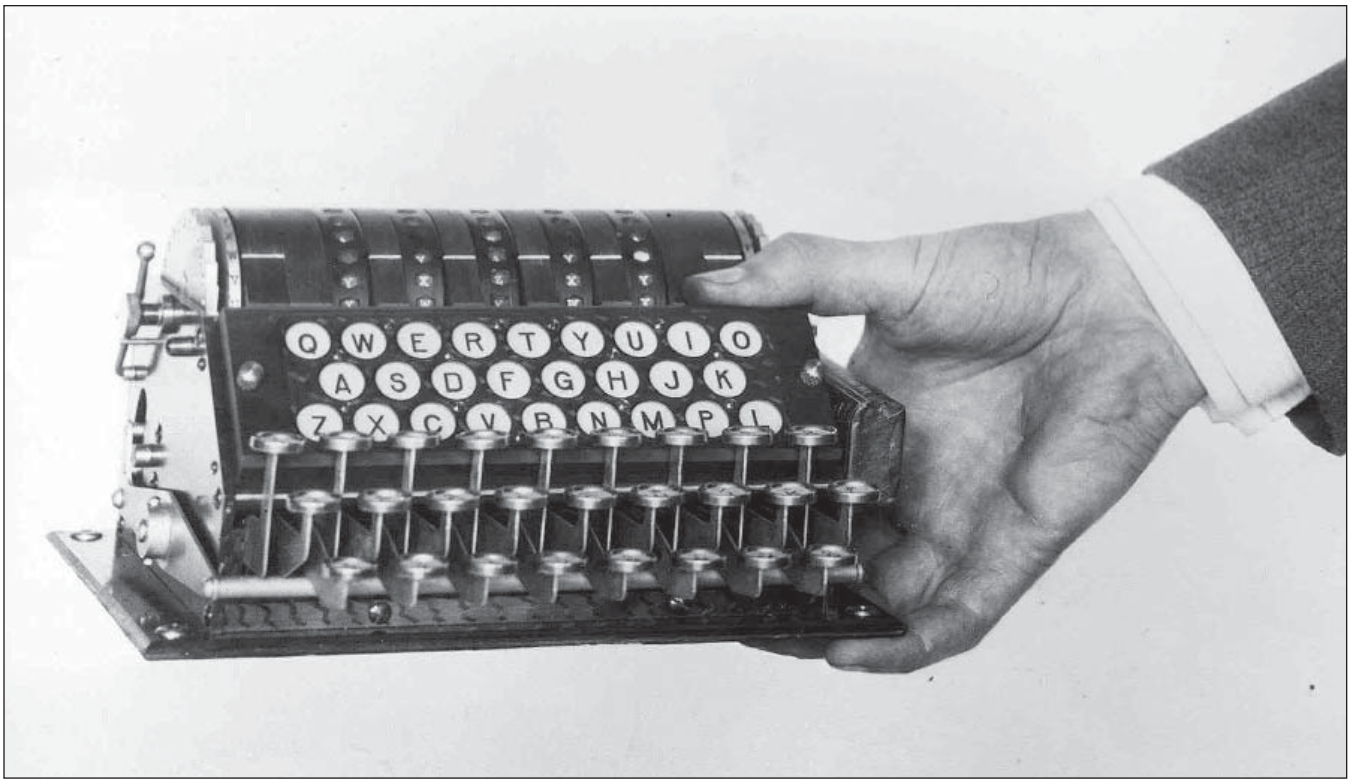
Many species have Identification Friend or Foe (IFF) recognition systems involving visual, olfactory, aural, and other signals. For example, some fireflies evidently differentiate themselves from interlopers by the intervals between, and intensity of, their flashes. Whales, capitalizing on ducting, communicate sonically over distances of hundreds of miles under water. In addition to recognition systems, wherever cooperating groups are involved, communications are used extensively for warning. Beavers do it with their tails, while vocal animals use a variety of barks, roars, and calls; insects use the color red, and, familiarly, squirrels and birds do it with chatter when they detect cats, snakes, or other predators.

## The First Human Signaling

It seems likely that early humans fell into the business of deception, camouflage, ambush, IFF, and intelligence gathering quite naturally and as a matter of logic and survival. For example, cave drawings show men with animal skins over their backs stalking prey. *Homo sapiens* brought something extra to the survival equation: an extraordinary capability to communicate.

Obviously, humankind engaged in remote signaling long before written, courier-delivered messages were used. It began with the first shout, continued with runners with oral instructions, smoke signals, rifle or cannon fire patterns, signal flags, and so on. In olden times, such signaling was used principally for military command and control. Adversaries attempted to intercept these signals to avoid surprise. Conversely, communicators began encoding military command and control signals to increase the odds of achieving surprise. In the protection and exploitation of those communications lie, respectively, the beginnings of communications security (COMSEC) and communications intelligence (COMINT).

Communications security techniques gradually came to encompass secret writing with invisible inks and other devices, and a host of techniques were devised for encryption through the use of various codes and ciphers. [According to Herodotus,] the Romans tattooed a dispatch on the shaved head of a messenger, then let the hair grow back before sending him on his way. In the sixteenth century, Leonardo Da Vinci wrote in mirror image to disguise the contents of his scientific notes, and Leon Battista Alberti invented




The Hebern 5-Rotor Bakelite machine from the 1920s was designed to provide privacy for commercial telegraphic traffic. *CCH collection*

the cipher disk. Gradually, more sophisticated techniques evolved. These included paper-and-pencil systems—codebooks, grids, transposition systems, simple ciphers, and one-time pads. Mechanical devices, such as multiple disk systems to facilitate polygraphic substitution, appeared at least as early as Thomas Jefferson's time.

## COMINT in World War I and the 1920s

During World War I, the US government's first communications intelligence effort was undertaken by Herbert Yardley and his staff [in the Military Intelligence Division's MI-8], and a few years later William Friedman was publishing mathematically based treatises on cryptanalysis. After World War I, different types of electromechanical cryptoequipment began to show up, largely through initiatives in the private sector both at home and abroad. Produced between the World Wars, these inventions seemed designed not so much with military and diplomatic requirements in mind as with the need to provide privacy for commercial telegraphic traffic with its growing speed and capacity. Early versions of the Enigma showed up around 1920 or so, to be followed in America by the Hebern rotor machine a few years later. Exploitation of telegraphic communications was perhaps among the earliest manifestations of industrial espionage and economic warfare through communications intelligence.

Looped teletypewriter tapes, which provided long sequences of pseudorandom key, and then truly random one-time tape systems, appeared next. By the late 1920s, wired rotor equipment was coming into its own.

In those days, encryption was all off-line—that is, a message was converted from plain to encrypted form with the resultant cryptogram written down, printed, or punched into a teletypewriter tape and subsequently sent to the recipient by whatever transmission means were available—usually by courier, radio, or telegraph. With the advent of the teletypewriter, there was a gradual transition from off-line to on-line cryptosystems, with correspondents using machines linked directly to a transmission means. This permitted messages to be decrypted instantaneously at the receiving end.

To this point, and into the future, most advances in both communications security and communications intelligence technologies were largely driven by advances in information-processing systems. Those systems became intelligence targets and demanded increasingly complex methodology for interception and processing of the transmitted data. Similarly, designers of protective systems had to assure both technical compatibility with the new communications systems to which they were applied and ever more robust cryptologics to cope with increasingly powerful mechanical and mathematical cryptanalytic tools.

## World War II Developments

By World War II, US military communications security efforts had been formalized into three principal components: cryptosecurity (preventing successful cryptanalysis), transmission security (preventing traffic analysis), and physical security (preventing hostile acquisition of sensitive cryptomaterials, including keys). Hostile signals intelligence efforts may or may not have been organized along similar lines, but they doubtless attempted to exploit weaknesses in all three areas.

Along the way, some transmission techniques evolved that were intended either as a substitute for cryptography or to augment it by making the communications themselves more difficult to intercept and, therefore, to exploit. They were designed to counter increasingly hostile capabilities to acquire and process transmitted signals. There were brute force efforts, such as protected wire lines run through conduits of concrete and steel and elaborately sheathed cables salted with a host of sensors designed to detect attempts at penetration and sound alarms. Low-probability-of-intercept systems were designed not only to thwart the derivation of intelligence but also to make direction finding and jamming more difficult.

Hostile communications intelligence, of course, had to match the innovations in both the communications and the communications security fields with increasingly sophisticated techniques of interception and analysis. Cryptology, however, remained and remains at the heart of both the COMINT and COMSEC disciplines.

As communications systems (like microwave transmissions) and noncommunications systems (like radar) increased in complexity and variety, COMSEC broadened its horizons and began to be referred to as signals security (SIGSEC)—first in the US Army and then more generally. Correlatively, both friendly and hostile COMINT began to be referred to as signals intelligence (SIGINT) as they focused on a widening variety of signals.

In looking at the cryptanalytic attacks and counterattacks that loom large in signals intelligence and signals security lexicons, each side enjoys certain advantages. Counterintelligence—the SIGSEC side—has an inherent advantage, at least in the business of designing high-grade machine cryptographic systems capable of withstanding massive cryptanalytic attacks, in part because SIGSEC system designers have full latitude in the selection and application of the

cryptoprinciple and, in some cases, are able to hide the nature of that principle from adversarial eyes—often for some years. And without knowledge of the algorithms underlying a modern cryptodevice, successful cryptanalysis may be difficult or impossible, even though some hostile SIGINT entities might be able to bring very large analytical resources to bear. SIGSEC authorities could even select the one-time principle, which, with keys properly generated and used, is probably secure—that is, immune to successful cryptanalysis. Fortunately for the SIGINT world, most such systems are notoriously inefficient, especially when netted communications are involved, and so are seldom used in machine systems these days. Of course, during World War II, some SIGSEC authorities overestimated the strength of their cryptomachines or underestimated the persistence and ingenuity of their adversaries—witness the German experience with Enigma and the Japanese with PURPLE.

On the other hand, SIGINT practitioners have the distinct advantage of being able to attack across a very broad spectrum of possible vulnerabilities, and only need to find one weakness, while the SIGSEC designer must try to anticipate and counter all possible attacks. Further, SIGINT may bring to bear analytic techniques that the SIGSEC designer would have no means to anticipate.

In the American inventory, paper-and-pencil systems persisted—especially at tactical levels—long after machine systems became available. This was true because such systems were cheap and expendable and generally thought to be adequately secure for perishable traffic in the field—that is, for traffic that would be of no value a few hours or days after it was sent. Except for the one-time pad systems (used more for special activities rather than in support of military operations), most manual systems—called Operations Codes or OpCodes—were not only weak but also slow. They required laborious procedures and frequent replacement (for example, a daily change of whole codebooks in some instances) to maintain their security. In contrast to cipher machines, hostile SIGINT had a distinct advantage when it chose to attack such systems. Essentially, the SIGSEC effort to protect tactical traffic during the 1940s and 1950s—and beyond—was a countermeasure to the easy exploitation of plain language communications in the field. (Note that during World War II, however, the United States did manage to field a small mechanical cipher machine for tactical use—the Hagelin CSP-1500/M-209. More than 100,000 copies were built. Used properly, it was quite secure, but it was very slow and required intricate set-up and operating procedures, and some codes and low-level ciphers persisted.)

## Into the Cold War

By the end of World War II, it was clear that hostile SIGINT held an edge over SIGSEC with respect to transmission security. Using traffic analysis techniques, analysts could derive a great deal of intelligence without decrypting the traffic itself even on links where highly secure machine cryptosystems were in use. Traffic analysis derives intelligence by examining message externals: callsigns, indicators, origins and destinations of messages, fluctuations in timing and message volume on a given link or net, together with more exotic means like radio-fingerprinting for locating and identifying originators and recipients of traffic.

Transmission security authorities in the SIGSEC world began to cope with this problem with a classic set of countermeasures—awkward at first but refined over the years. Callsigns were encrypted with some difficulty. The technique of traffic flow security was introduced, first with one-time tape systems and later with key generators. Reels of one-time tape, 100,000 characters

long, ran continuously on various links until they were exhausted, whether actual traffic was being enciphered or not. Each tape was then discarded and a new one put in place. The pure one-time key could not be differentiated from encrypted traffic. This was true because the tapes were completely random and, according to the axiom that "anything added to random is random," the cipher text was random, too, through the earlier mentioned use of low probability of intercept.

Attempts were also made to frustrate traffic analysis systems, thus denying traffic analysts the external data needed for their work. These systems mainly involved the use of very short, high-speed so-called burst transmissions or spreading signals over a broad swath of the radio spectrum with their distribution governed by a randomizer or pseudorandomizer. In fact, some transmission systems designed for high-speed, high-capacity communications were, for a while, thought to be inherently secure because of the difficulties they posed to a would-be interceptor.

The enormous growth in sophistication of communications systems proved a mixed bag for both signals intelligence and signals security interests. Satellites began dumping telephonic and other communications into huge swatches of real estate—"footprints" available to all takers. Formerly, hostile SIGINT might have required a dangerous wire-line tap or intrusion into the line of sight of a point-to-point microwave transmission to acquire these signals. On the other hand, demodulation of these signals was not always easy, and the sheer volume of traffic could overwhelm interceptors.

On the countermeasures side, SIGSEC authorities had to match or exceed the speed and capacity of these multichannel communications in order to apply cryptography. With the possible exceptions of computer technology and the early development of large scale integrated chips (where cryptologic organizations drove the state of the art), advances in the field of communications electronics occurred first and then were adopted or adapted by cryptologists. Vacuum tubes, subminiature tubes, the transistor, and more sophisticated chip technology all showed up in both crypto machinery and analytic equipment as time went by.

M-209 cipher machine in use in a South Pacific island jungle during World War II. *CCH collection*

SIGSEC compounded hostile SIGINT's problems once again when cryptoequipment called key generators (KGs) became prevalent. Although a few rudimentary machines were built as early as World War II, they did not become common until the late 1950s. KGs not only made traffic flow security (transmission of uninterrupted random data indistinguishable from real encrypted traffic) easy to produce, but they also were able to handle point-to-point and netted traffic in enormous volumes and at speeds as high as the associated communications system could bear. They generated streams of random

but deterministic key to which plain text could be added—usually modulo 2—to form a cipher ready for transmission to addressees. Since the key streams were deterministic, any machine using the same key and starting from the same initial setting could duplicate the key stream exactly and use it to decrypt traffic from a like machine.

In the early 1950s, the SIGSEC counterintelligence problem took on a new dimension—the need for emanation security to cope with the TEMPEST phenomenon. TEMPEST involves the unintentional radiation (electronic leakage) of intelligence from most information-processing equipment, including printers, copiers, cipher machines, computers, etc. (Actually, the phenomenon had been discovered at Bell Labs nearly a decade earlier during World War II, but caused only fleeting concern at the time and was literally forgotten for some years after the war ended.) The TEMPEST problem was complicated by the fact that this radiation was both ubiquitous and difficult to cure. Because of the practical difficulties hostile interests would face in safely exploiting the phenomenon in most environments, it presented a classical milieu for protracted debates among cryptoequipment designers on just how much should be spent to cure the problem. At about this time, cost-benefit analyses and similar efforts to examine security measures on quantitative rather than qualitative grounds, and trade-offs between maximum security and minimum cost, were de rigueur. The arguments showing almost universal vulnerability on the one hand and very little demonstrated threat on the other naturally affected the scope and pace of corrective action for several years. Eventually, technology came to the rescue with system designs that made it possible to control the TEMPEST problem relatively painlessly when new information processors were being built. Retrofitting existing radiators, however, was in most cases impracticable, and it was necessary to create security zones or, in high-threat locations, to encapsulate equipment in Faraday cages (screen rooms) as a countermeasure.

Well into the 1960s, most machine cryptography involved record (written) communications. Although some voice cryptography (ciphony) dated back to World War II, the technology came nowhere near meeting the demand of millions of telephone and radiotelephonic links used throughout government and industry. The high-level ciphony machines were expensive, and the encryption techniques either penalized voice quality or demanded large chunks of expensive bandwidth for transmission of the cipher signals. As a result, relatively few machines were available at the strategic level, and the Intelligence Community was the principal user. It is true that a fairly large number of tactical voice encryption devices were fielded in those days, most of them built in response to critical, short-suspense requirements in Vietnam, but their rate of use was disappointing for a variety of reasons. This general dearth of ciphony equipment resulted in a bonanza for the SIGINT adversary. There for the taking were millions of telephonic conversations on wirelines, field radios, and microwave and satellite links.

Rectifying this situation has been the SIGSEC community's most formidable counterintelligence task during much of the second half of the twentieth century. Technological breakthroughs, drastically revised manufacturing and marketing strategies, and a revolutionary change in the protective security doctrine that had been applied to cryptoequipment in the past were now required.

One new technology was a means to transmit ciphony signals over ordinary telephone lines without appreciably degrading voice quality: Linear Predictive Coding. It provided a way for decreasing the number of bits previously

required to describe an element of speech accurately, thereby reducing the bandwidth needed for transmission. Another was the design of an elaborate system for remote electronic distribution of keys so that individual communicants could talk securely without having to key their own machines.

The strategy for getting these ciphony systems built cheaply and used extensively involved putting several major electronic firms into direct competition in building equipment with whatever form factor they chose and with as many or as few bells and whistles as they saw fit—being required only to use the cryptoprinciple provided by the government and ensure that its product could communicate with those offered by competing companies.

The doctrinal change was to treat the machines as unclassified when unkeyed. This greatly facilitated the distribution of these machines to relatively unprotected environments throughout government and in key industries where sensitive information was involved.

All of these initiatives resulted in the Secure Telephone Unit III (STU-III), one of the most successful cryptographic programs in history, with a quarter of a million secure terminals located in government and industry.

Such work, together with the ability to encipher many canals in multichannel communications systems simultaneously (bulk encryption), represented substantial progress in hardening the plethora of unprotected circuits that hostile SIGINT could attack.

COMSEC had evolved into SIGSEC, and that field began to expand even further as protective techniques, particularly cryptographic techniques, were applied to progressively broader applications, notably data encryption and computer security. By the same token, SIGSEC found itself countering a more varied arsenal of intelligence-gathering techniques encompassing everything from computer hackers penetrating sensitive networks and databases to bank fraud through manipulation of computer-driven Electronic Funds Transfer (EFT) technologies.

## The Achilles Heel: Physical Security

Throughout this evolution, however, COMSEC and its companion disciplines had an Achilles heel. Emission security and, increasingly, computer security had been added to the original triumvirate of cryptosecurity, transmission security, and physical security. Despite all the other advances, one element in the protective envelope lagged behind: physical security—more specifically, the threat posed by subversion of our own personnel.

The problem was not simply a matter of preventing the theft of cryptoequipment and their sacrosanct keys by agents in the night. SIGSEC kept up with that fairly well with state-of-the-art locks, safes, and alarms (with rapidly changing keys), and with cryptographic networks compartmented into thousands of independent entities so as to limit the scope of any individual loss through theft. The problem was not penetration from the outside; it was subversion from within—a few of our own cleared, trusted people, the so-called cognizant agent.

If hostile SIGINT could sponsor the subversion of cleared individuals within the cryptologic community and through them acquire the keys on which the security of every cryptosystem ultimately depends, they could perform what has been called “practical cryptanalysis”; that is, they could read traffic directly like any legitimate recipient. Most such keys were generated centrally and distributed worldwide through vulnerable courier

systems; in some instances, these keys were held in thousands of locations by individual users. All that hostile SIGINT needed was to subvert a few strategically placed individuals such as crypto-custodians with access to a broad range of keying materials, and theater or worldwide secure communications could be compromised. And over the decades, a few such individuals were always available, with greed overwhelmingly their motivation—the Walker family affair* being the most notorious case in point in recent years.

Enter electronic keying, one of the newer countermeasures in the protective arsenal. If you can't trust cleared people, and a compromised key utterly destroys cryptosecurity, then you need a way to distribute and use that key, which does not expose it to every Tom, Dick, and Harry in the network. As noted earlier, the STU-III program includes a feature whereby individual desk sets are keyed initially from a remote key distribution center and then generate their own keys call by call. From the user's standpoint, the feature is a boon because the user is relieved of the keying burden. From the security officer's perspective, it is a blessing because the key exists only in electronic form, is deposited in the guts of the machine, and is difficult to extract.

## SIGINT and SIGSEC Strengths

Throughout the evolution of signals intelligence activities and their signals security counterparts, the two disciplines remained formidable adversaries, each with increasingly impressive capabilities. The success of modern-day SIGINT lies in the fact that, to the extent it can defeat SIGSEC (or when it encounters none), SIGINT is the premiere intelligence discipline when measured in terms of the timeliness, accuracy, reach, and authenticity of its product. It can often deliver that product almost instantaneously—at least in raw form. It involves relatively few ambiguities, cannot be doubled, and is difficult to spoof or deceive. It can operate hundreds or thousands of miles from its target, night and day, regardless of cloud cover, and generally at little risk to its practitioners. As military strength and capability to project power are diminished, forewarning of an impending attack becomes even more critical so that counterforce can be marshaled and deployed. SIGINT, friendly or otherwise, becomes even more valuable because of the warning it can often provide. It is, in short, a force multiplier in an increasingly austere military environment.

Correlatively, since SIGSEC is directed against the acquisition and exploitation of friendly signals by adversaries (hostile SIGINT), it is often the most critical counterintelligence asset available to military commanders. Without it, against even only moderately sophisticated adversaries, achieving surprise is often difficult or impossible, and a commander may find himself in violation of one of the cardinal principles of warfare. SIGSEC, then, may be viewed as a force multiplier in its own right.

Thus far this article has been, in general, attempting to trace the evolution of friendly SIGSEC and its adversarial counterpart—hostile SIGINT—implicitly involving different governments. Perhaps, in addition, it might be useful to discuss relationships between SIGSEC and SIGINT organizations when they are on the same side. Inherently, there is some competition and the potential for friction between them.

There is a dilemma. On the one hand, SIGSEC authorities may feel obliged to prolif-

* In 1985, a spy ring consisting of former US Navy personnel John Walker, Jerry Whitworth, Arthur Walker, and Michael Walker were convicted of (or pled guilty to) charges of passing classified US intelligence material to the Soviet Union from 1968 to 1985. The ring reportedly helped the Soviets decipher more than one million encrypted US naval messages. —Ed.

erate sophisticated cryptographic systems into environments offering little physical security and with protective caveats offering no real insurance against occasional system loss. Their only alternative is to allow sensitive communications in the government contractual world to continue to be largely unsecured, to offer the private sector no protection against industrial espionage, bank fraud, computer penetration and manipulation, and so on through exploitation of their unsecured communications. Note the earlier discussion of the STU-III program in which 250,000 pieces of first-class voice security equipment have been distributed throughout government and industry.

But this exposure of cryptoprinciples in order to extend coverage amounts to a massive technology transfer. It relieves adversarial SIGINT entities of the often expensive and time-consuming diagnostic procedures involved in determining the basic cryptologic they are up against—how it works—when a new encrypted signal crops up on the air. So at the same time easily exploited plain language communications are denied, cryptanalytic efforts against secured traffic may be facilitated. There may be, of course, a claim that the cryptoalgorithms are so strong that hostile knowledge of them is of no consequence so long as specific keys can be kept unknown. And this may well be so, but there is a disturbing element of hubris in that argument. Be that as it may, the risk was carefully calculated, and the trade-off quite deliberate. And the effects are not confined to hostile SIGINT alone.

By making excellent cryptosystems more or less readily available to any foreign government or private company with a sufficient technological base to adopt or adapt them, SIGSEC complicates the friendly SIGINT job. There is no ready solution to this dilemma. Friendly SIGINT authorities might wish to inhibit the spread of good cryptosystems in vulnerable environments by negotiating some kind of nonproliferation treaty with their counterparts, but this would amount to a denial of legitimate security requirements and would likely fail. SIGSEC authorities might attempt to placate the friendly SIGINTers by trying to reimpose tough security standards on equipment to reduce the probability of their loss, but that too would likely be doomed to failure, particularly if a number of cats were already out of the bag. Further, the reimposing of such standards on nongovernment users might drive them to commercially available equipment of uncertain value. Worse, they might revert to plain language communications to avoid the trouble and expense that strict security rules entail. Other options like fancy protective packaging might price the equipment out of the market.

However such matters are resolved within a given government, a balance between SIGSEC and SIGINT interests ought somehow to be struck because both must be responsive to national security interests. Both are essential, and their respective activities must not be allowed to affect one another adversely.

As noted, cryptology remains at the heart of both disciplines, and there is nothing inherently different about the analytic tools and techniques used in exploiting foreign cryptosystems and those used to ensure the integrity of one's own. Therefore, the two disciplines should cooperate: technical assets like computers ought to be shared, and cross-fertilization should be carried out through the exchange of technical and managerial personnel.

SIGSEC is faced with new priorities in a changing world. Earlier, it was postulated that a key purpose of SIGSEC is to assist users in achieving surprise. The statement was made in the context of tactical or strategic surprise in mil-

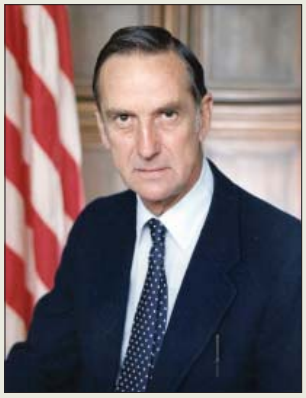
itary operations, but it applies to other arenas as well—be it diplomatic negotiations, a war on drugs, or technological and economic warfare in which we are increasingly engaged. In any of these fields, it may be crucial to deny your opponent foreknowledge of what you're going to do and when you're going to do it. Surprise can offer an enormous advantage whether you are hitting a beach, buying out a company, producing a better mousetrap, or negotiating a treaty. If the other guy knows your bottom line, you aren't negotiating at all—you only think you are.

Technology transfer is accelerating at the same time we are engaged in international competition of increasing scope and scale. There is a need to control that transfer to ensure our economic advantage. Together with other forms of industrial espionage, adversaries can exploit insecure communications within and between contractors and their sponsors and among the contractors, thus frustrating efforts to control the flow of technologies to competitors around the world.

Ultimately, personnel security problems are unlikely to be solved by draconian security measures, polygraphing, surveillance, and the rest. Rather, the answer may lie in technologies that greatly reduce the number of people who can access logic and key—"cleared" or not—technologies, perhaps, like removing hard-wired cryptologic from machines altogether and replacing it with remotely programmable devices that can be changed at will, thus rendering moot the issue of cryptoprinciple loss.

It would appear that the SIGSEC world will continue to face formidable challenges in the struggle to counter hostile SIGINT. There are existing problems, of course, and new ones will arise with innovations by the opposition—an opposition apparently diminished as far as the former USSR is concerned, but at the same time broadened as we engage increasingly in technological and economic warfare on a global scale.

**Editor's note.** This article first appeared in a slightly different form in the Spring/Summer 2006 *Cryptologic Quarterly*.



**David Boak** began his career as a government civilian in 1948 with the Army Security Agency. Boak was known for his contributions to the communications security activities of NSA and held senior positions in the Agency. He served as chief of NSA Pacific (the Agency's senior representative to the US Command in the Pacific) and as commandant of the National Cryptologic School. Honors he received included the Meritorious Civilian Service Award (twice), the Exceptional Civilian Service Award, and the Cryptologic Literature Award. He retired from NSA in 1985. Boak had a distinguished World War II record. He trained with the 10th US Army Mountain Division and served with the OSS, landing in North Africa. He parachuted behind German lines in France in support of the French Resistance. Later he was sent to India and drove the Burma Road into China where he helped train Chinese troops, following which he parachuted with the Chinese behind Japanese lines. He received a BA in English literature from the University of North Carolina and an MA in international affairs from George Washington University. He attended the Air War College and the Federal Executive Institute. He passed away in April 2006 and was inducted into the Cryptologic Hall of Honor in 2010.

# The STONEHOUSE of East Africa

Mark Nixon


US Army Headquarters, Kagnew Station, Ethiopia (now Eritrea). *David Anthony Marcos, Army Security Agency, 1965–1968*

In time, a small World War II Italian radio relay station in Ethiopia, "Radio Marina," would become the US Army's Kagnew Station and home to the Army Security Agency/National Security Agency's (NSA's) STONEHOUSE facility.[1] Among its missions, STONEHOUSE kept an alert ear on Soviet progress in the international space race from the mid-1960s until 1975.

After the Italian surrender of the capital city Asmara in 1941 and a short British occupation of Radio Marina, the US War Department took control of the facilities in 1943. The army quickly recognized that Asmara, with its extremely high altitude 7,600 feet above the Red Sea, was a location uniquely suited for a fixed radio station.[2]

With the signing of a 25-year base rights agreement between the two governments on May 22, 1953, the designation "United States Army Radio Station: Kagnew Station" was formally documented—or simply "Kagnew Station" to all who lived there. *Kagnew* is the Amharic word meaning "to bring order out of chaos."[3] According to legend,

Tract A, US Housing and Consulate (former location of Radio Marina), 1973. *Public Affairs Office, United States Army Garrison, Kagnew Station*

Support structures for the iconic STONEHOUSE antennas are lifted over a railroad bridge along the Asmara-Massawa road, 1964-1965. *Public Affairs Office, United States Army Garrison, Kagnew Station*

it also was the name of the horse King Menelik rode when he rallied the Ethiopian army to victory against the Italians in the 1896 Battle of Aduwa.

Eventually Kagnew Station would provide support to two Army Security Agency stations, a US Navy communications station, a US Army strategic communications Defense Communications Agency facility, a communications facility for the Diplomatic Telecommunications Service, the US Consulate General in Asmara, and the relatively small STONEHOUSE facility.

In 1964-1965, the STONEHOUSE facility acquired two enormous antenna systems, a visual juxtaposition of the modern world against the ancient Ethiopian plateau. The massive custom-built antennas, and the machinery to lift them over bridges on the road to Asmara, had to be shipped from the United States to Ethiopia and then taken on a harrowing journey to a perch overlooking the Red Sea.[4]

As one former NSA dependent recalled to CCH, "I can attest to the frightful properties of the road from Massawa. The Italians ran car races on that road and there were crosses all over the

place where people met their demise."[5]

The culture of Asmara was relaxed in contrast to the seriousness of the STONEHOUSE mission, which included the interception of Soviet signals from deep space and high-altitude communications satellites.[6] Working almost a mile-and-a-half

*Right:* Section of the Asmara-Massawa road near Nefasit.
*US Army Public Affairs Office, Kagnew Station*

*Below:* Road from Massawa to Asmara, above the clouds.
*Courtesy of Don Dement Photography*

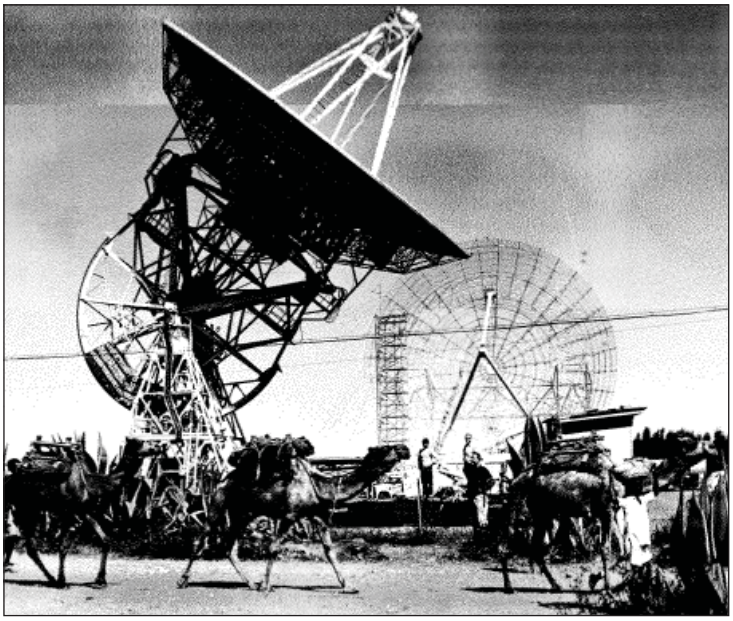

Site forklift sinks into the ground during installation of the 150' antenna. Handwritten captions read, “After this we should have quit,” “We didn’t,” and “Motor pool to the rescue.” *Courtesy of William Semenuk*

*Above:* STONEHOUSE and its massive "ears" were visible for miles outside of Asmara, Ethiopia. *Below:* A camel train strolling past STONEHOUSE and its iconic antennas. *Courtesy of Don Dement Photography*

above sea level, high above the clouds, site personnel often faced challenges similar to those documented during the installation of the 150-foot antenna in the photos on previous page.

Although the work was highly classified at the time, the size of the STONEHOUSE antennas assured that the *location* was not: The dual antennas were visible for miles. With the installation complete, the giant antennas lay poised to glean valuable signals intelligence from outer space.

One typically bright sunny day, the massive antennas were unable to locate a mission-critical signal in support of a US space launch. (STONEHOUSE provided limited support to tracking US space launches in addition to its primary intelli-



Local amenities could be sparse, and visitors to STONEHOUSE from far away were welcome—especially those bearing gifts. *Courtesy of Don Dement Photography*

gence missions.) Fearing that they had failed to support an important and costly US launch, the site staff were demoralized until they were later informed that the launch vehicle had unexpectedly deviated from its course, and there was no way STONEHOUSE could have detected the signal. Their confidence restored, STONEHOUSE personnel continued to provide valuable intelligence from outer space through the mid-1970s.

## When Two Worlds Collide

Life at STONEHOUSE brought unique challenges and rewards. The short commute to STONEHOUSE from Asmara and Kagnew Station had its own form of rush hour traffic: "Commuting to and from the facility on very narrow roads, one would frequently have to stop or slow down due to shepherds moving their flocks of sheep or cattle against the background of the giant antennas."[7] At times, camels caused the holdup.

Many visitors to STONEHOUSE stayed in the homes of those permanently assigned to the facility or at the local Nyala Hotel, where they could count on a wake-up roar from one of Emperor Haile Selassie's lions each morning.

As most American personnel permanently assigned abroad will attest, STONEHOUSE personnel knew they might be called upon at any time to "go the extra mile" to ensure mission success. In 1967, William Semenuk discovered how coveted a bright red Dodge Coronet could be in a nation unaccustomed to that specific kind of luxury. Semenuk was summoned to the station provost marshal's office one afternoon. His car had caught the eye of the Ethiopian minister of transportation, who wished to purchase it for the emperor's annual visit and dental checkup at Kagnew Station. A deal was quickly made, and the car was painted black in time for the emperor's visit. As for Semenuk, he left the office that day with cash in hand, an immaculate Land Rover loaner vehicle, and a story to tell his grandchildren about his personal contribution to international relations.[8]

## The Closing of STONEHOUSE

On January 31, 1975, open warfare between Eritrean rebel groups and the Ethiopian military around Asmara forced American personnel and dependents into emergency shelter at Kagnew Station (by this time administered by the US Navy and known as Naval Communications

Emperor Selassie on the road to Kagnew Station in his new Dodge Coronet, 1967.
*Courtesy of Claude Warwick*

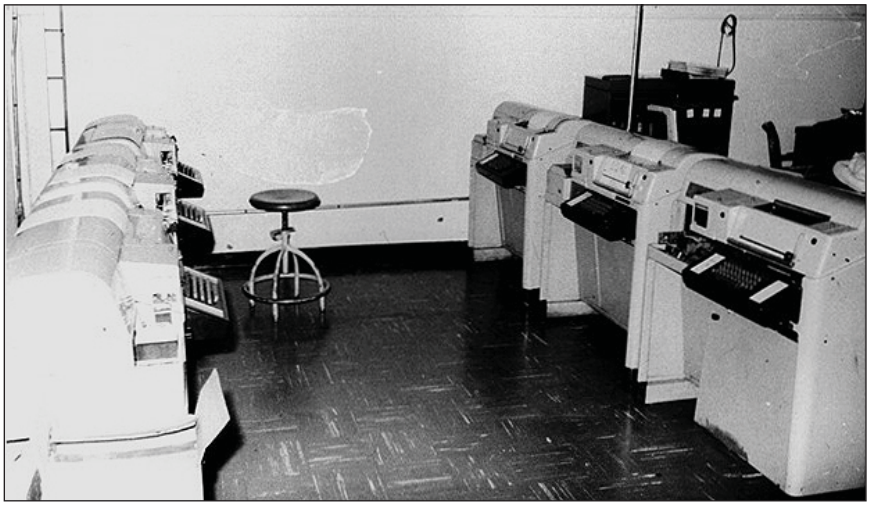
Station Asmara) and at the American consulate. Within days, American dependents were evacuated to the Ethiopian capital of Addis Ababa before leaving for Europe and the United States.

As it became evident that STONEHOUSE's days were numbered, NSA established an Asmara Task Force. NSA quickly assigned a crisis manager to lead a team consisting of all cognizant NSA organizations. The team took up residence in the National Signals Intelligence Operations Center on February 2, 1975, to provide immediate assistance to site operations. Of paramount importance to the team were the effective evacuation of personnel, disposal of valuable intelligence equipment, and the cessation of STONEHOUSE operations as the uncertainty over the outcome of the violence continued.[9]

On February 6, 1975, STONEHOUSE dependents evacuated from Asmara and attempted to leave the country via Addis Ababa airport. One scene chronicled in the "DoD STONEHOUSE Facility Seminar Report on the Evacuation and Closure," accepted by DIRNSA on July 23, 1975, typified the situation:

> The families experienced difficulties in exiting Addis Ababa Airport. They apparently required exit visas which they did not have. [Name withheld] recited excerpts from the Declaration of Independence, the National Anthem and the Ethiopian/US Treaty, and the airline offi-


Brass plate mounted on obelisk at Kagnew Station entrance, as seen on the first page of this article. The plate is now in storage at the National Cryptologic Museum. *NSA photo*



Teletype equipment at the STONEHOUSE facility used to communicate with NSA, Fort Meade. *Courtesy of family of David Williams, former chief of STONEHOUSE*

cial finally relented and allowed them to leave. Because of her action, two other dependent families of the American Consul in Asmara were also allowed to board the plane.

Once most of the dependents had departed from Asmara, the Asmara Task Force began to focus on the safety of the remaining site personnel and the protection of sensitive equipment and information.[10]

Highly sensitive equipment resident at STONEHOUSE included the KG-13 cryptographic key generator and the KW-26 and KW-7 cryptographic equipment for teletypewriters. The KW-26s were not in use at the time and were destroyed first. Shortly thereafter, the KG-13s were destroyed, along with all other cryptographic material—except the KW-7s, which were necessary to protect the primary remaining communications link to the American consulate.

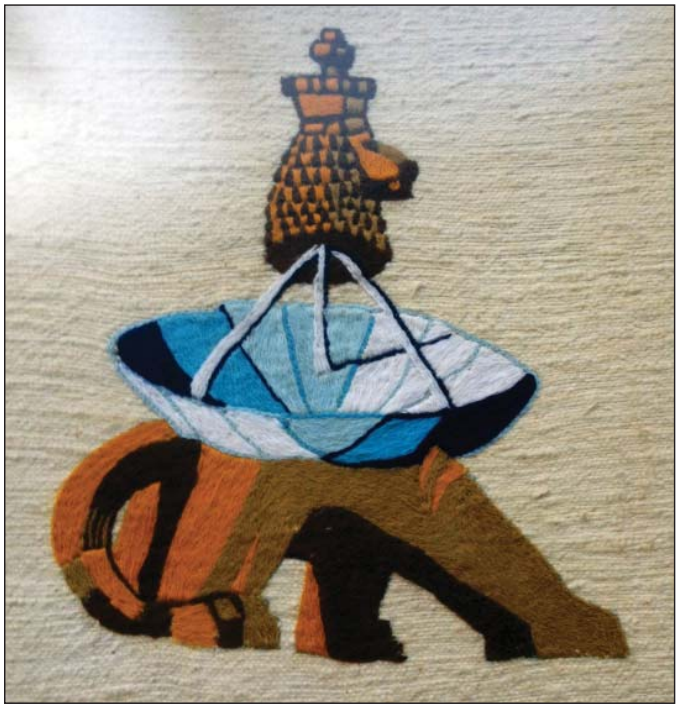
As a testament to American manufacturing and NSA's pride in ownership, the STONEHOUSE station chief would later observe, "…the manufacturing standards of NSA's crypto machinery are sufficiently high that total destruction, to the point where no identifiable elements remain, is not always possible.… Particularly resistant are the little metal ID plates carrying the security classification, the equipment nomenclature, and the *Agency's name*"[11] [emphasis added].

Packing and shipping of government property continued for another month. Eventually, the remaining property was returned home as NSA's remaining personnel departed.[12] At the request of the consul general, three NSA contractor personnel stayed behind to perform teletype main-

tenance, radio support for the consulate, and medical support for the remaining American community.[13]

On March 4, 1975, the sun set for the final time on STONEHOUSE operations.[14] America's signals intelligence team had kept an alert ear pointed toward the heavens from a remote land. Embedded in an ancient culture, this team truly went where no SIGINT personnel had gone before and in a style uniquely their own!

*Top:* Document destruction at STONEHOUSE with 150-foot antenna in background.
*Bottom:* Destruction of KG-13 equipment cases at STONEHOUSE. *Both photos, National Security Agency*



Unofficial STONEHOUSE logo created when NSA took over site operations; it incorporates the Ethiopian lion of Judah. *Courtesy of family of David Williams, former chief of STONEHOUSE*

## Notes

1. Public Affairs Office, *A History of Kagnew Station and American Forces in Eritrea* (US Army, 1973), 40.
2. Ibid.
3. Theodore M. Vental, *The Lion of Judah in the New World: Emperor Haile Selassie of Ethiopia and the Shaping of Americans' Attitudes toward Africa* (Santa Barbara, CA: ABC-CLIO), 2011.
4. Former Army Security Agency employee William Semenuk discussions with author, March-May 2016.
5. Comment to author from former NSA dependent who lived in Asmara and is now an NSA employee, January 19, 2016.
6. CCH interview with former NSA employee John O'Hara, May 18, 2016.
7. Ibid.
8. Discussions, Semenuk.
9. US Department of Defense, *STONEHOUSE Facility Seminar Report on the Evacuation and Closure* (Washington, DC: US Department of Defense, June 1975), C-2, C-3.
10. *STONEHOUSE Facility Seminar Report*, B-14.
11. *STONEHOUSE Facility Seminar Report*, B-16.
12. *STONEHOUSE Facility Seminar Report*, B-21.
13. Ibid.
14. Ibid.

**Editor's note.** This article first appeared in a slightly different form in the 2016-02 *Cryptologic Quarterly.*

**Mark Nixon** has held many positions with the National Security Agency during a 40-year career. Indulging a lifelong interest in history, he joined the Center for Cryptologic History as a staff historian in 2015 with a concentration on aspects of communications security and information assurance. Mr. Nixon holds a B.S. degree in Natural Resource Economics from the University of Maryland, College Park, and in 1998 received an M.S. degree in Contract and Procurement Management from the University of Maryland, University College.

# A Layman's Guide to the Mysteries of Linguistics

Jack Gurin

This article, originally written in 1978 by former NSA linguist and Cryptologic Hall of Honor member Jacob "Jack" Gurin, introduces readers to the complex world of linguistics. While some of the theories explored here (like the idea of a universal grammar) have been challenged by subsequent scholarship, the article provides valuable insights into the state of linguistic understanding 40 years ago. —Ed.

Although they are often referred to by the same term, "linguist," the foreign language specialist and the scientific linguist tend to be worlds apart in the nature of their scholarly pursuits. Multilinguists often find that nothing in their training or experience prepared them for a session on computational linguistics, syntactic theory, or case grammar. What follows is an attempt to introduce the uninitiated to some basic concepts and purposes of linguistics without resorting to the esoteric jargon and convoluted reasoning that seem to characterize so much of what is written on the subject.

When I began to study language as a youngster in school, the course I planned to follow seemed clear enough. I could select first one, then, later on, another foreign language, and perhaps even a third if my enthusiasm remained high and my grades were satisfactory. These courses in foreign languages did not make me a linguist, for that term was reserved for those who were fluent in a foreign language, or who were to be admired for their scholarship in some language studies only in its written form, or who, although not really very good, earned their living as translators or interpreters. But it all began, for my friends and me, with the study of foreign language in junior high or high school. If one persisted, one could become a linguist.

I thought I knew what a linguist was. The late Dr. Sydney Jaffe was a superb linguist; among his many accomplishments was his mastery of French literature, his doctoral dissertation being on the language of the French stage in the 19th century. Norman Wild and Jack Murphy are obviously linguists; they know, and know well, more languages than anyone has a right to know.* I was a linguist

*Dr. Sydney Jaffe, the founder of NSA's Crypto-Linguistic Society, is a member of the Cryptologic Hall of Honor. Norman Wild, also a member of the Cryptologic Hall of Honor, was an expert in Cambodian, Chinese, Japanese, Korean, Lao, Thai, and Vietnamese. John D. "Jack" Murphy, who knew at least a dozen languages, was once referred to as "a one-man-gang linguist." —Ed.

during the Second World War because I employed the Japanese language as my military occupational specialty, translating captured documents and interrogating prisoners of war.

But I find now that my right to use the title "linguist" is disputed, as is the right of almost all of my colleagues who struggled through to some approximation of master of one or more foreign languages. (I say "almost all of my colleagues" because some are accepted by the challengers as being one of their own.) On several occasions I have had to clarify my status after being introduced to a scientist or engineer as a linguist. I have had to add, almost apologetically, that my special field was foreign languages, not linguistics, and each time I was pained to see the light go out in the eyes of my new acquaintance and the lines harden around his mouth. A more acceptable term, I gather, would have been "polyglot" or "multilinguist."

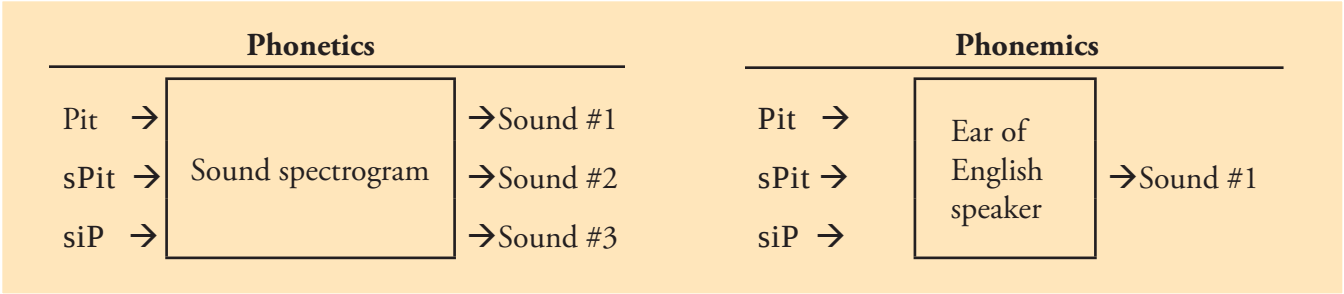
This time I decided to approach the subject of linguistics with justifiable caution, and I find that if one retains one's courage, it is not nearly so formidable. As a matter of fact, it may be a little pitiable, since there is a good chance that these earnest scholars are chasing a will-o'-the-wisp.

To begin with, I had to agree with the scientific linguists' claim that the ability to speak a language fluently does not necessarily confer a *linguistic* knowledge of it—this is to say, an understanding of its systematic processes and structures—any more than the ability to play a good game of billiards confers or requires any knowledge of the laws of mechanics that operate on the billiard table or the ability to drive a car competently implies an acquaintance with the operating principles of the internal combustion engine. I also had to accept the fact that the study of linguistics might or might not involve a foreign language. As a matter of fact, most of the work done by American linguists today is in the English language, which seems to pose enough problems to keep them occupied for some time to come.

Perhaps the best place to begin is with the near-miracle that occurs in each child as he masters the rules of his native language. I believe it is fair to say that, by the age of seven, a child's linguistic competence is, to a great extent, similar to that of an adult. He will learn more words and phrases, to be sure, and one can hope that his style of speaking and writing will improve with time, but by that age he has mastered the system. He is comfortable with the phonological system of his language; he is capable of understanding and producing an indefinite number of sentences; and he can make judgments about grammaticality, ambiguity, and paraphrase.

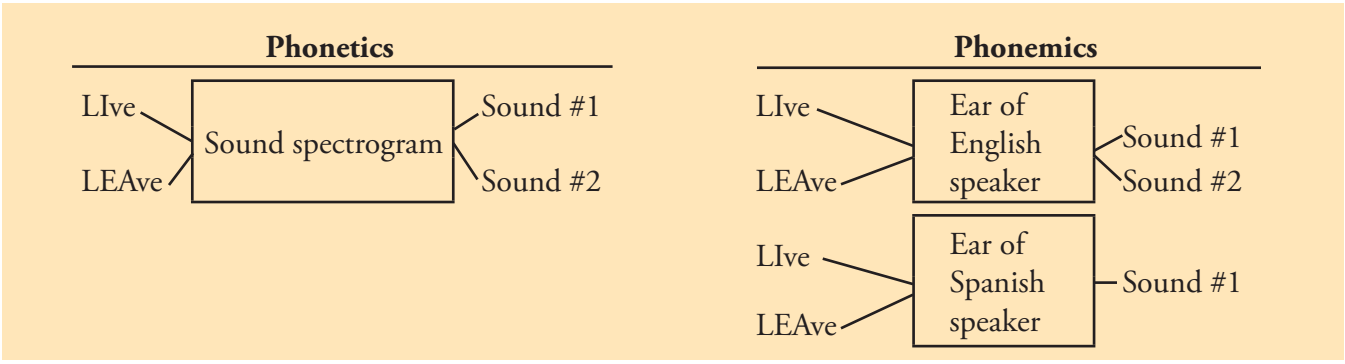
It might be useful to look at these aspects of the language system more closely. To begin with, it is important to distinguish between *phonetics* and *phonemics*. Phonetics gives us an objective description of speech sounds and how they are produced, without regard to the language. Phonemics describes and classifies the sounds of a specific language according to the way those words are referred to in the consciousness of speakers and listeners of that language. I think I am making phonemic noises, but actually the noises are phonetic sounds, which others hear through their phonemic filter. The filter permits them to discount my New York accent and any other imperfections in my delivery.

Perhaps the following illustration will make the distinction clear:




The speaker of English will accept the *p* of "pit," of "spit," and of "sip" as variants of a single entity, a phoneme spelled *p*, even though, as sounds, they are very different. In "pit" the *p* is strongly uttered and is followed by a perceptible puff of breath; in "spit" it is gentler and unaspirated; in "sip" it is imploded—the lips are not opened.

Here is another example showing the dependence of phonemics on a particular language:




*Live* and *leave* have vowel sounds that, while similar, constitute two different phonemes in English. Everything else in the two words being the same, the distinction between the vowel sounds of *leave* and that of *live* makes for a basic difference in the meanings of the two words. On the other hand, a speaker of Spanish would regard them as two variants of the same *i* sound, and if the Spanish word *vivo* used either variation, the meaning would not be affected. One version might sound deliberate and emphatic, while the other might appear hurried or careless.

The child, then, knows which sounds belong in his language and which do not. He has a firm grasp of the phonemic scheme of his language. He will hear and be able to mimic new words in his language, for they will be made up of familiar phonemes. Even nonsense words are repeatable because of this.

The phonemic scheme, by the way, includes stress and intonation. With regard to stress, we recognize the difference in meaning for *con*test and con*test*, con*tract* and *con*tract, and so on. Stress also permits us to differentiate "the White House," where the president lives, from "the white house," where one of our neighbors lives, as well as "blackbird" and "black bird," "dumbwaiter" and "dumb waiter," and so on.

The child will find it funny if you violate the rules for intonation in the sentence. "What's com-

ing up—the street?" by providing a rising inflection to the last word in the sentence. Another example of the not very elegant humor arising from a violation of the inflection rules is the sentence "What's for dinner tonight—mother?"

Evidently the phonetic scheme is secure enough to permit an occasional exception to come in without changing the basic nature of the scheme. The "shm" combination just does not occur at the beginning of any English word, but that did not prevent Al Capp's fabulous creature, the Shmoo, from being taken to the hearts of many readers of his comic strip, name and all. And the "ts" combination at the beginning of a word occurs only in the word spelled "tsetse," as in tsetse fly, but it doesn't provide any special difficulty for speakers of English, who normally adapt it to an already existing pattern: "tetse." But other combinations are a different matter. Many students of Russian never do master the initial sounds of "kto" and "chto," which, being in the phonemic scheme for Russian, pose no problems at all for little Ivan and Masha. Americans tend to insert a vowel between the *k* and *t* or the *ch* and *t*.

I said earlier the child can make judgments about grammaticality, ambiguity, and paraphrase. If you change the word order, or substitute a noun in the place in a sentence where one would expect a verb, the child will sense that your utterance is not grammatical. For example, if you were to say "Asleep is your sister?" you may be sure that you will be rewarded with a strange look. And if you ask the child "Please ball the kick to me," you won't get the same reaction as if you say "Please kick the ball to me." You broke the grammatical rules.

As for *ambiguity*, there is more than one meaning of each of the following, and one cannot be sure which is meant without clarification.

1. John was too far away to see.
2. Careless pedestrians and drivers are dangerous.
3. Smoking cigarettes can be a pain.

For any native speaker of English, rephrasing these ambiguous sentences clears up the matter immediately.

1. John was too far away to be seen.
2. Careless pedestrians and impatient drivers are dangerous.
3. Smoking cigarettes, left in an ashtray, can be a pain.

The point here is that the rules of the language permit both the ambiguity and ways to remove it.

*Paraphrase* is the converse of ambiguity. Two or more sentences, outwardly different, all mean the same thing. Even the youngster will know, without hesitation, that any of the variations indicated in the following sentences may be used without altering the meaning.

4. The strict teacher / The teacher *who is strict* } { *knows* / *knows that* }

*the student did not write* { *the assignment down.* / *down the assignment.* }

(Note that the word order was changed in the last part of the sentence.)

But a different language change in the word order can change the meaning of the sentence:

5. *The student knows that the strict teacher did not write the assignment down.*

And another change in the word order makes the sentence ungrammatical:

6. *The strict teacher knows that the student did not down write the assignment.*

Finally, every native speaker of English can differentiate between the meaning of the following sentences:

7. *John is eager to please.*
8. *John is easy to please.*

They look similar and even sound similar. But they are different in their very essence, and to illustrate that, one needs only to turn them around. You can say:

9. *It is easy to please John.*

but not

10. *It is eager to please John.*

How lucky for us that we know the rules of the language so well! But what are they?

The traditional grammatical concepts are based largely upon the system originating with the Greek grammarians, who were describing their own highly inflected language. The Greek grammatical categories included such items as numbers, gender, and case, which apply to nouns, adjectives, and pronouns; also tense, mood, voice, person, and number, which apply to verbs. Many languages that are still fairly close to their Indo-European origin permit a neat breakdown into *parts of speech*—nouns, adjectives, pronouns, verbs, adverbs, articles, prepositions, conjunctions, interjections—but it is important to realize that other languages do not.

It was only when the grammatical system of the old Indo-European languages was applied to languages of different families, such as Chinese or the American Indian tongues, or even to the languages of the same family which had evolved away from the original family, that one realized the system was not universally applicable. Modern linguistics has attempted to create a new grammatical system to account for all languages—or at least to come a lot closer than the old descriptions.

Traditional grammars that we have used, either for our own language or to study a foreign one, are so cluttered with detail that it is extremely difficult to find underlying general rules. They are far from trustworthy models for the representation of the language if one thinks of the language as it exists in the minds of native speakers.

Perhaps it would be best to distinguish between the grammar that seeks to be *descriptive*, bringing to light the knowledge that underlies actual language use, and the kind of grammar that one usually encounters in schools, the *prescriptive*, which contains the rules for what the language *should be*.

Prescriptive grammars attempt to change actual language use by prohibiting certain forms and insisting on the use of others. Such prescriptive efforts occasionally succeed in creating attitudes about language that are difficult to change, even though they are awkward to defend. There are many who cringe at sentences such as:

*I don't have none.*
*You was wrong about that.*
*Charlie is taller than me.*

There is nothing really wrong with any of these sentences. But in 1762, a British prescriptive grammar was written by Bishop Robert Lowth titled *A Short Introduction to English Grammar, with Critical Notes*. Partly influenced by the Latin language and partly because of personal preference, Bishop Lowth decreed that "two negatives make an affirmative"; that *you* should be followed by *were*, whether singular or plural; and that in comparative constructions, the subject form of the pronoun should follow *than* (*Charlie is taller than I*). He had set himself up in business as arbiter of language style and had no right to

do so. But his grammar was widely used in the schools, and people gradually came to accept this man's personal opinions as gospel. It is interesting to note that, 200 years later, it is still natural for people to use these prohibitive forms, and it takes vigilance to keep them out of the conversations and writings of "decent" people.

Another of Lowth's preferences was for "I would rather" as opposed to "I had rather," but both forms have been used freely by educated speakers. Eighteenth-century grammarians had legislated that "between" was to be used only with pairs and "among" when larger numbers are involved. Most of the time this rule is observed, but one also finds "An agreement between three people," "between us lawyers," "between meals," and "a number between one and five." The distinction between "shall" and "will," which was carefully drilled into my head in school, I now ignore, as do almost all of my contemporaries. The rules for the use of these words, laid down arbitrarily by Lowth and others, were the bane of students for at least 200 years.

We are still subject to the dicta of individuals who prescribe the correct usage of words in the English language, and many of us lean heavily on their advice. But in a recent supplement to the Sunday *Washington Post*, Jim Quinn took a strong stand against those who prescribe "proper" usage of the English language.[1] He gives many examples from respected works of literature of flagrant violations of such currently honored rules, no doubt horrifying many who consider the violations to be prima facie evidence of illiteracy or at least poor taste. He arrives at two possible conclusions:

> Something is wrong with all native-born speakers of English. Alone of all people in the world we are unable to learn our own language.
>
> Or else—something is wrong with the rules. And the books that print the rules. … And in fact it is the books … that are wrong.[2]

The linguistic specialist would probably argue that the true test of correctness is de facto usage by the social group at the highest social and educational levels. But it is not likely that this sensitive issue can be resolved here.

By the way, modern linguistics does not deny the existence of differences in language use. It fully recognizes that some usages are restricted to members of particular social classes or regions of the country. In fact, the field of sociolinguistics is devoted to the study of such social differences in language, and the investigation of regional dialect differences has been a major concern of American linguistics for at least fifty years.

Until late in the nineteenth century, linguists worked in historical linguistics. Perhaps the most illustrious breakaway from the old approach was Ferdinand de Saussure, who proposed that an entirely different kind of study was the only scientific approach to language. In a series of lectures given at the turn of the century, Saussure established some of the bases on which modern linguistic thinking is built. Although he drew on a restricted range of languages, mostly the familiar languages of Europe, he developed ideas that appear sound today.

He saw two fundamental dimensions of language study:

- *synchronic*, in which languages are treated as self-contained systems of communication at any particular time; and
- *diachronic*, in which the changes to which languages are subject over the course of time are treated historically.

He made the distinction between the linguistic competence of the speaker, which he called *langue*, and the actual utterance, which he called *parole*. He also showed that any *langue* must be thought of and described synchronically as a system of related elements (lexical, grammatical, and phonological) and not as an aggregate of self-sufficient entities.

Today's linguists make a distinction in the case of competence and performance as was made by Saussure in *langue* and *parole*. Linguistic competence is the term for subconscious knowledge about sounds, meanings, and syntax possessed by all speakers of a language. After all, knowledge of the language is by no means conscious. Speakers of a language are not aware of what they know; they cannot provide a complete description of the sounds they use when they speak, nor can they state all of the rules they follow in converting their thoughts into speech or writing. And since linguistic competence is a mental reality, not a physical one, the isolation of competence from performance is a difficult task. Only performance is directly observable.

The challenge of American Indian languages provided a good part of the stimulus for synchronic linguistics in America during the 1920s and after. In this field, for the most part, the linguist learned the language and worked out his descriptive analysis at the same time. Two American linguists who worked with Indian languages were Edward Sapir and Benjamin Lee Whorf. Sapir emphasized the strong relationship between language and culture, while Whorf, an engineer, also stressed the scientific approach. According to Whorf,

> Linguistics is an experimental science. Its data results from long series of observations under controlled conditions, which, as they are systemically altered, call out definite, different responses … Linguistics has developed techniques which enable it to specify exactly the patterns with which it is concerned.[3]

Whorf developed another interesting point as a result of his studies into the Hopi language, a semantic rather than phonemic one. He posed the problem a European would have in attempting to discuss geometry with a Hopi Indian. Newtonian geometry requires space and time as coordinates, categories also found in most European languages. [Whorf believed t]he Hopi did not have a grammatically necessary distinction of time as [he knew] it. Instead, [Whorf thought] the Hopi were required to distinguish degrees of intensity. He [believed] that he and the Hopi could not discuss the same world.

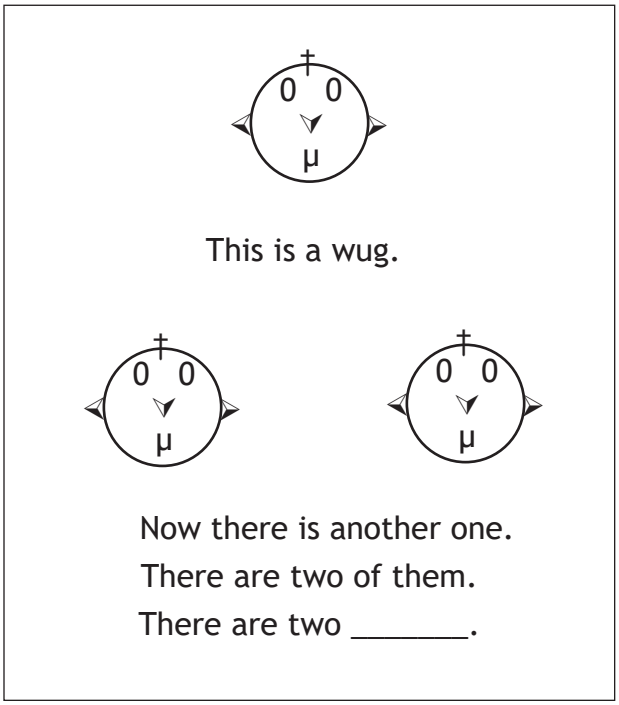
Leonard Bloomfield, another well-known name in American linguistics, started a tradition of empirical linguistic description in an effort to make linguistics an autonomous science. He was profoundly influenced by the behaviorist psychology of John B. Watson and others, so fashionable in the 1920s and 1930s. His attitude led to an emphasis on classification and description as the sole, or at least as the principal, work of scientific linguists. More recently, linguistics has shaken free from Bloomfield's influence and has again taken up the goal of explaining, as well as describing, language. Bloomfield also concerned himself deeply with "meaning," seeking to reduce it to the psychological concept of stimulus and response. As a mechanist, he dismissed ideas like "mental images" or "feelings." To him, all these were ultimately bodily processes.

Noam Chomsky, by the way, maintains that the concept of "grammatical" cannot be identified with "meaningful" or "significant" in any semantic sense. He points out that the following two sentences are equally nonsensical, but that

any speaker of English will recognize that only the first is grammatical:

1. *Colorless green ideas sleep furiously.*
2. *Furiously sleep ideas green colorless.*

Let us return to the children to examine another aspect of language—morphology. Morphological rules are those that govern the changes made in words in order to equip them for their roles in expressing different meanings. Plural endings, for example, are provided to nouns when the count is more than one. Past tense endings are provided to verbs to indicate that the event occurred some time ago. A child exposed to English morphology quickly learns these morphological rules, as indicated by studies that employ nonsense words, never heard before by a child, to which he is asked to give the correct morphological form. In one test, a number of nonsense words were made up, following the rules for possible sound combinations in English. Pictures to represent the nonsense words were then drawn on cards, and a text, omitting the desired form, was inserted onto each card. An example, to illustrate the plural form by adding *s*, is shown in the figure below.




Of course, this proved to be no great problem to the children. Examples of some of the other questions are given below:

1. This is a gutch. Now there is another one. There are two of them. There are two _____.

2. (Picture of a man with a steaming pitcher on his head) This is a man who knows how to spow. He is spowing. He did the same thing yesterday. What did he do yesterday? Yesterday he _____.

3. (Picture of a dog covered with irregular green spots) This is a dog with quirks on him. He is all covered with quirks. What kind of dog is he? He is a _____ dog.

4. (Picture of a man doing calisthenics) This is a man who knows how to mot. He is motting. He did the same thing yesterday. What did he do yesterday? Yesterday he _____.

5. (Picture of a man balancing a ball on his nose) This is a man who knows how to zib. What is he doing? He is _____. What would you call a man whose job it is to zib? A _____.

This test, which I am sure you did not find particularly difficult, was completed satisfactorily by children aged four to seven. While the answers were not always right so far as English is concerned, they were consistent and orderly answers. There can be no doubt that children in this age range operated with clearly delimited morphological rules.

Any attempt to describe the subconscious knowledge of grammatical rules possessed by native speakers of a language is an ambitious undertaking, and one that offers no assurance of success. The investigator must rely on indirect evidence, then formulate a reasonable hypothesis about the kind of knowledge people must possess in order to behave as they do in language.

No individual speaker of English will ever produce or hear all of the sentences of his language. On the basis of his knowledge, however, he is potentially capable of producing any one of them or of comprehending any grammatical sentence he encounters. In other words, productivity in language results from the speaker's underlying linguistic competence, which is never reflected completely by his performance. Since speakers are capable of producing an indefinite number of grammatical sentences, they must have a mastery of the principles that generate, or produce, those sentences. These principles constitute the grammatical rules of the language. In addition to generating sentences, however, the grammar must also reflect the knowledge underlying the speaker's ability to determine when a sentence is ungrammatical, ambiguous, or a paraphrase of another sentence, as was mentioned earlier.

Many polyglots are put off quickly, when they look into theories of languages or generative grammars, by the appearance of the rules, which look like equations or formulae. We are much more comfortable with a rule that may state that "verbs denoting desire require an object in the dative case." But for a theory of language that is not dependent on the language or the speaker (or his intuition) it will be necessary that it be couched in formal terms, explicit in its statement of relationships, so that by a series of almost mechanical steps the forms of the language may be produced in proper sequence and combination, with a minimum of interpretation left to the intelligence of the reader or user of the theory. The steps should be as clear to a speaker of Japanese as to one who thinks in English.

Think of the relationship between the words *essay* and *translate* in the following sentences:

*The essay was difficult to translate.*
*Now you have to translate the essay.*

The relationship is the same.

Now look at the relationship, obviously a different one, between the words *student* and *translate* in the next two sentences:

*The student was anxious to translate.*
*The student has to translate the essay.*

Again, the relationship is the same, but one cannot substitute one set of relationships for the other and come up with:

*The essay was anxious to translate.*
or
*The student was difficult to translate.*

A theory of language must come up with an explicit basis for explaining the native speaker's understanding of the relationship between the sentences. Similarly, it must show the difference between the following sentences, which look similar:

*The candy is to eat.*
*The man is at work.*

Another group of sentences that a language theory must account for:

1. *His swimming was a mistake.*
2. *His swimming was mediocre.*
3. *His swimming was fantastic.*
4. *For him to swim was a mistake.*
5. *His having swum was a mistake.*

Here we must account for the fact that the phrase "his swimming" is understood in differ-

ent ways in (1) and (2); that (3) can be understood in two ways; that the way in which (1) is understood is closely related to the way in which (4) and (5) are understood; and the "His having swum was fantastic" is no longer ambiguous. All of these must be accounted for, as well as the fact that we do not say "For him to swim was mediocre."

While there is no way to prove the theory, some linguists believe that when a person speaks, he starts out with a set of concepts he wishes to express; he then converts those abstract concepts into a form suitable for expression in speech. When someone listens, he hears the sounds produced by another; he then attempts to convert those sounds into the meanings the speaker has tried to convey. The same process holds for writing and reading as for speaking and listening.

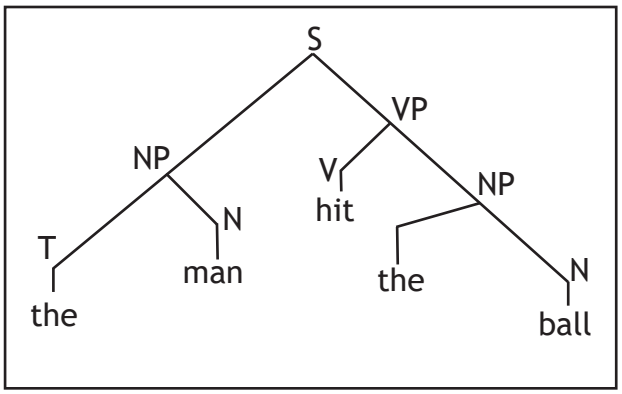
Meaning originates in the mind, and linguistics includes the study of the relationships between meaning and form. The mind is not directly observable; so there is no reason to assume that every aspect of the process will be directly observable. The form in which a sentence is expressed is called the *surface structure* of that sentence. By examining the surface structure, one investigates only the communication channel; other parts of the system, pertaining to meaning rather than to surface form, are not available for direct examination.

The other side, the one that some linguists believe approaches meaning (a position that other linguists attack vigorously), can be referred to as *deep structure*. These linguists account for the relationship between the deep structures and the surface structures by means of a set of syntactic rules known as *transformations*.

The deep structure of a sentence contains all the concepts that speakers understand to be involved in the sentence, regardless of how the sentence comes out in its final form. Sentences that are paraphrases of one another therefore will have the same deep structure, but ambiguous sentences will be quite different.

Determination of deep structures is a complex and difficult undertaking. Nothing is really known about the nature of the deep structure level of language, and the professional literature of linguistics contains debates over whether particular deep structures proposed for even the simplest level of sentences are actually valid. Some linguists have argued that a level even more abstract than deep structures is necessary to account for meaning.

At this point let us look at a simple example of transformational analysis. The sentence "*the man hit the ball*" is a terminal string generated by a set of six rules—the "grammar" of that particular sentence. The following is a diagram representation of the derivation of this string. Transformational-generative grammarians widely use diagrams such as this one because they show at a glance where the parts of the string come from.




(i) Sentence →NP + VP
(ii) NP →T + N
(iii) VP → Verb + NP
(iv) T→ the
(v) N → man, ball
(vi) V → hit

→ means Converts to. S, sentence. NP, noun phrase. VP, verb phrase. T, article. N, noun. V, verb.

The object of the preceding is to determine the structure of a simple sentence and to prepare for relating it to other sentences that may be encountered. The way these sentences are related to one another can be specified by transformation rules. These rules may involve deletions, additions, and changes of order, as well as taking two or more simple sentences and linking them into a more complex structure.

For example, if we think of our sentence "*the man hit the ball*" as

| | | | | | | |
|---|---|---|---|---|---|---|
| $NP_1$ | + | (*auxiliary*) | + | *V* | + | $NP_2$ |
| *the man* | | (*past*) | | *hit* | | *the ball* |

We may show how it may be transformed into the passive voice, "*the ball was hit by the man*" as follows:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $NP_2$ | + | (*aux*) | + | *V* | + | *by* | + | $NP_1$ |
| *the ball* | | was | | *hit* | | *by* | | *the man* |

Similarly, we can transform "*the man hit the ball*" into a yes-no interrogative sentence, "*Did the man hit the ball?*" or a wh__ interrogative sentence, "*Who hit the ball?*" and so forth. All these sentences relate to each other and, some will maintain, are transforms of the underlying same structure, "*the + man + past + hit + the + ball*."

Why should we involve ourselves in this seemingly impenetrable jungle of philosophy and mathematical logic? Where might we end up if we follow it?

Well, for one thing, it could lead to an understanding of the universals of language, transcending the barriers of individual languages and dialects. To learn a language means to learn the structures underlying sentences, as well as their surface forms. Yet deep structures are not observable; they are highly abstract. How, then, do children manage to learn them? A hypothesis shared by many modern linguists and psychologists is that human beings are born with an innate capacity to learn languages, and this capacity includes the universal properties of the language.

In his *Aspects of the Theory of Syntax*, Noam Chomsky writes:

> A theory of linguistic structure that aims for explanatory adequacy incorporates an account of linguistic universals, and in it attributes tacit knowledge of these universals to the child. It proposes, then, that the child approaches the data with the presumption that they are drawn from a language of a certain antecedently well-defined type, his problem being to determine which of the (humanly) possible languages is that of the community in which he is placed. Language learning would be impossible unless this were the case.

As a consequence of these assumptions, Chomsky sees it as one of the main tasks of linguistic theory to

> develop an account of linguistic universals, that, on the one hand, will not be falsified by the actual diversity of languages and, on the other hand, will be sufficiently rich and explicit to account for the rapidity and uniformity of language learning, and the remarkable complexity and range of the generative grammars that are the product of language learning.

Just as some newborn animals have a brief period during which they are able to learn what they must know to survive, so do humans during their early years, or so it seems. Konrad Lorenz found that newly hatched ducklings regarded the first thing they saw as "mama" and followed it devotedly after that. He arranged that his assis-

tant, wearing brightly colored socks, should be at the right place at the right moment, and so thereafter the ducklings followed the socks wherever they might go. Perhaps the human child begins life with a super-capability to learn his own language, good for only about the first seven years of life. And perhaps he has, in addition, a foreknowledge of the universals of language on which to build his skills.

The study of universal grammar is the study of the nature of human intellectual capacities. The grammar should describe the conditions a system must meet to qualify as a human language, conditions that will permit the development of language knowledge by the individual from language experience. In a sense, linguistics is a subfield of the psychology of cognition.

In spite of years of continuing interest and scholarship in the subject of language, we are no closer to understanding the miracle of spoken human communication than we were. Technological advances permit us to examine spoken utterances by machine, and we can display the spoken word graphically. We can measure

**Jack Gurin** was one of NSA's leading language analysts. He retired from the Agency in 1980 and passed away in 2004. In 2007, Gurin was inducted into the Cryptologic Hall of Honor. This article was originally published in the Winter 1978 issue of *NSA Technical Journal*.

A graduate of New York University, Gurin has been described as "… a moving force … always … where the action was." He was a published translator of Tolstoy, a World War II US Army captain who served as a Japanese translator and interpreter, and a Russian language analyst and speech researcher who became NSA's chief of language research. Gurin epitomized the 21st-century term "change agent." He formed the Plain Language Exploitation Group in 1947 after target changes led to a loss of exploitable encrypted intercept. He expanded his group in nontraditional ways: breaking precedent in a segregated organization, he systematically hired and trained African Americans in cryptology.

Gurin also led the way in what are now known as the less-commonly-taught languages. He predicted, correctly, that the liberation of nations from colonial empires would result in many targets shifting to languages NSA was unprepared to handle. He conceptualized and implemented a program to produce reference and training materials in these languages. His foresight helped prepare NSA/CSS for today's challenges. Convinced that American cryptologists would eventually be swamped by voice communications, Gurin drove technology solutions that were unheard of in his time. He pushed to digitize dictionaries so that language analysts could quickly conduct research, and sought to create voice recognition systems. While his vision outpaced some of the technological solutions available at the time, every one of his ideas is a reality today.

the component structure and even imitate the human voice reasonably well without using the human vocal apparatus. But we are a long way from constructing a machine that will understand speech, and we may never succeed in that task.

The study of linguistics is in some ways a philosophical tour of never-never land, with questionable application to any of the practical problems that concern us. But it is also likely that, if the nature of language were better understood, we might be able to devise ways to use our people much more efficiently, leaving the donkey work, now dependent on the human ear with minimal demands on the brain, to the machine instead.

## Notes

1. Jim Quinn, "Plain English," *The Washington Post Magazine*, December 11, 1977.
2. A comment from NSA linguist Jim Child: "It is always possible to admit to the validity of prescriptive rules as enforcers of language etiquette ('don't set the table with the knife at the left of the plate,' etc.) and the fact of language change as historical reality. Most people mix these very different things."
3. Benjamin Whorf, "Science and Linguistics," in J. B. Carroll, ed., *Language, Thought and Reality* (Cambridge, MA: M.I.T. Press, 1956). Some of Whorf's ideas regarding time have been challenged by members of the linguistics community since this article was originally published in 1978. —Ed.

**Editor's note.** This article appeared in a slightly different form in the Fall/Winter 2008 *Cryptologic Quarterly*.

# A Space Worthy of its Namesakes: The Friedman Conference Center

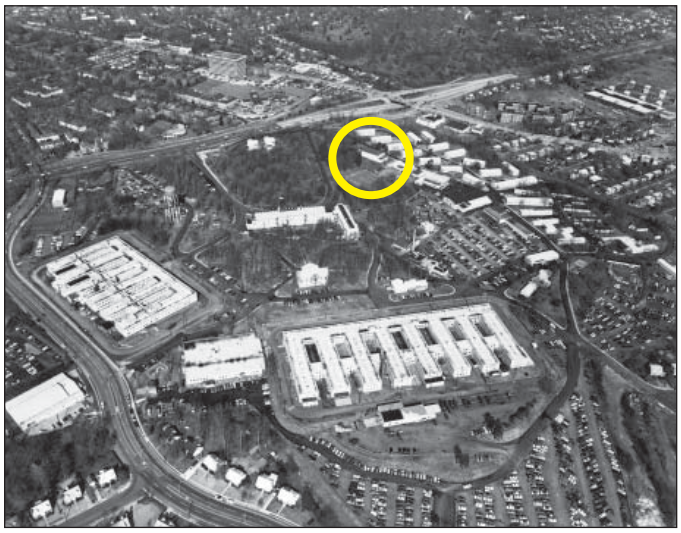
Sarah Parsons

Today, when NSA employees hear the word "Friedman," they are likely to think first of a place, not a person. NSA has been naming rooms, buildings, and streets after cryptologic pioneers since the 1970s. None are as synonymous with their namesake as the Friedman Auditorium, named in 1975 for "the dean of American cryptologists," William F. Friedman.[1] Of course, since the 1999 induction of cryptologist Elizebeth Friedman into the Cryptologic Hall of Honor, the word Friedman has also come to refer to two pioneering cryptologists who happened to be married to each other. (See the 2006 Center for Cryptologic History publication, *The Friedman Legacy: A Tribute to William and Elizebeth Friedman*, for a detailed account of the important contributions the pair made to the field of cryptology.)

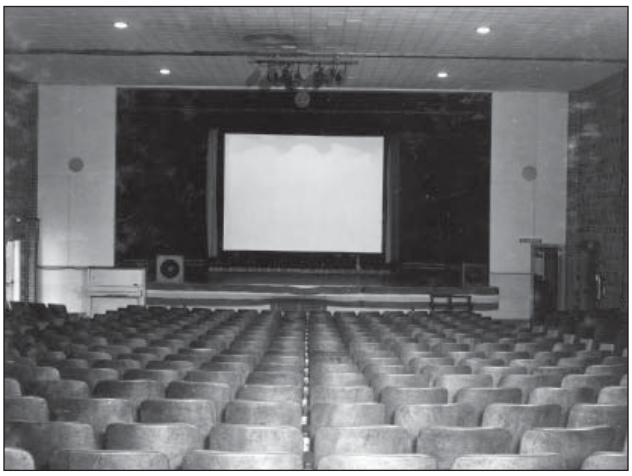
The Friedman Auditorium has been NSA's communal meeting place since the opening of the Agency's first building at Fort Meade, Maryland, in 1957 (i.e., "OPS1," today known as the William and Elizebeth Friedman building). Over the decades, "the Friedman" has been used for assemblies, training sessions, and presentations that required special projection and acoustical capabilities. Luminaries in the fields of science and technology, like Admiral Grace Hopper and Dr. Carl Sagan, have graced its stage to address the NSA workforce. To mark the auditorium's 2018 renovation and renaming as the Friedman Conference Center, this article takes a look at the Friedman's history (the place, not the people), but as is often the case with history, the stories of the place and the people intersect.

## The Idea for an Auditorium

Before there was a Friedman Conference Center, there was a Post Theater—more specifically the Arlington Hall Post Theater. In this standalone structure, the Armed Forces Security Agency, NSA's predecessor, hosted large ceremonies for its workforce located at Arlington Hall Station.[2] Constructed in 1944 after a directive mandated a major increase in Arlington Hall's staff, the theater held 620 seats and opened on August 12, 1944. Initially the theater was used to show popular movies, but it eventually became a ceremonial space as well.[3] Fittingly, one of the last major events held at the Post Theater was the 1955 retirement ceremony and National Security Medal presentation for none other than William Friedman, considered



The Arlington Hall site circa 1980. The circled building is the location of the Post Theater. *Library of Congress, Prints & Photographs Division, HABS VA1560*



The Arlington Hall Post Theater in July 1948. *National Security Agency, NSA Archives accession 50988, HIST-111-003*

by many to be the father of modern American cryptology.

The decision to relocate NSA north to Fort Meade was made in 1952. Some offices began making the move into existing buildings by 1955, but the first Operations building was not completed until 1957. NSA officials proposed the construction of an auditorium in the Operations building from the very beginning of the design phase, but it was not an easy sell. Leadership within the US Army and Department of Defense believed an auditorium, and other proposed features, were extraneous and exceeded the military austerity standards.[4]

Fortunately, NSA had strong leadership in Lieutenant General Ralph J. Canine as director, NSA (DIRNSA). The general justified the need for the auditorium and other features to the US Army G-4 Logistics, the army chief of engineers, and eventually even the secretary of defense. General Canine successfully argued that the auditorium was "essential for operations" and he refused to "settle for a shabby, poorly constructed building." He demanded that the building and its central auditorium be "modern for 50 years."[5] The general got his wish.

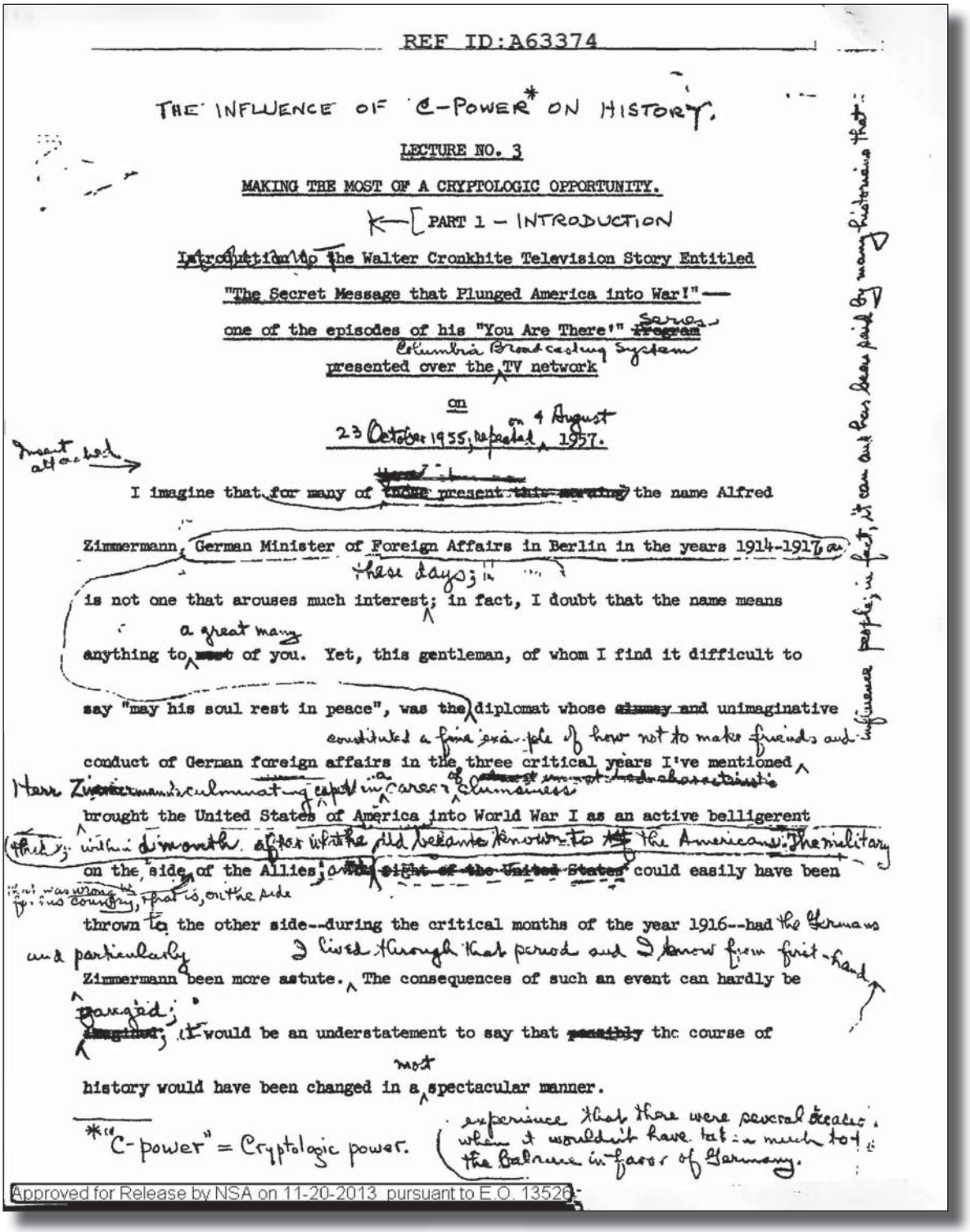
Groundbreaking for the Operations building occurred in 1954, but redesign and other construction issues pushed the move-in-ready date to 1957. The total cost for the entire building was roughly $35 million, only about two million over the budget. The auditorium originally featured a flat (rather than sloped) floor without permanently affixed seating. This allowed for flexible arrangements that could accommodate 400 to 500 people. For the first 18 years, the space was simply known as "the auditorium." It was, after all, the lone auditorium on the entire NSA campus, which only included a few buildings.[6]

The auditorium served as a place for briefings, lectures, award ceremonies, and other events that drew a large audience. William Friedman addressed an audience at least once in this space. He delivered a lecture on the World War I Zimmermann Telegram, titled "The Influence of 'C' Power on History" ("C" being "cryptologic"—a

Lieutenant General Ralph Canine (*left*) seemed to have a way with words. During William Friedman's retirement ceremony in the Arlington Hall Post Theater, he had everyone laughing, including the director of Central Intelligence, Allen Dulles (*far right*). Friedman is second from right; Solomon Kullback is seated at left. *NSA Archives accession 50988, A-7*

play on Alfred Thayer Mahan's 1890 work *The Influence of Sea Power on History*). This was delivered to the Crypto-Mathematics Institute in September 1958. (See the notes for his lecture on the next page. The audio file of the lecture is available on www.nsa.gov.)

Friedman, who was officially retired at that point, had continued working as a special consultant to the director, Lt Gen John A. Samford, researching and writing a history of cryptology. He captivated the audience, who already viewed him as a cryptologic legend from the war years (both World War I and II). This lecture eventually formed a portion of Friedman's *Lectures on Cryptology*, which the Agency published in the 1960s and declassified in the 1980s.[7]



REF ID:A63374

THE INFLUENCE OF "C-POWER"* ON HISTORY.

LECTURE NO. 3

MAKING THE MOST OF A CRYPTOLOGIC OPPORTUNITY.

PART 1 - INTRODUCTION

Introduction to the Walter Cronkhite Television Story Entitled

"The Secret Message that Plunged America into War!" —

one of the episodes of his "You Are There!" series

presented over the Columbia Broadcasting System TV network

on

23 October 1955, repeated on 4 August 1957.

I imagine that for many of those present this morning the name Alfred

Zimmermann, German Minister of Foreign Affairs in Berlin in the years 1914-1917 as

these days,

is not one that arouses much interest; in fact, I doubt that the name means

a great many

anything to most of you. Yet, this gentleman, of whom I find it difficult to

say "may his soul rest in peace", was the diplomat whose dismay and unimaginative

conduct of German foreign affairs in the three critical years I've mentioned

brought the United States of America into World War I as an active belligerent

within a month after it had become known to the American military

on the side of the Allies; a fact which could easily have been

thrown to the other side--during the critical months of the year 1916--had the Germans

Zimmermann been more astute. The consequences of such an event can hardly be

imagined; it would be an understatement to say that the course of

most

history would have been changed in a spectacular manner.

*"C-power" = Cryptologic power.



William Friedman's draft lecture notes for "The Influence of 'C' Power on History" delivered in the auditorium in 1958. *National Security Agency, William Friedman Collection of Official Papers, Document Reference ID A63374*

General Canine, USA, retired at a 1967 award ceremony in the auditorium. He fought for an auditorium that would be "modern for 50 years." *NSA Archives accession 49467, photo CX-895*

## The Memorialization

It is not surprising then, that the day after William Friedman's death in November 1969, an NSA employee suggested that the auditorium be named in his honor. Using formal suggestion channels, the employee advocated for the memorialization, citing the importance of Friedman's efforts to train new generations of cryptologists. In particular, he stated, "I teethed on his *Military Cryptanalysis* works in the late '40s, as a GI studying with Lambros Callimahos,[8] and helped on Callimahos's revision of those works in the early '50s, starting as a civilian in AFSA's Technical Division under Mr. Friedman."[9]

NSA leadership wrangled over the suggestion for five years, undecided over whether individuals,

An audience in 1967; note the folding chairs (10 years after the auditorium's debut) and the film crew in the background. *NSA Archives accession 49467, photo CX-895*

Deputy Director Benson K. Buffham and Elizebeth Friedman unveil the bust of William Friedman during the memorialization ceremony on May 21, 1975. Abraham Sinkov (*rear*) and Lambros D. Callimahos (*right*) watch. The bust was displayed in front of the auditorium for two decades. Today, it is on display inside the National Cryptologic Museum. *NSA Archives accession 41228*

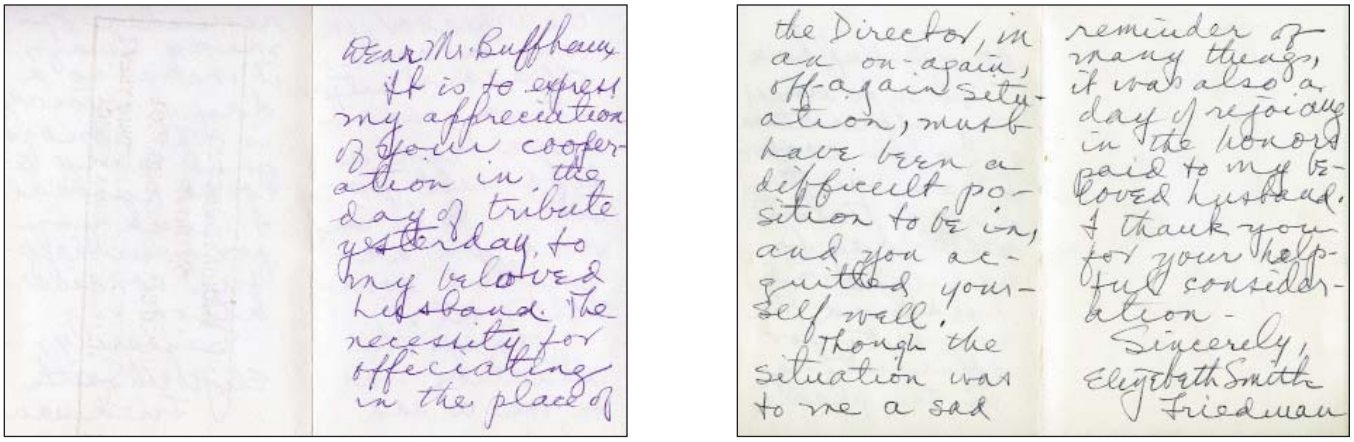
particularly civilians, should be memorialized in a semipublic way (despite the fact that Friedman's name and association with government cryptology had been public since the days of World War II).

The chief of the NSA History Office advocated for its memorialization. He expressed that it was important for NSA to have a "collective sense of cryptologic history, of heritage, of traditions." He said, "Cryptology is an ancient art, but a large government cryptologic organization is something comparatively new. An organization such as the army, the navy, or the State Department has its own history, traditions, and heroes—which fuse into an intangible yet very real part of the organization, or more precisely, of what the organization *means* to those who are a part of it."[10] Eventually, Agency senior leadership from each major directorate took an official vote on the matter, but deadlocked in a tie. DIRNSA Lt Gen Lew Allen put the matter to rest by approving the action himself in November 1974 and requesting a formal ceremony to mark the occasion.[11]

The dedication ceremony occurred on May 21, 1975, on what would have been William and Elizebeth Friedman's 58th wedding anniversary. Family, former colleagues, and distinguished figures from the Agency's past and present attended. Originally planning to preside over the ceremony, General Allen was instead called to Capitol Hill to testify to the newly formed Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (i.e., the Church Committee). In his place, Deputy Director Benson K. Buffham (also a member of the World War II Arlington Hall period) stepped in as the master of ceremonies.

During the event, Friedman's colleagues remembered him as a monumental figure in American cryptology. Buffham marked the occasion by stating, "the dedication of this auditorium will provide a constant reminder of [Friedman's] contributions" and "will stand as an enduring memorial to this man who was… the [f]ounder of the science of modern American cryptology." Four of Friedman's colleagues (and famed NSA leaders) spoke about their mentor. Frank B. Rowlett remarked, "… if it had not been for Billy Friedman's wisdom, his foresight, and his technical knowledge I don't think we would have been as well off so far as cryptography was concerned


Newly memorialized entrance to the William F. Friedman Auditorium in May 1975. *NSA Archives accession 41333*



Dear Mr. Buffham,
It is to express my appreciation of your cooperation in the day of tribute yesterday, to my beloved husband. The necessity for officiating in the place of the Director, in an on-again, off-again situation, must have been a difficult position to be in, and you acquitted yourself well.
Though the situation was to me a sad reminder of many things, it was also a day of rejoicing in the honors paid to my beloved husband. I thank you for your helpful consideration.
Sincerely,
Elizebeth Smith Friedman

Thank-you note from Elizebeth Friedman to Benson K. Buffham for the memorialization ceremony in honor of her late husband. *NSA Archives accession 41228*

in World War II." Abraham Sinkov described Friedman as "[a] cryptologic genius. A brilliant organizer, and a wonderful teacher." Solomon Kullback remembered that, "[t]o him cryptography, cryptanalysis, was not only an art but a science. A serious science." And, finally, Friedman's youngest protégé Lambros Callimahos expounded that "[e]verything he touched turned to plain text."[12] Elizebeth Friedman would later remark that she was appreciative of the Agency's efforts to remember her husband. In the month following, the *NSA Newsletter* revealed that more than 400 people attended the ceremony.[13]

Elizebeth Friedman died five years later in 1980. By the 1990s, it became clear to NSA historians and others that even though Elizebeth had never worked for NSA, her role in her husband's development as a cryptologist was critical to his career. His adoration of her and fascination with her cryptanalytic work at Riverbank Laboratories in the 1910s introduced him to the field. During the period between the world wars, both Friedmans worked as cryptologists for the government—Elizebeth for the US Navy, Coast Guard, and Federal Bureau of Investigation, chasing down Prohibition-era bootleggers and Nazi spies in Central and South America;[14] and William for the US Army Signal Intelligence Service, gradually building up a peacetime civilian-based cryptologic organization. With this knowledge in hand, NSA renamed the auditorium and the entire OPS1 building for both Friedmans. The OPS1 building dedication ceremony was held in 2002. The Friedmans' son, John, who had attended the 1975 dedication, returned to deliver a moving tribute to his parents' unwavering commitment to their family, their profession, and their country.

## The Significance

The Friedman Conference Center continues to be a central place for large meetings, ceremonies, conferences, lectures, and town halls at NSA. In addition to senior leadership, special guests have included US presidents, vice presidents, secretaries of defense, directors of central intelligence, directors of national intelligence, leaders in private industry, Holocaust survivors, World War II Native American codetalkers, and even an archivist of the United States. The Center for Cryptologic History held its first Symposium on Cryptologic History in the Friedman Audi-

torium in 1990. And on September 11, 2001, some employees remember sitting in the Friedman Auditorium as they listened to a briefing on NSA's new Perimeter Security Anti-Terrorism plan as the interrupted, breathless announcement was made about the terrorist attacks on the United States.[15]

In the tradecraft of cryptology, understanding and building upon knowledge of the past is critical. In addition, esprit de corps matters when the challenges seem overwhelming. The Friedman Conference Center is an important part of NSA's institutional memory for these reasons. In the simplest of terms, it is just a physical space. But to those who have worked at NSA since the first operational building opened at Fort Meade in 1957, it is much more. Underneath the modern design and state-of-the-art audio-visual technology lies a figurative historic fabric that ties generations of NSA employees together with a common mission. During the introduction to General Paul Nakasone's first Global Town Hall as DIRNSA, then Deputy Chief of Strategic Communications Wayne Murphy summed up the symbolism of the Friedman Conference Center:

> Perhaps you're here for the same reasons your predecessors assembled in this same room over 60 years ago—to marvel in the blessing that we all share to be a part of defending this nation. As you are listening to this Global Town Hall today, take some time to consider those who came before us in this room, those who spoke from this stage, those who walked across it, graduating from a program that marked a turning point in their career, some of whose faces now adorn our Hall of Honor. Think of those who assembled here, swapped ideas and went on to solve some of nation's hardest problems. Think of the fears, doubts, and worries they overcame by the reinforcing feeling of being in a room with a diverse set of colleagues, each with gifts and strengths to bring to the fight. Think of the words these walls have absorbed and events they have witnessed, the traumatic and triumphant, the points in our shared history that this room has contained. A room can be a powerful thing if we make it so, if we reflect on its history and take advantage of the opportunities that this kind of assembly can present.[16]

The Friedman Auditorium during a ceremony in the late 1970s. *NSA Archives accession 49467*

The Friedman Conference Center, while on the surface just another space on a large campus, has meaning to all the people who have contributed to NSA's mission to defend the nation and secure the future.

## Acknowledgments

I wish to thank Amanda H. Ogden, from the State Department's Foreign Service Institute, for help researching Arlington Hall and pointing the Center for Cryptologic History to the Historic American Building Survey resources at the Library


Entrance to the renovated Friedman Conference Center, which opened in 2018 at Ft. Meade, MD. *NSA photo*

of Congress and Arlington Public Library. I also thank Dave Sherman, former NSA senior official, and Rob Simpson, National Cryptologic Museum librarian, for their assistance and patient ear.

## Notes

1. As stated by Frank B. Rowlett in the foreword to William Friedman, *The Friedman Lectures* (Ft. George G. Meade, MD: National Security Agency, 1965).
2. The US Army's cryptologic organization was headquartered at a place known as Arlington Hall from 1942-1949. Prior to its life as an army post, the site was the Arlington Hall Junior College for Girls. In 1949, the Armed Forces Security Agency (AFSA) was established to consolidate the military cryptologic elements. Arlington Hall became the headquarters of AFSA's communications intelligence mission, and the communications security mission was centralized at the Naval Security Station on Nebraska Avenue in Washington, DC. AFSA became the National Security Agency in 1952, and part of the rationale for moving to Fort Meade, MD, in 1955 was the overcrowding at both locations.
3. "Arlington Hall Station," Written Historical and Descriptive Data, Historic American Building Survey, National Park Service, US Department of the Interior, 1989, 10. Prints and Photographs Division, Library of Congress, VA, 7-ARL, 12, accessed on February 2, 2019, http://www.loc.gov/pictures/item/va1560/.
4. "Agreements between AFSA-NSA and Army Authorities re New Site," 1955, National Security Agency, Document Reference ID A315885, 8.
5. "Agreements between AFSA-NSA and Army Authorities re New Site," 17.
6. Thomas Johnson, *American Cryptology during the Cold War, 1945-1989, Book I: The Struggle for Centralization, 1945-1960* (Ft. Meade, MD: National Security Agency, 1995), 245; Ralph J. Canine, "Memorandum for the Secretary of Defense: Status of Funds—NSA Construction Project," February 24, 1956, National Security Agency, NSA Archives

accession 22754; "Agreements between AFSA-NSA and Army Authorities re New Site," 2; Movement Group, "Auditorium," January 23, 1953, National Security Agency, NSA Archives accession 24824, Document Reference ID A283275, 1-3.

7. William F. Friedman, "Friedman's Lecture on the Zimmermann Telegram at the Semiannual Meeting of Crypto-Mathematics Institute, September 1958," National Security Agency, Voices from the Past, accessed on February 1, 2019, https://www.nsa.gov/70/documents/resources/everyone/digital-media-center/video-audio/historical-audio/voices-from-the-past/friedman-zimmermann-transcript.pdf. Lecture notes, Document Reference ID A63374, accessed on February 2, 2019, https://www.nsa.gov/news-features/declassified-douments/friedman-documents/assets/files/lectures-speeches/FOLDER_167/41758819079795.pdf.
8. Lambros Callimahos was one of William Friedman's protégés. An expert on cryptanalysis techniques, he coauthored a text on military cryptanalytics with William Friedman.
9. "How the Friedman Auditorium did *NOT* get its Name!" *Cryptolog*, 3rd issue (1990): 23-24, accessed on February 2, 2019, https://www.nsa.gov/70/documents/news-features/declassified-documents/cryptologs/cryptolog_119.pdf.
10. "Memorandums For/Against Naming the Auditorium or Operations Building for Mr. Friedman," November 1974, National Security Agency, NSA Archives accession 50405, Document Reference ID A61775.
11. "Memorandums For/Against Naming the Auditorium or Operations Building for Mr. Friedman."
12. "William Friedman Honored," May 1975, National Security Agency, NSA Archives accession 49511, Box 807, Folder 4.
13. *NSA Newsletter*, June 1975, National Security Agency, Center for Cryptologic History NSA Newsletter Collection.
14. David P. Mowry, *Listening to the Rumrunners: Radio Intelligence during Prohibition* (Fort George G. Meade, MD: Center for Cryptologic History, 2014), 17-21; Jason Fagone, *The Woman Who Smashed Codes: A True Story of Love, Spies, and the Unlikely Heroine Who Outwitted America's Enemies* (New York: Harper Collins, 2017), 223-47.
15. NSA TV center video ATVC #624.
16. Introductory remarks by Wayne Murphy, Director's Global Town Hall, August 9, 2018, National Security Agency, XStreaMedia Video 56213.

**Sarah Parsons** joined the National Security Agency's Center for Cryptologic History in 2017 as a historian. Prior to that position, she worked as an archivist and records manager within NSA's Associate Directorate for Policy and Records where she led the joint project to inventory, declassify, and release official records created and maintained by the renowned cryptologist, William F. Friedman. Before her government career, she worked as a curator and archivist at the Baltimore and Ohio Railroad Museum and as the assistant director of the American Association (now, Alliance) of Museums' Information Center. She earned a bachelor's degree in history from Salisbury University in 2002 and a master's degree in historical studies with a concentration in public history from the University of Maryland, Baltimore County in 2008.

New releases from the Center for Cryptologic History!

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