Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 25 July 2011

FROM: Center for Cryptologic History | Run Date: 07/25/2011

☒ KI27 (U) A number of diverse intelligence sources came together in 1944 to provide a solid answer to questions the U.S. military had been asking since the prewar period. ULTRA, the product of cryptanalysis of high-grade Japanese systems, stood at the center of the analytic effort.

(U) Were the Japanese manufacturing aircraft in Manchuria, and, if so, what types and how many?

(U) The Japanese had occupied Manchuria since the early 1930s. Named Manchukuo, and nominally an independent nation within the Japanese empire, the country actually was a Japanese puppet state. The Japanese extracted raw materials there for its own industry in the home islands and also had established a heavy industrial plant within Manchukuo for civilian trade with China or supply of Japanese forces on the mainland. Did that industrial presence include aircraft manufacturing?

(U) Prewar U.S. military intelligence had seen a reference to a "Manchuria Aircraft Company," but had no details of any kind about its location or its activities. Examination of captured or downed Japanese aircraft during the war failed to turn up any nameplates that indicated Manchurian origin.

(U) In April 1944 a number of ULTRA messages contained references to a "Manchuria Air Depot" in the city of Mukden (today's Shenyang). The depot was deploying a "Type 2 Single Engine Advanced Trainer (SEAT)" to Japanese forces in China, Taiwan, the Philippines, and Malaya. Since Mukden was not on the usual air route from Japan to these delivery points, the messages indicated the strong possibility that the aircraft were manufactured in the city.

(U) Some messages used an acronym, "Man Hi," which could be expanded in Japanese to read "Manshu Hikoki," i.e., "Manchuria Aircraft." At least one message referred to Man Hi producing Type 2 trainers.

(U) Analysts next looked at ULTRA messages regarding shipments from Japan to Manchuria. They determined that shipments included propellers, landing gear, and a few other aircraft components, but no aircraft engines. The analysts concluded it was probable the engines were manufactured in Manchuria.

(U) Further analysis of the traffic indicated that in May the Manchuria Air Depot had promised delivery of 105 planes to its principal customers. Combined with messages requesting components, this information suggested that the Depot was turning out approximately 150 aircraft per month.

(U) In a search of documents, an MI analyst found a translation of a letter from the (pre-war) Mitsubishi Corporation in New York that referred to both the Manchuria Aircraft Company and the Air Depot. The letter made clear that these were one and the same.

(U) The document search revealed a Mukden street address for the company; however it was in Japanese, not Chinese. After considerable work, the Chinese address was found in an industrial yearbook, and the company could be pinpointed on a map of Mukden.

(U) A document captured in Hollandia turned out to be instructions to an inspector who was scheduled to visit the Depot. This document contained a drawing of the Depot and surrounding buildings

(U) In mid-June, the U.S. Army Air Force conducted photoreconnaissance of Mukden. The resultant photos showed buildings suitable for aircraft manufacture and an adjacent airfield. However, of about 125 small planes nearby, only 40 were seen with engines, and the main building did not have the ventilation required for construction/testing of motors; this led to the conclusion that the engines were manufactured elsewhere.

(U) Additional analysis of the photographs found another building, some miles away, that corresponded to the shape of the one in the Hollandia drawings. Although the Manchuria Aircraft Company and the Air Depot were one entity, it had two locations in Mukden.

(U) Further details emerged about the SEAT aircraft itself and about Japanese aircraft manufacturing. Also, based on clear identification of the SEAT from the air, image analysts could identify air training bases in territory occupied by the Japanese.

(U) Colonel Alfred McCormack, who was responsible for much of the organization and operational methodology of Army COMINT and military intelligence, called this "detective work," and argued that it was erroneous to think in terms of separate kinds of intelligence, ULTRA and non-ULTRA. He also remarked "In many cases of the hardest work no definite results are produced, at least for a long time; but when results appear they are very rewarding."

(U) The aircraft was a variant of a design from the Nakajima Company, and designated the Ki-27 (pictured). Later in the war, Japanese units in Manchuria used this aircraft in a ground attack role and for kamikaze attacks on Allied forces, making the complex analytic chain even more valuable in determining the strength of the enemy.

(U) Want to discuss this item with interested -- and interesting -- folks? Visit the Center for Cryptologic History's blog, "History Rocks." (go history rocks)

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

(b)(3)-P.L. 86-36

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 1 August 2011

FROM: Center for Cryptologic History | Run Date: 08/01/2011

(U) According to an ancient military axiom, "Without intelligence, one is vulnerable; without security, one is defenseless." U.S. cryptologists had a long and difficult mission trying to deny information to the enemy from its own and South Vietnamese communications.

(U) Just as there was a long history of providing in-country SIGINT support during the Vietnam War, there was also an equally long history of providing COMSEC monitoring to improve the communications security of U.S. military advisers.

(U) Sometime in 1960, at the prompting of his signals officer, Major General Charles J. Timmes, chief of the Military Assistance Advisory Group Vietnam (MAAG-V), asked the Army Security Agency (ASA) to help maintain secure communications for his men. In late 1960, ASA's 104th Detachment, which consisted of 6 personnel, went TDY to South Vietnam to monitor MAAG-V communications. This small detachment arrived in-country several months before the arrival of the 3rd Radio Research Unit (RRU), the first SIGINT unit in South Vietnam, in May 1961.

(U) The detachment identified numerous violations and problems. For example, some soldiers had never used a one-time encryption pad during their entire tour in Vietnam. As a result of these findings, Colonel Robert T. Walker from ASA Pacific issued cryptographic equipment to MAAG-V elements and recommended procedural changes in the transmission of messages. Walker also established control over the assignment of callsigns and frequencies.

(U) In February 1962 the 3rd RRU received authorization to establish its own COMSEC mission. When the 104th Detachment completed its TDY and departed South Vietnam in March 1962, it left its equipment for the benefit of the 3rd RRU. Thus, the 3rd RRU was able to deploy mobile COMSEC monitoring teams; the first of these teams was sent to Da Nang.

(U) On March 1, 1963, the 7th RRU was organized; its mission was solely COMSEC The 7th RRU depended on the 3rd RRU for administrative and logistical support, but had its own separate mission. As the U.S. military commitment to South Vietnam grew, ASA provided more COMSEC support. In a few short years, ASA COMSEC support grew from a small detachment to a separate organization for the COMSEC problem. As the number of army troops expanded, the COMSEC organization eventually grew to battalion strength.

(U) ASA was the first Service Cryptologic Agency to establish COMSEC support for the U.S. military in South Vietnam because it was the first to send personnel in country. However, COMSEC support became an integral part of the duties of all Service Cryptologic Agencies during the Vietnam War.

(U) The photograph shows an operational building used by the 7th RRU.

(U) Can't get enough cryptologic history? Come blog with us at "History Rocks." (go history rocks)

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

DERIVED FROM: NSA/CSSM 1-52, DATED: 20130930, DECLASSIFY ON: 20380930
Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

(b)(3)-P.L. 86-36

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 24 August 2011

FROM: Center for Cryptologic History | Run Date: 08/24/2011

(U) The Netherlands had its counterpart to Herbert Yardley, the pioneer in U.S. cryptologic history who became head of our first interdepartmental cryptologic organization, the "American Black Chamber "

(U) Holland had its counterpart in Henri Koot, the "godfather" of Dutch military cryptology. Like Yardley, he had a very interesting background, and was seminal to the evolution of his nation's cryptologic organization into what, over time, became an extensive and important enterprise.

(U) Koot was born on Bali in 1883, the son of a Dutch East Indies colonial administrator of European extraction and a Chinese mother. He always showed an aptitude for languages, and was fluent in many of the tongues of modern-day Indonesia. Upon completing secondary school, he was accepted into the Royal Military Academy. Graduating third in his class in 1904, Koot was commissioned into the Dutch East Indies infantry. Thereafter followed a series of military posts and assignment as a civil administrator on various islands throughout the archipelago. In 1911, he studied at the Higher Military Staff College at The Hague.

(U) With war looming in 1914, the Dutch Army created a new organization, Division IV of the General Staff (GS 4). It was tasked with carrying out censorship, counter-intelligence, and cryptologic activities. In recognition of his talents, especially in mathematics and analysis, Lieutenant Koot received a transfer to this new unit upon its creation. Armed solely with a natural ability to solve complex puzzles, Koot sought to decipher foreign intercepts as well as to improve Dutch communications security. By war's end, his section had grown to twelve officers, and he had received a meritorious promotion as well as the Medal of Honor from the Dutch queen for his cryptologic activities. In 1919 the cipher division became an independent department (GS 3c), with Koot as its head.

(U) Within a year's time, Koot was made chief of a new Cryptographic Bureau, like the Black Chamber a centralized and interdepartmental government agency that nominally fell under the purview of the Ministry of Foreign Affairs, although it also received funding from the military services. His organization did attempt to attack the ENIGMA, the encryption device already in use by the Germans, although Koot concluded -- perhaps too soon -- that it was unbreakable without access to its key. Koot also trained an entire generation of Dutch cryptologists, especially in the Army and Navy, in cryptography and espionage.

(U) The worldwide economic downturn hit every nation on Earth by the early 1930s. Unfortunately, and oddly similar to the fate of Yardley's outfit, the Dutch government decided that it could save money by shutting down the Cryptographic Bureau; then-Major Koot was dismissed, effective January 1, 1933. He went back to heading the Army cryptologic unit. But, unlike Yardley, Koot successfully rebounded. By 1939 he was a full colonel, and notably had established a series of listening posts throughout the Dutch colonial empire. He also had developed a new code system for Dutch forces on the eve of the Nazi invasion of the Low Countries in May 1940.

(U) The Netherlands capitulated to the Germans before the end of the month. Dutch cryptologic activity ceased, except for a few officers who managed to escape and were taken into Britain's Government Code & Cypher School; also, one officer augmented the Signals Intelligence Service of the U.S. Army. Koot stayed in Holland during the occupation, and soon after the Dutch surrender was arrested by the Germans. After a few months, he was released and remained in his country, working under the auspices of the Red Cross.

(U) Koot secretly used his position to aid the Resistance. When the true nature of his activities was suspected, he was rearrested. Able again to persuade his captors to release him, Koot soon thereafter was appointed as commander of Interior Forces, a collection of Resistance and other military elements operating under the Dutch government-in-exile. In April 1945 he received temporary promotion to major general; this enabled him to negotiate the surrender of the German military command in Holland, since his German counterpart insisted on dealing only with an officer of equal rank.

(U) After the war, he received a knighthood and the Military Order of William. Additionally, he was offered the leadership post of the newly created *Bureau Nationale Veiligheid* ("Bureau of National Security" in English, abbreviated BNV), a reinvigorated security service. He turned down the opportunity but remained in military service until 1947. Koot, one of the greats of cryptology, albeit little known outside of his homeland, died a little over a decade later.

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

DERIVED FROM: NSA/CSSM 1-52, DATED: 20130930, DECLASSIFY ON: 20380930
Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

(b)(3)-P.L. 86-36

Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 29 August 2011

FROM: Center for Cryptologic History | Run Date: 08/29/2011

(U) The old cliche that "the enemy of my enemy is my friend" is well illustrated by the cryptologic relationship between Poland and Japan.

(U) We lack details about the depth of the relationship, but there is no doubt that it endured over decades.

(U) Both countries viewed Russia, later the Soviet Union, as an enemy.

(U) A sympathetic relationship between Poland and Japan began about the time of the Russo-Japanese War of 1904-05. Poland then was not independent, but was a component of the Russian Empire. Russian officers of Polish ethnicity were captured by the Japanese, and found their negative feelings about Russia were shared by their captors. In the decades that followed, friendly feelings and good relations continued between them.

(U) In the early 1920s, Army officers from newly independent Poland traveled to Japan to train Japanese cryptologists and help develop a communications intelligence capability. During its war against the USSR to keep its independence, the Polish military had developed an active COMINT capability that supported their war effort at key points. (See *History Today*, April 16 and 19, 2010.)

(U) The Japanese-Polish cryptologic cooperation was aimed directly at Soviet communications. In addition to working with the central government, Polish cryptologists also traveled to Harbin, the capital of Manchukuo (the Japanese puppet state in Manchuria) to support Japanese army COMINT efforts on the Asian mainland.

(U) It is known that as Poland was attacked by Germany, the Japanese helped some Polish intelligence officers escape. In addition, the Polish government in exile in London approved the long-term residence of a Polish cryptanalyst in Manchukuo to assist the Japanese in monitoring the Soviets. Note that these two incidents occurred even though the Free Polish Government was a member of the Allies and Japan was a partner to Germany -- that is, officially they were enemies.

(U) The photograph shows the General Staff building in Warsaw, where Polish intelligence, including its cryptologists, were located before World War II.

(U) Can't get enough cryptologic history? Come blog with us at "History Rocks." (go history rocks)

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

DERIVED FROM: NSA/CSSM 1-52, DATED: 20130930, DECLASSIFY ON: 20380930
Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

(b)(3)-P.L. 86-36

(U) History Today - 11 October 2011

FROM: Center for Cryptologic History | Run Date: 10/11/2011

(U) Hungary had a highly proficient communications intelligence service before and during World War II. Unfortunately, due to the destruction and dislocation caused by the war, for the most part the service is known primarily in broad outline. Only a few details are now available.

(U) The Hungarian service, known as Section X (sometimes as Sub-group X), was founded in 1920 by Hermann Pokorny, pictured, who had spent a career in the Austro-Hungarian military intelligence organization. When the map of middle Europe was rearranged after WWI, he went with the new nation of Hungary. (See History Today of September 16, 2010, for more information on Pokorny.)

(U) Between the world wars, the primary targets for Hungarian COMINT were the Soviet Union, Romania, and Turkey. The latter was a target because it was believed to have good information on the USSR. Details are hard to come by: it appears they made little progress against Soviet ciphers, but had a fair amount of success against Romanian and Turkish diplomatic traffic.

(U) During World War II, Section X was a "second party" to the German Army and Air Force cryptologic organizations. The Germans treated them poorly in terms of cooperation on cryptanalysis, but apparently valued Hungarian intercept on the Balkans, which was much better than any German service could do.

(U) Details about the fate of Section X after the war, when the country was occupied by the Red Army, are few. Some sections surrendered to the U.S. Army and provided the Allies with valuable information about wartime efforts. It seems that those who were captured by the Soviets were used to help build a new cryptologic service, then, after a few years, were purged because of their wartime cooperation with the Germans.

(U) A one-time chief of Section X recalled one odd prewar use of its decrypts.

(U) During a period when Hungary was seeking to build better relations with Ankara, Section X solved the cryptosystem used by the Turkish military attache in Budapest. A series of decrypts indicated the attache was sending false -- and sometimes damaging -- reports to his leadership.

He sent reports of meetings that had not occurred and fabricated statements allegedly from the Hungarian government that were unflattering to Turkey.

(U) Based on these decrypts, Hungarian intelligence assigned an agent to establish a close friendship with one of the attache's female employees. When the agent became familiar with the milieu, he burgled the attache's safe in such a way that it looked as if only the attache could have done it.

(U) Further decrypts confirmed that the ambassador blamed the attache, who was in need of money to support a fast lifestyle, and had him recalled.

(U) Can't get enough cryptologic history? Come blog with us at "History Rocks." (go history rocks)

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

(U) History Today - 15 August 2012

FROM: Center for Cryptologic History | Run Date: 08/15/2012

(U) In 1941, when the Japanese attacked Pearl Harbor, the U.S. was unable to read Japanese army codes. Due to limited budgets and manpower, William Friedman and his band of army cryptologists were limited in the range of systems they could work and, in any case, little intercept of Japanese Army communications was available. Throughout the 1930s they worked and had great success breaking and reading Japanese diplomatic ciphers. With the great expansion of the Army cryptologic organization at the start of World War II, and greater availability of intercept, U.S. Army cryptanalysts turned their attention to the Japanese army code.

(U) The Japanese army code was a challenging problem. It was a book-based hand encipherment system. First, each word of a message was transferred into a four-digit number taken from a codebook. Next, each four-digit number in the message was enciphered by using an additive table, that is, a list of random numbers. The next available numbers from the additive table were added -- in noncarrying addition -- to the four-digit numbers in the first draft of the message. The product of this addition became the message. This system proved to be an effective encryption method.

(U) U. S. cryptanalysts were never able to break low-level Japanese army communications. It was difficult to get enough intercept because the Japanese used low-power transmitters. Also, these armies communicated vertically rather than laterally. Therefore, if the 78th Regiment wanted to get a message to the 79th Regiment, it had to send it to the 20th Division, which then sent it to the 79th Regiment. The response from the 79th Division went back to the 20th Division, then to the 78th Regiment. This cumbersome system was further complicated because each regiment had its own code.

(U) Ironically, higher-level Japanese army communications were less secure. Japanese area armies expanded rapidly and could not use low-power transmitters because of the distance that they covered. Rapid expansion made more communication necessary, which gave the Americans more to study.

(U) The U.S. read its first Japanese Imperial Army message in September 1943. By February 1944, the U. S. was decrypting 20,000 Japanese army messages per month. This was indeed a remarkable achievement.

(U) A Japanese Army codebook is on display in the National Cryptologic Museum.

(U) The photograph shows a training class for analysts at Arlington Hall Station, where much of the strategic Japanese traffic was worked.

(U) Like to blog? Want to discuss historical topics with interested -- and interesting -- folks? Visit the Center for Cryptologic History's blog, "History Rocks." (go history rocks)

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Comments/Suggestions about this article?

(U) The religious reformer Martin Luther was subject to considerable opposition in his day from the nobility that supported the Roman Catholic Church. One of his staunchest foes was George the Bearded, Duke of Saxony, pictured.

(U) On a couple of occasions, Luther's correspondence was intercepted, read, and published. Luther, however, in the words of one historian, "was one of those men who cannot sit down tamely under a wrong...."

(U) One of Luther's letters to Dr. Link, a preacher at Nuremberg, fell into the hands of Duke George. The duke published it, accusing Luther of plotting to foment disturbances.

(U) Luther responded with a public treatise of his own. He did not admit or deny writing the letters, but said that, if they were his, Duke George's use of them was tantamount to a confession that the duke had "abstracted my property without my privity or consent." Luther questioned the right by which Duke George could take or retain another person's property. He also suggested that if the two were reversed, if Luther had acted this way with a letter of the duke's, the reformer would be in danger of losing his head.

(U) Finally, Luther quoted the commandment against theft to the duke.

(U) In another place, Luther suggested that he should have "learned how to give him such a cut over the nozzle in my answer that he would have lost all inclination for a further quest."

(U) This incident and several similar ones prompted the nineteenth century British diplomat (and sometime journalist) Eustace Clare Grenville Murray to argue for the inviolability of diplomatic correspondence and to argue against the national cryptanalytic activities of the nations of Europe. The Martin Luther incident was cited at length in his 1855 book *Embassies and Foreign Courts: A History of Diplomacy*.

(U) The stakes were too high, however. European nations continued to use their "black chambers," and some nations, such as Great Britain, which had temporarily discontinued its diplomatic cryptanalysis, resumed activities early in the twentieth century.

(U) History Today - 26 September 2012

(b)(3)-P.L. 86-36

FROM: Center for Cryptologic History | Run Date: 09/26/2012

(U) During the Vietnam war, the typical military tour in country lasted one year. This practice created continuity problems, and many folks counted the days till their time was up. Movies and books frequently portray U. S. military personnel from the Vietnam War era in a less than favorable light, emphasizing drug addiction and other problems. Although such problems existed, there is another side of the story.

(U) Many military and civilian personnel maintained a record of distinguished service during the Vietnam War, many serving multiple tours in South Vietnam. Here are a few examples of outstanding service by cryptologists from among many that could be selected.

(U) Some folks did their first tour in South Vietnam in uniform and later went back as civilians. For instance, [redacted] was a Vietnamese linguist in the Army Security Agency and served as one of the early pioneers at Phu Bai. He joined NSA as a civilian in 1965 and for the next ten years continued to work the Vietnam problem. He had many additional TDYs to Vietnam as well as a PCS assignment in 1974-75.

(b)(3)-P.L. 86-36

(U) [redacted] was an Army Security Agency Vietnamese linguist who served at Pleiku in 1967. He was curious and enjoyed the work, branching into traffic analysis. After Vietnam, he continued his military service at NSA and worked on the same problems. After his time in the military, [redacted] was invited to become an NSA civilian. He took this job so he could go back to South Vietnam. In 1970 he began his second tour, which lasted for two years. This time he was stationed in Saigon as a civilian, but he found the work just as rewarding.

(U) Some military cryptologists did more than one tour in South Vietnam. For instance, [redacted] served in 1966 and 1967 with the 6994th Security Squadron of the Air Force Security Service as part of a detachment from Nha Trang; he flew in the airborne radio direction finding program. He noted that the EC-47 planes, where he sat as a "back ender" doing traffic analysis, were older than the men who worked in them. In September 1969 [redacted] left the Air Force and joined the Army. In a few short weeks, he was back in South Vietnam for his second one-year tour, this time as part of a direct support unit providing SIGINT to the First Cavalry. [redacted] found both tours rewarding, but felt that his services in the second tour were greater because he was closer to combat.

(U) [redacted] was a warrant officer in the Signal Corps, with communications security responsibilities. His first tour in Vietnam was from November 1967 through November 1968. He helped to protect Tan Son Nhut Air Force Base during the Tet offensive. He went back for a

second tour in 1971 to manage distribution of communications security equipment and manuals to the South Vietnamese. found his greatest challenge was to educate both the American and South Vietnamese military on the need to follow communications security practices.

(U were civilians who did multiple tours in South Vietnam. came to South Vietnam from April 1968 to May 1969, serving with the Cryptologic Support Group for the Military Assistance Command Vietnam; he helped to explain SIGINT to the military commanders. also had at least one TDY that lasted several months. His second tour was from January 1973 to January 1974, during Vietnamization. He was the chief operations officer and worked with the South Vietnamese so that they could stand on their own after the withdrawal of U. S. troops.

(U) pictured, holds the record for longest service among civilians in South Vietnam. He began his in-country service in 1961 and ended his first tour in 1964. did numerous TDYs throughout the country at various intercept sites, and went back for his last full tour in South Vietnam in 1974. As the person in charge of U.S. SIGINT personnel in South Vietnam, he faced numerous challenges. He successfully arranged for evacuation of all U.S. SIGINT personnel, and himself left South Vietnam within hours of the fall of Saigon on April 30, 1975.

(U) Like to blog? Want to discuss historical topics with interested -- and interesting -- folks? Visit the Center for Cryptologic History's blog, "History Rocks." (go history rocks)

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 24 January 2013

FROM: Center for Cryptologic History | Run Date: 01/24/2013

(U) The country went through an ordeal at home as well as abroad during the Vietnam War. It was an armed conflict fought with the most modern of technology, in a relatively undeveloped country, against an enemy that made up for its military disadvantages with help from the Communist bloc and a sheer will to win. The U.S. military applied its war-making machine in an intensive manner, including carpet bombing and the introduction of an immense number of ground troops. The war seemed to drag on without the "light at the end of the tunnel" repeatedly promised by political leaders.

(U) The American public turned against the war over time. Dissatisfaction first erupted at universities and then began to spread, slowly at first, but ultimately university protestors joined forces with civil rights activists to become an all-encompassing social movement. Within two years of the first organized domestic protest in 1965, massive rallies occurred, even in the nation's capital. Indeed, policymakers were no longer welcome at -- nor felt safe entering -- most college campuses across the country.

(U) It is notable that a former military cryptologist was at the forefront of one aspect of this movement.

(U) Jeff Sharlet could speak with authority on the war. He had attended a military prep school, and then went to college at Indiana University. He soon left school to enlist in the army, and was assigned to the Army Security Agency (ASA). The major reason for his enlistment was a promise of training in a major European language, with subsequent posting on that continent. He was soon disabused of that plan when he received orders to study Vietnamese at the Army Language School (now DLI). After training of nearly a year, he was a qualified linguist and was sent to the field.

(U) Sharlet spent the first half of 1963 at Stotsensberg Station on Clark Air Force Base in the Philippines. From there, he was deployed to the war zone. He spent time with the 3rd Radio Research Unit at Davis Station, followed by assignment to intercept duty at Phu Lam, and then to operational support at Phu Bai. Before he left Vietnam in May 1964, he had seen a great deal of the Vietnam War.

(U) He returned to the United States and went back to college in Indiana just as the war and protests were ramping up. He joined a radical student organization known as Students for a Democratic Society, eventually becoming a chapter president, and began to participate actively in major protests Enrolling at the University of Chicago for graduate school gave him a platform by which to champion those like himself. He got in on the ground floor when the Vietnam Veterans Against the War was formed.

(U) Most importantly, Sharlet established himself as editor and publisher of the first veterans' antiwar newspaper, *Vietnam GI*. Its first issue made a huge splash in January 1968. By the summer, his newspaper had a circulation of at least 30,000, not counting the hands through which illicit copies were passed among active duty military. This newspaper was heralded at the time and since as having provided a voice to antiwar protesters in the military.

(U) Sharlet unfortunately passed away prematurely from cancer well before he was thirty.

(U) A fuller examination of Sharlet's life and his newspaper will appear soon in our periodic series known as *Cryptologic Almanac*. If you are not already a subscriber to the *Almanac*, become one via the SID Listprocessor ("go listproc-do") and select ESS1364.

(U) Want to discuss this item with interested -- and interesting -- folks? Visit the Center for Cryptologic

History's blog, *History Rocks*. ("go history rocks")

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

(U) History Today - 14 June 2013

(U) This article is based on an obituary published by the Kryptos Society.

(U) Dr. Hugh Gingerich earned his PhD in mathematics at the University of Illinois in 1942. He taught at the University of Maryland in the early 1940s, but had issues with the university's administration. He took a position with the Carnegie Institute of Washington, D.C., in 1944.

(U) In 1946, at the recommendation of other mathematics PhDs who were working in cryptology, he was recruited by the Navy's cryptologic organization, then known as Communications Supplementary Activity, Washington (CSAW). He made the transition to AFSA in 1949 and to NSA in 1952.

(U) Among many other achievements, Gingerich wrote what was likely the first operational program for a digital computer at NSA. He programmed ATLAS I, NSA's first computer, to attack some anomalies in the VENONA messages (communications of the Soviet espionage organization that had imperfectly produced one-time pads.)

(U) Gingerich had his idiosyncratic work habits. In the 1950s he was known sometimes to work in a phone booth, where he could get the quiet he needed. He also decided to adopt a personal 28-hour day, and carried on his activities without regard to others' schedules. This lasted until he met [redacted] a Portuguese linguist, in 1950. Once they were married, he returned to a more conventional day.

(U) His Ph.D. dissertation at the University of Illinois, "Generalized Fields and Desargues Configurations," was a seminal work, although he himself did not maintain academic connections. In 1990, according to one recollection, a visiting professor was lecturing to NSA mathematicians and made a reference to "Gingerich's Theorem" -- unaware that Dr. Gingerich was sitting in the next room.

(U) Dr. Hugh Gingerich died in 1998 at the age of 82.

(U) We do not have a photograph of Dr. Gingerich. Pictured is ATLAS, the first cryptologic computer, on which he did some important work.

(U) Like to blog? Want to discuss historical topics with interested -- and interesting -- folks? Visit the Center for Cryptologic History's blog, *History Rocks*. ("go history rocks")

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa

(b)(3)-P.L. 86-36

(U) History Today - 24 June 2013

(U) In earlier days of cryptology, handwriting was without question paramount to success - a person had to be able to read what was written, which meant the person on the other end also had to write legibly.

(U) This would have applied to Commodore Isaac Chauncey and his staff, we suspect. Chauncey, one of the great U.S. naval commanders of the early 1800s, was battled-hardened after fighting the Barbary Pirates in the Mediterranean Sea for many years.

(U) At the outset of the War of 1812, he was placed in charge of naval operations on Lakes Ontario and Erie, where he would be working in coordination with the U.S. Army against British and Canadian forces. Secretary of the Navy Paul Hamilton sent Chauncey a cipher on September 1, 1812, just in case he needed to have secret communications with the Navy Department.

(U) As you can imagine, given the era, this cipher was simple enough - appearing to be nothing more than a simple substitution cipher (i.e., one symbol replaces another; e.g., A=M). Hamilton used all letters of the alphabet, a period, and then ten digits, numbers 1-9 ending with zero. On top of each of these, he wrote in the cipher by hand. This is easily breakable (as are presumably all simple substitute ciphers).

(U) What Hamilton did, though, was use many of the lower row, i.e., plaintext, symbols as ciphers, in most cases simply writing them differently. Since writing styles are different, this could easily lead to confusion.

(U) For example, Hamilton used what appears to be a capital *J* to encipher *p* while the small *j* is enciphered with what looks like a *v*. When writing back to Hamilton in code, Chauncey would presumably have had to write the symbols the exact same way that Hamilton wrote them if Hamilton were to understand a message. For his part, Hamilton did go to great lengths to avoid confusion. For example, he also used easily written symbols, e.g., triangles and equal signs, to encipher.

(U) By this time, cryptologists undoubtedly were long aware of the pitfalls of handwritten ciphers and codes. Good copying skills must have been essential, possibly even an art in themselves. Still, one wonders how serious a problem this was. Do we know of incidents where a handwritten cipher was misread - with major ramifications - because it was not legible enough? Nowadays, of course, with modern technology, this type of situation is far less likely to happen.

(U) For the record, there is no indication that this code was ever used by Chauncey. He would prove to be a good commander, helping the Army capture both York (Toronto) and Fort George in the spring of 1813 and besting the squadron of Commodore James L. Yeo in the "Burlington Races" in the fall.

(U) The main source for this item, as well as the code, is the *The Pictorial Field-Book of the War of 1812*. The original code, according to the field book, is in possession of the New York Historical Society.

(U) Can't get enough cryptologic history? Come blog with us at *History Rocks*. ("go history rocks")

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Comments/Suggestions about this article?

(U) History Today - 26 June 2013

(U) Commonplace today, remoting was an unproven, even bold, idea when it was first implemented.

(U) During the Vietnam War, although COMINT was a major source of intelligence, it often involved considerable danger to the intercept operator. Much of the enemy's communications were low-powered and line-of-sight. Because of the mountainous terrain and jungle, collectors often had to work close to enemy transmitters.

(U) During the early phases of the war, intercept units often were colocated with combat troops, which afforded protection for them. As U.S. forces began to draw down near the end of the war, however, many intercept sites could not be protected.

(U) As this was happening, NSA engineers developed a pioneering concept known as EXPLORER, appropriately enough. This involved placing remote-controlled intercept systems in isolated areas, often where there were small bases of friendly troops.

(U) In late 1970, EXPLORER was placed on Hill 950 in Military Region I, with a Special Forces unit of four Americans and thirty-one Montagnards. The system had four receivers, all of them controlled by voice intercept operators at the Army Security Agency field station in Phu Bai. There were no COMINT-cleared personnel on Hill 950.

(U) It was calculated that the time delay between an operator's command in Phu Bai, the receiver acting on it at Hill 950, and relay of the signal back to the operator was less than a quarter of a second. The operator did not have to know that his intercept receiver was more than sixty miles away.

(U) The concept was validated by the quantity and quality of the intercept. EXPLORER, within a month, was producing up to 2,000 minutes of intercept every day, making it the second major producer of VHF intercept in Southeast Asia.

(U) When the concept was judged to be a success, EXPLORER was upgraded to eight receivers in March 1971. EXPLORER II was deployed in February 1971, and EXPLORER III in December.

(U) The original EXPLORER site was overrun by the North Vietnamese and Viet Cong in June 1971, not long after the upgrade, as part of a general enemy offensive. One American and about fifteen Montagnards were killed. The Special Forces unit and its allies were forced to withdraw in the face of this attack, but, before leaving, they used thermite to destroy the EXPLORER system.

(U) Ironically, the loss of the EXPLORER site helped gain acceptance for the concept of remoting. Had a COMINT site on Hill 950 been manned, there would have been forty or fifty cleared individuals on the hill, and the human losses could have been many times more tragic than they were.

(U) The success of EXPLORER pointed the way toward future methods of intercept in dangerous or hard-to-support areas.

(U) The photograph shows part of the intercept site at Phu Bai.

(U) Like to blog? Want to discuss historical topics with interested -- and interesting -- folks?

Visit the Center for Cryptologic History's blog, *History Rocks*. ("go history rocks")

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

NSADaily *Defending Our Nation. Securing The Future.*

(U) History Today - 26 July 2013

Run Date: 07/26/2013

(U) The Center for Cryptologic History is the occasional focal point for cryptologic-related questions from outside the Agency. One recent query involved dozens of century-old postcards posted from Ft. Myers, Virginia, to Berryville, Virginia in 1916. Among the lines of plain text on the cards were several of cipher text composed using unknown symbols.

(U) Historians at CCH immediately identified the mystery lines as the Freemason Cipher, also known as the Pig Pen Cipher.

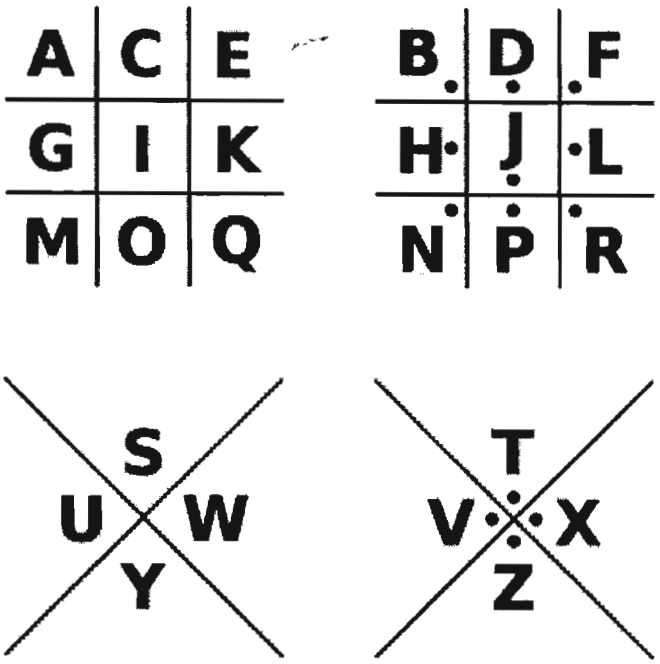
(U) Freemasons reportedly used this system to secure their communications from one lodge to another in the 17th and 18th centuries. This cipher substitutes simple geometric fragments for letters of the alphabet and has been popularly used for centuries to provide a modicum of privacy from the casual observer.

(U) To further confound a less-than-determined adversary, the Freemason Cipher can be used employing any of numerous variants and super-encipherment techniques. These enhancements were frequently used by Civil War prisoners of war in letters written to family and friends.

(U) In the case of the hastily composed postcards, the Freemason Cipher was the choice of two young lovers, William and Kitty. The author, more likely than not, lived in a crowded quarters and wished to keep his private thoughts from his companions and from the prying eyes of postal employees.

(U) In a happy postscript, the two were married a year later and enjoyed more than five decades of connubial bliss. The Center for Cryptologic History forwarded the solution as well as the Freemason Cipher variant key to William and Kitty's descendants so that they could access their treasure trove of family history.

(U) Try your hand at decrypting the two examples of William's tender words to Kitty by using the following key


A C E
G I K
M O Q
B D F
H J L
N P R
S
U W
Y
T
V X
Z

(U) History Today - 31 July 2013

(U) One of the first major long-distance bombing raids conducted by the U.S. Army Air Force in World War II was against the German-held oil fields at Ploesti in Rumania. The raid was launched on August 1, 1943.

(U) As it happened, German signals intelligence was able to pick up a lot of clues about the impending action.

(U) SIGINT units of the German Air Force High Command in Italy were monitoring the communications of the U.S. Ninth Bomber Command, operating out of Benghazi, Libya. The high volume of traffic related to practice missions in the last few weeks of June indicated that an unusual bombing raid was being planned.

(U) Just before the raid was launched on August 1, U.S. voice communications indicated to the Germans that a long-range flight by bombers was about to begin. Maintaining continuity on U.S. communications, the Germans followed the bombers on their normal course to Italy and then the sudden turn to the northeast. German SIGINT continued to locate the bombers as they flew over the Balkan region.

(U) In the early hours of the 1st, the Ploesti region went on alert. Fighter aircraft from nearby locations reinforced normal defenses at Ploesti.

(U) When U.S. planes were hit by German fire, they broadcast distress messages in the clear as they returned to base. This allowed German units along the route back from Rumania to Libya to locate and attack them.

(U) In the battle and its aftermath, the Germans downed fifty-three aircraft and there was a heavy toll in aircrews lost.

(U) There were many reasons for the heavy American losses in the Ploesti raid. However, it is apparent that poor communications security contributed significantly to the losses.

(U) The photograph shows an American bomber at Ploesti.

(U) Can't get enough cryptologic history? Come blog with us at *History Rocks*. (go history rocks)

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Comments/Suggestions about this article?

Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 10 December 2013

FROM: Center for Cryptologic History | Run Date: 12/10/2013

(U) On December 11, 1941, Germany and Italy declared war on the United States. This was in accord with their agreements under the Tripartite Agreement of September 1940, which had included Japan in their mutual military arrangements.

(U) The U.S. had been in a period of crisis with Germany ever since the United Kingdom and Germany went to war. There had been no direct clash between the two countries, however; this declaration was prompted by the fact that the U.S. and Japan were now at war.

(U) There had been a COMINT hint that this would occur.

(U) In 1940 the U.S. Army's cryptologic organization, the Signal Intelligence Service, had solved a Japanese machine-generated diplomatic cipher. This was known to the Americans as PURPLE. The Navy joined in exploiting this system, and the two services alternated days in decrypting and distributing intelligence from it.

(U) The Japanese ambassador in Berlin, Oshima Hiroshi, was also a lieutenant general in the army, and proved to be a lucrative source of information about German military matters.

(U) On August 14, 1941, Ambassador Oshima reported meeting a high-level contact who had been at German General Headquarters the previous day. The contact reported that questions about the United States had arisen in the meeting, and Adolph Hitler had said that "if a clash occurs by any chance between Japan and the United States, Germany will at once open war against the United States." Oshima was satisfied that the quotation was genuine.

(U) Britain's cryptologic organization, the Government Code & Cypher School, sent Prime Minister Winston Churchill a copy of the decrypt with this quotation Churchill asked whether President Franklin Roosevelt had seen it; the head of MI-6, Britain's Secret Intelligence Service, was able to confirm that FDR had indeed been given the decrypt.

(U) The photograph shows Oshima meeting Hitler.

(U) Like to blog? Want to discuss historical topics with interested -- and interesting -- folks? Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

(b)(3)-P.L. 86-36

Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 29 April 2014

FROM: Center for Cryptologic History | Run Date: 04/29/2014

(U) In the spring of 1975, as the South Vietnamese military crumbled under North Vietnamese attacks, a relative handful of NSA employees in Saigon continued to provide SIGINT support to the Americans still in country, mostly in the U.S. embassy.

(U) The personnel got reservations on the earliest flights possible to send their families out of the country. They themselves, however, stayed on as long as possible and resisted suggestions that they depart. More than once the senior NSA official had to issue a blunt order to a subordinate to leave the country.

(U) Four NSA personnel were still working in country when intercept in April made it clear that the final North Vietnamese assault on Saigon was imminent. The information showed that the attack would begin in the area of Tan Son Nhut airbase -- where the NSA personnel were located -- although the timing was uncertain because leaders of the Communist forces were themselves not sure how soon they could be in position to commence.

(U) The senior NSA person was astounded to find that this SIGINT warning was not being accepted in the U.S. embassy. Senior people there believed that the enemy was engaging in communications deception to intimidate the South Vietnamese.

(U) The attack began at Tan Son Nhut with an aerial bombardment on April 28, followed by artillery.

(U) The last group of NSA personnel was evacuated by helicopter to a U.S. ship on April 29. They found that only a few of their South Vietnamese colleagues escaped; most were left behind.

(U) The senior NSAer from Saigon recalled, "...it is clear that there was much about the ending that left bitterness in our mouths. But when I look back, I'm glad I was there for the end. As long as I live, I will ever be grateful and immoderately proud of the NSA people who were there, doing the best they could because it was worth doing."

(U) Discuss historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

(b)(3)-P.L. 86-36

[redacted]

Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 17 June 2014 - Gene Grabeel

Run Date: 06/17/2014

(U) Former schoolteacher Gene Grabeel was hired in 1943 by one of NSA's predecessors to begin a cryptologic effort against a target that had been neglected during the war. Soon she and an Army officer began looking over the collected traffic: Russian diplomatic cables. Or so they were believed to be. It turned out that there was KGB and GRU (secret police, more or less) traffic among the diplomatic cables.

(U) This was the beginning of the project known today as VENONA.

(U) Grabeel stayed in various leadership roles on the VENONA effort, even though others became more prominent at the phenomenally difficult cryptanalysis involved. The VENONA traffic was a code, which was vulnerable to what we call bookbreaking, but was superenciphered with one-time pads, a series of random numbers rendering the system unbreakable. However, fortunately for the U.S., wartime pressures had caused the Soviets to reuse some one-time pads, making some messages just barely vulnerable to decryption -- "two-time pads" are merely almost unbreakable.

(U) As a result of their efforts on VENONA (among other things, in some cases), people such as Meredith Gardner, Genevieve Grotjan Feinstein, and Richard Leibler were inducted into the Cryptologic Hall of Honor. Another result of those efforts was people like Julius and Ethel Rosenberg, Klaus Fuchs, Alger Hiss, and William Weisband* losing their jobs, or worse.

(U) The only vulnerable traffic was from about 1940 to 1948; as time went on, Grabeel and her cohorts worked increasingly aged traffic, although it remained valuable for many years. She was not the only one who stayed for decades; the work took so long to understand that it did not encourage new people to come in and learn how to do it.

(U) Grabeel retired in 1973, after thirty years on that same target. The VENONA effort was finally halted in 1980, when the amount of return from working the decades-old traffic was no longer deemed worth the effort involved.

(U) The *Cryptologic Almanac* overview of VENONA is here; the Center for Cryptologic History's VENONA Story is also available, as is a three-volume *History of VENONA*.

(U) The photos show Grabeel at the start of her career, and in 1995, when her and her colleagues' work was declassified and announced to an astonished world.

**Or see his Intellipedia entry on Intelink.*(U) Discuss historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").

(U) Larger view of photo 1 - Larger view of photo 2

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 23 July 2014

Run Date: 07/23/2014

(U) U.S. forces during the Vietnam War unfortunately tended to underestimate the technical capabilities of the enemy forces. This led to carelessness in the use of communications. All too many radio messages from American or South Vietnamese units were sent in plain language or using rudimentary, self-made cipher systems.

(U) Interrogation of enemy prisoners or defectors often revealed that their forces had highly proficient SIGINT capabilities. It often happened that the only limitation on the exploitation of U.S. radio messages was a lack of personnel who understood English.

(U) One "rallier," who defected in 1967 after ten years with the Viet Cong, told how his unit had gotten extremely accurate information about U.S. operations from their own intercept and from North Vietnamese intelligence reports that had obviously been based on COMINT.

(U) He claimed that in his ten years fighting, his unit had never been taken by surprise.

(U) One mark of the other side's proficiency was their ability to intrude successfully on U.S. communications nets. In one instance, at the U.S. air base in Da Nang, the Viet Cong used equipment at a captured guard post to send the American guard force to the opposite side of the base from where they intended to attack. Their subsequent attack caused millions of dollars in damage.

(U) At the American base at Pleiku, the Viet Cong imitated the voice of a guard sergeant with a Hispanic accent, said that they were preparing hot food, and asked for the number of troops in each bunker. Fortunately, something went wrong with the communication and the deception was recognized.

(U) A redacted version of this book is available on the NSA website on the worldwide web, and mirrored on NSAnet at:

[redacted]

(U) The photo of an enemy radioman was captured during the war. It is not clear whether he is working with his own communications or performing intercept.

(U) Discuss historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

DERIVED FROM: NSA/CSSM 1-52, DATED: 20130930, DECLASSIFY ON: 20380930
Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

(U) History Today - 02 July 2014

Run Date: 07/02/2014

Throughout the early summer of 1863, Union Army and Navy units under MG Ulysses Grant and Admiral David Porter laid siege to Vicksburg, one of the last Confederate strongholds on the Mississippi River.

During the siege, the Confederates had insight into Union movements because they were copying Union flag signals and solving the cipher system that protected messages. All too often, however, the inside knowledge had little effect because the besieged Confederates did not have the force available to take appropriate actions.

A Confederate position on the Devil's Backbone, a hill north of the city, allowed signalmen to observe the Union signal station and copy messages sent out by flag. At this time, the Confederates had solved the Union cipher system and could read the messages. Commander of the observation position was Mathew H. Asbury, a Signal Corps officer from Louisiana.

In early July, fighting was suspended while Grant considered the latest proposal concerning capitulation from General John C. Pemberton, commander of the garrison inside Vicksburg.

On the night of July 3, a message was sent from Grant's headquarters to Admiral Porter. (The visual signal system used flags in daylight, torches at night.)

The message said that the Union council of generals had recommended that all personnel captured at Vicksburg be sent north to prison camps. However, Grant had decided that he could not spare enough guards and transport ships to do this. He also believed that the Vicksburg garrison was so demoralized that its men, if paroled, would spread dissatisfaction wherever they went throughout the south.

Inside Vicksburg, this secretly acquired knowledge that they would be spared imprisonment apparently made the difference in the decision to give up the city.

Pemberton decided to surrender Vicksburg on July 4. He and his men were paroled, but they gave up a large store of weaponry to the Union forces.

Disgraced, Pemberton was never given another command as a general officer. He accepted an assignment as a lieutenant colonel in an artillery unit. A native of Pennsylvania, Pemberton returned to his home state after the war.

The key message on July 3 was genuine; that is, it gave a true account of the decision by Grant to reject the recommendation of his senior officers. Looking at the situation in the light of the modern experience of COMINT, however, one wonders if it might have been sent knowingly, with a recognition that the Confederates could read Union signals and with the hope that it would push the Confederates into surrender. This is nowhere confirmed in available records and remains nothing more than speculation.

(U) Discuss historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 14 July 2014

Run Date: 07/14/2014

(U) MEMORIES OF STONEHOUSE

(U) During the Cold War NSA operated a collection facility at the Army's Kagnew Station in Asmara, Ethiopia. The Stonehouse facility had an 85-foot antenna and a 150-foot antenna. The antenna feeds were frequently changed for special events, and John O'Hara, an NSA senior scientist, would sometimes head TDY teams responsible for those changes. Here are some of his memories of Stonehouse/Asmara from his TDYs.

(U) Kagnew Station was originally created as an Italian communication facility during WWII and was named Radio Marina. After the Italians were defeated there in 1941, it was controlled by the British military administration until 1943, when they handed it over to the United States.

(U) The Stonehouse facility was located about a mile outside the city of Asmara. While commuting to and from the facility on the very narrow roads and streets, one would frequently have to stop or slow down due to drovers moving their flocks of sheep or cattle against the background of giant antennas. This led one member of our team to remark that they were living in both the first and twentieth centuries.

(U) The city of Asmara and the surrounding countryside were very pretty. One evening we piled into three vehicles and went to a place called "The Escarpment." Just as the sun was setting, we saw a caravan of people on foot crest a mountain top near us and we watched them pitch camp for the night. The men were bearing huge baskets hanging from bars on their shoulders, and the women were bearing packs on their backs; we were told they were people collecting cactus fruit. This was like a scene from the Bible.

(U) We would be provided with a rental car. When we would first take it out, the gas meter was always on zero. There would be only enough gas to make it to the nearest service station, which was owned by the same guy who owned the rental car place.

(U) The hotel rarely had hot water for bathing. The water was either cold or at best lukewarm. We were told that the water in the hotel where we stayed was unsafe to drink so we would lug gallon bottles of Gatorade from Kagnew Station back to the hotel to drink and brush our teeth.

(U) The hotel was near Emperor Haile Selassie's palace, where the Emperor kept lions They would start roaring very early in the morning and we could hear them from our hotel. We referred to them as "Selassie's roosters."

(U) Changing antenna feeds on those monster antennas was no trivial task. You certainly could not be afraid of heights, because the feed for the 150-foot antenna was about 100 feet above the ground. Feed changes would sometimes be delayed because high winds precluded working at those heights.

(U) Eritrea was an independent state that had been ceded to Ethiopia as a protectorate by the League of Nations after World War One. In 1961 Ethiopia annexed it as a province. This led to establishment of the Eritrean Liberation Front (ELF) and its quest for independence.

(U) The ELF was fighting for independence from Ethiopia (which they finally won in 1991), and they were conducting guerrilla warfare. As a result, the Ethiopian authorities halted any traffic in and out of the city from sundown to sunrise. The ELF was ambushing and kidnapping people and holding them for ransom; if no ransom was paid, the hostages were frequently killed. We were instructed never to go out on the streets alone. If one drove out of the gates of the city, there had to be at least two vehicles. Since we had to drive into the desert to bore sight the antennas, this applied to us.

(U) On one bore sight trip we were miles from Asmara in what appeared to be an uninhabited area. After we were there for about an hour, a group of about ten pre-teenage boys appeared and started pestering us for money and cigarettes. We could see no houses or tents for miles, so we wondered where on earth they came from.

(U) We frequently worked long hours. One night I returned to the hotel about 10 p.m. to find two heavily armed soldiers standing at the outside entrance; there were two more inside. This was a little surprising, but when I got off the elevator at my floor, two more armed soldiers were standing there. I was now very curious, so I went back down to the front desk and asked what was happening. The guy at the desk said some General was having a meeting and the guards were just there to provide protection from any possible ELF attacks. I was so tired that I had no trouble falling asleep but I was glad to see that the soldiers were gone the next morning.

(U) Emperor Haile Selassie would occasionally come by in a motorcade and there would be thousands of people on the street to watch him go by. On one such occasion I saw mounted police use their horses to forcibly move people out of the way in a very nasty manner.

(U) Thanks to the chief of security at Kagnew Station, I received a private tour of Haile Selassie's palace grounds, conducted by Selassie's chief of security. That was a unique experience. The palace grounds were very opulent and were like a zoo, with all kinds of exotic birds and lions. I was really impressed with Selassie's heavily gilded private chapel.

(U) The palace grounds were enclosed by thick walls, and I often wondered how many Ethiopians actually got to see or know what was behind them. The ELF eventually did get an independent Eritrea. I wonder what happened to the animals and what the status of the palace is today.

(U) Haile Selassie was emperor of Ethiopia from 1930 to 1974, when he was overthrown. He was thought to be a descendant of King Solomon and the Queen of Sheba and was widely known as the Lion of Judah; many of his followers considered him to be divine. It is not clear how he died, but his body was supposedly found in 1975 buried under a toilet on the palace grounds.

(U) For a photograph of Emperor Haile Selassie visiting Kagnew Station, see the History Today of January 12, 2005.

U) Discuss historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 26 June 2014

Run Date: 06/26/2014

(U) Early in World War II, the German military had commandos tasked with capturing enemy intelligence documents. These units could operate ahead of the front lines, and might wear enemy uniforms to gain the access they sought

(U) These units operated during the German invasions of Poland, Yugoslavia, and Greece early in the war. British authorities learned from decrypts of messages that commandos in Athens had immediately raided British Army Headquarters in search of documents

(U) Several British officers pushed for creation of a similar unit One of those advocating this was CDR Ian Fleming, pictured, a special assistant to Admiral John Godfrey, director of Royal Navy Intelligence.

(U) This resulted in the establishment of 30 Commando, also known as the Admiralty Intelligence Unit, also known as 30 Assault Unit, or, less formally, as "Fleming's Private Army." Operating first in North Africa, over the course of the war, this unit captured invaluable material the Germans had kept secret A good deal of this was cryptologic material, including cipher machines and many documents on German cryptanalytic work against Allied ciphers

(U) This effort probably was a precursor to the TICOM (Target Intelligence Committee) teams of personnel from Bletchley Park who were sent into recently liberated areas near the end of the war Their mission also was to acquire cryptologic materials as well as identify German cryptologic personnel

(U) Fleming in the course of the war came up with other proposals for covert operations, hoping to be part of the action However, he knew too much and was never allowed to travel to locations where he might be captured Yes, this is the Ian Fleming that wrote the James Bond novels after the war.

(U) Discuss historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks")

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified. 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

DERIVED FROM: NSA/CSSM 1-52, DATED: 20130930, DECLASSIFY ON: 20380930
Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

NSA Daily *Defending Our Nation. Securing The Future.*

(U) HISTORY TODAY - 12 September 2014

Run Date: 09/12/2014

(U) We hear a lot about the SIGINT successes of the Allies in World War II, but less about the achievements of the Axis -- which were, fortunately, few in number.

(U) During the war, plans were made for U.S. or UK forces to be based in the Soviet Union: some of them, including the setup of a UK SIGINT intercept (Y) site at Polyarnoe known as "Wye Cottage," came to fruition.

(U) Another site was in Poltava, USSR (now Poltava, Ukraine), where the U.S. Army Air Force (USAAF) built a base. The idea was to shuttle bombers: planes flying from elsewhere would hit their targets, land at Poltava, refuel and rearm, and then attack other targets on the way back to their homebase. The whole plan was called OPERATION FRANTIC.

(U) OPERATION FRANTIC, like other attempts to base U.S./UK forces in the USSR, was dogged by Soviet intransigence from the start, and after a major German airstrike on June 21, 1944, the project dwindled in size and ended in September 1944.

(U) The German airstrike was the result of work by the Luftwaffe's cryptanalytic bureau, the Chiffrierstelle, Oberbefehlshaber der Luftwaffe (Chi-Stelle-OBdL). The Chi-Stelle-OBdL learned of a USAAF overflight going to Russia, and was able to determine the day it would occur, but not the final landing site in Russia. This turned out to be enough, as a Luftwaffe force was alerted, followed the overflight to Russia, and attacked the USAAF bombers after they landed.

(U) During interrogation after the war by TICOM (Target Intelligence Committee), Hermann Goering described this as the only example he could remember of Chi-Stelle-OBdL having a success against high-level traffic.

(U) The TICOM program was a joint British-U.S. effort at the end of the war to capture German cryptologic personnel, records, and equipment. Read an article about TICOM in a *History Today* from April 14, 2014.

(U) The photograph shows the FRANTIC airfield, with both U.S. and Soviet aircraft.

(U) Discuss historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks")

(U) Larger view of graphic.

(U) Have a question or comment on *History Today*? Contact us at DL cch or cch@nsa.ic.gov.

(U) FRANTIC airfield, with both U.S. and Soviet aircraft.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

DERIVED FROM: NSA/CSSM 1-52, DATED: 20130930, DECLASSIFY ON: 20380930
Dynamic Page -- Highest Possible Classification is
~~TOP SECRET//SI/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL~~

(b)(3)-P.L. 86-36

[redacted]

1/23/2015

NSA Daily *Defending Our Nation. Securing The Future.*

(U) History Today - 10 July 2014

Run Date: 07/10/2014

(U) After a period of slow advances over the Owen Stanley Mountains in New Guinea, in which U.S. and Australian forces made limited gains at a cost of heavy casualties, the commander of the Southwest Pacific Theater, General Douglas MacArthur, in mid-1944 launched a daring series of amphibious landings behind Japanese lines to capture enemy bases on the north coast of New Guinea.

(U) MacArthur was supported in his decisions by decrypts of Japanese communications that revealed accurate data about enemy strength and deployments. As the battle was being fought, decrypts about movements of enemy reinforcements forward allowed General George Kenney, MacArthur's air officer, to prevent them from intervening in the battle.

(U) The decrypts for planning were produced by Central Bureau (CB), a combined U.S. and Australian cryptologic organization. The commander of CB was Colonel Abraham Sinkov, one of William Friedman's original staff, now in uniform.

(U) As the struggle to control New Guinea continued, CB consistently provided high-quality COMINT to MacArthur and Kenney about the Japanese troop numbers, status, and supply situation. Tactical intercept also was vital to decision making.

(U) A decrypt of a Japanese message sent on May 28 revealed Japanese plans for a counterattack on American positions in the coastal city of Aitape. The Japanese 18th Army listed the supplies it needed for the attack and said that they had to arrive at the port of Wewak by the end of June. A message of June 20 said that the attack was to begin about 10 July, with a strength of 20,000 Japanese troops. This message also explained the deployment of each enemy division in the attack.

(U) The attack happened as described, but the Americans were ready for it. The decrypt of an after-action report from the Japanese commander showed that most Japanese artillery had been destroyed and a large number of troops lost. The supply situation was dire: the commander illustrated this by saying the men had made ten-days' ration of rice last twenty-five days by eating it raw instead of cooking it.

(U) The photograph shows Americans landing at Aitape.

(U) Discuss historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").

(U) Larger view of photo

(U) Have a question or comment on "History Today"? Contact us at DL cch or cch@nsa.

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed: 01/23/2015

[508 Accessibility]

(b)(3)-P.L. 86-36

NSA Daily *Defending Our Nation. Securing The Future.*

(U) HISTORY TODAY - 16 January 2015

Run Date: 01/16/2015

(U) The recent motion picture about Alan Turing, *The Imitation Game*, shows many of the interesting characters who worked at Bletchley Park during World War II. In order to emphasize certain aspects about the life of Dr. Turing, the script sometimes portrayed these other characters differently from the way they were in real life.

(U) One of these was John Cairncross, who -- after the end of the war -- confessed to spying for the Soviet Union.

(U) Although much about his spying career is still murky, *History Today* would like to compare what we do know with the way Cairncross was portrayed in the film.

(U) SPOILER ALERT ON: In *The Imitation Game*, Caincross is portrayed as a cryptanalyst working in the section headed by Alan Turing, which is trying to solve the German Navy ENIGMA machine and develop the cryptanalytic *bombe* to exploit it on a regular basis. In a private conversation, Cairncross reveals that he has recognized that Turing is homosexual. When Turing later finds out that Cairncross is secretly bootlegging decrypts to the Soviet Union, Cairncross stops him from revealing this by threatening to make Turing's secret public. Later, Turing learns that British intelligence knew of Cairncross' illicit life all along and was using him to pass disinformation to the Soviet leader, Joseph Stalin. **SPOILER ALERT OFF**

(U) In the 1930s, Arnold Deutsch was one of the most effective Soviet agents in the West. Assigned to the UK, Deutsch recognized that the government recruited heavily from among those who attended elite universities. Accordingly, he recruited at least four promising individuals at Cambridge University. During the worldwide Depression many students and professors flirted with Communism; a few actually saw the USSR as a model for the future and were willing to engage in underground activities.

(U) Three of the "Cambridge Four" -- H.A.R. "Kim" Philby, Donald MacLean, and Guy Burgess -- entered the British diplomatic and intelligence services after graduation; Anthony Blunt, a professor, joined British counterintelligence during the war. Altogether, they provided a large trove of British secret documents to the Soviets.

(U) John Cairncross, born 1913, came from the working class but attended the University of Glasgow and Trinity College, Cambridge. Placing first in the Civil Service examination, he was accepted into the Foreign Office. When war came and he was about to be taken into the Army, he arranged a transfer to Bletchley Park on the strength of his knowledge of foreign languages.

(U) It is not clear when and how he was recruited as a spy. It has been speculated that he joined the Communist Party as early as 1937.

(U) In addition to general knowledge of British SIGINT activities, Cairncross gave the Soviets decrypts from the German TUNNY machine, a sophisticated cipher device used by senior enemy commanders. It is most likely that the information Cairncross provided enabled the Soviets to prepare in advance for the major German offensive at Kursk in 1943.

(U) Prime Minister Winston Churchill had been passing warnings about the upcoming battle in the form of sanitized SIGINT reports. The material Cairncross provided was more detailed. Moreover, Stalin

placed more confidence in intelligence information that was obtained through covert channels.

(U) There is no evidence that British intelligence services were cognizant of Cairncross' espionage activities at the time, nor that they used him to send false information to the Soviets.

(U) In 1944 Cairncross transferred to the MI-6 counterintelligence section, where he worked for -- Kim Philby. Coincidence? Perhaps. Whatever the truth, Cairncross was able to continue passing decrypts to the Soviets; his section received SIGINT needed for its work.

(U) Two of the Cambridge spies, Burgess and MacLean, escaped to the Soviet Union in 1951, just before they were to be arrested. Papers found during the subsequent investigation implicated Cairncross. He was fired from the government, but not prosecuted.

(U) Cairncross worked as a professor of French at two U.S. universities, specializing in 17th century poets. Later, he worked at a bank in Rome. After his secret life became public, he retired to the south of France and died there in 1995.

(U) Historians of espionage have often argued that the Cambridge Four were actually a quintet; they debate whether or not Cairncross was that fifth man. A defector from the KGB in the 1990s said he was, but that did not end the debate. There was only a little interaction among group members; their common factor was the place of their recruitment. The other members of the Cambridge spy ring were from the upper class, whereas Cairncross was not, and, anyway, Cairncross had a reputation as a loner.

(U) In *The Imitation Game*, Cairncross is shown as a mathematical cryptanalyst who worked in the same section as Alan Turing. In actuality, Cairncross translated decrypts from the German and barely knew Turing. His autobiography, *The Enigma Spy*, published posthumously in 1997, mentioned Turing only once, in an offhand way.

(U) Cairncross wrote: "I never got to know anyone apart from my direct operational colleagues. We did eight fully-occupied hours of work and then were transported back to our respective lodgings with families in the surrounding villages. Even within my hut [work place], I never met some of the more important personalities...."

(U) *The Enigma Spy* is available on a noncirculating basis from the library at the National Cryptologic Museum.

(U) Share historical topics with interesting folks. Visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").

(U) Have a question or comment on *History Today*? Contact us at DL cch or cch@nsa.ic.gov

Content Steward: Corporate Communications, Messaging & Public Affairs, DN1, 963-5901 (email)
Page Publisher: Corporate Web Solutions, DN22, 963-8642 (email)

Last Modified: 01/23/2015 | Last Reviewed. 01/23/2015

[508 Accessibility]