

~~TOP SECRET UMBRA~~

Chapter 4

The Soviet Problem

THE EARLY DAYS

From Stettin in the Baltic to Trieste in the Adriatic, an iron curtain has descended across the Continent. Behind that line lie all the capitals of the ancient states of central and eastern Europe . . . all these famous cities lie in what I might call the Soviet sphere, and all are subject, in one form or another, not only to Soviet influence but to a very high and in some cases increasing measure of control from Moscow.

Winston Churchill, 6 March 1946

The end of World War II did not result in a large number of unemployed cryptologists. That it did not was due almost entirely to the advent of the Cold War and an increasing concern with what came to be called the Soviet Bloc. (In the 1950s, believing in a worldwide Communist conspiracy, Americans called it the Sino-Soviet Bloc.)

Wartime cooperation with the Soviet Union began to break down in early 1945. Through a series of late-war conferences among the Allies, it became clear to the West that the Soviet Union did not intend to retreat from Eastern Europe at the end of the war. An increasingly frustrated Roosevelt administration became less and less constrained about public references to the rift with Stalin, but Roosevelt himself remained convinced up to his death in April 1945 that the rift could be healed by diplomacy. His successor, Harry Truman, did not share this optimism.

The administration moved to check Soviet expansionism abroad. As a result of strong pressure, Stalin removed Soviet troops from Iran later in the year. Meanwhile, Greece was faced with a USSR-inspired internal Communist threat, while neighbor Turkey faced an external threat by Soviet divisions massed on its borders. Truman again faced down Stalin, announcing the Truman Doctrine, a promise to come to the aid of countries in that area faced with Communist subversion or external threats. Administration policy toward the USSR hardened with the publication, in the magazine *Foreign Affairs*, of an article by George Kennan, late deputy chief of mission in Moscow, postulating the Cold War doctrine which became known as "containment."

The next year a democratically elected government in Czechoslovakia fell to a Communist coup, and the new government became an effective satellite of the USSR. Meanwhile, Soviet troops remained in Poland and East Germany, while Communist governments took over in Hungary and the Balkans. In June 1948 Stalin tried to cut Berlin off from the West, and Truman initiated the Berlin Airlift to resupply the city. The

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Truman administration also saw the Korean War as the first move in a Soviet-inspired military offensive.

The Advent of BOURBON

American cryptology had dabbled with the Soviet problem over the years, with indifferent success. Yardley, in his book *The American Black Chamber*, claimed to have broken Soviet diplomatic codes. The truth is that, though Yardley's MI-8 worked Soviet diplomatic traffic, only a single instance of success was ever recorded, and in that case the transposition being attacked was based on the German language.¹

Friedman's Signal Intelligence Service obtained MI-8's traffic upon MI-8's demise in 1929 and made a brief, unsuccessful attempt to solve the codes. Then in 1931 a Soviet espionage front posing as a trading company called AMTORG came under the glare of Representative Hamilton Fish of New York, who subpoenaed some 3,000 AMTORG cables from the cable companies in New York. Fish turned them over to OP-20-G, which, having at the time only two cryptanalysts (Safford and Wenger), failed to solve them. The cables were then transferred to SIS, which also blunted its spear. This was virtually the only attempt at Soviet diplomatic traffic by the services during the 1930s, and Friedman's people doubted that any Soviet codes could be solved.²

They were, in fact, wrong. [REDACTED] attack on Soviet military systems throughout the 1930s. The primary target was COMINTERN (Communist International) traffic, [REDACTED] But when, in June of 1941, Hitler's army invaded Russia, the British allowed the Soviet problem to wither. GCCS made a brief attempt to turn the USSR into a COMINT Third Party, and even established an intercept site in Russia near Murmansk in 1941. The dialogue came to a quick halt when the Soviets began inquiring into British success against ENIGMA. In 1942, the Radio Security Service and the London Metropolitan Police discovered an extensive Soviet illicit network in Great Britain, and Stewart Menzies, head of British intelligence, directed that work be renewed against Soviet communications, especially KGB, GRU, and COMINTERN nets likely to carry information of counterintelligence value.³

In the United States, SIS was collecting a small amount of Soviet traffic on a casual basis as early as 1942. On 1 February 1943 the Army opened up a two-person Soviet section. The inspiration for this effort was the Army's successful attack on Japanese diplomatic communications, in which the Japanese discussed their efforts against Soviet systems. The Japanese material gave SIS some handholds into Soviet systems. OP-20-G came in later, opening both intercept and cryptanalytic study in July 1943. Because the USSR was a wartime ally, the effort was rigidly compartmented and known to only a few. In August 1943 the Army and Navy cryptologists began cooperating on the new Soviet

(b) (1)
(b) (3)-50 USC
403

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

problem and, during 1943 and 1944, cooperatively worked a number of Soviet cryptographic systems.⁴

Meantime, the Navy, in order to collect Soviet naval traffic, had opened up an intercept effort at Bainbridge Island in Washington State. Tightly controlled, it was headed by Louis Tordella, later the deputy director of NSA.⁵

By the end of the war, both cryptologic organizations were mounting extensive efforts against Soviet communications, despite the official designation of the USSR as an ally. OP-20-G, concentrating on Soviet naval communications in the Pacific from Skaggs Island and Bainbridge, employed 192 people, while ASA had almost 100. They had both been surreptitiously training Russian linguists for a year.

But the effort was charged with political implications. Roosevelt was trying to maintain the fragile alliance with the USSR and was being challenged on the left by Henry Wallace, a potential political rival who felt the administration was anti-Soviet.

In this atmosphere Brigadier General Carter Clarke of the Army G-2 paid a visit to Preston Corderman (chief, SIS) and Frank Rowlett several months before the end of the war. Clarke said that he had received informal instructions - allegedly from the White House - to cease any effort against the Soviet problem. It appeared that someone in the White House had gotten word of the compartmented Soviet problem and had concluded that it did not accord with the current diplomatic situation. (It was discovered years later that the White House staff was in fact infiltrated by a single Communist or "fellow traveler," who may have been in a position to know about the Army program.) Clarke did not desire that the program be closed, and in fact SIS (soon to be renamed ASA) received a steady increase in resources for the program.⁶

In June 1945, with the war coming to an end, the Navy proposed formal collaboration with the Army on the Soviet problem, which was then referred to as the RATTAN project. The Army wanted a more integrated effort, but they eventually agreed to organize under the more decentralized Navy scheme.

At the same time, ANCIB proposed to LSIB that their cooperation against Germany, Italy, and Japan now be extended to include the USSR. The Americans proposed that the cooperation be fully as close as it had been during the war. This included sharing all details, including the status and method of cryptanalytic attack, and the exchange of raw traffic and code/cipher recoveries. The British agreed, and in August the two sides arrived at an unwritten agreement predicated on an understanding arrived at in June between Rear Admiral Hewlett Thebaud, chairman of ANCIB, and [redacted] for LSIB. This historic agreement extended bilateral cooperation into the Cold War and established the basis for what became known as the BRUSA Agreement. The two sides agreed to call the new project BOURBON.⁷

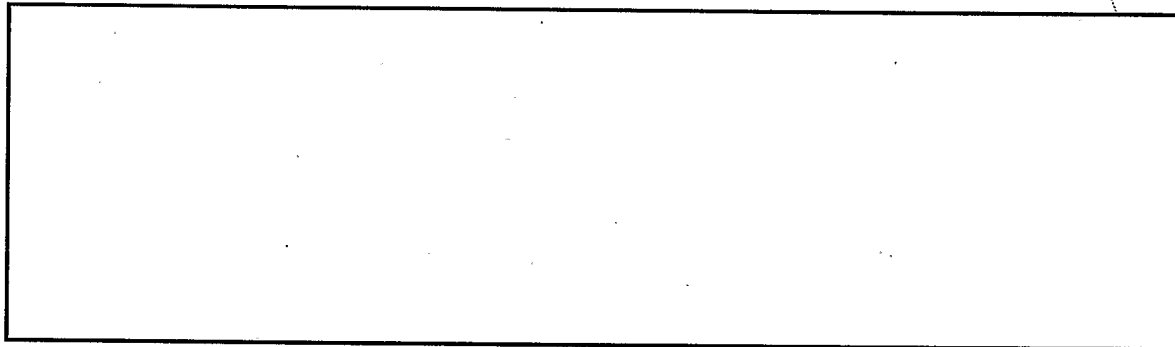
(b) (3) - P.L.
86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

During the mid-1940s the two sides mounted a relentless attack on the wartime generation of Soviet ciphers. The British provided much of the cryptanalytic expertise, the Americans most of the processing capability. They used whatever material they could get their hands on, including information on the Japanese cryptanalytic attack. TICOM debriefings of German cryptologists also gave the two partners useful information about Soviet systems.



VENONA

Alone and compartmented, the effort against Soviet diplomatic traffic had continued throughout World War II. In the long run this tightly held problem would have the greatest impact on American history in the postwar period and would become the most widely known. It was called VENONA.

In the early years of the war, the Army received incidental Soviet diplomatic traffic, most of it through its arrangements with the cable companies, which carried a large bulk of common-user communications. Since New York was the terminal for the transatlantic cable, Soviet diplomatic traffic was routed through that city. The Army arranged with the cable companies to get copies of most of the cables that the Soviets were sending, both to and from Washington and, more important, to and from AMTORG. Much of this traffic was believed to be KGB-related.

In 1943, ASA had mounted a secret effort to attack these communications, but they looked impossible. They were produced from codebooks enciphered by means of one-time additive tables. Assuming no re-use, there was no point in continuing. But ASA was not assuming anything, and Lieutenant Richard T. Hallock of ASA directed that his small section machine punch and process the beginnings and endings of some 5,000 messages to test for depths. In October 1943, ASA found the first indication that the additive pads may have been used more than once, a find which was to change the history of the postwar world.⁹

Hallock and his small band of cryptanalysts had found what is called "manufacturer's re-use" caused by the first German invasion of the Soviet Union in 1941. The KGB's additive pad generating facility produced two sets of some pads, presumably because of the

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

pressures associated with the rapid German advance toward Moscow. These were disseminated to widely separated KGB organizations, which were unaware that they had duplicate pads. ASA never found depths of more than two, and at that depth, decryption was only theoretically possible but practically a back-breaking job, assuming one ever got hold of the depths themselves.

Months went by, but finally ASA cryptanalysts, in November of 1944, were rewarded with their first depth. This was followed by others, and it appeared that they might be able to eventually break some traffic. But the job still looked gargantuan.

While one section worked on identifying depths, another worked on the underlying codebooks that were slowly emerging from under the additive key. This effort was led by a reclusive linguist and bookbreaker named Meredith Gardner. A Texan originally, Gardner had obtained a Master of Arts in German from the University of Texas and had been a Ph.D. candidate at the University of Wisconsin before going to work teaching at the University of Akron. He had joined SIS in 1942, and although he began in the German section, he quickly switched to Japanese, where he proved his linguistic gifts by picking up this extremely difficult language in just three months. At the end of the war, he switched again, this time to the Soviet problem and spent his first several months learning Russian. In December 1946, he had only recently emerged from language school when he made a major break into a KGB message, decrypting and translating a digraphic sequence of a 1944 message from New York to Moscow sending English text. Gardner found that the KGB used the code values for "spell" and "end spell" anytime they needed to encrypt a foreign word or other term that did not appear in the codebook. It was these two values that yielded many of the early breaks.

In December 1946, Gardner broke a portion of a KGB message that listed American scientists working on the atomic bomb. This message turned heads. Why would the KGB be interested in such information? ASA immediately turned the translation over to the Army G-2, and Carter Clarke had General Omar Bradley, the Army chief of staff, briefed on the message. G-2 expressed a continuing interest in any messages that contained like information.¹⁰

Through the war ASA had proceeded virtually unaided, but after World War II several outside factors speeded the tortuously slow process of additive key diagnosis and recovery and bookbreaking. The first was the defection of a Soviet GRU cipher clerk, Igor Gouzenko, from the Soviet embassy in Ottawa, in September 1945. The case caused a sensation because Gouzenko indicated the existence of a possible Soviet effort against the American atomic research effort.¹¹

Because Gouzenko worked with communications, Frank Rowlett of ASA was invited to interrogate him. During his sessions Rowlett learned much about the way the KGB codebooks were put together and how the additives were used. This information cut time off ASA's cryptanalysis effort.¹²

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

A second outside source of information was a 1944 FBI burglary of AMTORG, during which the agents carried off stacks of unenciphered messages with their cipher text equivalents. In 1948 the FBI turned over this bonanza to Gardner, who began comparing the traffic against transmitted messages. In this way he could identify some of the code group meanings because he had both plain and cipher texts.¹³

A third outside source was called "Stella Polaris," a Byzantine story which began in the early days of World War II. When, in June 1941, Germany invaded the USSR, the Finns went to war against the Soviets, siding with Germany against their mortal enemy. On 22 June a Finnish unit, presumably security police, entered the Soviet consulate in the Finnish town of Petsamo, near the Russo-Finnish border. Here they found the Soviet communications people frantically destroying cryptographic material. Some of it was burned beyond use, but certain of the codebooks were recovered more or less intact. These codebooks were property of the First Chief Directorate of the KGB - they were, in fact, the same codebooks which, in the mid-1940s, Meredith Gardner was working on.

The charred codebook fragments were turned over to the Finnish COMINT service, headed by one Colonel Hallamaa. By 1944 the war was not going well for Germany, and Hallamaa became concerned about an impending Soviet invasion of his homeland. He arranged to smuggle the contents of the Finnish COMINT archives, including the Petsamo trove, to Sweden, where photocopies were made. Copies of the Petsamo materials wound up in the hands of the Swedish, German, and Japanese COMINT organizations. Along with the documents went Hallamaa and the entire Finnish COMINT service.

At some point information got out to the newspapers, and the fact that Finnish intelligence people were working hand in glove with the Swedes became public knowledge. Knowing that the KGB was almost certainly after him, Hallamaa and most of his people fled to France, where, after the war, they worked nominally with the French intelligence people, but were actually controlled, according to some sources, by the British. So it was that the British got their own copies of the Petsamo codebooks. At the same time (1945) an OSS representative began working with Hallamaa, and the OSS, too, received its own copies (although not, perhaps, a complete set).

The codebooks eventually made their way to ASA and AFSA. Since by this time a number of intelligence services had copies, which source did AFSA get? In the days after the war, a TICOM team obtained a copy from the Germans, and it was this set that first made it all the way to Meredith Gardner's office. Shortly thereafter AFSA began obtaining Petsamo materials from the British under the codename Source 267 and may, at some point, have received copies from OSS/CIG, but these were no more than duplicates of materials they already had.¹⁴

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The Stella Polaris find did not break the KGB codes. They were fragmentary and pertained only to one version, [REDACTED]

[REDACTED] But they did shorten the time involved in the laborious bookbreaking process by providing Gardner with "models" of Soviet codes on which to base his own recoveries.

After reading some of Gardner's earlier translations showing the scope of KGB operations in the United States, Carter Clarke, the Army G-2, called on the FBI for help. His first contact was in July 1947; it was with Wesley Reynolds, the FBI liaison with Army G-2. Reynolds had joined the FBI in New York in 1941 after several years of law practice with his father and older brother. He had begun liaison work with G-2 in 1942, and ten years later jumped ship to NSA, where he became NSA's first professional chief of security.



Wesley Reynolds served as a link in the NSA-FBI liaison and later became NSA's chief of security.

Reynolds concluded that VENONA could turn out to be a full-time job, and he appealed to Mickey Ladd, head of the FBI counterintelligence operations, for a dedicated agent. Ladd assigned one Robert Lamphere, who, like Reynolds, had joined the bureau in 1941. Lamphere had worked virtually his entire career in counterintelligence, mostly in New York. He knew the territory, but he did not yet know ASA and Meredith Gardner.

What ensued was one of the most remarkable partnerships in intelligence history. The shy, brilliant Gardner, speaker of half a dozen languages, brought to the relationship his ability to break codebooks and produce translations of extremely difficult material. Lamphere brought his detailed knowledge of KGB operations and personalities, along with his contacts within the counterintelligence community. Together they worked over the fragmentary texts of old KGB messages.

One of the first products of this marriage of convenience came in 1948. It was a decrypt of a message sent in 1944, in which the KGB reported on the recruiting efforts of an unnamed spy. Using the FBI counterintelligence file, Lamphere identified two possible candidates: [REDACTED] an employee of the Navy Ordnance Department, and [REDACTED] an engineer working on airborne radar for Western Electric. Both had been under FBI suspicion for possible Communist liaisons. Neither was ever brought to trial, but it was the first fruit of the Gardner-Lamphere relationship.

(b) (1)
(b) (3) -50 USC 403
(b) (3) -18 USC 798
(b) (3) -P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The next lead was a 1948 translation of a verbatim quote on the progress on the Manhattan Project given by one Klaus Fuchs, a respected British atomic scientist, also sent in 1944. The information became urgent when, in September of 1949, the USSR exploded its first atomic bomb. It became clear through the COMINT information provided by Gardner where the scientific information for the USSR's atomic bomb project was coming from. Fuchs was arrested in late 1949, confessed, and was convicted of espionage. Just as important, he led the FBI to a contact in America, Harry Gold, and Gold, in turn, led to the unravelling of an entire network of spies at work for the USSR.



Klaus Fuchs

As the atomic spy network was undone in 1950 and 1951, Lamphere played the information now pouring in through counterintelligence work and confessions against the AFSA KGB decrypts. Most important for Lamphere's subsequent work was an agent covername, ANTENNA/LIBERAL, whose true identity, Julius Rosenberg of New York City, was fully confirmed in June of 1950, based on a series of cascading confessions coming from the network originally unearthed during the Fuchs interrogations earlier in the year. (Gardner later contended that the original tentative identification of Rosenberg was actually done by G-2 before Lamphere became involved.)¹⁵

One of the most sensational spy trials was that of Alger Hiss, a top State Department official who had traveled with Roosevelt to Yalta in 1945. Fingering originally by a KGB defector, Walter Krivitsky, in 1941, Hiss was publicly named in 1947 as a spy by two reformed Communists, Elizabeth Bentley and Whittaker Chambers, before the House Un-American Activities Committee. He was never taken to court for spying, but in January 1950 he was convicted of perjury for lying about his associations with Chambers, and he served a prison term. Although the evidence in court was all assembled from testimony and confessions, along with some circumstantial evidence produced by Chambers, VENONA traffic from the 1945 period contained possible confirmatory evidence that Hiss was probably a GRU asset. The covername ALES was identified in the March 1945 traffic as an individual who flew to Moscow after the Yalta Conference. Hiss was identified as the probable culprit based on the fact that there were only four other possibilities, including the secretary of state himself. The VENONA traffic refers to an individual who could fit the description of Hiss, which could confirm that Hiss was indeed a spy.¹⁶

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Julius and Ethel Rosenberg (on right) shown with another accused spy, Morton Sobell

The most famous spy of all was Kim Philby, the British MI-6 liaison officer assigned to work with the Americans on the VENONA project. VENONA also became the lever which pried open the Philby spy ring, and Philby watched it all unfold. He kept to himself until, in early 1951, the FBI went after one HOMER, the covername of a KGB agent identified originally in VENONA traffic. HOMER, the FBI suspected, was actually one Donald Maclean, a first secretary of the British embassy who, as part of his duties, was in charge of the coderoom in Washington. As such, he had passed the text of certain Churchill-Roosevelt messages to Moscow, and these appeared in decrypted VENONA traffic. Because of his position as liaison with the Americans on VENONA, Philby knew the axe was about to fall, and he warned Maclean of impending exposure. Maclean fled to Moscow with a fellow spy, Guy Burgess, who had been posted to Washington with Maclean. Brought under suspicion by Hoover's FBI, Philby resigned his post and in 1963 fled to Moscow himself.¹⁷

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Kim Philby strikes a smug pose during a 1955 press conference after a British investigation failed to definitely finger him as a Soviet agent.

All the readable VENONA messages which supplied information about U.S. spies were transmitted by 1946 or earlier. Most of the decrypted traffic came from ASA's 1944-45 files and was not decrypted until the late 1940s and early 1950s. But exploitation efforts continued for years and were not finally closed down until 1980. By then, the traffic being worked was thirty-five years old. The reason for this long delay was simple. VENONA translations were incredibly difficult, each one requiring approximately one man-year of work.

The VENONA material played a key, although by no means exclusive, role in catching the atomic spies and the Philby ring. Most of the evidence came from meticulous counterintelligence work by the FBI, not from COMINT. VENONA frequently confirmed what the FBI had suspected, but it never had to be used in court. All the prosecutions stood solely on evidence gained from other sources. What, then, was its historical importance?

First, VENONA provided the prod. Early VENONA decrypts revealed the scope and direction of KGB operations. It confirmed that fragmentary information provided by people like Krivitsky and Gouzenko, and public allegations by Elizabeth Bentley and Whittaker Chambers, was precisely on target and had to be pursued. With VENONA in hand, Lamphere got his marching orders.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Second, it was the evidence that led to the arrest and confession of Klaus Fuchs, the first atomic spy unmasked. Subsequent actions were taken based on an unravelling skein of evidence provided by the conspirators themselves. One arrest led to a confession, another arrest, and still another confession. The investigation proceeded in whirlwind fashion, gaining momentum as it roared around every corner. At that point VENONA simply confirmed and solidified what the FBI had learned from its sources.

Third, it began the exposure of the Philby spy ring, surely Britain's most infamous confrontation with traitors. Although the FBI was already onto Maclean, it might never have proceeded further but for the bits of information that VENONA was unearthing. At the very least, the ring would have operated months, if not years, longer before being unmasked.

The guilt or innocence of Alger Hiss, the decision to execute the Rosenbergs, the culpability of the Philby ring, the very existence of the atomic spy ring and what J. Edgar Hoover called the "Crime of the Century" quickly acquired stark political overtones. They got all mixed up in McCarthyism, and in the 1960s the New Left took up the mantle in behalf of Hiss, the Rosenbergs, and a wide variety of others who, justly or unjustly, had been hauled before the House Un-American Activities Committee and the McCarthy hearings. In the early 1970s a National Committee to Re-Open the Rosenberg Case took up the cudgels in behalf of the executed couple. Believing that the documents would prove them right, they used the Freedom of Information Act to pry off the lid of the FBI investigation and began publishing articles purporting to show how the FBI materials proved that Hiss and the Rosenbergs were innocent. Then in 1983 two former true believers, Ronald Radosh and Joyce Milton, published a book entitled *The Rosenberg File*, which showed that a dispassionate examination of the documents proved just the opposite.

What had they got hold of? It was FBI papers based on the VENONA translations. Unknown to NSA, the FBI had released them through the FOIA process (a release which led to a change in the way such FOIA requests are handled).

Not many people still believe in the innocence of the Rosenbergs. Even those who hold firm to the belief that McCarthy's methods were wrong (and that encompasses most Americans) understand that the KGB had done some serious spying. McCarthy so sensationalized and distorted the anti-Communist campaign in the 1950s that an entire era came into disrepute. The historical importance of VENONA is that this entire episode in American history was not dismissed as a figment of someone's imagination. No matter how lurid and disreputable portions of the anti-Communist campaign became, the spy network can no longer be regarded as a fairy tale.

As for its long-term significance for cryptology, NSA learned several important lessons. First, the difficulty of an effort is not an automatic disqualifier. VENONA was one of the most intensely difficult projects that American cryptology has ever undertaken. The

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

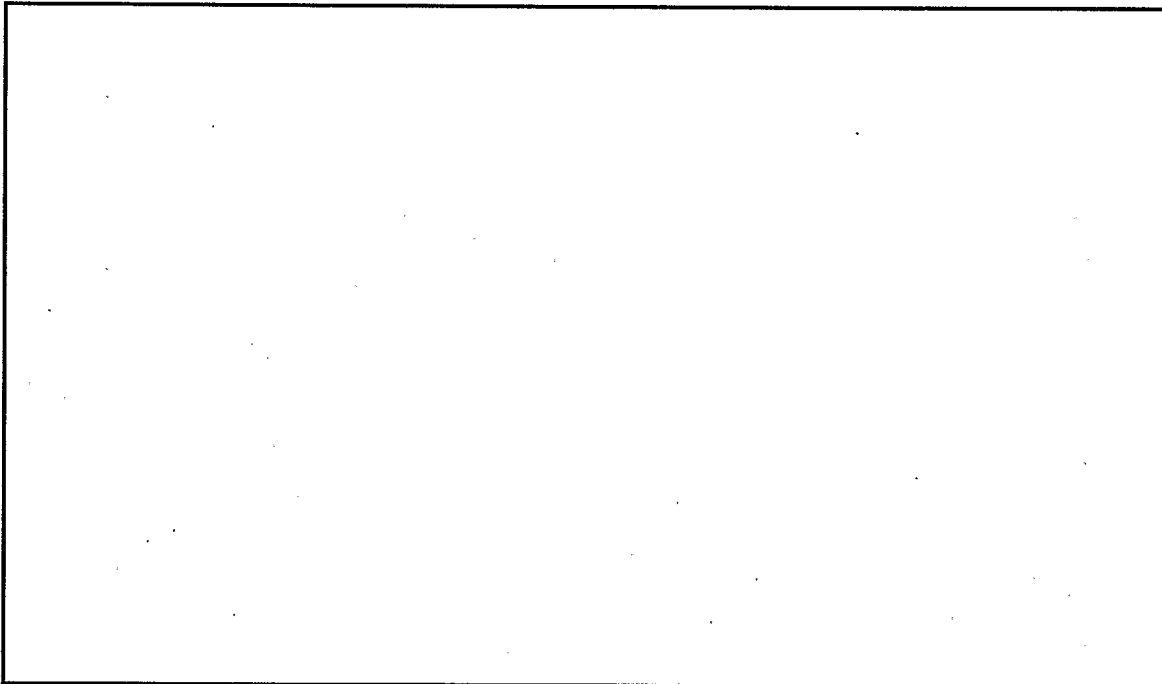
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

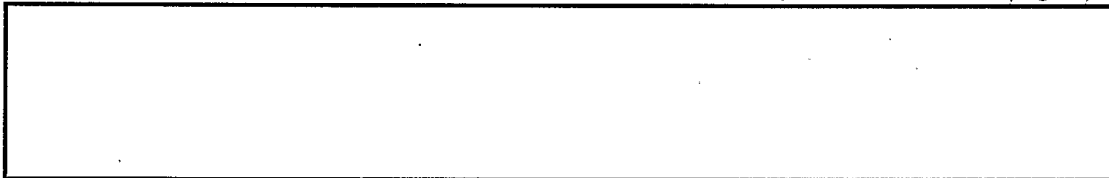
cryptanalytic effort was gargantuan. But the results would rock the foundations of post-war America.

Second, it illustrated the absolute essentiality of cross-fertilization. COMINT without counterintelligence was just as unthinkable as counterintelligence without COMINT. Yet if the effort had been undertaken during World War II, with the intense competition between the military services and the FBI, it might have fallen on the rocks of secrecy, and the atomic spies might never have been uncovered.

"Black Friday"



(AFSA had not yet been created, and there was no mechanism to resolve interservice security squabbles and investigate



~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~

NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~TOP SECRET UMBRA~~

[redacted]

But if one went looking for spies, there was no end of possibilities. The most obvious suspects were those three miscreants, Philby, Burgess, and Maclean, who were in a position to know the general outlines of the American [redacted] attack on Soviet systems, even though they were unacquainted with the technical details.

But a very likely contributor was one of America's own. William Weisband, who had been working in ASA for the duration of the war and into the late 1940s, was later discovered to have been a KGB agent. Weisband, whose story will be covered in more detail in chapter 7, almost certainly provided information critical to the Soviet COMSEC effort. He was the U.S. cryptologic effort's first traitor.

ASA and AFSA Turn to Radioprinter

As the [redacted] problem became more difficult, ASA turned gradually to a new source of Soviet traffic. Through [redacted] interrogations and later contacts with foreign COMINT specialists, ASA had become aware that the Soviets had begun using radioprinter,

[redacted]

ASA had very little intercept capability for such a sophisticated system, and early intercepts were copied onto undulator tape, whose readout was laborious and time-consuming.

Confronting the same problem, NSG and ASA received a postwar allocation of something over \$200,000 to design and build intercept equipment. Working in the basement of Arlington Hall under the cafeteria, they began building [redacted] positions whose output was punched paper tape onto which was also printed the Cyrillic characters, a big improvement over undulator tape. (Printers were then viewed as too expensive and their output too bulky.)

[redacted]

The outputs were huge, and ASA and NSG were quickly flooded with Russian language material. NSAers Jacob Gurin and [redacted] who headed up the transcription effort, began hiring Russian linguists from a former OSS organization that had been transferred to the State Department. They also began scouring college campuses for linguists and set up language training at civilian universities.

(b) (1)
 (b) (3) -50 USC 403
 (b) (3) -18 USC 798
 (b) (3) -P.L. 86-36

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
 NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[Redacted]

Printer seemed to be the wave of the future.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

THE SOVIET STRATEGIC THREAT

[Redacted]

(b) (1)
(b) (3)
OGA

The United States emerged from World War II with a lock on nuclear weapons technology and strategic delivery systems. The Soviet Union represented a threat only from the standpoint of a land war on the Eurasian landmass.

This enviable pinnacle of security did not last very long. On 3 September 1949, an Air Force weather reconnaissance aircraft detected an unusually high concentration of radioactivity over the North Pacific east of the Kamchatka Peninsula. The Soviets had exploded a nuclear device. The timing was a shock. The intelligence community had adjudged the Soviet program still several years away from actually exploding a device.

The arms race was on, and America's lead in nuclear technology seemed to be disappearing. The U.S. exploded its first hydrogen bomb in 1952; the Soviets followed a year later, another surprise to the intelligence community.

In 1953 American military attachés in Moscow observed Soviet strategic bombers in apparent series production. If true, this would give the Soviets a delivery capability for their newly acquired atomic weapons. Stuart Symington, senator from Missouri and former secretary of the air force, fastened on this information to propound the famous "bomber gap" thesis. This information was later proved wrong by early U-2 photoreconnaissance flights, but the public perception profoundly altered intelligence priorities and led to an almost paranoid focus on Soviet strategic systems.

In 1956 Symington originated the "missile gap" controversy which was to influence the presidential election of 1960. Symington was apparently being fed data from Air Force sources that SAC believed the Soviets might have slipped ahead of the United States in the development of strategic missile delivery systems. The launch of *Sputnik* in 1957 appeared to confirm Symington's contentions, and every failure of a U.S.-developed launch system over the next several years just drove another nail in the lid. The concentration of intelligence energies on the Soviet advanced weapons problem became fierce.

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

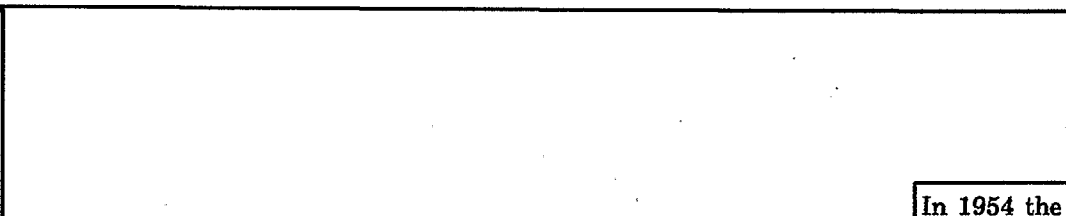
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~**How It Began**

The Soviet missile program had originated in 1945 when a covey of German missile scientists fell conveniently into Soviet hands. Working at Peenemunde on the North Sea coast, this group had developed the V1 and V2 missiles, the latter a true ballistic missile capable of distances in excess of 200 miles. The captured scientists were hustled off to a research institute in Bleicherode, East Germany, and then in 1946, amid great secrecy, were transferred to the Soviet Union itself. They were first set up in a new Scientific Research Institute 88 at Kaliningrad on the Baltic Sea. Their first test center, established in 1947, was at a remote desert site called Kapustin Yar, some 100 miles east of Stalingrad.

The Germans labored in Kaliningrad, Kapustin Yar and other locations until 1950 or 1951. By that time the Soviets had themselves the rudiments of a missile program. They had succeeded in replicating the V2 and a primitive indigenous missile, called the R-10, had been designed with German help. At that point the Soviets returned the Germans to their homeland, where they brought the CIA up to date on the Soviet program. None of the first Soviet rockets, designated R10-15, ever amounted to more than "designer toys," but the most advanced, the R-15, was designed for a nuclear payload and was to have a range of 3,700 statute miles.²⁰

Reports of Soviet missile development reached the Oval Office, and the president demanded more information. But there were precious few assets to be had. In the latter days of Stalin's reign, the Iron Curtain completely closed off the Soviet Union from CIA HUMINT penetration - they had no secret agents in the USSR. There was no photography, the U-2 still being several years away. Virtually the only asset available was SIGINT.



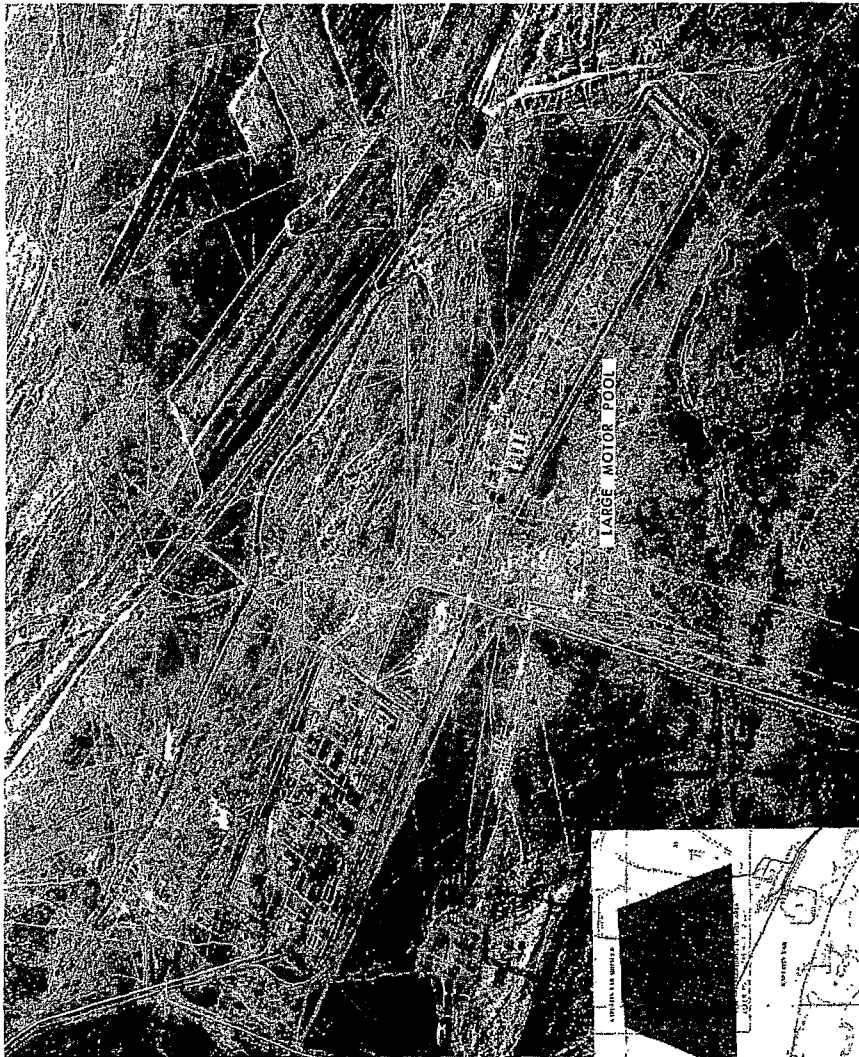
In 1954 the German scientists who had worked on the project told American intelligence about a system of communications between the missile and its ground station, a derivative of a system the Germans had developed at Peenemunde in World War II. It was a 16-channel PPM system operating in the 60 MHz range that the Germans called MESSINA. The U.S. intelligence community called it "telemetry."²¹

(b) (1)
 (b) (3) - 18 USC 798
 (b) (3) - 50 USC 403
 (b) (3) - P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

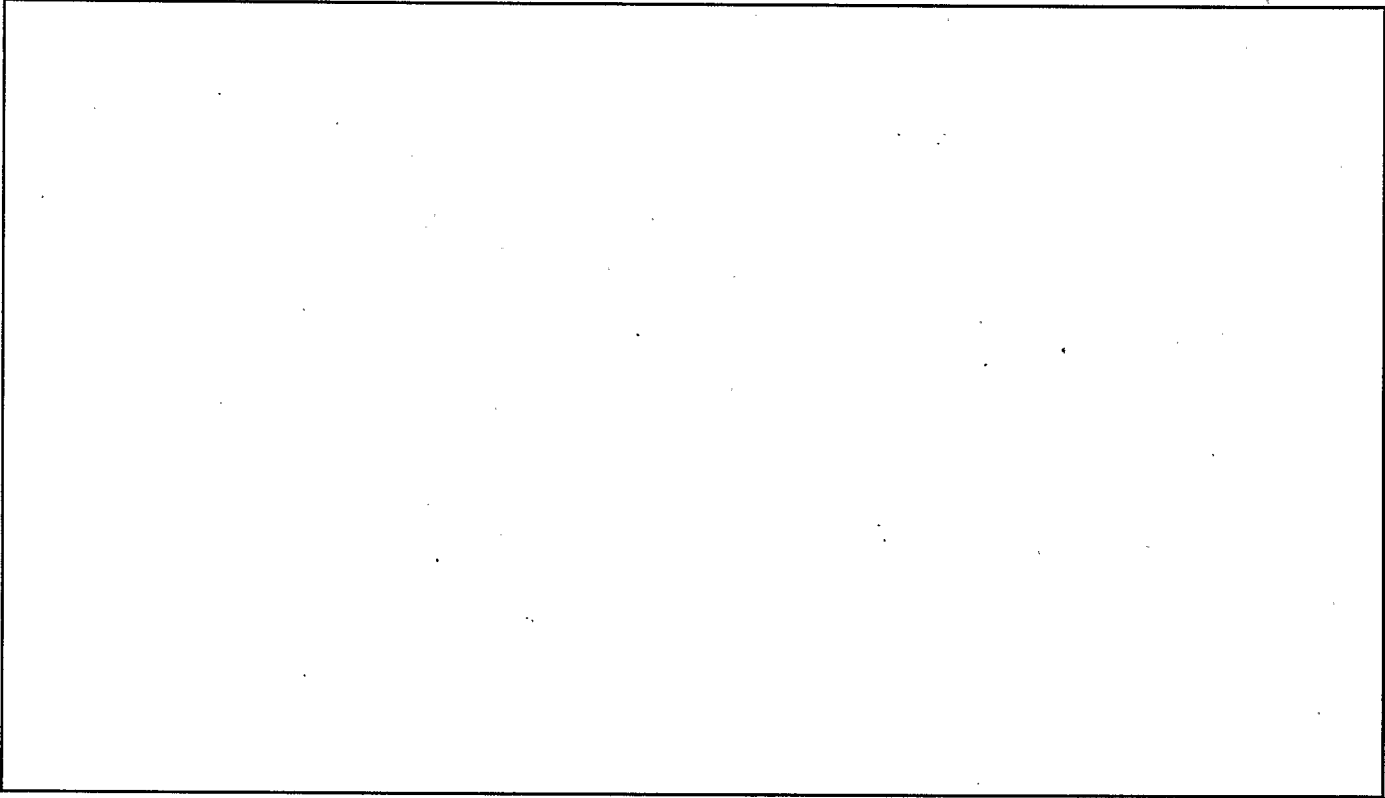


Missile fabrication and assembly area,
Kapustin Yar. This 1959 U-2 photograph provided excellent
detail on a range complex [REDACTED]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~



(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403

(b) (1)
(b) (3)
OGA

~~TOP SECRET UMBRA~~

The American Response

This section contains multiple redacted areas, represented by black-outlined rectangles of varying sizes. Dotted lines originate from these redactions and converge on the exemption codes in the top right corner of the page.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

In 1957 the Soviets opened a new range at Tyura Tam, some 700 miles east of Kapustin Yar. [REDACTED] that this would be the site for the Soviets' first ICBM launches, and a CIA-driven search through U-2 photography in the summer of 1957

[REDACTED] confirmed this.²⁶

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Moreover, [REDACTED] became more and more a cue card for U-2 missions. When U-2 pilot Francis Gary Powers was shot down in 1960, he was on a dangerous cross-Soviet mission searching for evidence of a new missile test site [REDACTED] which had been recently identified [REDACTED] as being possibly missile associated.²⁷

[REDACTED]

[REDACTED] this discovery led to the elevation of the problem to division level. By 1958 it had become the Advanced Weaponry and Astronautics Division [REDACTED] which concentrated NSA's resources into a single organization. It came to be referred to

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

as "SMAC" (Soviet Missile and Astronautics Center). [redacted]

[redacted]

[redacted] SMAC established a new operator-to-operator communications system which became known as the [redacted] Joseph Burke, now regarded as the "father of SMAC," is believed to have originated this system.³⁰

(b) (1)
(b) (3)
OGA



Joseph Burke

To orchestrate the system, SMAC established an all-night watch, virtually eliminating the call-in system for this critical project. SMAC was one of the organizations that eventually got NSA out of the eight-hour-per-day mode, and it pioneered in the development of tip-off systems and quick reaction capabilities. In both concept and technology, it long preceded NSOC.³¹

NSA had numerous competitors in the missile arena. The Air Force had launched a small detachment of ATIC (Air Technical Intelligence Center at Wright-Patterson Air Force Base, Ohio) in San Antonio. Collocated with Air Force Security Service, SMTIG (Soviet Missile Technical Intelligence Group) consisted of a cross-section of the Air Force intelligence disciplines, but it was dominated by SIGINT people. Its analysis directly overlapped much of what NSA was doing. In addition, CIA was well along on its missile analysis effort and included SIGINT as well as other intelligence disciplines in its program.³²

The Soviet Atomic Bomb Project

While the Soviets were developing delivery systems, Stalin directed that the development of the nuclear weapons themselves be given the highest priority. Working with information provided by the atomic spies in the West, and with captured German nuclear physicists, the Soviets raced to get the bomb. Their first test site was constructed at Semipalatinsk (now referred to as "Semey"), a remote Siberian location, and for some years the Soviets used that site exclusively. The Semipalatinsk monopoly on nuclear tests

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

(b) (1)
(b) (3)
OGA

~~TOP SECRET UMBRA~~

was finally broken in 1955 with the explosion of an underwater device in the sea off Novaya Zemlya, a large Arctic island northeast of the Kola Peninsula.⁸³

As with the missile development program, so it was with nuclear weapons;

[Redacted]

The American system for monitoring Soviet nuclear tests consisted of a complex of seismic and infrared sensors positioned around the world. The entire system depended,

[Redacted]

The bomber and missile gap controversies in the late 1950s triggered a search for an operational Soviet strategic nuclear delivery organization. With the launch of *Sputnik* in October 1957, this became a white-hot priority,

[Redacted]

The Soviets did not yet have a nuclear delivery organization, all the information from Senator Symington notwithstanding. In January 1960 the USSR publicly announced the formation of a new Strategic Rocket Forces (SRF) command,

[Redacted]

In 1960, DCI Allen Dulles directed that the chairman of the Guided Missile and Astronautics Intelligence Committee (GMAIC) organize a study group to completely evaluate the Air Force contention that there was a missile gap. Using [Redacted] photographic evidence collected from the U-2, the committee concluded that only the test site at [Redacted] was capable of launching a missile. This contradicted the latest national intelligence estimate, which postulated that there would be thirty-five operational launchers by mid-1960. Dulles then directed that a permanent Deployment Working Group be established to comb all the evidence thoroughly.

The crash of the U-2 piloted by Francis Gary Powers on 1 May temporarily ended overhead photography as a source of intelligence, and the committee had to proceed from [Redacted] Using old photographs and up-to-the-minute [Redacted] the

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

group finally concluded that only Tyura Tam and possibly one to three other operational launchers existed, including Verkhnyaya Salda and Yur'ya. Plesetsk was still assessed as unfinished. [redacted]

The paranoia of the 1950s receded to be replaced by the optimism and military force projection policies of the 1960s. By the time Kennedy became president, Dulles had proved that the Soviets still presented no real strategic nuclear threat, although clearly that threat was on the horizon. During the dark days of the 1950s, though, when no one really knew what went on behind the Iron Curtain, [redacted]

[redacted] It was President Eisenhower's hole card.

The Chinese Threat

Compared with the Soviet Union, China could hardly be considered a strategic threat. But Stalin and Mao appeared to be on friendly terms. China had intervened in Korea, and many Americans (including some in the intelligence business) believed in an overarching Communist conspiracy - the Sino-Soviet Bloc. If Stalin had the bomb, could Mao be far behind?

American suspicions of a close Sino-Soviet relationship were confirmed through COMINT by the exploitation of COMINTERN communications. This traffic showed a long-standing liaison between the COMINTERN and Mao's forces, going back to the 1930s. When, in the late 1940s, ASA first began exploiting Soviet plain-language printer, analysts discovered that the Soviets were sending World War II lend-lease equipment to Mao, who was then attempting to overthrow Chiang Kai-shek. Clearly, the USSR was the major arms supplier for the Chinese armies, and the Soviets had nuclear weapons.³⁸

During the 1954 Quemoy and Matsu crisis, Secretary of State John Foster Dulles pledged American arms in defense of Formosa. The pledge was repeated during the 1958 renewal of the offshore islands imbroglio, but Dulles persuaded Chiang to renounce the use of force against the PRC, and the islands never again caused a confrontation between the U.S. and China.³⁹ Meanwhile, however, U.S. intelligence poured ever-increasing resources into the China problem.

In many ways, China resembled the USSR [redacted]

[redacted] resources to go against the second-most-serious threat were scarce.

[redacted] The Chinese program was delayed for several years by the Sino-

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

(b) (1)
(b) (3)
OGA

Soviet rift, [redacted] China's strategic defense system did not make rapid progress until the 1960s.⁴⁰

[redacted]

The Early Days of Overhead

The early days of the new Eisenhower administration represented the blackest period for U.S. intelligence on Soviet forces and strategic capabilities. [redacted]

[redacted]

[redacted] If the United States could not penetrate the Iron Curtain [redacted] they would have to do it from the air.

Attempts had already been made. In the late 1940s the CIA had tried to float high altitude balloons over the USSR, equipped with cameras and recorders. This so-called [redacted] program failed dismally. The few balloons that floated all the way from [redacted] to [redacted] yielded little useful information.⁴²

More determined were deliberate overflights of Soviet soil. SAC had a highly compartmented (and still obscure) overflight program, carrying a variety of sensors. This dangerous approach to intelligence collection was augmented by the RAF, which mounted occasional overflights. But their participation was limited and ended after one famous incident in 1953. At American behest, RAF aircraft overflew Kapustin Yar, [redacted]

[redacted] They came back with their planes shot full of holes and allegedly told the Americans that if they wanted that sort of thing done, they could jolly well do it themselves. [redacted]

[redacted]

A series of ground-breaking studies in the early 1950s urged Eisenhower to plunge into advanced technological alternatives. One of the most attractive proposals was

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

suggested by the Surprise Attack Panel, a committee set up under Dr. James R. Killian, president of MIT. Dr. Edwin Land, a member of the panel and inventor of the Polaroid camera, suggested that a camera could be devised which could take pictures from very high altitudes, if the Air Force could build an airplane from which to mount such a camera. In November 1954, Allen Dulles got [redacted] to build some thirty new aircraft which had been designed for just such a purpose by Kelly Johnson, the top designer at Lockheed. They were called U-2s.⁴⁴

There was at the time no guarantee that the U-2 was the answer. In fact, the Eisenhower administration continued to play with the balloon option. Project [redacted] consisted of more than 500 balloons which were floated across the USSR from Europe to Asia in early 1956. [redacted]

(b) (1)
(b) (3)
OGA

[redacted] and some of them may have [redacted]. But [redacted] was no more successful than [redacted] and of the 500, only forty-four were ever recovered after their long ride from west to east.⁴⁵

The U-2 project was a very risky gambit by an administration desperate to find out what was happening in the Soviet Union. Advanced equipment was placed aboard an aircraft easily picked out on radar, and defensible only because of its operational altitude. If the Soviets ever got a weapon that would shoot that high, the U-2 could be a sitting duck.

This was undoubtedly in Eisenhower's mind when in 1955 he broached the Open Skies proposal to Khrushchev. The U-2 had not yet been launched, but when it was, it would be a target.⁴⁶

From the time of the first U-2 overflight on 7 April 1956, to the shutdown of Francis Gary Powers on 1 May 1960, the Eisenhower administration launched twenty-four missions. The objective was photography, and the targets related to Soviet strategic systems. The aircraft also carried an [redacted] package, but this was probably used for internal defense (presumably to warn the aircraft of the presence of unfriendly threats) and to target the cameras.

[redacted]
[redacted]
[redacted] in special rooms - only a few individuals at each site were cleared.
[redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

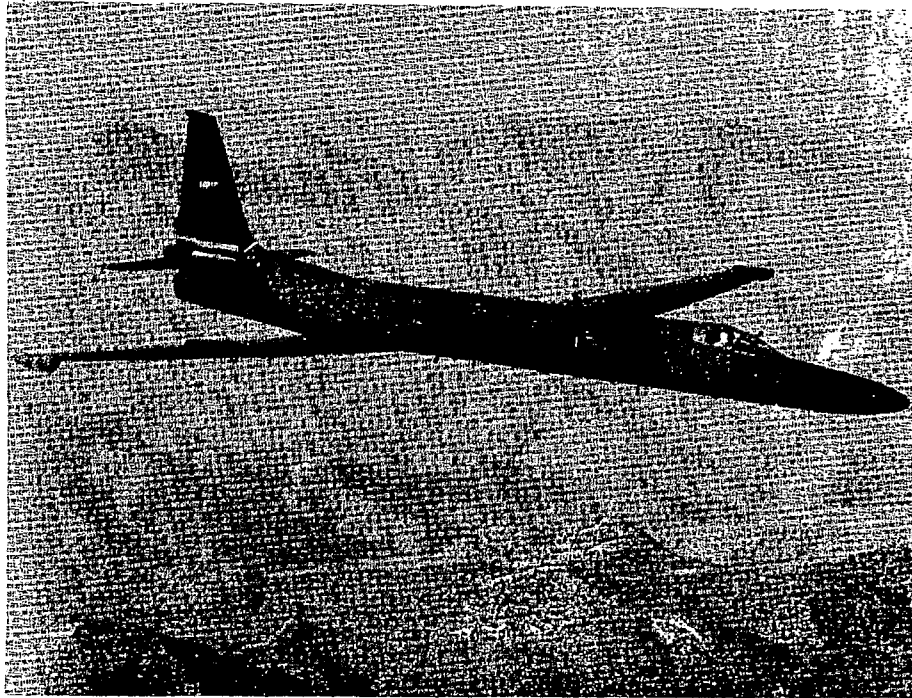
~~TOP SECRET UMBRA~~

~~HANDLES VIA TELETYPE TO THE COMANT-GONPROB-SYSTEMS-JONPHL~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

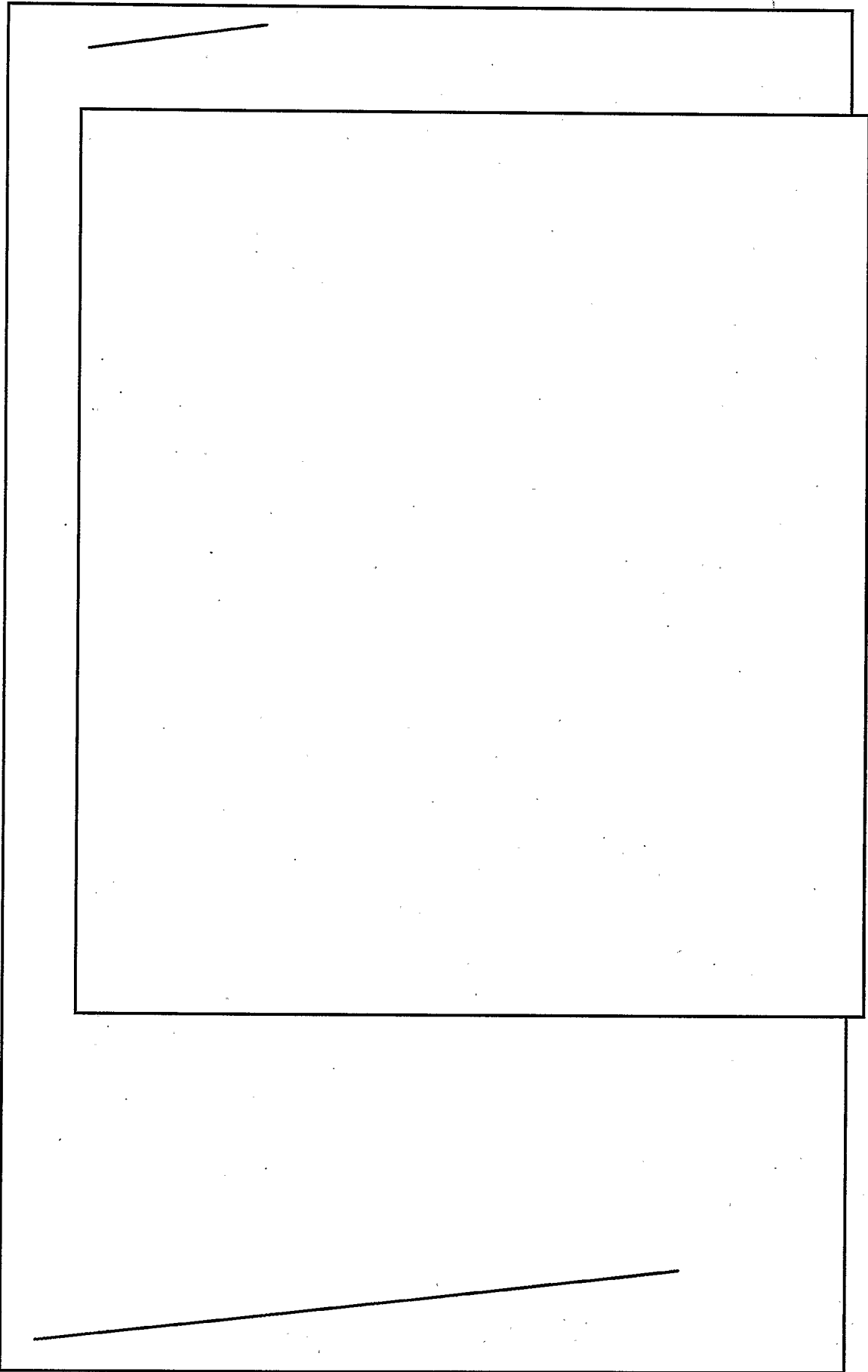
181

~~TOP SECRET UMBRA~~

U-2



~~TOP SECRET UMBRA~~



(b) (1)
(b) (3)
OGA

~~TOP SECRET UMBRA~~

Prior to the Powers flight, NSA began to note increased [redacted]

[redacted]

Henry Fenech, the NSA official in charge of the operation, stated that a mission just prior to the infamous May Day flight was chased by a Soviet interceptor aircraft all the way to Afghanistan. It was obvious to Fenech that the Soviets were loading up.⁴⁹ Powers took off on 1 May 1960, [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Back at NSA, Fenech reported to CIA that the aircraft had probably been lost to unexplained causes. It was the first loss of a U-2.

[redacted]

CIA was desperate to know what had really happened to the aircraft, and in early 1962 General C. P. Cabell, deputy director of the CIA, decided to trade Soviet spy Rudolph Abel for Powers. In March 1962, only a month after the return of Powers, CIA called a board of inquiry, and into the middle of it marched Fenech, accompanied by NSA Director Laurence Frost, Deputy Director Louis Tordella, and Assistant Director for Production Oliver Kirby [redacted]

Both the Soviets and Powers said that the plane had been shot down at high altitude with an SA-2. [redacted] Fenech told CIA that it appeared Powers had begun a descent well before the SA-2 hit. Had he gone to sleep? Was it inattention or hypoxia? Did he flame out and search for a lower altitude to restart his engines? All Fenech knew was that [redacted]

[redacted] Fenech did not believe what Powers had told CIA. The CIA crowd was not amused, and Fenech underwent a long and hostile grilling by the board.

[redacted]

What really happened? We will probably never know. Powers died in a helicopter crash in 1977, so no more information is available from him. But the [redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

leaned so heavily on was suspect. [redacted]

[redacted] Moreover, the Soviet officer who was in charge of the SAM battery that supposedly shot Powers down stated after the end of the Cold War that the air defense operators were so shocked at the shutdown that they didn't believe it, and for twenty minutes or so they continued to reflect the aircraft on its presumed track to cover up their befuddlement.⁵³ If the Soviet defenders did not know for sure what had happened, and if they covered up information so as not to look bad up the line, the chance at ever arriving at the truth looks very dim indeed. The theory that he was downed by an SA-2 at very high altitude (68,000 feet) appears more plausible today than it did in 1960.

[redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

THE ATTACK ON SOVIET CIPHER SYSTEMS

[redacted]

Baker Report, 1958

When it was created, AFSA inherited a Soviet problem that was in miserable shape.

[redacted]

There were only two bright spots. The first was unenciphered radiprinter, which carried valuable [redacted] information. These links had not yet begun to go to cipher.

[redacted]

Even the darkest days, however, had their rays of hope. Howard Engstrom, a World War II cryptologist now in the civilian computer business, suggested in 1950 that AFSA might make progress by establishing a research institute comprising eminent civilian scientists to attack the problem, very much in the pattern of Los Alamos of the Manhattan

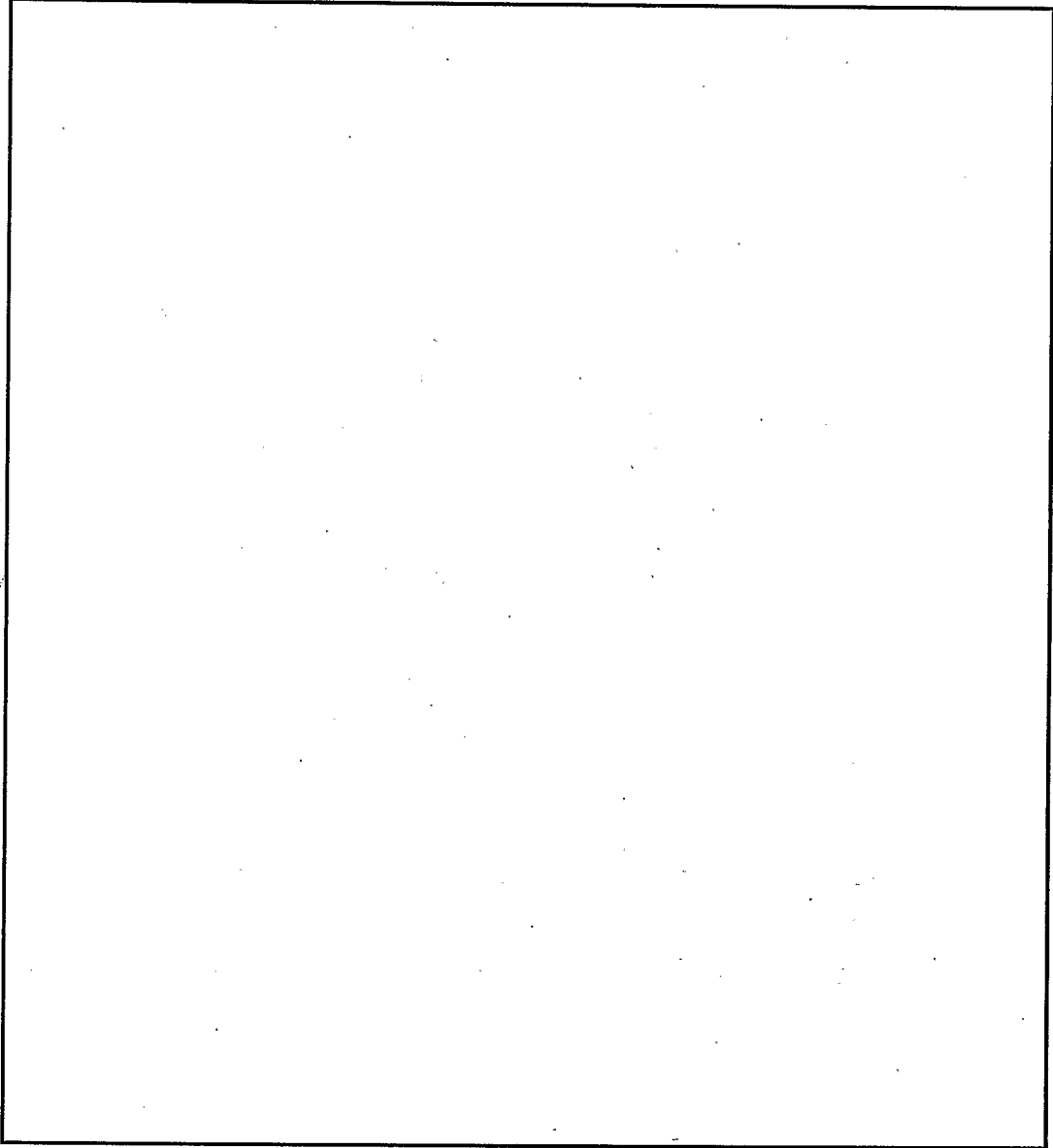
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Project.⁵⁴ Then, two years later, AFSA's Scientific Communications Advisory Group (SCAG, a predecessor of NSASAB), chaired by Engstrom, [redacted]

[redacted] given sufficient resources and a strong research and development effort. The need for a skilled civilian work force or the employment of an outside research institute was essential. AFSA did not have a strong enough civilian work force, and the Brownell Committee made this point forcefully that same year.⁵⁵

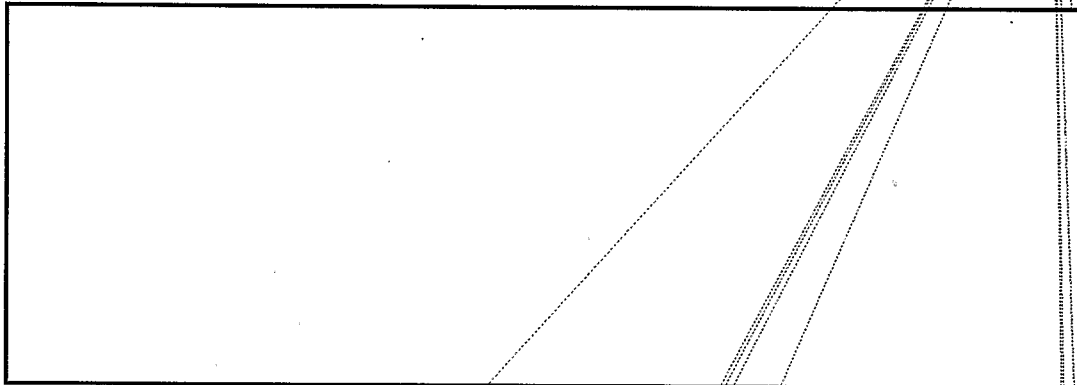


(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



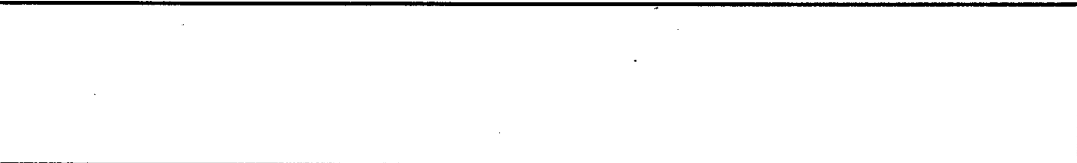
As NSA struggled with the [redacted] problem, two camps formed concerning the prospects for success. The first group felt that the effort was hopeless and should not be funded. The 1957 Baker Panel leaned toward this viewpoint. The committee recommended that an effort be kept alive [redacted] but it was pessimistic about long-range chances for success.⁶¹

A second group felt that the United States would never know whether it would be possible or not because of inadequacies at NSA. The organization was too skewed toward military manning, was not hiring the right kinds of civilians, and did not have an adequate budget.

[redacted] This opinion was well entrenched at CIA and was led by former NSAer Frank Rowlett. A variant on this interpretation was offered by the Baker Panel, which suggested that the internal NSA structure could not cope with the complexities of high-grade systems. That job should be given entirely to a Los Alamos-style civilian research institute.⁶²

But within NSA itself there was a strong undercurrent of disagreement with both camps. Representative of this view was the report of a committee chaired in 1956 by Navy captain Jack Holtwick. Holtwick felt that a concentrated attack would yield enough [redacted] alone to justify the effort, and he recommended a massive computer attack. Such a super-high-speed computer would cost in the neighborhood of \$5 million per year, a considerable sum in those days.

[redacted] NSA would need [redacted] and would probably have to have some of the work done at a private research organization (the Los Alamos option again). [redacted]



~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

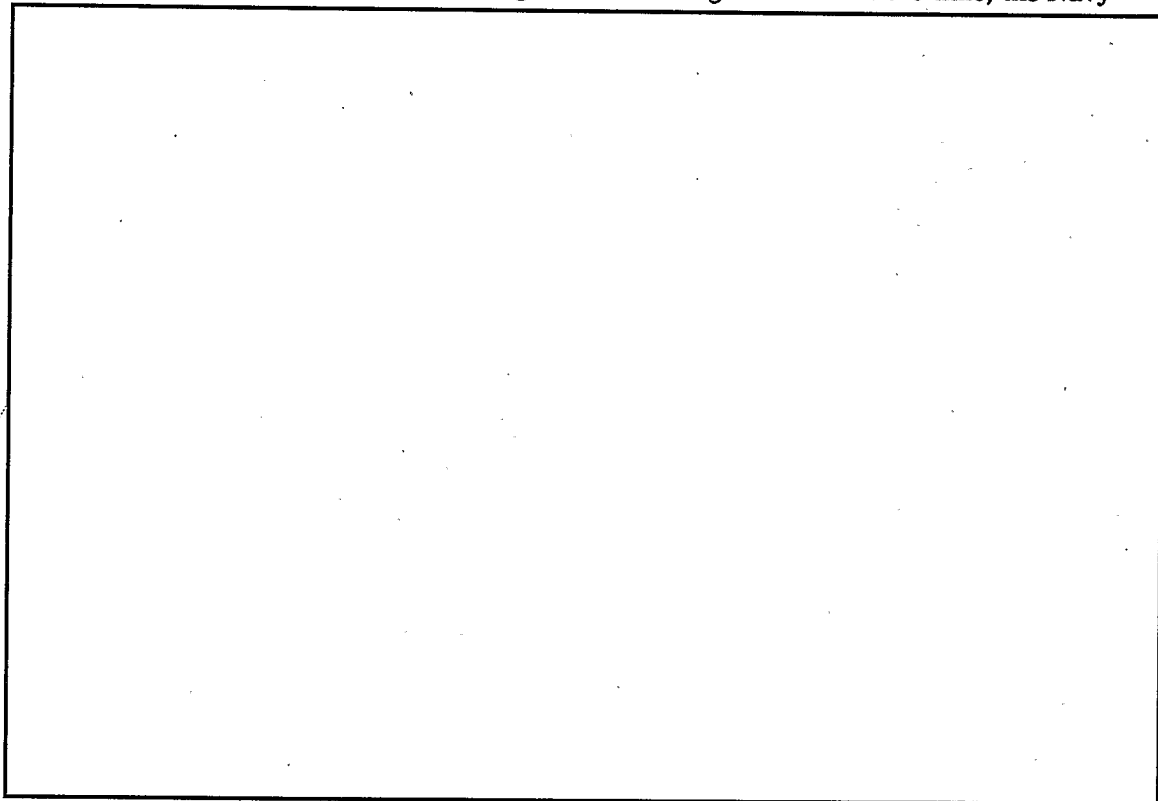
~~TOP SECRET UMBRA~~

TRACKING SUBMARINES - THE STORY OF BURST TRANSMISSIONS

Late in World War II, German scientists had once again come up with a serious threat to Allied cryptologic efforts. This time, they had devised a way to compact lengthy manual Morse messages into messages lasting only a few seconds. When played at normal speed, a message sounded like a burst of noise in the receiver. The Germans called it KURIER and intended it to be on submarines, agents (spies), and eventually aircraft for low-probability-of-intercept communications. Early models were deployed before war's end, and GCCS intercepted transmissions on at least one occasion. Fortunately, however, KURIER was still in the experimental stage.

When the war ended, a German submarine surrendered in Argentina, the nearest landfall. Aboard the sub was a German scientist with extensive engineering notes and knowledge of the system, and he was willing to talk to the Americans about it. Even luckier, the British captured an actual KURIER system, and both the British and Americans experimented with it, primarily for the purpose of building burst systems for their own submarines.⁶⁵

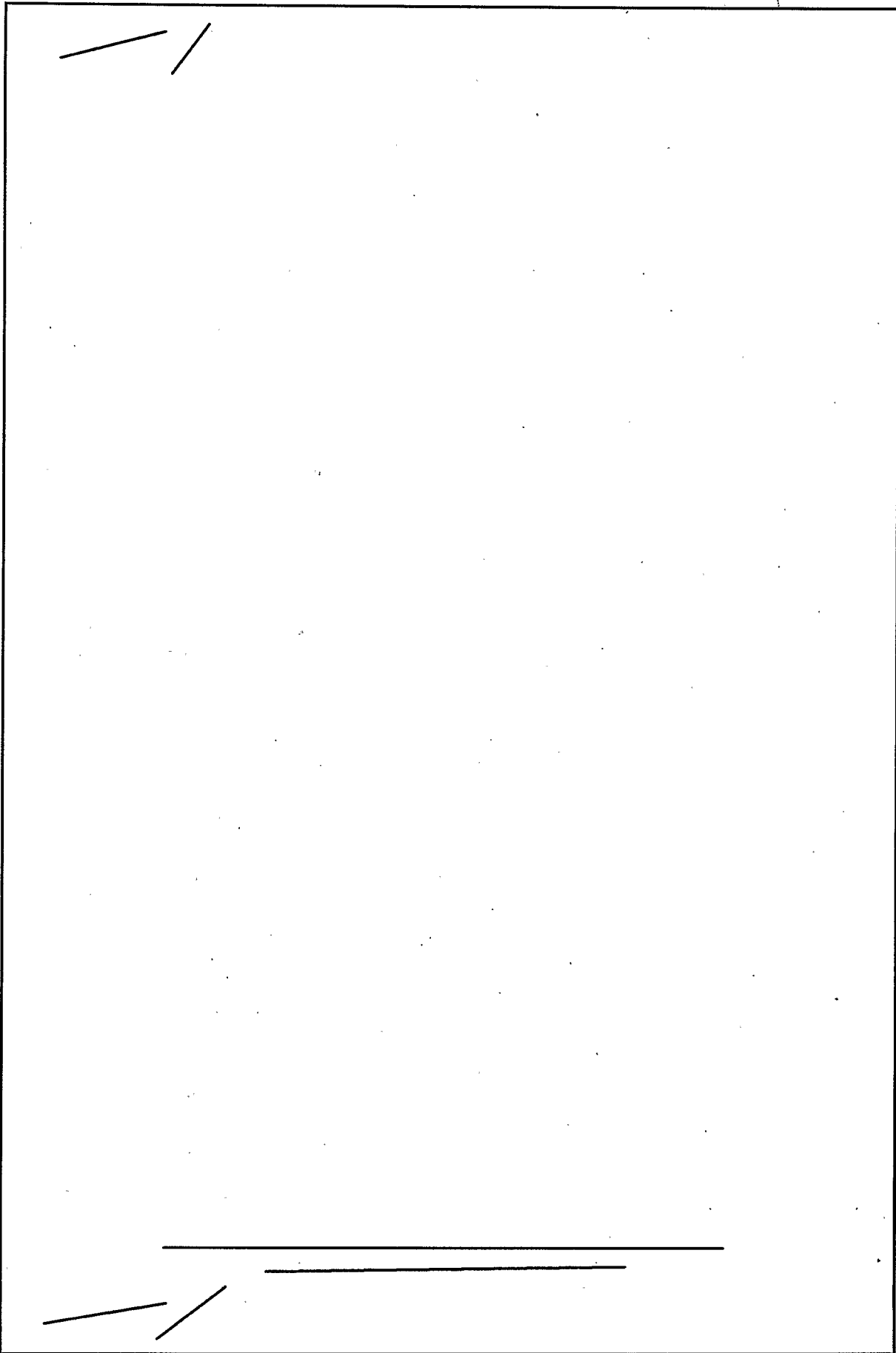
Unfortunately, the Soviets also captured German scientists working on KURIER, and the TICOM teams discovered this during their debriefing sessions. At the time, the Navy

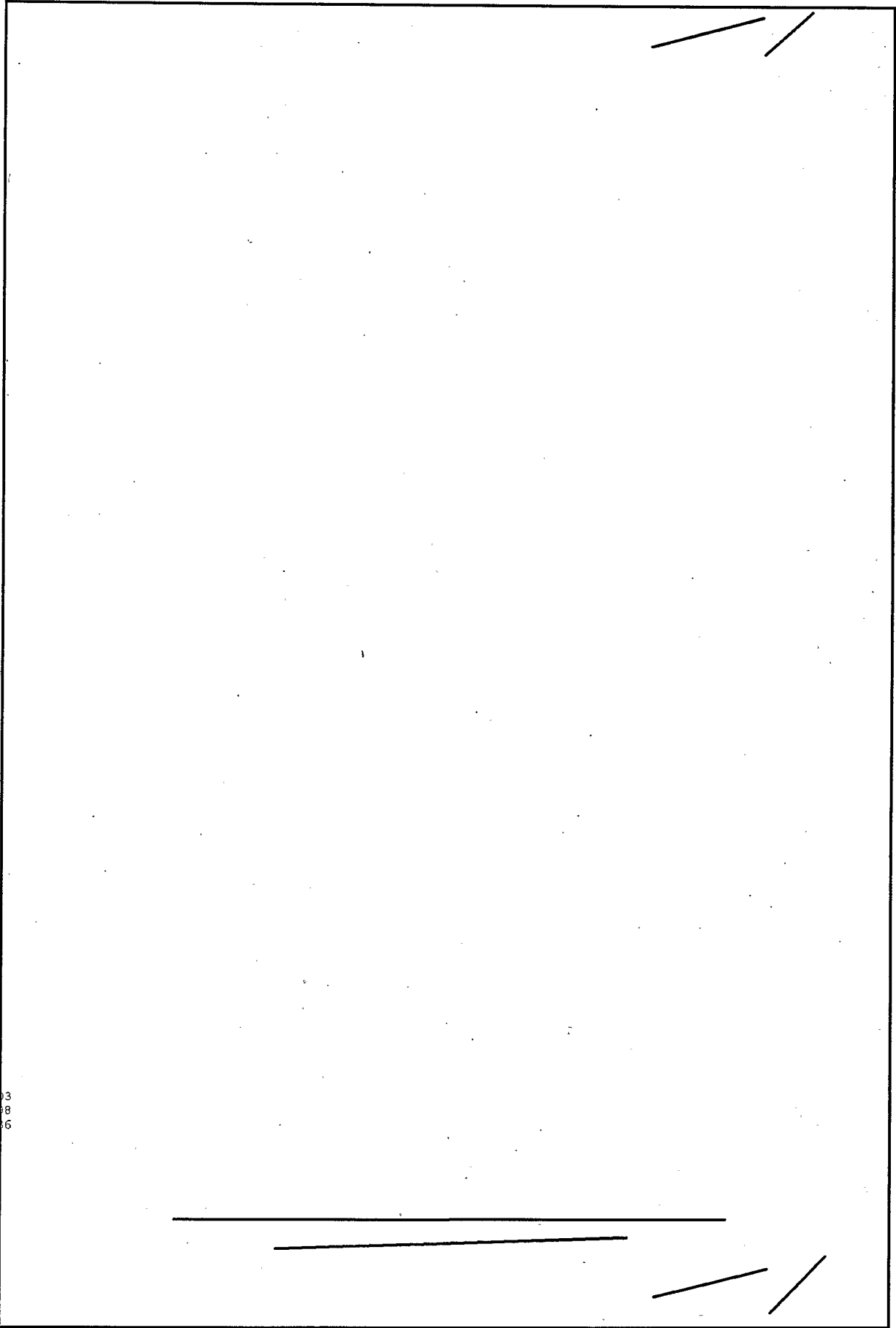


(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~





(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-E.O. 13526

~~TOP SECRET UMBRA~~

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

Notes

1. [redacted] "Soviet Manual Systems Since 1945: A History of Their Cryptography, Usage and Cryptanalytic Exploitation"; unpublished draft available in CCH.
2. Ibid; see also Frank Rowlett, "Recollections of Work on Russian," unpublished manuscript dated 11 Feb. 1965, available in CCH; see also NARA, SRH-001, 296.
3. Robert L. Benson and Cecil Phillips, *History of Venona*, published in March 1995. The name "KGB" will be used throughout this book to refer to the Soviet intelligence organization and its predecessors, the MVD and NKVD.
4. [redacted] "Before BOURBON: American and British COMINT Efforts against Russia and the Soviet Union Before 1945," *Cryptologic Quarterly*, Fall/Winter 1993, 1-20; Benson and Phillips, *Venona*; Frank Rowlett, "The Story of Magic," Ch. VII, 53; manuscript available in CCH.
5. Rowlett, VII.53; Oliver R. Kirby, "The Origins of the Soviet Problem: A Personal View," *Cryptologic Quarterly*, Vol II, No. 4, Winter 92; ; Louis W. Tordella, series of oral history interviews beginning 28 June 1990 by Robert Farley, Charles Baker, Tom Johnson and others, NSA OH 8-90.
6. Rowlett, "Recollections . . ."; see also Oliver R. Kirby oral interview, 11 June 1993, by Charles Baker, Guy Vanderpool, [redacted] and David Hatch, NSA OH 20-93. Tordella interview.
7. Howe, "Narrative History of AFSA/NSA, Part I"; [redacted] "Early BOURBON," 1994.

[redacted]

9. Benson and Phillips, *Venona*.
10. Benson and Phillips, *Venona*; Kirby, "The Origins of the Soviet Problem."
11. Robert T. Lamphere, and T. Schachtman, *The FBI- KGB War, a Special Agent's Story* (New York: Random House, 1986).
12. Benson and Phillips, *Venona*.
13. Lamphere and Schachtman, 78.
14. For information on the Petsamo Incident and the Stella Polaris project, refer to the following: Lamphere and Schachtman (not the best source); interview with Hallamaa in Madrid in 1951, in NSA/CSS Archives, ACC 7975N, CBRJ 22; Benson and Phillips, *Venona*, Stella Polaris document collection in NSA/CSS Archives, ACC 1177-79, 11369-76, 12504, 19043N, 19044, CBRJ 23.
15. Benson and Phillips, *Venona*.
16. Ibid.
17. See David Martin, *Wilderness of Mirrors* (New York: Ballantine Books, 1980).
18. Brownell Report, 106-08, in CCH Series V.F.7.13.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

19. No history of Black Friday was compiled at the time, partly because of the fragmented nature of cryptology in those days. The best versions have only recently been compiled: [redacted] "Beyond BOURBON - 1948. The Fourth Year of Allied Collaborative COMINT Effort Against the Soviet Union," *Cryptologic Quarterly*, Spring 1995; and Benson and Phillips, *Venona*. For additional information, see oral interview with [redacted] 10 May 1985 by [redacted] and Robert Farley, NSA OH 03-85; oral history interview with Cecil J. Phillips, 8 July 1993, by Charles Baker and Tom Johnson, NSA OH 23-93; oral history interview with Herbert L. Conley, 5 March 1984, by Robert Farley, NSA OH 01-84; and Oliver R. Kirby, "The Origins of the Soviet Problem..."

20. Details of the early Soviet program can be found in [redacted] "Early History of the Soviet Missile Program (1945-1953)," *Spectrum*, V (Summer 1975), 12-19; [redacted] "The Soviet Land-Based Ballistic Missile Program, 1945-1972: An Historical Overview," unpublished manuscript available in CCH.

21. [redacted] "The Soviet Land-Based Ballistic Missile Program..."

[redacted]

26. Oral interview with Ray Potts and [redacted] 16 May 1994.

[redacted]

29. Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence*. (New York: Basic Books, Inc., Publishers), 143-44.

30. [redacted] "The Soviet Land-Based Ballistic Missile Program..."

31. Tevis interview.

32. Amato interview.

33. [redacted] "History of the Soviet Nuclear Weapons Program," intelligence report available in CCH.

[redacted]

38. Kirby interview.

39. O'Neill, 279.

40. Background papers for the 1967 Eaton Committee, available in CCH; oral interview with Milton Zaslow, 14 May 1993, by Charles Baker and Guy Vanderpool, NSA OH 17-93.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

41. Ray S. Cline, *The CIA under Reagan, Bush and Casey* (Washington, D.C.: Acropolis Books, 1981), 200-201; "Report of the Secretary's Ad Hoc Committee on COMINT/COMSEC," June 1958 (Robertson Committee), CCH Series VI.C.1.11.; "Tibetan Revolt of 1959," informal paper prepared for Eaton Committee in 1967, available in CCH.

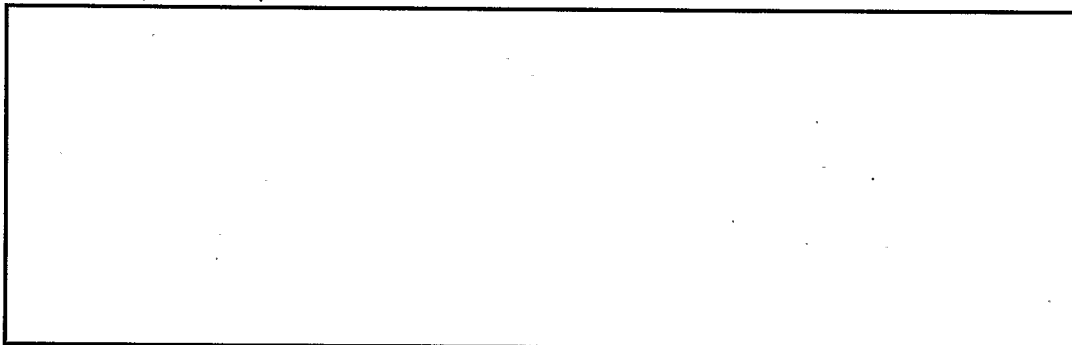
42. Burrows, *Deep Black*, 62-3.

43. Burrows, *Deep Black*, 67; Michael R. Beschloss, *Mayday: Eisenhower, Khrushchev and the U-2 Affair* (New York: Harper and Row, 1986), 77-79; Oral interview with Henry R. Fenech, 30 Sep 1981, by Robert Farley, NSA OH 8-81.

44. Stephen A. Ambrose, *Eisenhower, Volume 2: The President* (New York: Simon and Schuster, 1984), 227-28.

45. Burrows, *Deep Black*; NSA/CSS Archives, ACC 24355, CBOH 36.; Ambrose, *Eisenhower*, 309-10.

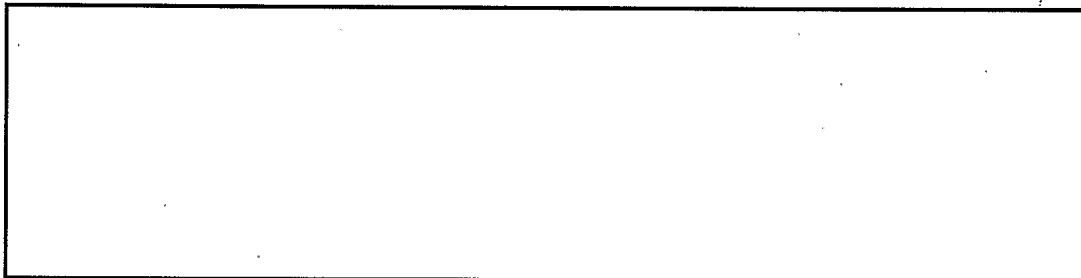
46. Ambrose, *Eisenhower*, 265.



53. *Vox Topics*, V. 3, # 3, 1992.

54. CIA-AFSA collaboration (Wenger file), in ACC 9142, CBIB 27.

55. Collins, V. II, 6; Brownell Report.



61. Baker Panel report.

62. Collins, V. II, 16, 23.

63. Holtwick.



(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

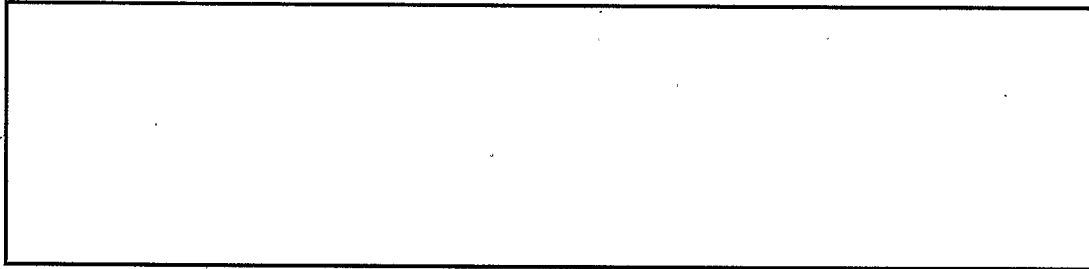
65. NSA/CSS Archives, ACC 3838, CBOH 11; O'Rourke interview; oral interview with [redacted] 17 July 1986, by Robert Farley and Tom Johnson, NSA OH 19-86.; NSA/CSS Archives, ACC 3838, CBOH 11L.

66. CCH Series V.R.1.7; V.B.2.7.

67. [redacted] "Radio Direction Finding in the U.S. Navy: the First Fifty Years," paper available in CCH; NSA/CSS Archives, ACC 3838, CBOH 11.

68. [redacted]

69. [redacted] "History of HFDF in the Pacific Ocean Prior to the Advent of Bullseye," 1981, in CCH Series VII 85.



(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Chapter 5

Building the Internal Mechanism

CRYPTOLOGY IS AUTOMATED - THE STORY OF EARLY COMPUTERIZATION

The trouble with machines is people.

Edward R. Murrow, 1952

Antecedents

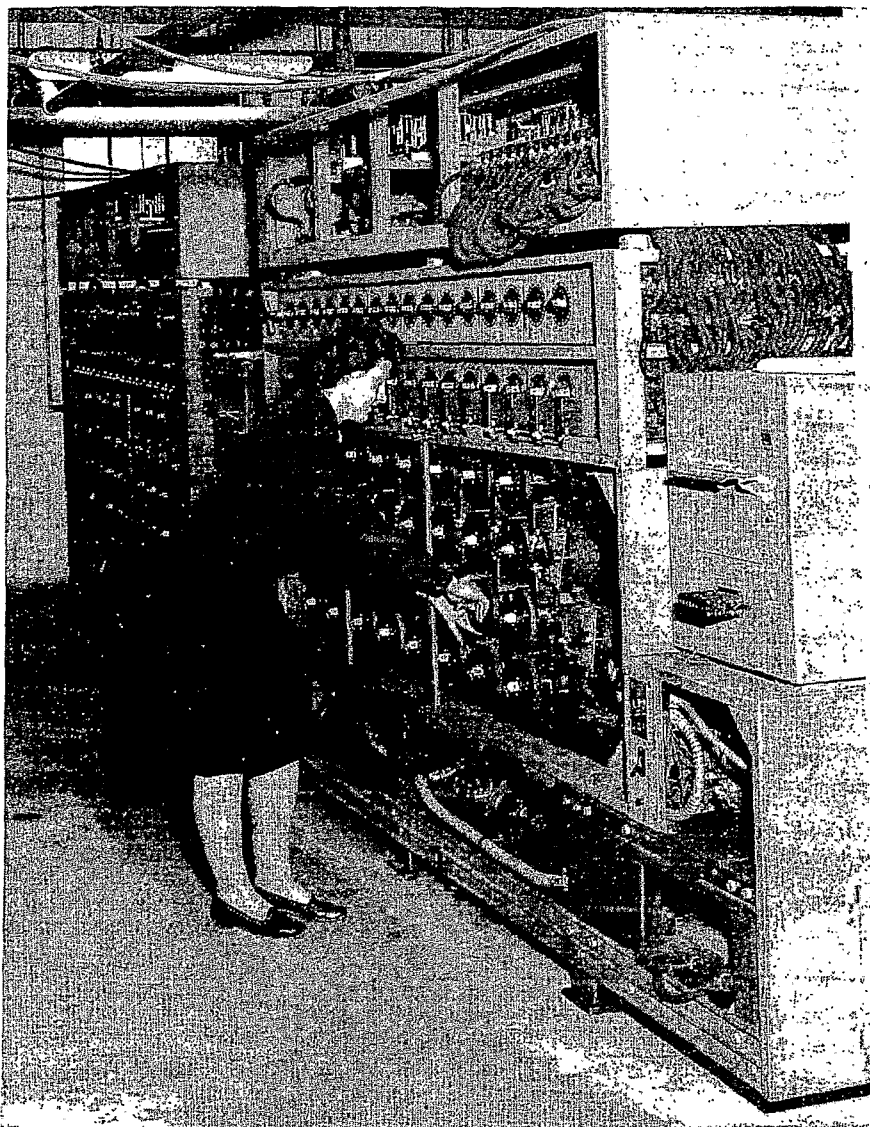
Modern cryptanalysis, with its emphasis on the manipulation of large amounts of data, was one of the earliest government enterprises to acquire the new office automation equipment being produced by a small company called International Business Machines (IBM). In 1931, OP-20-G obtained some of the new IBM machines and quickly employed them in the cryptanalytic process to sort large amounts of data and determine likes and unlikes. In 1935 Signal Intelligence Service (SIS) acquired the same type of equipment for the same purpose. By World War II "EAM" (electronic accounting machine) equipment had become commonplace in COMINT processing, and it contributed mightily to codebreaking, especially in the Pacific Theater. By the end of the war, OP-20-G and SIS combined were using more than 700 IBM-type machines.¹

Of the two, the Navy seemed to be further along. During the 1930s and into the early war years, OP-20-G had attempted a partnership with Vannevar Bush, the renowned MIT (Massachusetts Institute of Technology) scientist, to build a faster comparator for analytic (read cryptanalytic) use. This rather bumpy relationship had so far yielded a number of notable technological and administrative failures when, in 1943, OP-20-G became a partner with GCCS in running attacks against the four-rotor German naval ENIGMA. They ultimately decided on a huge, clunky mechanical marvel which has been dubbed the "American bombe." A technological dinosaur when compared to the devices Bush was experimenting with, the bombe at least worked and was used in the last two and a half years of the war to break German naval ENIGMA keys. The Navy development and contract monitoring operation was called the Naval Computing Machine Laboratory (NCML); it was located on the grounds of National Cash Register in Dayton, Ohio, the prime production contractor.²

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



**The American Navy Bombe
A Navy WAVE checks rotor settings during World War II.**

Although a very fast comparator, the bombe was not a true computer. It did not have a stored digital program which could be modified. But even as the Navy designed and built the bombes, the British were moving ahead into the era of true computers. To attack systems even more complex than ENIGMA, GCCS was developing a computer which

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

employed an electronically generated key that was compared with the German cipher text. Although it did not have a true internally stored program, the settings were operator-adjustable according to how close he or she thought they were to a cryptanalytic solution. They called it Colossus. Some contend that it was the world's first true computer, although Colossus must compete for that honor with ENIAC, which was being developed at the University of Pennsylvania's Moore School of Electronics to generate complex artillery ballistics tables for the Army. Either Colossus, designed for cryptologic use, or ENIAC, for ballistics, probably deserves the title of the world's first computer.³

Postwar Developments

OP-20-G could see the technological possibilities in the bombe, and it was decided even before the war ended that the effort should continue. But National Cash Register had no intention of continuing the association. They wanted to return to making cash registers. So at the end of the war, NCML was physically evicted, along with the remainder of its undelivered bombes, and the project came to a halt.⁴



Howard Engstrom

OP-20-G needed a prime contractor with which to work. Months before the war ended, Howard Engstrom, a key figure on the bombe project, decided to start a new company specifically to do business with OP-20-G. At war's end, he left the Navy and took with him the best and brightest technicians at NCML. They set up a new company called Electronic Research Associates (ERA), under the wing of an already established firm called Northwestern Aeronautical Corporation in St. Paul, Minnesota. The Navy made no specific promises regarding contracts for the fledgling company, but none were needed. Engstrom and associates had a corner on the technological expertise that OP-20-G required, and contracts flowed almost immediately.⁵

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The relationship between ERA and the Navy was emblematic of the way relationships had developed between the cryptologists and private industry. During the war OP-20-G had developed a close relationship with IBM, Eastman Kodak, and National Cash Register. SIS had a similar kind of relationship with Bell Laboratories and Teletype Corporation. Those businesses kept a stable of cleared people who could do jobs quickly and quietly for the cryptologists. In the COMINT and COMSEC businesses, it did not pay to advertise.⁶

Both the bombe and ENIAC had been developed through classified wartime military contracts. Thus computing in the United States began in the rarified atmosphere of tight security. Though the cryptanalytic aspects were not publicized, the Army relationship with the Moore School became a matter of public knowledge in 1946 when the inventors of ENIAC, John Mauchly and J. Presper Eckert, gave a series of lectures on electronic computers. As the two men left the Moore School to establish a computer manufacturing company, they dispersed their knowledge nationwide in what became known as the Moore School Lectures. Many felt that this lecture series launched the computer industry in the United States.⁷

Howard Engstrom had found out about the Moore School Lectures, and he suggested that the Navy send a cryptologist to observe. Thus, when the lectures began, sitting in the back of the room was Lieutenant Commander James T. Pendergrass, a Navy mathematician employed at Nebraska Avenue. Pendergrass delivered a report to the Navy on the Moore lectures which focused attention on the emerging new computer technology. This resulted in negotiations with ERA which led to the construction of the Atlas machine.⁸

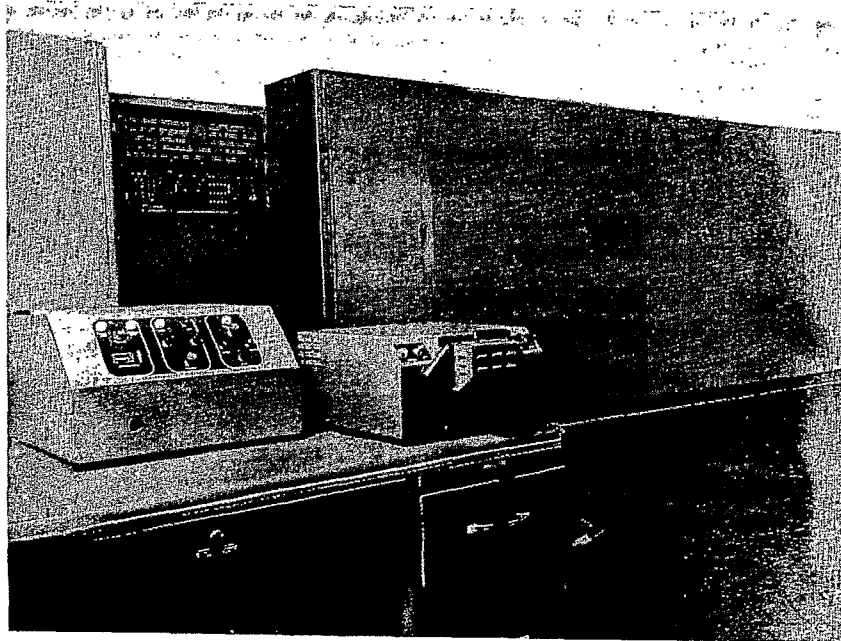
Like the bombe before it, the first generation of postwar cryptologic computers produced highly specialized machines, called in those days "rapid analytic machines" (RAMs). Each machine was constructed for a different purpose and attacked a different cryptanalytic machine or problem. Programs were particular rather than general, and inputs and outputs were of specialized design. A list of AFSA machines, both present and projected, in 1952 contained sixty RAMs, as opposed to only eight that had more flexible objectives.⁹ An example of a RAM was [redacted] which was developed by ERA to attack [redacted]¹⁰

Even in those early days computer companies were willing to take on difficult developmental tasks. For instance, operating under a 1947 contract, ERA developed the world's first magnetic drum storage system as part of a RAM project called GOLDBERG.¹¹ A successor project, called ATLAS (also built by ERA), applied the drum storage technology to a more general purpose cryptanalytic processor. ATLAS was ERA's first major computer development, and it led to the company's first commercial product, the ERA 1101, produced after the company had become merged with Remington-Rand-Univac to form the first major American computer company.¹²

(b) (1)
 (b) (3)-50 USC 403
 (b) (3)-18 USC 798
 (b) (3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Atlas I

While NSG forged ahead, ASA was trying to catch up. In ASA, the role played by Engstrom, Tordella, and Pendergrass was at first taken on single-handedly by Samuel Snyder, one of Friedman's most talented prewar cryptanalysts.

Snyder's 1947 paper "Proposed Long-Range Cryptanalytic Machines Program for Literal Systems" played a seminal role in ASA's first postwar venture into the new technology. In it, Snyder proposed that ASA develop its own analytic computer based on extensive research into existing technology. Snyder himself did most of this early research, drawing at first on information provided by Pendergrass and Howard Campaigne of NSG. He made pilgrimages to the fountainheads of computer research: Aberdeen Proving Grounds to see ENIAC, Bell Labs to see its Relay Computer, IBM to see

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

the IBM Selective Sequence Calculator, and MIT to see its Differential Analyzer. He attended a lecture series at the National Bureau of Standards (NBS) which concentrated on Univac products (Univac had been formed in 1946 by Mauchly and Eckert), Raytheon computers, and the Ace Computer (one of the earliest British entries into the commercial computer field). Snyder suggested that ASA team up with NBS, which already had some expertise in the field, and he proposed that ASA form a committee to guide the effort.¹³

ASA decided to go ahead with development of a general-purpose analytic computer called ABNER. Working through NBS, ASA arranged for subcontracts on mercury delay memory and for magnetic tape drives from Technitrol and Raytheon, respectively. Snyder contended that ABNER I, which was released for use in 1952, was the first machine that placed primary emphasis on nonarithmetic operations. Although it played a role in the development of later computers for cryptologic applications, one expert in the field called Abner "barely functional." This was an appellation that could have applied to many of the early experiments in machine-age cryptology.¹⁴

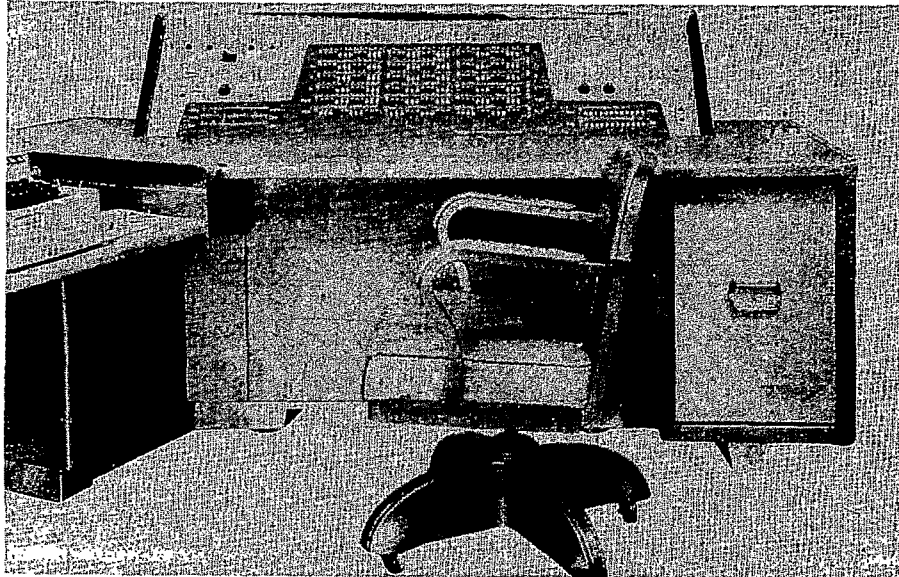
The early cryptologic computers were troglodytic. They were physically programmed in binary instructions input via paper tape. They used octal numbers and words twenty-four bits long. There was no "computer language" as such. Memories were tiny by today's standards - the drum memory for ATLAS, for instance, held only 16,000 words. There being no more advanced technology available, vacuum tubes were used for relays, despite the obvious disadvantages this created in terms of heat buildup and tube replacement. Early computers were usually "down" more often than they were "up." When they were "up," though, they provided answers faster than anything imaginable.¹⁵

Vacuum tubes were on the way out, to be replaced by transistors, developed at Bell Labs in the 1940s by future Nobel prizewinner William Shockley and others. NSA scientists were among the first to apply the new transistor technology to computers, and in the mid-1950s it developed an in-house computer called SOLO, the world's first computer to be entirely transistorized. SOLO was subsequently marketed commercially by the contractor, Philco, as the Transac S-1000.¹⁶

Other innovations were on the way. In the mid-1950s NSA began making the transition from centralized computer operations to remote job access systems. The first remote job access computer, ROGUE (for Remotely Operated General Use Equipment), used hardware called Alwac III developed by a small firm called Logistics Research, Incorporated. ROGUE had three remote terminals connected to a small central processor.¹⁷

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

SOLO

RAMs like ROGUE were good for specific jobs, but cryptologists recognized very early that they would require more generalized systems to process very large volumes of data. A study in the mid-1950s depicted just how much material must be massaged. Raw traffic arrived in courier shipments every day at the rate of thirty-seven tons per month. An additional thirty million groups of traffic arrived (in Tecsumized form) via teletype. Traffic from some entities (particularly the mechanization-resistant manual Morse intercept) received less than 50 percent detailed processing - the rest was held in case it was needed.¹⁸

As early as 1946, NSG began the search for a computer that could hold very large volumes of data. Studies of mass data handling methods led to a contract between the Navy and Raytheon in 1951 to develop and produce a machine called NOMAD that would be physically and financially the largest cryptologic machine yet. But the NOMAD contract went badly off schedule from the first, and the contract was killed in June 1954.¹⁹

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The best general-purpose computer in the early days was an IBM product, the 701, designed in partnership with NSA. NSA leaned toward magnetic tape rather than disks, and the 701 had the first truly functional tape drives controlled by vacuum columns.

The 701 was followed by the IBM 705, which became the mainstay for general-purpose computing. Coming on line in the mid-1950s, the 705 was a nonfixed-word-length machine. It had the best sorter around, an assembler (called a "transembler") that mimicked punched card machines. The 705 had a major impact on data processing, and it made it possible to begin processing massive volumes of data rolling in from the rapidly expanding network of collection sites around the world.²⁰

Parallel to the general-purpose processors was a line of special-purpose scientific machines. Notable was the IBM 704, which had a 36-bit word, punched card input, and tape drives for storage.²¹

Cryptology still needed a general-purpose system. A committee, formed to review the demise of NOMAD, specified the requirement for a system that could be of use to both traffic analysts and cryptanalysts. For the traffic analyst, it would have to have large storage, have a file capability for collateral information, and be capable of sorting quickly. For the cryptanalyst, it should be able to tackle

To achieve the requisite flexibility, the system would require a general-purpose mainframe with special-purpose peripherals. The project was called FARMER.²²

At the time, IBM was working on a project to extend the performance of its latest product, the 704, by a factor of 100. They called it STRETCH. IBM approached both NSA and the Atomic Energy Commission (AEC), the two government agencies that it felt would have the most use for such a system. AEC agreed to proceed, but NSA ultimately decided that it wanted something specifically optimized for cryptologic applications. However, IBM was on the right track, NSA concluded, and awarded Big Blue contracts for research in high-speed memory (SILO) and to design a general processing system for Agency use (PLANTATION, later called RANCHO).²³ The entire project was eventually folded into a gigantic effort to develop a large-scale computer. It was called HARVEST.

The most difficult part of the project turned out to be designing the magnetic tape drives. Under a project called TRACTOR, IBM developed new tape drives and a unique automatic cartridge loading system having 100 times the speed of the IBM Type 727 tape drives then in use. Each of the three TRACTOR units managed two tape drives, and it automatically retrieved and hung data tapes in a robotic environment that was the wonder of the U.S. government. It made for great theater and was on the mandatory show-and-tell tour for years.

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 796

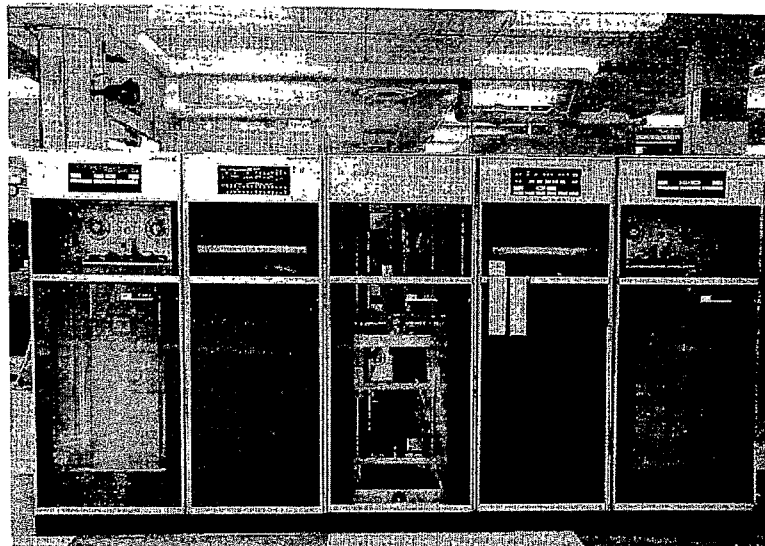
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



HARVEST



HARVEST tractor units

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

HARVEST worked after a fashion and remained the Agency's central processor from the time it went on line in 1962 until it was finally retired in 1976, a phenomenal life span for any computer system. But those who had to make it work remember it as balky, difficult to program, and not performing anywhere near the specifications that had been set for the system. It was a transitional machine.²⁴

NSA's most lasting contribution to computer history was undoubtedly Project LIGHTNING. LIGHTNING resulted from NSA's reaction to outside criticism that it could not break [redacted] systems and to proposals that this part of COMINT be transferred to an outside research organization. Pricked by the criticism, Canine initiated an all-out attack [redacted]

[redacted] As part of the project, Canine proposed that NSA develop a computer that would advance the state of technology by three orders of magnitude. He decreed that the goal was a "1,000 megaHertz machine," and at a USCIB meeting in August of 1956 he requested \$25 million seed money. The sum angered the Defense Department and placed NSA's budget in jeopardy. In order to get it approved, General Samford took his case directly to President Eisenhower and his top scientists, Vannevar Bush and Jerome Wiesner. Eisenhower came down hard in favor, and he authorized the use of his name to push the project ahead.²⁵

Three major contractors participated - IBM, RCA, and Sperry Rand Univac - but Ohio State University, Kansas University, Philco, and MIT also performed lesser roles. LIGHTNING never resulted in a computer, but the research teams turned up information that drove the next generation of commercial machines. Among the most significant findings were in the field of cryogenics. IBM's Dudley Buck developed the cryotron, and through his research IBM proved the now-obvious axiom that the lower the temperature, the faster the computer. Sperry Rand Univac concentrated on thin magnetic field devices and, through these early experiments in chip technology, found that computer speed would increase when components were subminiaturized in order to place them closer together. RCA concentrated on applications of the tunnel diode, one of the fastest switching devices known.²⁶

As the 1950s wore on, cryptologists broadened computer applications to include far more than just cryptanalysis. NSA first used computers to generate COMSEC material in 1959, when the COMSEC organization began employing the Univac File Computer for that purpose. And for the processing of intercepted traffic for traffic analytic applications, the IBM 700-series computers continued to be the mainstay.

(b) (1)
 (b) (3) - 50 USC 403
 (b) (3) - 18 USC 798
 (b) (3) - P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[REDACTED]

For scanning in the field, CDC (Control Data Corporation, the successor to ERA) developed the concept of key word search under a project called FADE-IN. Text scanning in the field was not implemented until the early 1960s. SOAPFLAKES was believed to be the first key word scan system at NSA.²⁷

Most of these processes were off-line. Intercepted traffic in Tecsumized or diarized form spilled off the communications lines in paper tape form and was carted off to another area of the building to be input to processing computers. But it was not the wave of the future. SMAC first began experimenting with the use of a computer to directly receive inputted messages from the field, and so avoid the paper tape step. This effort used Univac 494s and was in a very early stage of development as the 1950s came to a close.²⁸

NSA COMMUNICATIONS IN THE PRE-CRITICOMM ERA

Equipment is obsolescent, insufficient in number and inadequate for the purpose. . . . Such essentials to operations as, for example, a place to put live traffic and operators' logs, are neglected in the installation and are provided, if at all, as an afterthought when operations begin. . . . Homemade bins in the aisles, traffic piled on the floor or clipped to overhead wires like clothes on a line, logsheets resting on machines, et cetera, are the inevitable result.

1955 study of the COMINT communications system

Rapid communications is the lifeblood of SIGINT. Cryptologists have grown so accustomed to virtually instantaneous access to remote corners of the globe that they could not operate any other way. But in the early days, they operated in a decidedly different mode.

AFSA, when created, had no indigenous communications at all. Instead, the organization depended entirely on communications paths and facilities provided by the services. COMINT passed from collection sites to Washington on armed service communications. It was encrypted off-line at the field site, then was passed to a local communications center manned by non-SI indoctrinated people, who put it on common user circuits for transmission. If the traffic originated at a Navy site, it was put onto naval communications; if it was an Army site, it went via Army communications; and so forth. The traffic was long, vertical umbilical, service-unique and electrically sealed until it reached Washington, where the information could then be passed to other services or to AFSA.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The message went via HF single sideband, passing through up to six relay centers before finally arriving at either Arlington Hall or Naval Security Station. It might have to be reencrypted up to five times, and the process required from twenty-four to forty-eight hours to send a routine message to the capital. Because of the many relays and inherent degradation of HF channels, up to 30 percent arrived undecipherable and had to be retransmitted. Messages required several hours for decryption, and the handling time for each message, including marking and routing to the intended recipient, took several more hours. The ASA communications center at Arlington Hall, for instance, was taking approximately four days (on top of the one to two days of transmission time) to deliver a routine message. The fastest possible handling time on the most critical information was not less than five to six hours from time of intercept, according to information furnished to the Robertson Committee in 1953.²⁹



Arthur Enderlin

One of NSA's communications pioneers, he helped develop the system throughout the 1950s and 1960s.

When AFSA came into existence, the communications system on which it relied was reported to be "in a deplorable and deteriorating state." Arthur Enderlin, one of AFSA's top communications people, conducted a study detailing the decrepit conditions and sent it to Admiral Stone. A disbelieving Stone decreed a full-blown study, which just confirmed Enderlin's contentions.³⁰

Nothing was done under Stone. But when Canine arrived, plans were immediately laid by Enderlin's successor, Lieutenant Colonel William B. Campbell, for a separate AFSA communications center to process traffic destined for AFSA organizations. In July 1952, the new communications handling facility opened in B Building at Arlington Hall, using Teletype Corporation Model-19s. This was a good first step, and it reduced the message handling time for routine messages to three hours, while cutting the message backlog to almost nothing.³¹

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

Another Canine push was for secure telephone communications. The NSA gray phone system, formally known as NSA/CSS Secure Telephone System (NSTS), began in AFSA's waning days with a total of 200 lines, 100 each for Nebraska Avenue and Arlington Hall. AFSA took possession of two-thirds of the telephone instruments, while the collocated SCAs got one-third. A month later (September) a new microwave system became operational between the two locations, ushering in an era of high-reliability, high-fidelity communications. At the time, the system required an operator to connect the two parties, just like commercial telephone circuits of the era. The following April NSA issued its first consolidated telephone directory.³²

AFSA began broadening its secure communications contacts with its customers. The Zone of Interior Connectivity (ZICON) net, originated in the early 1950s, consisted of landline communications paths between AFSA and its principal customers: the three services, State, and CIA. Later, the National Intelligence Indications Center in the Pentagon was added, as well as SAC and CONAD (Strategic Air Command and Continental Air Defense Command) for the Air Force.³³

The COMINT Comnet

By 1952 it was already clear that the growing volume of cryptologic communications would not permit newly established NSA to pursue the old way of doing business. Already, the daily group count was considerable and would grow in the ensuing years, as the following table shows.

Table 1
Total Mean Daily Average Group
Count at NSA³⁴

Year	Count
1952	648,000
1953	1,247,117
1954	1,322,552
1955	1,320,073
1956	1,227,158
1957	1,424,351
1958	1,729,430
1959	2,059,763
1960	2,615,377
1961	3,896,211
1962	4,306,910
1963	5,089,777
1964	6,134,601

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

Spurred by the studies by Enderlin and Campbell, and by the insistence of Canine, NSA devised a plan to establish a worldwide cryptologic communications system. Initially, NSA would establish a network of dedicated channels on the service communications systems, manned only by SI-cleared people to eliminate the multiple encryption-decryption exercises.

But the ultimate plan was to establish a separate system, called the COMINT Comnet. The dedicated circuits would gradually be internettted into a series of relay stations, manned only by SI-cleared people. Initially there were to be six of these relay centers, but the number would expand along with the system of field sites that they serviced.

Intercept sites would feed into the relay centers, which would bulk-forward traffic (primarily intercepted material) back to NSA.

The relay centers would operate initially using torn-tape relays, but would eventually transition to automated relay systems, thus significantly reducing handling time. Once in the system, a message would never have to be reencrypted. When it reached NSA, it would be distributed internally using facsimile equipment. In 1953 Canine announced to a field site commanders' conference that the ultimate objective was to be able to return priority traffic through the communications system within five to ten minutes, while routine traffic would flow through in no more than an hour.³⁵

Canine was able to obtain, in short order, direct communications circuits to Stateside users, GCHQ and CBNRC (as the Canadian cryptologic organization was then called). By the end of 1952 NSA had nine such circuits and plans for six more in the near future. These on-line circuits formed the basis for the COMINT Comnet.³⁶

But the rest of the plan depended on service cooperation, and that was a different matter. Planning for the COMINT Comnet was entrusted to the Joint Communications Electronics Committee, a joint JCS-level planning body whose chairman, Admiral John Redman, had been a prominent member of the Navy cryptologic team during World War II. But Redman was also a dedicated Navy man, and he viewed the proposed Comnet as cutting down on the channel capacity available for other, uniquely service, uses. Under such auspices the plan for a Comnet did not have a bright future.

A steering committee called CENSA (Communications-Electronics - National Security Agency) decreed that each service would fund its own portion of the Comnet. And there was where the rocks were. The services had other funding priorities, and moneys

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

never seemed to be available for the Comnet. Every year NSA communications planners enthusiastically charged up the hill, only to be beaten back again.³⁷

By the mid-1950s, the system was only partially funded, and so far no one had agreed on an automated switch for the new relay centers. The centers that existed were entirely manual operations, in which traffic from an incoming circuit generated a perforated tape on the Mod-19. When the reperforator finished chattering, a communications center operator coiled up the tape and carried it across the room to an outgoing circuit for onward relay to the next center. Coiled tapes sat in boxes behind teletypewriters, awaiting transmission. Communication centers were chaotic, operators were overworked, and twelve-hour shifts were standard.

(b) (1)
(b) (3) - P.L. 86-36

Meanwhile, NSA did what it could to improve the operation. The greatest technical innovation of the 1950s was the introduction of the Burroughs-produced KW-26 on-line encryption device. The KW-26 was a marvel of its day [redacted]

[redacted] almost doubled transmission speed. Serial #1 of the KW-26 was placed in operation at the new NSA communications center at Fort Meade in 1957. The last of these devices was not pulled off the line until 1988. In the ensuing thirty-one years it became the mainstay of cryptologic communications around the world, the most secure and reliable on-line encryption device the United States had ever fielded.³⁸

The new communications center at Fort Meade was planned to overcome the inherited inadequacies of the facilities at Arlington Hall and Nebraska Avenue. Canine had wanted NSA Fort Meade to start life with KW-26s, but the acquisition plan ran behind schedule, and the new communications center on the 2-E corridor began with a hodge-podge of equipment.

But on one thing Canine was insistent - he would not move to Fort Meade without a secure ("gray") phone system. The secure phone system had expanded rapidly, and by 1956 it linked NSA with most important Washington-area customers. In 1957 work began on the microwave tower on Fort Meade that was needed to carry the gray phone system to Washington. The Chesapeake and Potomac Telephone Company provided the path, while Motorola provided the radio equipment for the link. Although Canine never actually moved to Fort Meade (he retired with his office still at Arlington Hall), his successor, General Samford, had a gray phone on his desk, courtesy of his predecessor.³⁹

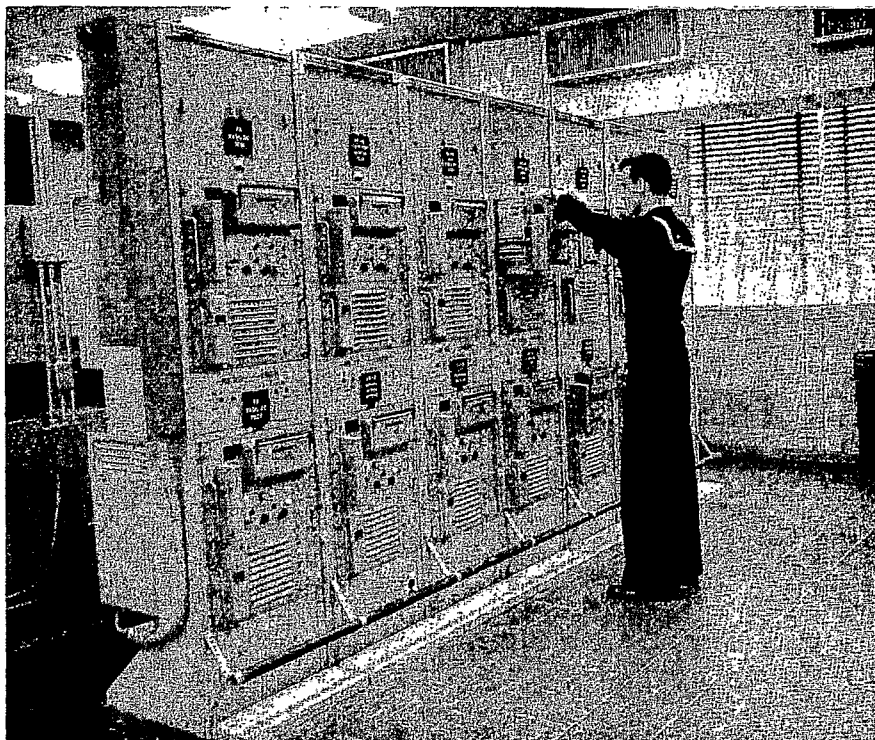
Meanwhile, the early flirtation with facsimile equipment for internal distribution had turned out badly. Fax, as it was called, could not handle the mountainous volumes of traffic flooding into NSA every day. So in 1954 the Agency decided on distributed teletypes. Teletype Corporation equipment was ordered, and equipments were parcelled out through the Production working spaces. A new communications router would be assigned to all incoming traffic. It would be called the DDI (Delivery Distribution Indicator) and would have a very long and prosperous life.⁴⁰

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

~~HANDLING INFORMATION CONTROLS GOVERNMENT SYSTEMS SECURITY
NOT RELEASABLE TO FOREIGN NATIONALS~~



A bank of KW-36s installed in NSA's communications center

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

In the fall of 1957, *Sputnik* went up, and the White House wanted all military and warning communications systems brought up to par. At the time, the COMINT Comnet was still in a state of partial being. NSA had managed to purloin some dedicated channels, and the cryptologic community operated a few relay centers around the world. But the system needed to be consolidated. More, it needed updated equipment, especially automated relays to get rid of torn tape relay arrangements. Moneys for these improvements had managed to find their way into military budgets throughout the 1950s, but they always seemed to disappear into the outyears as the services took care of more pressing requirements. All involved had grown cynical, and the budget for FY59 was not even covered with the fig leaf of outyear moneys. It contained nothing at all for the COMINT Comnet, and this was how the Eisenhower administration found it in early 1958.⁴¹

SECURING AMERICAN COMMUNICATIONS

It became apparent to me early in my work in the Signal Intelligence Service that it was more important to secure our own messages than to read the communications of others. . . . I think it is imperative that our history show the importance of our communications security effort as compared with intelligence production.

Frank B. Rowlett

The COMINT Comnet would be no good if it were not secure. The business of securing American communications had always been integrated with the task of breaking the communications of other countries. Thus from the earliest days the cryptologic coin had two sides: COMINT and COMSEC. During World War II, Signal Intelligence Service had a COMSEC arm, and it produced COMSEC equipment and materials for the Army around the world. In the Navy the integration was more tenuous and the COMSEC mission more diffuse, but closely allied offices of OP-20 were involved in both functions. When the Air Force was created, it gave COMSEC responsibilities to USAFSS. Thus the uniquely complementary aspects of COMINT and COMSEC were recognized from the first. They were never, as they were in Germany, divided among various organizations. Although the two were, as World War II naval cryptologist Joseph Eachus once said, "natural enemies," the dependence of one on the other was firmly established.

The Era of the Wired Rotor

Since the Revolutionary War, the U.S. government had been using manual (mostly paper-based) code systems for communications security. With the advent of radio in the early part of the twentieth century, communications security became even more important. At the time, only manual codes and ciphers were available. Encrypting and decrypting was a laborious process which slowed down communications and limited the amount of information that could be sent from place to place.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Paper codes were archaic solutions to modern communications requirements. After World War I, inventors around the world worked on the problem, and almost simultaneously three or four of them came up with the same solution - a mechanical device consisting of rotors which moved to a different position each time a letter was depressed on a keyboard. In the United States, the inventor of the hour was an eccentric Californian named Edward Hebern. Hebern tried to sell his device to the Army and Navy, but they found it to be both inherently insecure and mechanically unsound. Because of this and patent and contractual difficulties, the relationship with Hebern was terminated.⁴²

This did not mean, however, that the services ceased work on rotor machines. Paralleling their competitors in the other industrialized nations, they made the wired rotor the basis for most COMSEC devices used during World War II. The most secure machine in the war, the SIGABA, was a wired rotor machine designed more or less jointly by the Army and Navy in the late 1930s. The SIGABA was large, heavy, and required a good deal of electricity. Some 11,000 were produced during the war. To communicate with the British, SIS devised a modified SIGABA called the CCM (Combined Cipher Machine), and the British used a very similar device on their end called Typex. CCM continued in use long after the end of the war and was not replaced until 1958, when the KL-7 was introduced for NATO use.⁴³



SIGABA

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

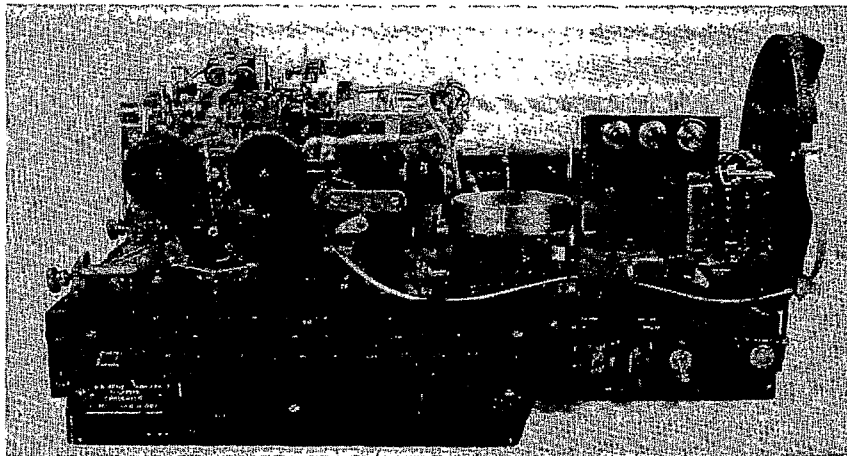
~~TOP SECRET UMBRA~~

For tactical use, the Army used a modified Hagelin machine called M-209. It was small and light, and being completely mechanical, it required no electricity, which made it ideal for foxhole use. But it was difficult and time-consuming to set up properly. (Nonetheless, it continued in use into the early 1960s.) Smith-Corona produced it in huge quantities for \$64 a copy - one former NSA official estimated that some 125,000 devices were built before it went out of production.⁴⁴

The wartime machines were, with two exceptions, off-line devices. One typed the plain text of the message on a keyboard, and the machine produced cipher text on (usually) a sticky-backed tape which could be glued on a paper and taken to the communications operator for transmission.

To handle the increasing volumes of messages, what was needed was a machine that could convert plain to cipher text on-line. SIS devised a solution early in the war. Called SIGCUM (Converter M228), it was not as secure cryptographically as SIGABA, and a new key setting was required for every message. As a result SIGCUM was used in only limited numbers.⁴⁵

A different sort of on-line machine was the SIGTOT, which used a one-time tape. One-time tape machines became known generically as Python systems because of the huge coils of cipher tape that they required. Python systems were used until the early 1960s, but they were cumbersome because of the enormous quantities of tape that had to be generated, handled, and fed through the TD (transmitter-distributor). They were not the long-term answer.⁴⁶



SIGTOT

(Note the paper tape threaded from the right-hand spool across the center of the machine through a perforator.)

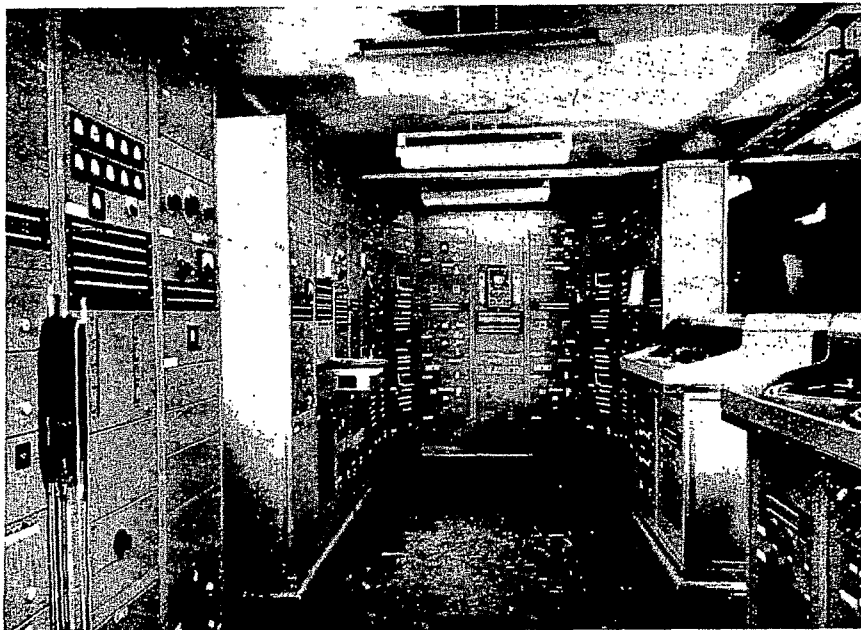
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The Early Years of Secure Speech

Voice was far more difficult to secure. Systems devised in the early days of World War II were cryptographically vulnerable, and better security was needed. Bell Labs built a more sophisticated system during the war to carry high-level transatlantic phone calls. Called SIGSALY, it was a true archetype. SIGSALY consisted of forty-five racks of equipment, weighed thirty tons, occupied an entire room, required thirteen technicians to operate, sucked up 35 kilowatts of power, carried only one voice channel, and cost \$1 million per copy. But given the cryptanalytic sophistication at the time, it was secure. At that price, the government ordered only twelve systems and installed them in the key capitals of the Western world, including Washington, London, and Melbourne. Churchill used it a few times, and, apocryphally, Roosevelt also tried it out once. He allegedly gave up on it, unhappy with the speech quality.⁴⁷ The United States entered the postwar era needing a much smaller and less costly secure voice system.



SIGSALY

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Organizing for COMSEC in the Postwar World

The SCAs slipped into the postwar period with their COMSEC authorities virtually unchanged. The newly renamed ASA was responsible for all Army COMSEC tasks. COMSEC functions were part of the same organization, and personnel rotated between COMINT and COMSEC jobs.

The Navy COMSEC functions were still less monolithic than those of the Army, and the tasks of engineering development, COMSEC research, production of keying material, and building COMSEC machines were spread out across several organizations. COMSEC functions involved the Bureau of Ships, Deputy Chief of Naval Communications for Administration, Deputy Chief of Naval Communications Supplementary Activities (CSA, i.e., NSG), and the Naval Code and Signal Laboratory. It was a complex bureaucracy, but the link-up with the COMINT and COMSEC organizations within CSA seemed to keep naval COMSEC moving in the same direction.⁴⁸

The newly created Air Force did not at first have a centralized COMSEC organization, and for the first year or two of its existence it was serviced by ASA. But when USAFSS was created in 1948, the Air Force assigned its centralized COMSEC functions to the new cryptologic organization.

The three service efforts were rather loosely coordinated by the Joint Communications-Electronics Committee. When one service developed and procured a COMSEC device with broad applicability, it took care of the requirements of the other services, a seat-of-the-pants approach to centralization which worked as long as everyone agreed on the program.⁴⁹ So when AFSA was created in 1949, all three SCAs were doing their own COMSEC.

Almost unnoticed at its creation, AFSA was anointed with centralized COMSEC responsibilities. Naval Security Station at Nebraska Avenue became the locus for COMSEC activities. Army colonel Samuel P. Collins and civilian Abraham Sinkov headed AFSA's COMSEC organization. Centralized COMSEC functions were placid by comparison with COMINT, and contributed little if anything to the demise of the organization. When AFSA collapsed, it was because of turmoil in COMINT, not COMSEC.⁵⁰

When in October 1952 President Harry Truman established NSA, he also signed a memorandum creating a centralized COMSEC function. The memo declared that COMSEC (like COMINT) was a national responsibility, and it set up the secretary of defense and the secretary of state as a special committee of the National Security Council for COMSEC. It also directed that a new central board be established, to be called the United States Communications Security Board (USCSB) to serve as an interdepartmental source of COMSEC policy.

~~HANDLE VIA TALENT KEYPHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

But his memo did not actually establish the board, and a year dragged by before USCSB received a charter. In the interim, Ralph Canine moved into the breach and acted as the central COMSEC authority for the United States. The COMSEC function at Nebraska Avenue continued as before while NSA waited for an official COMSEC structure to be set in place.⁵¹

The long delay in establishing an official COMSEC charter, NSC 168, was due to disagreements over wording and authorities for NSA. Canine objected to the lack of specific centralized authorities for NSA, and to a provision which placed DIRNSA under the JCS for COMSEC. He was successful in getting the offending sentence removed and in strengthening his other authorities. In October 1953, NSC 168 was published, and USCSB was officially launched.⁵²

Besides DIRNSA, USCSB comprised representatives from State, Defense, Treasury, FBI, the three services, CIA, AEC, and Justice. At the first meeting, the board began an unstated but unswerving policy of always electing the Defense representative as the chairman. This was normally the top scientific and technical official, and in the 1960s Harold Brown, Eugene Fubini, Finn Larsen, and Gardiner L. Tucker, all deputy secretaries of defense for research and engineering, successively chaired USCSB.⁵³

NSC 168 did not give Canine the whip hand for COMSEC that NSCID 9 did for COMINT. The COMSEC process was very different, and it was never amenable to the rigid structure and centralized control that applied to COMINT. Centralized authority was couched in terms of cajolery rather than direction. NSA had specific technical authorities to prescribe cryptoprinciples and cryptosecurity rules. But organizational authorities such as budget, research and development, cryptosecurity monitoring, program review and the like were expressed in less authoritarian terms such as "develop," "plan," "prepare," "formulate," and "insure." The services retained much of their COMSEC functions and structure (generally resident within the SCAs). If a technical standard were violated, pulling the offender back into line was to be done through the parent service. NSA could not force a service to employ cryptosecurity on a given link; it could only point out the consequences of noncompliance. Canine did not have central budgetary authority over COMSEC, and he could not force a service to allocate money to COMSEC.⁵⁴

However, if a service decided to encrypt communications, NSA ruled the technical specifications with an iron hand. It produced all the keys, wrote the procedures, governed all compromise reporting and evaluation, established key succession requirements, and so forth. In this respect its COMSEC authority approximated its hold over COMINT.⁵⁵

Unlike USCIB (later USIB), USCSB did not become a strong and vital organization. During the 1950s it held only a single meeting per year. In 1960 it met four times to solve the problem of release of crypto equipment to NATO (a difficult issue which is covered on the following page) and to deal with the problem of communications security (see p. 221). After that it did not meet again for eight years. It named only one standing committee, the

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403

(b) (1)

~~TOP SECRET UMBRA~~

Special Committee on Compromising Emanations (SCOCE) - TEMPEST. NSA acted as its secretariat and effectively did all the work.⁵⁸

Far more than just prescribing COMSEC policies, NSA became deeply involved in the design and production process. The Agency generated keying material using a wide variety of techniques. NSA also designed COMSEC machines and simply turned the production process over to a contractor after all the designs were completed. The contractor in those days was little more than an assembly organization. All the interesting work was done in-house.⁵⁷ This would change in the 1980s under Walter Deeley's "New Way of Doing Business."⁵⁹

AFSAM-7

In the early 1950s AFSA, and later NSA, pushed ahead [redacted] to develop their first central, multiservice encryption device, the AFSAM-7, later the KL-7. Although the Army wanted a [redacted] rotor and the Navy only a [redacted] rotor, Canine decreed uniformity, and NSA adopted the Army's [redacted] rotor as the standard. The KL-7 proved immensely popular, and some 20,000 were produced at the very reasonable cost of \$1,200 a piece. Weighing only thirty pounds, it could run off either AC or DC power (including a jeep battery).

The Navy strongly resisted the AFSAM-7/KL-7 development. After rejecting several modifications designed to satisfy their requirements, they adopted a modified device called a KL-47. The KL-47 was to have a long and interesting history. The Navy ended up using it extensively aboard ship. [redacted]

When the AFSAM-7 was still new, the JCS proposed giving it to NATO countries. This got NSA into a very murky area. Defense and State had for years been concerned about the security of U.S. defense information on NATO communications. [redacted]

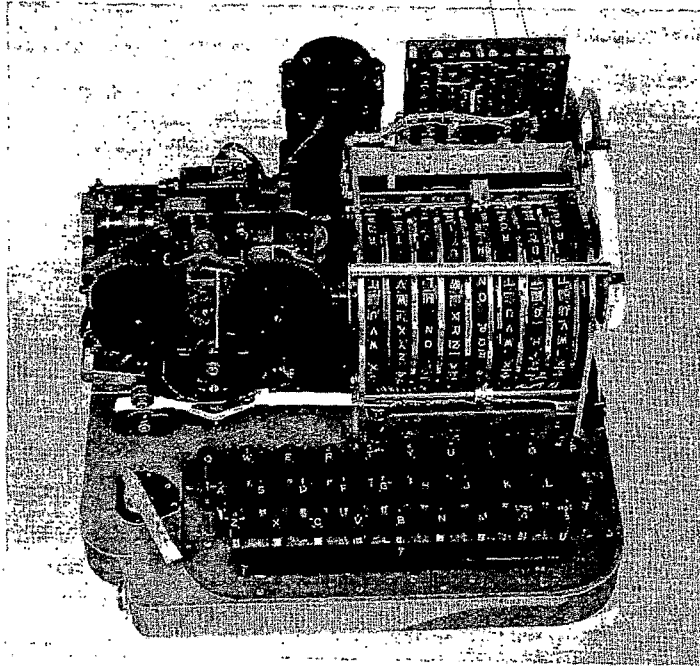
(b) (1)
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

(b) (1)

~~TOP SECRET UMBRA~~



AFSAM-7

Several different systems, including Typex and M-209, were loaned for NATO use, but none of them solved the problem of availability and security. Then in 1953 the JCS proposed the brand-new AFSAM-7, the best off-line system the U.S. had. State and CIA both opposed the decision, but after several years of acrimonious disagreement, USCIB approved the AFSAM-7 for transfer to NATO. NSA voted with the majority

[Redacted]

[Redacted]

The Push for On-line Encipherment

The conversion of record communications to on-line encipherment was probably the most significant COMSEC development of the postwar era. In the space of a few years NSA led the U.S. government into the era of secure circuitry.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

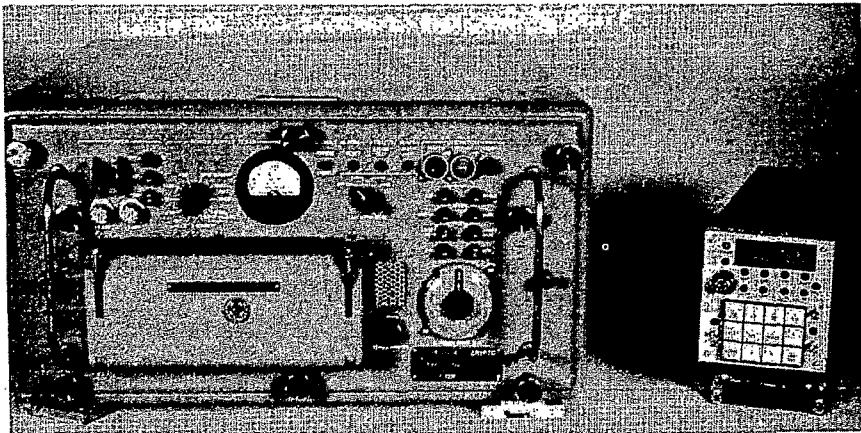
~~TOP SECRET UMBRA~~

After the war, the cryptologic community began the search for a reliable and efficient on-line device. For a time it appeared that one-time tapes were the answer. The British developed the 5UCO or the Secretape, which achieved limited use during the early 1950s. But tape production and handling were still a nightmare, and the volume of communications required in the 1950s dictated another solution.⁶⁰

Circuit speeds were beginning to exceed the capability of mechanical rotors to keep up. What was needed was an electronic key generator. The solution was the NSA-developed KW-26, the first on-line electronic key generator to come into wide use in the United States. First fielded in 1957, the KW-26 remained the mainstay of U.S. enciphered text communications for thirty years. According to a former NSA COMSEC official, the KW-26 made the Agency's COMSEC reputation.⁶¹

The KW-26, because it was electronic rather than electromechanical, had no moving parts, and its speed was limited only by the speed of the associated teletypewriters, which at that time was up to 100 words per minute. Built during the transition from tubes to transistors, the KW-26 had a little of both. It had a simple-to-set key system using cards manufactured at NSA. When an operator pulled the card out of the machine, a knife sliced it in half so that it could not be reused. Its chief disadvantage was that it could be used only for point-to-point circuits, which dictated that a huge number of machines be manufactured. At one time the NSA communications center alone had 336 of them.⁶²

The point-to-point modus limited the KW-26's utility in the Navy. Naval communications were marked by wide-area fleet broadcasts to large numbers of ships afloat. Naval vessels needed the capability to tune into a broadcast at any time during the day or night and just receive traffic - transmitting messages was a much smaller communications function. To solve this problem, NSA designed the KW-37, a crypto device that permitted a ship's communications operator to tune into the fleet broadcast using a cryptographic catch-up function.⁶³



KW-37

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The next on-line crypto device to be widely adopted was the KG-13. Unlike the KW-26, it was a general-purpose key generator, which meant that it could be used for more than just teletypewriter security. Fully transistorized, it was smaller and lighter and was suitable for a wide variety of uses. It could encrypt voice and, with the HY-2 vocoder, became the backbone of the Autosevocomm voice encryption system in the 1960s.⁶⁴

From SIGSALY to Modern Voice Encryption

As soon as the war was over, the paleolithic SIGSALY was scrapped. Surely the U.S. could find something smaller, lighter and cheaper. In the late 1940s AFSA developed a voice encryption device called the AFSAY-816, which was used to encrypt the new secure voice system between Arlington Hall and Nebraska Avenue. Using a primitive vacuum tube key generation and pulse code modulation, it produced good voice quality. The drawback was that it needed a 50 KHz carrier.

When computers came into general use in cryptology, NSA judged that the AFSAY-816 was cryptographically suspect and replaced it with the KY-11, [REDACTED]

[REDACTED] The KY-11, however, had the same drawbacks as the earlier AFSAY-816. It was a large system and was kept in the communications center. It sucked up huge swatches of bandwidth, making it appropriate for the microwave systems in the Washington area, but hardly anywhere else.⁶⁵

Because it required communications center security, the KY-11 was not suitable for general executive level use in Washington. To remedy the problems of size, weight, and security protection, NSA developed the KY-1. It was packaged in a single cabinet about half as high as an ordinary safe and was secured with a three-position combination lock. It was distributed to very high-level users like the secretary of defense, secretary of state, DCI and others. It was the first voice security system installed in private residences, and one of the early models was placed in Eisenhower's farm in Gettysburg.

To use it must have been mildly frustrating, as it was a half-duplex, push-to-talk system. Voice quality was high, but at a familiar cost - it required wideband voice circuitry. By the mid-1960s, it had been replaced by the KY-3.⁶⁶

NSA's first entry in the narrowband sweepstakes was the KO-6, a multipurpose equipment which could encrypt speech signals as well as others. It could compress and digitize speech into a narrowband transmission system, but only at considerable cost. The KO-6 weighed a ton, required three kilowatts of power, and, according to one NSA expert, "provided almost intelligible narrowband secure voice." As a result, it was seldom used in the voice mode.⁶⁷

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

TEMPEST

During World War II, Bell Laboratories, under contract to develop various devices for the Signal Corps, was working on a one-time tape mixing device called a 131-B2. Engineers in the lab noticed that every time the device stepped, a spike would appear on an oscilloscope in another part of the lab. [redacted]

Bell Labs reported this to the Signal Corps, but the report attracted little attention. So the Bell engineers mounted an intercept effort, copying and reading plain text from the Army Signal Corps communications [redacted]

This time the Signal Corps took notice and asked Bell Labs what could be done. The Bell engineers found that the problem was caused by [redacted]

[redacted] The resulting signal could emanate through the [redacted] They suggested that the problem could be corrected by shielding the keying devices, by filtering the power lines, or by masking. They built a modified mixer using both shielding and filtering. But the Signal Corps refused to buy it because it virtually encapsulated the machine, making it difficult to work on and was subject to heat buildup. Instead, they sent a message to the field urging commanders to control [redacted] their communication centers to prevent hostile signal monitoring.⁶⁸

The Germans knew about this problem and understood the potential for obtaining plain text from close-in ranges. The USSR, which was using the technique by the 1950s, very likely learned it from captured Germans. There is evidence that other Allied governments knew about it, too. Despite this, the Americans forgot what they had learned during the war. For all practical purposes, it was rediscovered by a CIA technician in 1951, while working on the very same 131-B2 mixers. CIA notified AFSA of its findings, and AFSA set to work on the problem. Designing countermeasures required time, however, and while equipment was being developed, AFSA issued instructions to the field requiring that all COMINT activities control a zone 200 feet in all directions of the communications center. As an alternative, a commander could require that at least ten teleprinters chatter away simultaneously, the idea being that this would introduce masking.⁶⁹

At this point, the newly established NSA decided to test all its equipment. The result - everything radiated. Whether it was mixers, keying devices, crypto equipment, EAM machinery, or typewriters, it sent out a signal [redacted] Plain text was being broadcast through [redacted] the electromagnetic environment was full of it.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Thus was the TEMPEST industry spawned. NSA initiated a joint project with the SCAs, which in the early years discovered problems much more rapidly than it could design solutions. In 1955 the problem of electromagnetic emanations was [redacted]. Moreover, there was hard evidence that in this one area the Soviets were far ahead of the U.S. technologically and that America's East Bloc embassies were all being penetrated. It was a Frankenstein House of Horrors.⁷⁰

The first big breakthrough was by Naval Research Labs, which redesigned the offending 131-B2 mixer and called it the NRL Mixer. NRL used a technique called low-level keying, in which the power was lowered to such an extent that a signal previously [redacted]. The KW-26 contained this circuitry, as did every crypto device after that. As long as the communications center used the device at the suppressed keying mode rather than at full power (an unwarranted assumption), it was reasonably well protected.⁷¹

By 1958 NSA was ready with the first generally applicable TEMPEST standards, which were published under JCS authority. According to the new guidelines, Department of Defense organizations could not use equipment that would radiate farther than the zone of control. [redacted] NSA published NAG-1, a TEMPEST bible that established TEMPEST measurement techniques and standards. The new rules did not, however, say anything about when the guidelines had to be met, nor did JCS budget money to fix the problem. Funds had to come from the individual commands and had to compete with all other funding priorities. Recognizing that the problem was far from fixed, USCSB in 1960 established its first and only subcommittee, the Special Committee on Compromising Emanations.⁷² But many years would pass before TEMPEST standards reached general acceptance.

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

Notes

1. NSA/CSS Archives, ACC 6851, CBKI 61.
2. Colin B. Burke, "The Machine Age Begins at OP-20-G: Or, Don't Do It This Way Again," presentation at the 1992 Cryptologic History Symposium, 28 October 1992.
3. [redacted] "The Secret War," in CCH Series IV.V.7.18; Joel Shurkin, *Engines of the Mind: A History of the Computer* (New York: W. W. Norton, 1984).
4. SRH-267.
5. Ibid.
6. Samuel S. Snyder, "The Influence of U.S. Cryptologic Organizations on the Digital Computer Industry," SRH 008.
7. Ibid.

~~HANDLE VIA TALENT KEYPHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

8. Ibid.; oral interview with Dr. Howard Campaigne, 29 June 1983, by Robert Farley, NSA OH-14-83.
9. NSASAB, "Technology for Special Purpose Processors," March 1978, in ACC 27451, CBUI 31; and ACC 10896, CBOC 33.
10. Douglas Hogan, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986, unpublished manuscript in CCH files.
11. Snyder, CCH series VI.D.3.7.
12. NSA/CSS Archives, ACC 10978, CBOC 33; ACC 6851, CBKI 61; ACC 10573, CBVB 57.
13. NSA/CSS Archives, ACC 11112, CBNI 55.
14. Snyder, "Influences," NSA/CSS Archives, ACC 10978, CBOC 33; Phillips interview.
15. Phillips interview.
16. Snyder, "Influence"; NSASAB, "Technology..."
17. Snyder, "Influence."
18. "Mechanization in Support of COMINT."
19. NSA/CSS Archives ACC 10978, H01-0601; Douglas Hogan.
20. Phillips interview.
21. Ibid.
22. Hogan, Snyder, "Influence."
23. Hogan.
24. Hogan, Snyder, "Influence"; Phillips interview.
25. Memos by Samford and Engstrom, dated Jan and Apr 57, in CCH files.
26. Hogan, Howard H. Campaigne, "LIGHTNING," *NSA Technical Journal*, IV, 3 July 1959, 63-67; Tordella interview, Kirby interview.
27. Hogan, Phillips interview.
28. Phillips interview.
29. "History of AFSA/NSA Communications Center," correspondence file in CCH Series VI H.1.2.; "NSA's Telecommunications Problems, 1952-1968," unpublished historical study available in CCH Series X.H.4.; George Howe, "The Narrative History of AFSA/NSA, Part V, Final Draft, Ch. XXVI-XXX," available in CCH.
30. "History of AFSA/NSA Communications Center."
31. "History of AFSA/NSA Communications Center"; videotape lecture on the history of NSA communications by [redacted] available in CCH.
32. "History of AFSA/NSA Communications Center"; NSA/CSS Archives ACC 33707, H01-0108-6.
33. "NSA's Telecommunications Problems..."
[redacted]
35. "History of AFSA/NSA Communications Center"; "NSA's Telecommunications Problems."

(b) (1)
 (b) (3)-P.L. 86-36
 (b) (3)-50 USC 403
 (b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

36. "NSA Review of U.S. Cryptologic Effort . . .," in CCH Series VI.EE.1.3.
37. George F. Howe, "Centralized COMINT Communications Centers: The Historical Record," unpublished manuscript in CCH Series X.H.5.
38. [redacted] videotape; Tordella interview; CAHA, ACC 33707, H01-0108-6.
39. "NSA's Telecommunications Problems . . ."; [redacted] "The National Security Agency's Gray Telephone System: Present and Future," Telecom Career Panel paper, 19 July 1982.
40. "NSA's Telecommunications Problems . . ."
41. "Implementation of NSCID 7," CCH Series VI.B.1.3.
42. Edward Fitzgerald, "A History of U.S. Communications Security: Post-World War II," unpublished manuscript available in E324; [redacted] "Theory of Wired Wheels," 11 March 1955, in CCH Series VI.EE.1.30; McConnell manuscript available in CCH; Ryon A. Page, "The Wired Wheel in U.S. Communications Security," unpublished manuscript in CCH Series VI.F.1.21.
43. Fitzgerald.
44. Boak lecture, 1991 Cryptologic History Symposium, available on videotape in CCH.
45. Page.
46. Page; David Boak, *A History of U.S. Communications Security*, rev ed 1973 (The Dave Boak Lecture Series).
47. [redacted] paper; "Evolution of Equipment to provide COMSEC" (lecture dated 1971) in CCH Series VI.F.1.6.; Oral History interview with Howard Rosenblum, 14 Aug 1991, by Robert Farley and Henry Schorreck, NSA OH 03-91.
48. Fitzgerald.
49. Ibid.
50. Burns.
51. William Nolte, draft history of NSA, available in CCH files.
52. "COMSEC Material (Historical) 1957-1970," in CCH Series VI.F.1.3.
53. "COMSEC Historical Material."
54. Ibid.
55. David Boak, written statement, Oct. 1994.
56. Memo for the Chairman, USCSB, "Capsule History of the USCSB, 12 January 1970," from the Executive Secretary, Thomas R. Chittenden, in COMSEC Historical Material.
57. Fitzgerald; "Manufacture of COMSEC Keying Materials (S3)," in CCH Series VI.F.1.12.
58. Oral interview [redacted] 2 Feb. 1993, by Charles Baker and Tom Johnson, NSA OH 2-93.
59. Collins, V. I., 45.
60. "Historical Study of NSA Telecommunications, Annual, 1973-1975," in CCH Series VI.A.1.10.
61. David Boak, *A History of U.S. Communications Security* (The David Boak Lecture Series), 1973.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

62. Ibid.

63. Boak; Howard Barlow speech at 1991 Cryptologic History Symposium.

64. "Evolution of Equipment to provide COMSEC" (lecture dated 1971) in CCH Series VI.F.1.6.
manuscript available in CCH.

65. Boak.

66. "Evolution of Equipment..."; Boak.

67. "Evolution of Equipment..."

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

68. Ibid.

69. Ibid.

70. Ibid.

71. Ibid.

72. Ibid.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

Chapter 6 Cryptology at Mid-decade

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

THE EARLY ASSESSMENTS

It has become exceedingly difficult to obtain significant information from covert operations inside Russia. The security zones at the border, the general restrictions in the interior, the thousands of security police, and the innumerable informers among the populace are brutally effective in limiting infiltration, exfiltration, and usefulness of agents. Therefore, we must more and more depend on science and technology to assist and to complement the best efforts of classical intelligence.

The Killian Board, 1955

The Eisenhower administration's intelligence focus was not on traditional espionage - it was on technical intelligence, whence, Eisenhower knew through personal experience during World War II, he could obtain vast quantities of information. His concern over the apparent breakdown in COMINT during the Korean War caused him to refocus again and again on NSA. Reports about NSA's performance began to flow back to him almost from the moment the Agency was created. The reports are important today because they indicate the direction that cryptology was to travel in subsequent years.

The Robertson Committee

The first reports on NSA were a product of President Eisenhower's concern with Soviet [redacted] capabilities. In the summer of 1953, the National Security Council began examining America's strategic vulnerabilities, and, with it, the intelligence system that must provide the warning. But Canine adamantly opposed granting COMINT clearances to the members of the panel, and USCIB backed him. Instead, Canine established a largely in-house examination of COMINT, chaired by Dr. H. P. Robertson of California Institute of Technology, a member of Canine's advisory panel, the NSA Scientific Advisory Board (NSASAB). Four of the seven members were from NSASAB, and the remaining two were from the Office of the Secretary of Defense.¹

Robertson reported during the dark days after "Black Friday," when Soviet [redacted] was still an unrevealed mystery. [redacted]

[redacted] The immediate result of this was the intercept, in 1954, [redacted]

[redacted] This opened up a new world [redacted]

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~TOP SECRET UMBRA~~

[redacted] The committee also recognized the indivisability of COMINT and ELINT and stressed the effort to fuse both sources into a single report.²

But Robertson made plain that NSA must be in the game for the long pull. The long pull was Soviet [redacted] and he urged an all-out attack on the new [redacted] systems introduced in the early 1950s. His committee recommended the development and deployment of new intercept [redacted] equipment.³

The Hoover Commission

The Hoover Commission was a far larger effort. Established by Eisenhower in 1954 and chaired by former president Herbert Hoover, it was at the time the most thorough re-examination of the federal government ever attempted. Hoover subcommittees delved into every cranny of the bureaucracy seeking improvements and economies. One such subcommittee was a task force chaired by General Mark Clark to investigate intelligence activities. The committee looked closely at NSA.⁴

The thrust of the Hoover Commission set the mold for all subsequent panels. Responding to the entreaties of Canine, it recommended increased authority for NSA in virtually every area of its operation. NSA should have the authority to prescribe equipment standards; it should prescribe all intercept and processing standards; it should inspect service cryptologic training and direct modifications as necessary. There was almost no area in which it did not feel that NSA should be further empowered.⁵

What the panel did for NSA it also recommended for the SCAs. They should have more authority within their respective services, and each should be at the level of a major command. At the time only USAFSS was at that level, although ASA was granted major command status before the report was published. This left only NSG at a lower level within its service. It noted that "largely because of its status as a major command, the AFSS has developed a dynamic and promising program for recruiting, developing and holding on to technically qualified military career personnel."⁶ The committee noted the dismal record of the three services in assigning people to cryptologic posts, and it recommended that security strictures be changed to permit military personnel offices to understand the importance of the jobs.⁷

More controversial was the panel's recommendation that NSA acquire additional authority over ELINT. Canine, who saw himself teetering over the black hole of interservice fighting, opposed this. He was having enough trouble unifying COMINT, without trying to swallow ELINT whole. USCIB noted that NSCID 17 had just been issued, and it urged that this new approach be tried before considering further integration of ELINT. (The impact of NSCID 17 will be discussed in chapter 7.)⁸

Clark and his committee proposed an all-out attack on Soviet high-grade ciphers, equivalent, in their words, to the Manhattan Project. It would require the best minds in

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

the country, equipped with the finest resources money could buy, but it would be worth it if even a portion of the Soviet [redacted] systems were unlocked. Canine hailed the potential resource augmentation with glee, but cautioned against a total commitment before NSA had thoroughly analyzed the prospects for success. USCIB supported him.⁹

Cryptologic personnel requirements weighed heavily on the committee. Clark urged an improved grade structure, including the addition of supergrades, higher pay for consultants, improved assignment of service officer personnel, better perquisites for NSA people assigned overseas (to be the equivalent of those received by CIA), and NSA exemption from the Classification Act. To improve the revolving door nature of military intercept operators (few of whom stayed in the service past their initial enlistment), Clark urged the assignment of civilians to intercept positions overseas.¹⁰

Clark and his committee were concerned about two other potential problems. The first was the state of COMINT requirements, which were expressed in a document called the Master Requirements List. This, they said, was about the size of the Washington phone directory, and about as specific. And since customers wanted COMINT to tell them everything, without narrowing the target further, NSA simply specified its own requirements. This had been going on so long that there was danger that the cryptologic community would become completely isolated from its customers and insensitive to them.¹¹

What was occurring in requirements, they felt, was also true in security. COMINT security had become so tight that cryptologists were isolated from their customers. In time of war there was real danger that essential information would not get to the battlefield because of clearance restrictions. Thus the system would defeat itself and become a vestigial appendage.¹² It was a debate that would rage for years within the intelligence community.

The Killian Board

Eisenhower's preoccupation with the Soviet nuclear threat spawned a number of committees to look at American vulnerability. By far the most important of those was the Scientific Advisory Committee, commonly known as the Killian Board. In July of 1954 Eisenhower asked Dr. James R. Killian of MIT to head a study of the country's capability to warn of surprise attack. Killian named a panel of the elite from academia, the scientific community, and the military.

(b) (1)
 (b) (3)-P.L. 86-36
 (b) (3)-50 USC 403
 (b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Dr. James Killian, shown here with General Samford at NSA

The committee quickly came to the conclusion that spying on the Soviet Union in the classical sense (agents and that sort of thing) was not the answer. The Soviet Bloc was too hard to penetrate. Warning, if it were to come in time, would have to come from technical intelligence like COMINT, ELINT, and photography. This recommendation was to begin a revolution in the way the government thought about, organized, and used intelligence. From that time on, technical intelligence became the "answer" to the problem of strategic warning. It would remain so for the duration of the Cold War.

As part of the Killian Board, the Land Panel was to achieve a measure of renown. Chaired by the farsighted Edwin Land, inventor of the Polaroid camera, the panel was to concern itself with the development of new reconnaissance programs. The Land Panel came to have a profound influence on the future of overhead photography, the U-2

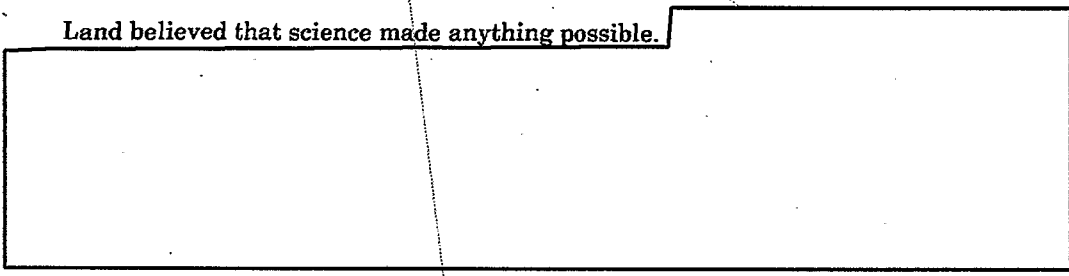
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

program, and intelligence collection satellites. It was this group that first envisioned COMINT and ELINT intercept packages aboard orbiting satellites.

Land believed that science made anything possible.



The Jackson Report

The most personal and confidential report on NSA was by William H. Jackson. One of the original members of the Brownell Committee, Jackson was appointed by Eisenhower to monitor NSA's progress and to make periodic progress reports through Sherman Adams, Eisenhower's chief of staff. In meetings with Jackson, the president expressed his personal concern that NSA should be effective, and Jackson kept him apprised of what still needed to be done.

Jackson insisted that NSA needed a strong research and development organization, and he regarded the appointment of a director of research in 1956 as a significant step forward. A more difficult matter was the naming of a chief civilian deputy. Canine insisted on running his own show and did not want, and refused to appoint, a civilian deputy. Only when Samford came aboard in 1956 and quickly named a civilian, Joseph Ream, as deputy was Jackson satisfied on this point.

Yet a third organizational problem was the matter of a point of contact for COMINT within DoD. Brownell had envisioned that COMINT matters would be handled at least as high as the assistant secretary level. This high-level attention had not occurred, and Jackson reported in 1956 that the nominal point of contact, General Graves B. Erskine, head of the Office of Special Operations, normally turned COMINT over to a lower-ranking staffer. In Jackson's view, this level of concern was wholly inadequate to the task at hand.

The objective of all this organizational to-ing and fro-ing was to put NSA in position to mount a full-scale attack "Only after such an attack has been made," Jackson noted, "can we determine safely, in the event of failure, that the effort is hopeless and the annual expenditure of forty odd millions can be saved."¹⁴

NSA was clearly still on probation. It was a probationary period that would not end with a bang but would slowly fade away. The corner was not turned during either the Eisenhower or Kennedy administration. NSA did not come off probation until the presidency of Lyndon Baines Johnson.

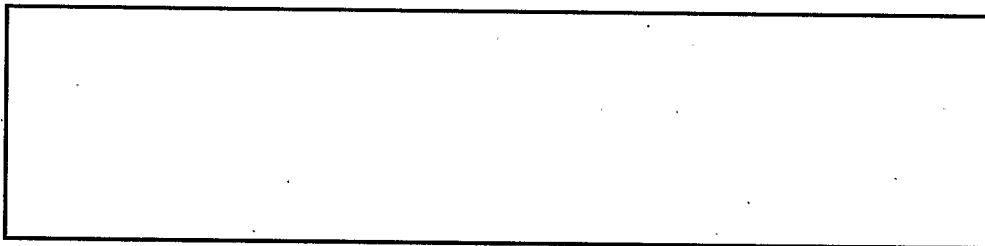
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

1956

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

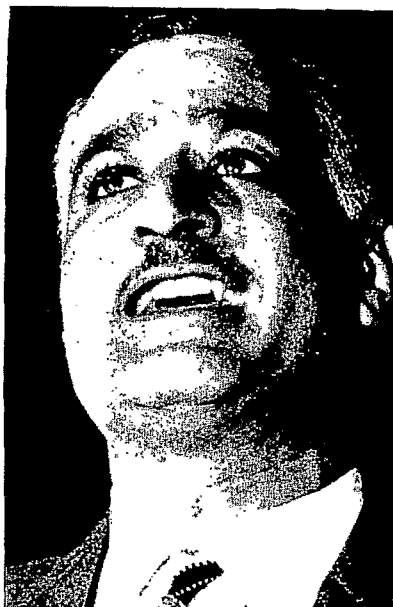


Certain years mark watersheds in cryptologic history. Nineteen fifty-six was such a year. Twin crises, Suez and Hungary, came virtually together in time to pressure a new NSA-managed COMINT system that had never been stressed in such a way. The conjunction of crises, rolled into a COMINT alert called Yankee, resulted in short and long term changes to the system. It was a year for cryptologists to remember.

Suez

Suez was a significant benchmark in the postwar American involvement in the Middle East. It also represented the greatest crisis in the post-World War II Western Alliance.

The creation of Israel in 1947 had been accompanied by war, dislocation, and bitterness. In 1952 the Egyptian government had been captured by hard-line pan-Arab, anti-Israeli nationalist military officers headed by Gamal Abdel Nasser. When Nasser officially took over the government in 1954, he set a course which resulted in a distinct tilt toward the East. When, in 1956, the Western nations hedged on earlier commitments to fund a Nile dam at Aswan, Nasser courted the



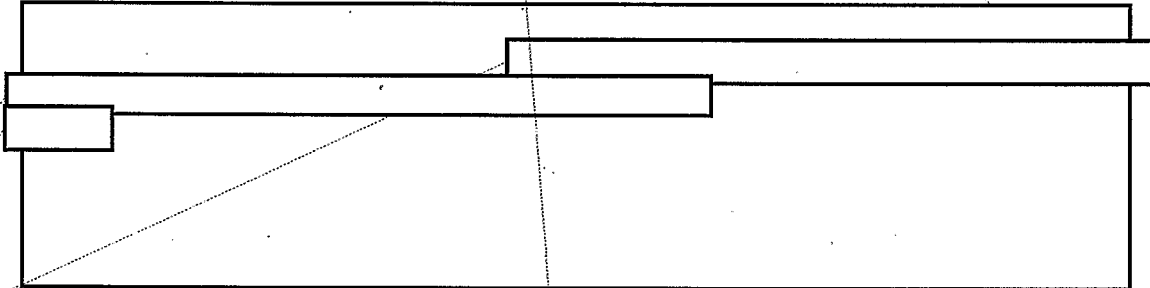
Gamal Abdel Nasser

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

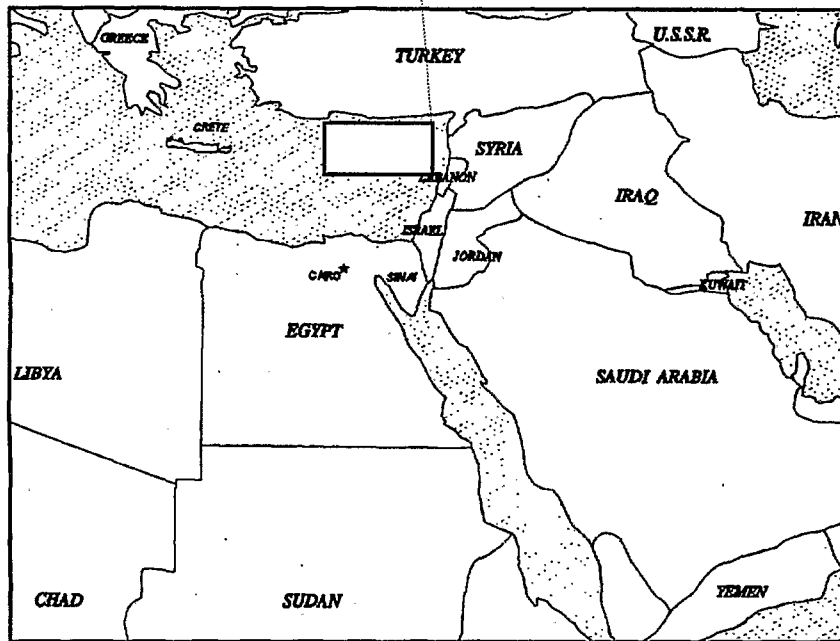
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Soviet Union, and eventually secured funding there. Meanwhile, his relationships with Great Britain grew so strained that in July of 1956 he nationalized the Suez Canal. At this point Great Britain and France began planning a military invasion to take back the canal. At the last minute they took Israel into the scheme, and they got the Israelis to agree to launch an invasion of their own. The resultant fighting would give Britain and France the opportunity to come in as "peacemakers" with sufficient armed forces to take back the canal. They did their best to keep the scheme secret from the American government, whose attitude toward the Arabs appeared to be more even-handed.



(b) (1)
(b) (3)
OGA

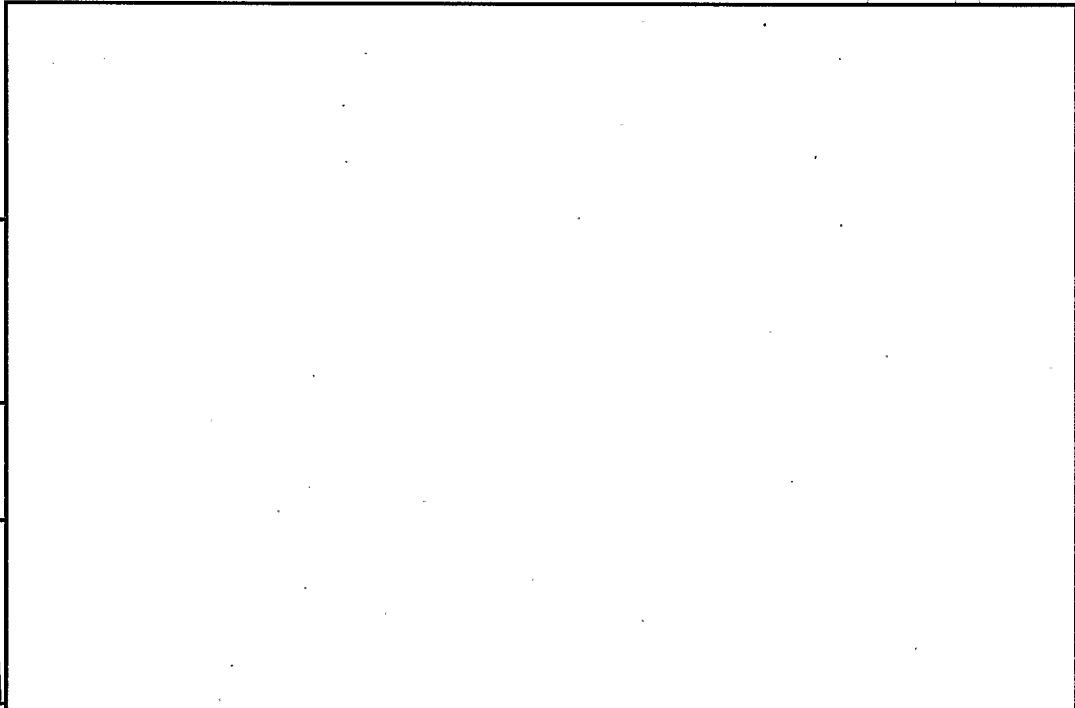


The Middle East in 1956

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



(b) (1)
(b) (3)
OGA

In the spring of the year, as the situation in the Middle East darkened,

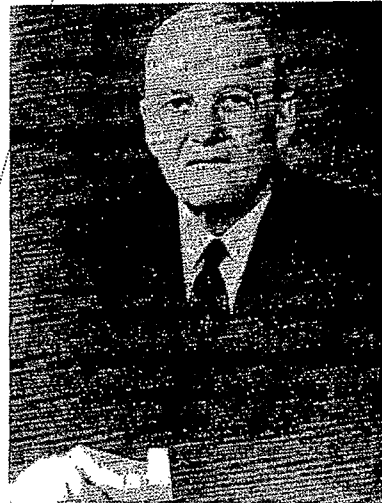


But the transition was only in its early stages when, on 29 October, the Israeli army struck Egypt in the Sinai.

Secretary of State John Foster Dulles expressed shock and outrage. The outrage was real - the shock was made up. His own brother, CIA chief Allen Dulles, had sent him two national intelligence estimates earlier in the fall which predicted the invasion.

Dulles was furious.

Allen



John Foster Dulles, Eisenhower's secretary of state, played a central role throughout the Suez Crisis of 1956.

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

(b) (1)
(b) (3) -50 USC 403
(b) (3) -18 USC 798
(b) (3) -P.L. 86-36

~~TOP SECRET UMBRA~~

[redacted]
[redacted] Timely reporting over a period of months could have left no doubt within the administration that Soviet diplomacy consisted of posturing. They were not going to go down to the Middle East to bail out anyone. Forces just weren't moving. The Soviets had their hands quite full with Hungary, whose crisis had flopped down directly on top of Suez.

[redacted]
[redacted] But they in no way approximated what was happening at the ministerial level.

[redacted] Such a strong alliance could not be torn asunder by Suez. As Peter Wright said in his book *Spycatcher*, "Only GCHQ, which had a formal charter of cooperation with its American counterpart, the National Security Agency (NSA), under terms of the 1948 UKUSA agreement, remained relatively immune to the turbulent currents which battered the previously intimate wartime Anglo-American intelligence relationship."¹⁵

Hungary

For the Soviets, the real problem in 1956 was the East Bloc. Domestic Hungarian unrest culminated in a revolution that Soviet troops put down violently in November of 1956.

The Hungarian revolution was a surprise to the intelligence community. But as events gathered speed, the Soviet reaction was not. [redacted] provided fairly complete indicators concerning Soviet military unit movements throughout the crisis. As Soviet forces moved into Hungary and concentrated on Budapest in the waning days of October, [redacted] tracked and identified the participants.

[redacted] there was very little else available to the White House about the unfolding Soviet reaction.

The National Security Agency did not specifically predict that Soviet forces would become involved - prediction was not its role. There was enough [redacted] to lead one to that conclusion prior to the 4 November Soviet takeover of the capital. But no one drew the strings into a bundle. It was all a hodgepodge of [redacted] poorly understood by customers.

[redacted] It was an opportunity lost.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

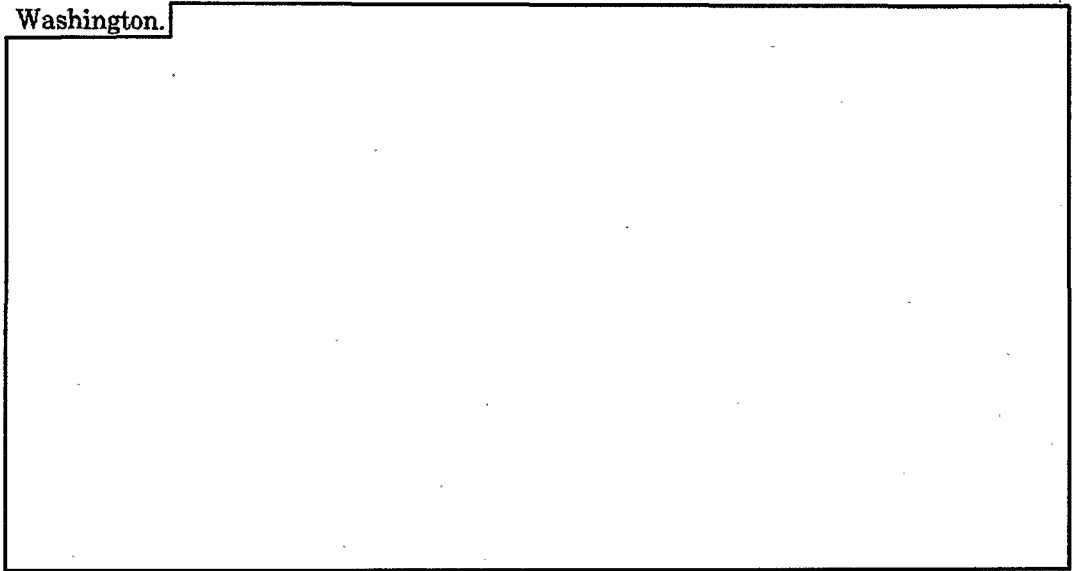
~~TOP SECRET UMBRA~~

The Yankee Alert

Suez occurred on 29 October; Hungary broke on 4 November.



Nineteen fifty-six was a bad time for NSA to get involved in crisis. The organization was in the middle of its move from downtown Washington to Fort Meade. Some analytical branches were in newly established quarters at Fort Meade, while others had remained behind at Arlington Hall. Communications between the two geographical areas were temporary, and much of the routine traffic was being couriered four times a day from Washington.



(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798

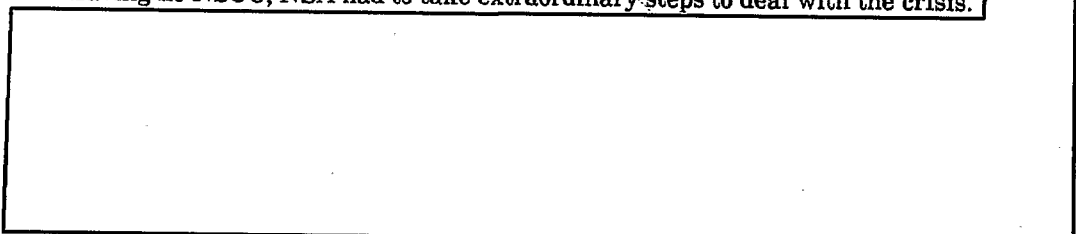
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

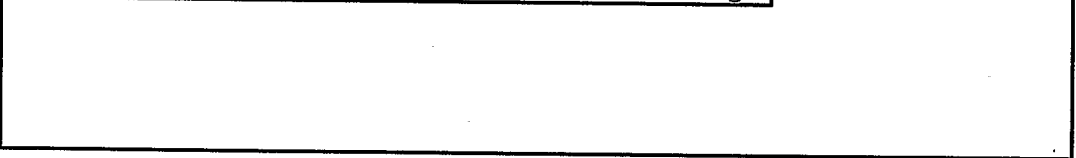
(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

~~TOP SECRET UMBRA~~

Having no NSOC, NSA had to take extraordinary steps to deal with the crisis.



NSA technical support to the field was slow in coming.



Lebanon, 1958

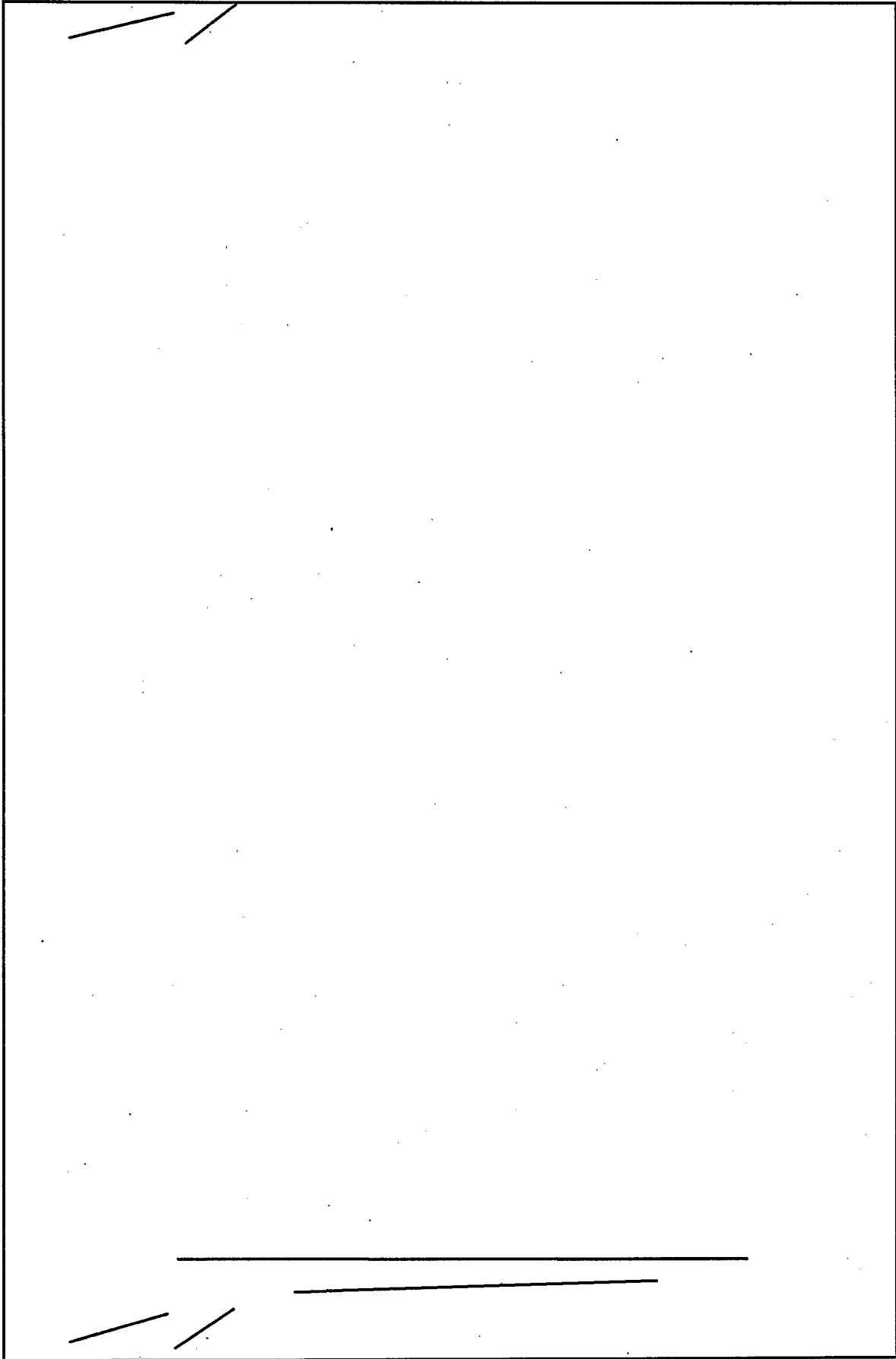
The Eisenhower administration was pulled into the Middle East quite by accident in 1956. But the president quickly yanked U.S. foreign policy into line with the new situation. In January 1957, in a State of the Union address focusing on the Middle East, he proclaimed what became known as the Eisenhower Doctrine: the United States would use its armed forces to help any country requesting assistance in maintaining its independence "against overt armed aggression from any nation controlled by International Communism."²² Just two short years later, he employed the new doctrine in its first test. The occasion was Lebanon.

Nasser had continued to extend his pan-Arabism, and he was the idol of the Middle East. In January 1958 he announced the formation of the United Arab Republic, an amalgam of Egypt and Syria, with Egypt clearly the dominant partner. The new UAR then launched a propaganda assault on the more conservative regimes in Lebanon, Jordan, Iraq, and Saudi Arabia. An arms race involving the U.S., Britain, France, and the USSR produced a Middle East that was "armed and dangerous."

On 14 July pro-Nasser forces overthrew the Iraqi monarchy and assassinated the royal family. Camille Chamoun, who headed the pro-Western government of Lebanon, believed that he was next and hurriedly requested American assistance. Eisenhower believed that Nasserists were about to take over the oil supply and decided, on the spur of the moment, and after consulting with virtually no one, to come to Chamoun's assistance. He ordered the Sixth Fleet to the Eastern Mediterranean and instructed the chairman of the JCS, General Twining, to put Marines ashore in Beirut the next day. Harold MacMillan, the British prime minister, requested that it be a joint operation, but Eisenhower wanted a unilateral action, and he suggested that British paratroops be deployed to Jordan rather than Lebanon.²³

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~



(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798

~~TOP SECRET UMBRA~~

1956 in History

By the end of 1958, the United States was firmly in the Middle East, [redacted]

[redacted]

By the time of the 1967 Arab-Israeli War, [redacted]

The problem proved difficult to address because of the wild mood swings between somnolence and war in the Middle East. But the cryptologic community eventually had a core of expertise and resources [redacted]

The Hungarian crisis marked the dawning of a new capability. [redacted]

[redacted]

Unfortunately, such sophisticated analysis, available in later decades, simply did not exist in 1956. [redacted]

[redacted] It was an art form that had to be learned.

As for crisis response, all was chaos. The cryptologic community proved incapable of marshalling its forces in a flexible fashion to deal with developing trouble spots. The events of the year did not demonstrate success - they simply provided a case study to learn from.

The Reorganization

Ralph Canine departed NSA on 23 November 1956. But before he did, he hired the management firm of McKinsey and Company to look at NSA's organization from top to bottom. The McKinsey study resulted in a thorough revamping of the way NSA functions that still had repercussions through the 1980s.

Canine was concerned with primarily two questions: would operations function more effectively on a functional or geographic organization, and to what extent should staff functions be centralized?

McKinsey introduced a modified geographical concept. Organization for COMINT would be along target (i.e., country or geographical) lines, but within that scheme, specific processes like cryptanalysis, [redacted] and resource tasking, would often appear in separate organizations. The new scheme brought with it a greater focus on targets, but retained many aspects of the factory-like origins of the business.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

When the team presented its findings to Canine only a few days before his retirement, it showed him a new organizational concept. Gone was the old numerical organizational system, replaced by pronounceable syllabic office designators. Thus DDO became PROD, and within PROD were four major offices:

GENS	[REDACTED]
ADVA	
ACOM	
ALLO	

The principle of pronounceable syllables was carried through the Agency. For instance, MATH was the Mathematical Research Division within R&D; RADE was the Radio Equipment Division; STED was the Communications Security Division; PERS was personnel; MPRO (pronounced em-pro) was machine processing; SEC was security, etc. It was a profoundly rational way to designate offices, but it did not do a very good job of obscuring office functions from an inquiring public. Ultimately, that was to spell the end of the pronounceability craze, although the basic organizational scheme would continue to the end of the Cold War.

As to the second question, relating to centralization of staff functions, McKinsey came down heavily on the side of decentralization. The firm viewed the director as being far too involved in day-to-day management of Production and only distantly concerned with the easier-to-manage COMSEC and R&D organizations. To correct this, McKinsey recommended that a virtually independent Production function be created. All ancillary functions would be gathered up under PROD, [REDACTED]

[REDACTED] and even some logistics functions. It was a powerhouse organization.

The director's staff was reduced in proportion to the matters transferred to PROD. Gone were such offices as Headquarters Commandant and Adjutant General, Army-type organizations whose very meaning is obscure today. To manage a potentially unwieldy Production organization, McKinsey created the staff system that carried through the Cold War: the 02, 03, 04, etc., way of staff organization.

By far the biggest organization in the Agency was GENS. Out of just over [REDACTED] people assigned to PROD, almost [REDACTED] called GENS home. The GENS organizational system, as modified by a 1957 re-organization, created a [REDACTED] organizational scheme that retained its character for more than thirty years. GENS-1 [REDACTED] GENS-2 [REDACTED] GENS-3 [REDACTED] GENS-4 [REDACTED] GENS-5 [REDACTED] and GENS-6 [REDACTED]

McKinsey was concerned about COMSEC. Once the move to Fort Meade took place, it would be physically divorced from the rest of NSA. To accommodate this, the firm

(b) (1)
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798
(b) (3) - P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

recommended special decentralization authority for COMSEC, including certain aspects of physical security, supply, and engineering.

The R&D organization, said McKinsey, should stick solely to research and development. Development of off-the-shelf equipment applications, local component fabrication, equipment repair, or anything that involved known or proven technologies, should come under some other organization – most notably, PROD. Regarding the fielding of COMSEC equipments, unless it involved pure research, it was not properly an R&D function, McKinsey said, and should be resubordinated to COMSEC. This was an issue, however, that would be replayed many times during the Cold War.²⁷

THE MOVE

It is desired that you take immediate action to recommend for my approval a suitable location for the Armed Forces Security Agency within a 25-mile radius of Washington . . . the new site survey should be carried out as a matter of high priority . . .

William C. Foster, Deputy Secretary of Defense, 1951

When AFSA was created in 1949, it was without its own facilities. The new organization was forced to borrow space at Arlington Hall and Naval Security Station (NSS).

In an appendix to the document that created AFSA, the JCS directed that AFSA prepare a plan consolidating COMINT and COMSEC into a single facility. After studying the problem, AFSA concluded that the two could not be consolidated into their existing buildings at Arlington Hall and Nebraska Avenue. In its September 1949 report to the JCS, AFSAC pointed out that the buildings in use at Arlington Hall were temporary structures designed for wartime use.²⁸

In the autumn of 1949, with the explosion of the Soviet nuclear device, atomic hysteria was sweeping Washington. To its original charge, the JCS added one other – that a standby location be procured which was outside the Washington area to minimize the possibility that American cryptologic capabilities be destroyed on the first day of a war.²⁹

Commander Arthur Enderlin, whom Admiral Stone had appointed to chair the study committee, was adamantly opposed to a standby location. He and his committee considered it a waste of money and refused to recommend an alternate site. The JCS demanded a recommendation, but Enderlin refused. Stone reiterated the order – Enderlin remained unmoved. Stone fired Enderlin and in his place appointed Captain Thomas Dyer, one of the leading cryptanalysts of World War II. Dyer was a known advocate of the alternate location concept.³⁰

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

But then Dyer turned the solution on its head. He recommended that the alternate become primary - this would effectively move the cryptologic headquarters out of Washington. Dyer carried the day, and his committee began to look at possible relocation sites in the spring of 1950. The selection criteria were developed over a period of months, but generally focused on the following requirements:

- a. Be within twenty-five miles of a city of at least 200,000
- b. Have work space totalling at least 700,000 square feet
- c. Possess a "reasonably equable climate"
- d. Be suitable for complete physical isolation by fences and the like
- e. Be accessible to mainline air, rail, and highways
- f. Not be less than twenty miles from the Atlantic Ocean
- g. Possess dependable and secure water and electric power sources
- h. Be accessible to commercial and military communications³¹



Thomas Dyer, chairman of the "Ad Hoc Site Board"

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The basic ground rule was that the location selected had to be on an existing military base. The move was to be completed by July 1955. One option the board looked at was to select a site that already possessed a building - like a hermit crab, AFSA could simply crawl in after modifying the shell. Locations in Kansas City, Tulsa, and St. Louis were considered. Another option was to construct a new building on a military installation. The board looked at Fort Knox, Kentucky; Fort Benjamin Harrison, near Indianapolis; Fort Meade, halfway between Baltimore and Washington; Brooks Air Force Base, near San Antonio, Texas; and Rocky Mountain Arsenal, near Denver.³²

Then in early 1951 the board sent AFSAC two recommendations - if the existing structure criterion were used, Kansas City should be the choice, and if a new building were wanted, Fort Knox was the way to go. This produced great controversy in AFSAC. Some pressed for an existing structure, maintaining that the lower cost and quick availability would help meet the July 1955 deadline. Others opposed moving into someone else's offices - that had been tried at Arlington Hall and Nebraska Avenue and had not worked. The Air Force pressed for Fort Knox, contending that it was less vulnerable to a Soviet nuclear strike. Stone and Major General Canine (who would soon become director of AFSA) both opted for Fort Meade. But in the end AFSAC voted for Fort Knox. The JCS approved the Fort Knox option in April, but only after another heated argument about the advisability of moving to a relatively isolated location. Many, including Stone and Canine, were concerned about the critical lack of housing in the Fort Knox environs, and some wondered if their civilians would accept the choice.³³

While orders were being cut and contract proposals were being written for the Fort Knox construction, AFSAC members argued vehemently over the functions to be moved. Dyer was the author of a plan to split COMINT into two parts - three-fourths of it would move to Kentucky, while some residual functions would stay in Washington, along with most of COMSEC and some liaison offices. He was opposed by Admiral Joseph Wenger, who felt that splitting COMINT would be disastrous. Ultimately, Wenger won, and it was decided to leave COMSEC in Washington, while all of COMINT would move to Fort Knox and Arlington Hall would be closed.³⁴

The board knew Fort Knox to be objectionable to some of the civilian employees because of its distance from Washington. The lack of housing was worrisome, as was the rigid segregation practiced in Kentucky in 1951. But AFSA pressed ahead with the selection anyway, until a startling thing happened: Someone decided to ask the civilians what they thought.

No one knows now who originated the civilian opinion survey, but by May of 1951 it was being circulated at Arlington Hall and Nebraska Avenue. The results were a show-stopper. Most of the civilians planned to resign rather than go to Fort Knox.³⁵ Without them, AFSA would find it difficult to operate. The problem had to be fixed.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The matter came to a head in October of 1951. Deputy Secretary of Defense William C. Foster told Canine, the new director of AFSA, that he had a problem. AFSA's civilians were not in favor of the move to Fort Knox, and neither were AFSA's two most important non-DoD customers, the State Department and CIA. Canine went directly to see General of the Armies Omar Bradley, the Army chief of staff. Bradley told him to meet with the JCS. At the JCS meeting in early December the Fort Knox move was cancelled, and Canine was directed to appoint another site selection board.

Canine's new selection board, still chaired by Dyer, but including some civilians, held hurried meetings in January and February of 1952. The new site had to be between five and twenty-five miles from the center of Washington. This placed it within the postulated blast zone of then-existing Soviet atomic weapons and thus violated a JCS stipulation that the new AFSA site had to be at least twenty-five miles from the Washington Monument. But Soviet atomic weapons were progressing all the time, and the twenty-five mile limit no longer made sense anyway. The JCS could have either atomic invulnerability or a skilled civilian work force, but apparently it could not have both.³⁶

The board looked at several sites in suburban Virginia, including Fort Belvoir, some land along the George Washington Parkway inhabited by the Bureau of Roads (later to become famous as the site of the new CIA headquarters building), and Fort Hunt. In Maryland, it considered several sites within the Beltsville Agricultural Research Center, White Oak (site of the Naval Ordnance Laboratory), Andrews Air Force Base, and Fort Meade.

Of those, Fort Meade was the only one on the original list. It was twenty-two miles from the Monument, the furthest removed of any site considered the second time around. Despite the distance from Washington, transportation difficulties would be solved by a new parkway then under construction between Washington and Baltimore. There was plenty of vacant land on Fort Meade for construction of headquarters and life support buildings. It was the obvious choice, and on 5 February it became official. (Considering that Canine said he had already selected Fort Meade himself, and had informed Lovett of that, the proceedings of the board may well have been window dressing.)³⁷

Fort Meade, named for the Civil War victor at Gettysburg, inhabited a thickly wooded 13,500 acre tract precisely halfway between Baltimore and Washington. Originating as Camp Meade during World War I, it had been a training facility during both World Wars I and II. During World War II some 3.5 million men passed through on their way to Europe and at the peak of the war 70,000 people inhabited the post. After the war it became a headquarters, first for the 2nd Army and later (in 1966) for the 1st U.S. Army.

When Canine first looked at it, Fort Meade consisted of hundreds and hundreds of temporary wooden structures being used as barracks, offices and training facilities, with only a few permanent brick buildings. The corner of the post that NSA proposed to use

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

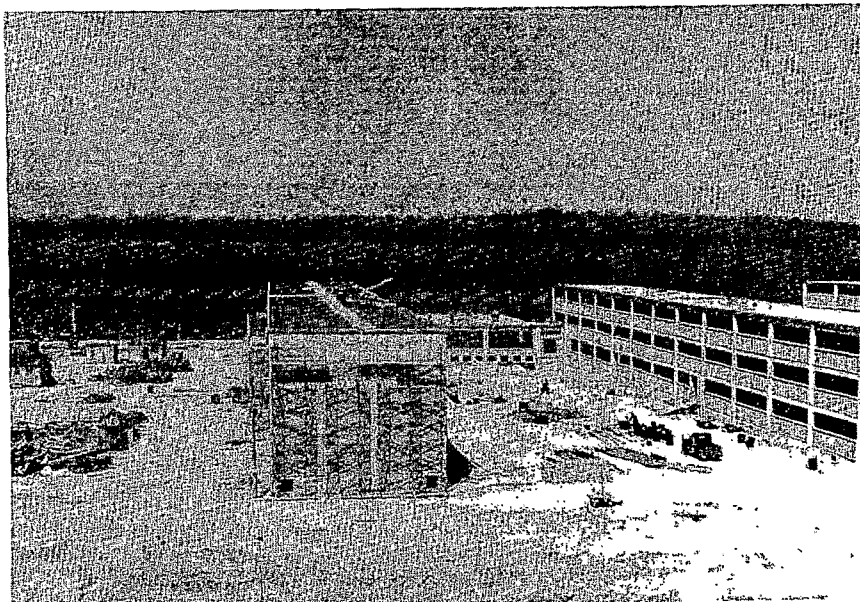
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

was uninhabited, but was near a major intersection - the new Baltimore-Washington Parkway and Maryland Route 32.³⁸

The new building would be U-shaped with double cross-members, designated the center and west corridors. Entry would be in the middle of the west corridor, the portion of the building facing Route 32. At 1.4 million square feet, it would be the third largest government building in Washington, smaller only than the Pentagon and the new State Department building. But it was designed for the AFSA population in 1951, and it did not take into consideration the growth that took place up to mid-decade, which left the new building critically short of space. The only solution was to leave someone behind, and that "someone" became the COMSEC organization, which remained at Nebraska Avenue until another building was completed in 1968.³⁹

In 1954 a contract was awarded to two co-prime contractors, Charles H. Tompkins Company of Washington, D.C., and the J.A. Jones Company of Charlotte, North Carolina. The contract price was \$19,944,452. Ground-breaking occurred on 19 July 1954. When the building was completed, the total cost turned out to be \$35 million, an overrun of almost 100 percent.⁴⁰



Barracks under construction, 1954

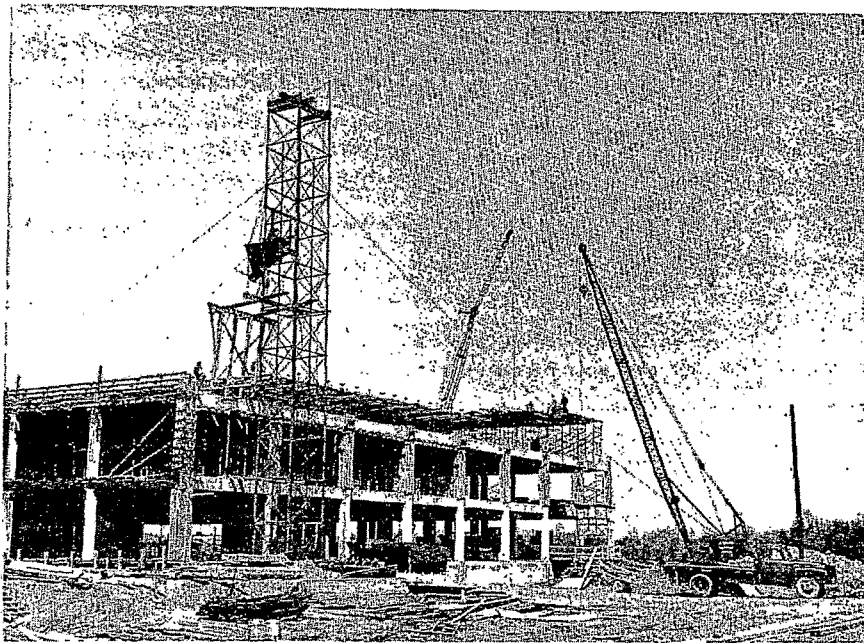
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

A few miscellaneous facts wowed the local community. It had the longest unobstructed corridor in the country, 980 feet long (center corridor). At its birth it had a German-made pneumatic tube system that could carry papers at twenty-five feet per second and could handle 800 tubes per hour. The cafeteria could seat 1,400, and the auditorium (later dedicated to William Friedman), 500. As its new occupant, NSA would become the largest employer in Anne Arundel County.⁴¹ It was a far cry indeed from the quaint but antiquated Arlington Hall, the stately Naval Security Station, and the firetrap A and B buildings at Arlington Hall.

NSA handled the move in stages. There was an "interim move," which put parts of NSA's operation into temporary quarters on Fort Meade. This had the advantage of moving the operation gradually so that large parts of it were not shut down for any period of time. The new operations building would not be ready for occupancy until 1957, and so the interim move also had the advantage of placing cryptologists at the new location in advance of the July 1955 deadline.



Headquarters construction, 1955, south wing

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

It began with an interim move to four brick barracks constructed for NSA use in 1954 just behind the proposed site for the main complex. The first to arrive, in November of 1954, was a contingent of 149 Marine guards to provide security. The other 2,000 plus people taking part in the interim move included virtually the entire population of GENS, plus enough communicators, personnel, and logistics people to keep them going. Heat for the operation was provided by an old steam engine which was brought in on the old Baltimore, Washington and Annapolis tracks, and was installed in a small copse of trees, which still exists, between the present OPS2A and the barracks area. (In fact, the original barracks themselves, now converted to living quarters, also still exist.)

GENS and its support staff became an outpost, connected to the main headquarters by inadequate electrical communications. Most classified material was couriered back and forth four times a day - the electrical circuits were reserved for only the most critical and time-sensitive information.⁴²



The NSA operations building in 1957

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

To NSA's military population, the move to Fort Meade was a matter of routine. The military moved frequently, and the relatively cloistered atmosphere of a rural Army post was closer to the normal state of affairs. Family housing was of the two-story brick variety, constructed under the Wherry Housing Act. More would be needed, and over 2,500 new Wherry units were planned to accommodate the increased military population occasioned by NSA's move.⁴³

For civilians, however, it was an entirely different matter. The move to Fort Meade was initially contemplated nervously by a standoffish civilian population. Most lived in Virginia and Washington and faced a long commute over narrow and traffic-clogged roads through the heart of a major metropolitan area. There was no beltway to take traffic around Washington - the trip north would have to be via Georgia Avenue, Colesville Road, New Hampshire Avenue and other city streets. The only plus to this situation was the brand new Baltimore-Washington Parkway, whose projected completion date was January 1955. That would take care of the drive north from Anacostia and would mark a very significant reduction in the driving time.

For those who did not own cars (a significant number in the early 1950s), there was public transportation. Although the old Baltimore, Washington and Annapolis Railroad, which had a spur that ran across the street from the planned NSA facility, had closed its passenger service in 1935, the Baltimore and Ohio Railroad still operated commuter train service from Washington's Union Station to Laurel. For \$1.82 per day, one could travel round trip to Laurel and back in thirty-six minutes aboard one of the two trains operating each morning and afternoon. Once in Laurel, the commuter could take the railroad-operated shuttle bus to Fort Meade for an additional round trip fare of 50¢; it required twenty-three minutes each way.

Unfortunately, the train and bus schedules did not match very well, and there was no bus service at all for a commuter catching the late train. For the early train, the total one-way commuting time from Union Station to NSA was one hour and twenty-three minutes, not including the time required to get from one's residence to Union Station. Both Greyhound and Trailways offered bus service from downtown Washington to Laurel in just thirty-seven minutes, and at 99¢ per round trip, it was a bargain. But neither service brought passengers to Laurel in time to catch the shuttle to Fort Meade, so commuters would be left high and dry in Laurel. For urbanites used to a short commute to Arlington Hall, this was not a happy prospect.⁴⁴

For most, this meant picking up the family and moving to the Maryland suburbs. To help with the move, NSA created the Meademobile, a trailer parked between A and B Buildings at Arlington Hall. The Meademobile carried information about Fort Meade and surroundings, including real estate ads, school and church information, and locations of shopping areas. On Saturdays NSA ran a special bus to Fort Meade so that employees could look over the area. For those who were still unsure, NSA announced that a move to

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Fort Meade would be regarded as a PCS, and the government would pay to move household effects. For many, that was the decider.⁴⁵

The closest community of any size was Laurel. Housing prices in Laurel ranged from \$8,990 for two bedroom homes to \$10,990 for three bedroom homes with basements. There was also a supply of apartments which could be had for rents ranging from \$79.50 to \$112.50 per month. In the other direction was the waterside community of Severna Park, whose houses ranged in price from \$6,000 to \$16,000. Waterfront lots could also be purchased in the subdivision of Ben Oaks, but the lots alone sometimes ran as high as a finished house in other areas. A little farther afield was Glen Burnie, where housing prices ranged from \$5,995 to over \$10,000. South was the planned community of Greenbelt, in the Washington suburbs. This was originally built with government subsidies, and a house there could be had for as low as \$4,700. Single bedroom apartments rented for \$51 and up.⁴⁶ Columbia had not been built yet.



The Meademoible at Arlington Hall Station, 1954

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The Saturday bus to Fort Meade, 20 April 1954

Whatever NSA did to entice civilians out to Fort Meade, it worked. Early estimates of civilian attrition by a panicky personnel office had ranged as high as 30 percent, but the actual attrition rate was less than two percentage points higher than would normally have been expected had there been no move at all.⁴⁸ By anyone's standards (except for the COMSEC population left behind at Nebraska Avenue), the move was a success.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Notes

1. Howe, draft report on the Robertson Committee, in CCH Series VI.X.1.4.
2. Robertson report, in CCH Series VI.X.1.6.
3. Ibid.
4. "Report on Intelligence Activities in the Federal Government, Prepared for the Commission on Organization of the Executive Branch of the Government by the Task Force on Intelligence Activities," [The Clark Committee of the Hoover Commission] App. 1, Part 1: The National Security Agency, May 1955, in CCH Series VI.C.1.8.
5. Ibid.
6. Eisenhower Library papers, available in CCH Series XVI.
7. Hoover Commission.
8. Ibid; Eisenhower Library papers.
9. Hoover Commission; Eisenhower Library papers.
10. Hoover Commission.
11. Ibid.
12. Ibid.

[Redacted]

14. Eisenhower Library papers.
15. Peter Wright (with Paul Greengrass), *Spy Catcher: The Candid Autobiography of a Senior Intelligence Officer* (New York, Viking Penguin, 1987), 98. The details of the Suez crisis are well documented in [Redacted] *The Suez Crisis: A Brief COMINT History*, U.S. Cryptologic History, Special Series, Crisis Collection, V.2 (Ft. Meade: NSA, 1988).

[Redacted]

21. Ibid.
22. T.G. Fraser, *The USA and the Middle East Since World War II* (New York: Simon and Schuster, 1989), 73.
23. Stephen A. Ambrose, *Eisenhower, Volume 2: The President* (New York: Simon and Schuster, 1984), 469-73.

[Redacted]

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

25. Ibid.



27. The McKinsey study and documents pertaining thereto are contained in ACC 26115, CBNE 48 and in the Garman Study. Personnel figures came from ACC 39741, H0-0311-4.

28. CCH Series V.F.5.1.

29. CCH Series V.F.5.1., VI.AA.1.5.

30. CCH Series VI.AA.1.5.

31. CCH Series V.F.5.1.

32. CCH Series V.F.5.1. and VI.AA.1.5.

33. CCH Series VI.AA.1.5.

34. CCH Series V.F.5.1., VI.AA.1.5..

35. CCH Series V.F.5.2.

36. CCH Series V.F.5.1.

37. CCH Series V.F.5.1.

38. CCH Series VI.D.2.5.

39. NSA/CSS Archives ACC 26404, CBOM 16.

40. CCH Series VI.AA.1.1.

41. *Washington Post*, 20 June 1957

42. VI.AA.1.1.; "Study of the Security Division," Feb 1955, in CCH Series VI.G.1.1.

43. Memo, G. B. Erskine to Secretary of Defense, 21 May 1954, in CCH files.

44. CCH Series VI.AA.1.3.

45. CCH Series VI.AA.1.1.

46. CCH Series VI.AA.1.3.

47. CCH Series VI.AA.1.3.

48. CCH Series VI.E.1.4.

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Chapter 7

The Eisenhower Reforms

THE POST-CRISIS CENTRALIZATION OF THE SIGINT SYSTEM

Following the mid-decade crises of Hungary, Suez, and *Sputnik*, President Eisenhower instigated a thorough reexamination of the intelligence system. For NSA, this meant sweeping changes and new challenges.

Criticomm

The long-stalled COMINT Comnet proposal was not jarred loose until the *Sputnik* crisis of 1957. *Sputnik* came as a complete surprise to the Eisenhower administration. Following as it did after Suez, Hungary, and Lebanon, it caused Eisenhower to focus hard on intelligence warning issues. Part of the administration's concern was for timely warning, and that meant timely communications. The Critical Communications Committee (CCC), which had representatives from various governmental organizations (including NSA), proposed communications criteria which clearly would require a totally new system.

The committee defined critical information (they called it "Critic" information, the first time the term came into use) as that information "indicating a situation or pertaining to a situation which affects the security or interests of the United States to such an extent that it may require the immediate attention of the president and other members of the NSC." The CCC then stipulated that such Critic information should get to the president within ten minutes of recognition that it meets Critic criteria.¹

It sounded like pie in the sky. No communications system then in existence could come close to meeting a ten-minute deadline. (Ten hours was more like it.)

When USCIB began looking at various proposals, the system that most closely resembled what the CCC wanted was the COMINT Comnet, which was still a mythic concept. Negotiations between NSA and the services had broken down, and the Air Force had even de-funded a previously agreed-to plan to open the first relay station at Chicksands.² The second Robertson Committee (see p. 259) strongly supported the establishment of the Comnet as a high-priority requirement, but noted that the CCC was already working in that direction anyway.³

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

In July 1958, the JCS approved a plan for a new Criticomm system. It involved establishing a network of automated relays worldwide, building on the rudimentary COMINT circuitry that NSA and the services had put together. The pattern the JCS used was the fledgling COMINT Comnet, and the expertise came from NSA. The new program was promulgated by the DCI as DCID 1/8, "Handling of Critical Communications."⁴

The DCID jumped the gun a little; Eisenhower had not yet been briefed. In August of 1958 General Samford, who had been in the traces for two years, and Louis Tordella, who had been NSA's deputy director for only a few days, were summoned to the White House to brief the NSC on the proposal. Tordella, who did the briefing, sold the program by stressing that at least 90 percent of the expected Critics would come from COMINT and that the COMINT Comnet proposal would enfold fully 200 out of the 245 potential entry points for critical information. The draft directive, NSCID 7, was already written and ready to go. All they needed was Ike's go-ahead. After Tordella had finished talking, the president turned to Donald Quarles, his deputy secretary of defense, and asked, "Don, can we do it?" Quarles said, "Yes, I think we can." "Let's do it," was all the president said, and it was done.⁵



President Eisenhower

His concern about strategic warning led to the creation of Criticomm and the Critic program.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The new NSCID made the secretary of defense the executive agent, and it decreed that the system would consist of the existing COMINT communications system augmented and modified as necessary. The DCI would establish Critic criteria. NSA was not mentioned, but it was hardly necessary. The JCS had already named NSA to manage the system. It was to be completed by 1961.⁶

No one was really sure how NSA would magically produce a system that could meet the ten-minute timeliness goal. COMINT communications at the time were a lash-up of NSA and service communications. Communication centers were basically "torn-tape" relays, and there was no hope of getting anything to the White House in that sort of time frame. NSA had been working on an automated switching device for several years, but had not yet come up with a switch that was acceptable to all parties. In this atmosphere someone would have to improvise.

NSA's communicators, headed by Arthur Enderlin, Max Davidson, and began tinkering with off-the-shelf commercial hardware that would permit a Critic to steam through the system untouched by human hands. A key element in their search was the shunt box, a device invented by Teletype Corporation that could recognize a unique combination of letters (for instance, ZZZ) and open up circuitry all the way to Washington. Nothing else would flow in that path until the "express train" had passed through.⁷

Back in Washington, NSA had created a system of direct communications, called ZICON, with its Washington-level customers. This communications group was expanded to include all organizations on distributions for the initial Critic. This included, in the early days, the White House and members of USIB (less FBI and AEC). Later, SAC (Strategic Air Command), ADC (Air Defense Command), TAC (Tactical Air Command), and STRICOM (Strike Command) were added and still later, the other Unified and Specified Commands.⁸

The advent of the KW-26 cryptoequipment was critical to the functioning of the new system. With it, the system speeded up to 100 words per minute, and messages zipped through at almost twice the previous speed.

Criticomm needed relay centers, and in 1959 NSA directed that the Army operate centers in Europe, Eritrea, the Philippines, Okinawa, and Japan. The Navy would do the job in Hawaii, while the Air Force would take on the same responsibilities in England, Turkey, and Alaska. NSA would operate the central hub at Fort Meade. At the same time the TCOM organization, which had so recently been subordinated to Prod, was once again made independent, in recognition of its new standing.⁹

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Through these and other hasty improvements to the system, NSA was able to report a dramatic improvement in handling time. In the early days of the program, Critics averaged one and one-half hours to reach the White House. Two years later, the time had been reduced to a mean elapsed time of ten minutes. Criticomm was still operated with jury-rigged equipment, but already the timeliness goal of having all Critics to the White House in ten minutes was within sight.¹⁰

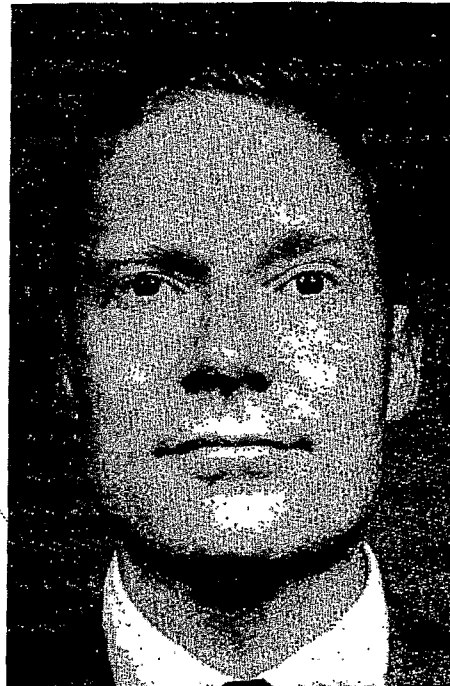
The Baker Panel

In 1957, two high-level committees were taking independent and simultaneous looks at NSA. Both were to have a long-range impact on American cryptology.

The Baker Panel was appointed by President Eisenhower to recommend to him whether or not there was a

[Redacted]

Chaired by William O. Baker, vice-president for research at Bell Laboratories, the committee quickly strayed from its intended charter. Baker wanted to look at everything, and his examination became the most intensive look at the cryptologic process ever performed by an outside organization.¹¹



William O. Baker

When Baker delivered his report to Eisenhower in February 1958, he began by answering the question directly put to him by the president:

No national strategy should be based on the hope or expectation that we will [Redacted]

[Redacted] Even with the greatest optimism, it is clear that no substantial

[Redacted]

(b) (1)
(b) (3) -50 USC 403
(b) (3) -18 USC 798
(b) (3) -P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

[REDACTED]

But this, said Baker, was not the whole story. Cryptology was a tremendously valuable asset to the nation, one which was producing most of the fast and reliable intelligence then available. It was doing it, [REDACTED]

[REDACTED] by putting together all the [REDACTED] disciplines, [REDACTED] The cryptologic system was capable of squeezing out of the ether a veritable cornucopia of information, if it were properly managed and funded. And this, said Baker, was the focus of his recommendations.

In order to properly employ the cryptologic system, NSA needed to focus on the important things. [REDACTED] had monopolized the talents of too many smart people. They should be spread throughout the organization, [REDACTED]

[REDACTED] This meant, in many cases, reallocating resources to ALLO and ACOM or to different divisions [REDACTED] What they had learned working [REDACTED] could now be employed against other [REDACTED]¹³

NSA should forget about developing a general-purpose computer and go for more RAMs. Baker was not impressed with Project LIGHTNING; he wanted smaller but more cost-effective efforts.

The Agency was receiving stupendous volumes of intercepted material, a product of the rapid expansion of overseas collection sites. Computers should be employed in processing this take, so that analysts could be free from manually logging [REDACTED] Machines should also be employed at collection sites to reduce the pile of material that had to be forwarded. This, to Baker, was the next great field of computer applications at NSA.¹⁴

Echoing the recommendations of the Hoover Commission, Baker felt that pure cryptanalytic research should be removed outside NSA, to a Los Alamos-style institute. This would isolate pure research from a production organization and reduce the temptation to employ the best minds in the day-to-day tasks of getting out the news.¹⁵

(b) (1)
 (b) (3)-50 USC 403
 (b) (3)-18 USC 798
 (b) (3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

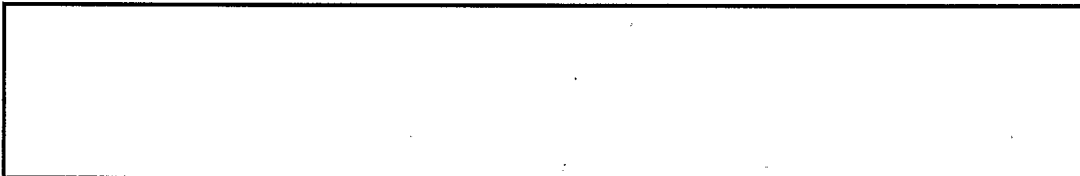
~~TOP SECRET UMBRA~~

As for the cryptologic system in general, it should be further centralized under NSA. Only by centralization could anyone integrate all the pieces of the puzzle and move the organizations involved in the same direction. Baker took dead aim at the AFSS processing center in San Antonio (AFSCC), which he singled out as an unwarranted duplicative processing facility. In fact, the entire collection and processing system should be overhauled under NSA's direction. Some field processing should be transferred to NSA, and the Agency should direct the services to close down redundant collection. NSA should centralize theater processing centers under its own jurisdiction. Better communications and machine processing systems could speed the flow of intercepted materials through those centers, and information would be distributed more quickly to customers. Moneys saved from the rationalization of the entire process could be applied to other parts of the system.¹⁶

Certain specific field operations should be improved under NSA leadership. For instance, analog signals should be converted to digital form for processing; the technology was already available. NSA should develop improved intercept and recording equipment and make them standard throughout the cryptologic system. Punched paper tape, used universally throughout the system, should be phased out in favor of magnetic tape.¹⁷

Finally, the two related disciplines of COMINT and ELINT should be combined under NSA direction. This was the ultimate rationalization of the system and was, according to Baker, long overdue. This generated controversy even at the White House. Deputy Secretary of Defense Donald Quarles said that ELINT had only recently been centralized under the Air Force, and he appealed for time to make it work. But Quarles was losing; it was the clear consensus of the meeting with Eisenhower that ELINT would ultimately be placed under NSA.¹⁸

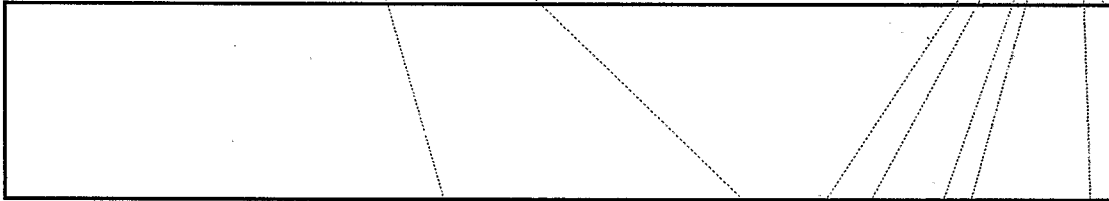
Baker's recommendation regarding a Los Alamos-style research institute met substantial skepticism. Some (like CIA) felt that it wasn't necessary. Edward Lansdale, deputy assistant to the secretary of defense for special operations, pointed out that success on high-level systems often stemmed from working medium-grade codes from the same country. Physically and organizationally separating cryptanalysts working those systems from those working high-grade systems would be technically unsound. Moreover, NSA would likely face severe morale problems if part of its mission were to migrate to a separate research institute led by higher-paid private consultants.



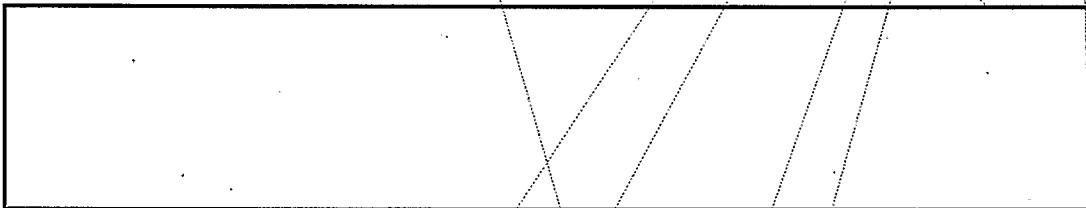
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



But the proposal that generated the most heat (although not the most light) was the ELINT proposal. The Air Force and Navy adamantly opposed it; CIA was standoffish. Even the director of NSA did not want the job unless he got with it a substantial grant of authority. The Navy called the treatment of ELINT "superficial"; the report suffered "from a lack of balance." USCIB was not sure what to do, and it played for time by establishing a task force to study the issue.²⁰



The Reuben Robertson Report

The second look at NSA stemmed from budgetary pressures. Eisenhower had for years been in a running battle with the Democrat-controlled Congress over the defense budget, and in 1957 Secretary of Defense Charles Wilson was looking for excess money anywhere he could find it. It occurred to him that he might find it in NSA's budget, and in January of 1957 he directed Deputy Secretary of Defense Reuben Robertson (a different Robertson than the H. P. Robertson who had chaired a committee in 1953; see p. 227) to establish an ad hoc committee to look at the COMINT and COMSEC budgets. He told Robertson that his objective would be to hold cryptology under [redacted] per year. Robertson chose to chair the committee himself, and on it he placed a number of under secretaries and assistant secretaries. It was very high-powered indeed.²¹

Robertson zeroed in on the [redacted] bottom line but couldn't find it. The cryptologic budgeting process, spread across the Defense Department, was a mess. He finally concluded that what the department really spent on cryptology was closer to [redacted] and he determined to try to hold *that* bottom line. But he found even that goal hard to reach. The reason was that cryptology was having an unexpectedly high payoff. Robertson found that much of what the United States knew [redacted] came from COMINT. He tried to effect economies, but it was unrealistic to attempt any rigid focus on [redacted].²²

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

When the committee first began, it took a very close look at collection. This, it figured, was where most duplication occurred. It recommended that total collection sites be reduced [redacted]. The economies thus effected would result in a net increase in total numbers of positions; the new positions would be financed by the station closures. This would scuttle plans for a continued major expansion of collection resources but would not really diminish the size of the system.²³

What the committee came to understand, in the end, was that apparent duplication of targets and positions was usually not actual duplication. [redacted]

[redacted] Only [redacted] cases were being copied on more than 1 position, and in most cases there was sound rationale for the duplication. What had appeared so simple at Wilson's level did not look at all simple up close.²⁴

Instead, the committee worked on station consolidations. Virtually collocated Army, Navy, and Air Force stations [redacted] should be combined, with AFSS hosting. A similar situation [redacted] should be resolved in the same way, with the Army as host, and [redacted] with the Navy as host. [redacted]

They noted with approval Air Force plans to close [redacted] and centralize the resources [redacted]. They especially liked [redacted] as collection real estate and recommended that the AFSS site at [redacted] be enlarged.²⁵ But most of these consolidations were already in the planning stages - Robertson simply gave them a shove.

The lasting contribution of the Robertson committee was in the budgetary mechanism itself. Robertson was a big advocate of centralization, and he wanted increased NSA control over the process. But he was frustrated by the difficulty of determining what the actual cryptologic dollar figure was. He dealt with cryptologic budgets from all three services, as well as NSA (and to a lesser extent CIA). He believed that this should all be rationalized somehow. So he recommended that all cryptologic budgeting be centralized under DIRNSA. It would be called the Consolidated Cryptologic Program (CCP).²⁶ The recommendation was acted on almost immediately, and fiscal year 1959 was set for the implementation target date.²⁷

The Marriage of ELINT and NSA

When a matter gets to the Oval Office, it can no longer be ignored. The marriage (some say an unhappy marriage) of NSA and ELINT began at last, following the recommendations of Baker to President Eisenhower. This forced a reluctant and disunited USCIB to further consider what it had already considered many times. USCIB appointed

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

a special study group under [] the CIA representative. So as to leave no doubt about which direction the decision was to go, Louis Tordella of NSA was made the deputy chairman.

Overriding strenuous objections by the Air Force, [] opted for a consolidated ELINT system under NSA. His report to USCIB in June of 1958 recommended that the NSC "appoint the secretary of defense as the executive agent of the government for ELINT and assign the Director, National Security Agency, the authority and responsibility for providing an effective, unified organization to control and direct the ELINT intercept, processing, and reporting activities of the United States Government." A new directive, NSCID 6, would replace NSCID 9 and would encompass both COMINT and ELINT.²⁸

NSCID 6 appeared to give NSA the cryptologic authorities it had been asking for. When the secretary of defense published the DoD implementing directives for COMINT and ELINT, however, they came out very differently. The COMINT directive gave DIRNSA operational and technical control of all U.S. COMINT operations except for a very restricted list of SIGINT-related operations not directly related to intelligence gathering (such as search and rescue and various electronic warfare operations). The ELINT directive, however, reserved this right to the secretary of defense himself. Only he had the authority to "determine the ELINT activities which are essential to provide support to commanders who plan and conduct military operations, and which must be directly assigned by the secretary of defense to provide an integral ELINT capability. . . ."

The services interpreted this to mean almost any type of ELINT collection or processing operation. General Samford told his immediate boss, General Erskine, that he assumed that the only ELINT collection that he actually controlled now was that being done by the SCAs. His assumption was correct.²⁹

At first NSA did not know quite how to organize the new mission. The key issue revolved around the competing desires to combine ELINT and COMINT on the one hand and to maintain a separate identity for the new discipline on the other. But ELINT arrived with old baggage - the central processing center, NTPC - and so the forces advocating a separate identity won a partial victory. After some indecision, it was decided to graft it onto an existing organization, and ELINT first landed in the Office of Collection within PROD. The name of the office was changed to COSA (Collection and Signals Analysis). It was a temporary way station on the way to its own home, W Group, established in 1968.³⁰

NTPC thus became the first clearly identifiable ELINT asset at NSA. When NSCID 6 was promulgated, it was decided to transfer the entire resources of the organization - the people, the equipment, the files - to NSA. This amounted to something over [] people, split rather evenly among the 3 services and [] and the equipment for third-echelon processing.³¹

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Along with ELINT came signal search. CIA and NSA had competed for the mission of spectrum search and signal cataloging since 1953, but in the long run the CIA effort was unworkable. The basic CIA SIGINT effort was too small to give it an adequate technical base for the search mission, and, anyway, it was as clearly a cryptologic mission as could well be imagined. NSCID 6 was the last straw, and in the summer of 1959 CIA gave up its effort. COSA, which under its previous incarnations had always had a signal search organization, lost a competitor (without, in this case, picking up assets).³²

Telemetry was another new arrival. Telemetry had always been handled as ELINT. The services, heavily reinforced by private contractors like HRB-Singer, General Electric, Jet Propulsion Laboratories, and Lockheed, all had telemetry collection and analysis efforts. Beyond that, CIA had an effort of its own, emphasizing (as did its ELINT mission) the cutting edge of technology. Third-echelon telemetry analysis had been concentrated at NTPC, but contractors still performed the major share of fine-grain analysis.³³

There was considerable discussion over the nature of telemetry. Was it really COMINT, as NSA contended, or really ELINT? Melville Boucher, an NSA telemetry analyst, once said that "telemetry has always been a gray area surrounded by fuzz seen through a thick mist." The answer would determine how telemetry reports would be handled - spread far and wide as straight-secret ELINT reports or bottled up by COMINT codewords. In the summer of 1959, coincident with the transfer of ELINT assets to NSA, the ELINT committee of USIB (renamed from USCIB by the publication of NSCID 6) decided, rather predictably, that telemetry was really ELINT and that it would go forth without hampering codewords. But that did not change its resubordination. The telemetry mission migrated to NSA where it eventually became TELINT and later FISINT.³⁴

Since NSA had no telemetry analysts, it would need help. ASA came first, agreeing to transfer its telemetry assets, including its contracts with JPL and HRB-Singer, to NSA. NSA established its first telemetry analysis effort under Joseph Burke, who became known as the father of NSA telemetry.

The transition from Air Force to NSA telemetry was more difficult. The Air Force retained a residual telemetry effort and resisted turning over its telemetry mission to NSA for months. In the end they did so only through the considerable persuasive powers of General Samford.³⁵

Once NSA took over telemetry, it found out just how chaotic the situation was. Each organization involved had its own equipment and used its own set of collection and processing standards. Telemetry tapes arrived at NSA in a hodgepodge of formats, and at first it was difficult to simply collect information on the formats involved.³⁶ To bring order

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

to the chaos, Louis Tordella, in the spring of 1960, created [REDACTED]

[REDACTED] it became a clearinghouse for technical information, and it marked NSA's first big initiative in consolidating the effort.³⁷

NSCID 6 did not solve the problems that had plagued ELINT. Within two years, the President's Foreign Intelligence Advisory Board (PFIAB) was already complaining that NSA had been given too meagre a grant of power.³⁸ It did eventually result in standardized technical rules and procedures, and in that sense the ELINT experiment of 1958 became a success. In the area of command and control, however, it was a dismal failure.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

The Kirkpatrick Committee

The tireless process of reviewing intelligence functions continued to the end of the Eisenhower administration. The last player in the game was the Kirkpatrick Committee. Chaired by Lyman Kirkpatrick of CIA, its purpose was to assess all defense intelligence programs, including SIGINT (a term that came into the language after NSCID 6 was inked).

Kirkpatrick, like the CIA whence he came, was distressed at the uncoordinated and duplicative nature of defense intelligence. Centralization was the only way to rationalize the system, and in SIGINT that meant more power to NSA. ELINT was out of control (an old refrain), and the decentralizing tendencies of the Unified and Specified Commands had to thwarted. Moreover, COMINT and ELINT had not been fused, as Baker had envisioned. This was due in some degree to classification differences and the tendency of COMINT people to shield their information from many of the people who really needed it.³⁹



Lyman Kirkpatrick

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Two of Kirkpatrick's recommendations would have a long-range impact on intelligence. First, he recommended that an "intelligence community staff" be established, responsive to the DCI. Second, and much more specifically germane to the SIGINT world, he called for a broader use of COMINT. The committee viewed the SSO system as having devolved into an obstructionist group that held information too closely and kept key players out of the inner circle. According to Kirkpatrick, the SSO system should "be staffed by personnel of rank commensurate with a courier function" and "avoid placing their own interpretation on material transmitted by the Special Security Officer System."

If true, the charges indicted a system which had been quite dynamic during World War II. The Kirkpatrick report marked the beginning of the end of that era of dynamism. He offered no prescription for the problem of interpreting SIGINT.⁴⁰ But the very next year NSA came up with the solution with the creation of a fledgling Cryptologic Support Group (CSG) system.

NSA Centralizes the Field System

Cryptologic centralization was having a profound effect on the field system. Some of this proceeded from the new authorities that NSA was gaining and from the new responsibilities that it was undertaking.

Much of it, however, emanated from a different source. In 1958 Eisenhower had succeeded in getting a sweeping Defense Reorganization Act through Congress. It took the JCS out of the direct chain of command and made them advisors and planners. Within the command structure, it created the Unified and Specified Commands. This marked a sea change in the way America did its fighting. Henceforth, wars would always be fought with combined commands, with component service forces integrated under a single military boss, the commander of the relevant unified command.⁴¹

Overseas, this reorganization demanded major changes in the way cryptology was organized. Now it was more important to render cryptologic support to the unified commander. The SCA theater headquarters, representing as they did only the cryptologic assets of a single service, were incapable of doing it. Only the NSA field organization could.

The first theater to change was Europe. NSAEUR, which had been established in Frankfurt, had exercised only a technical support role within the cryptologic community. But as early as 1955, an experienced NSAEUR analyst was sent to join the CINCEUR staff at Camp des Loges, outside Paris.

42

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

In that year, NSAEUR, over the strenuous objections of ASAEUR, gave its small staff at Camp des Loges augmented authority to represent the cryptologic community to CINCEUR. The new functions involved theater-wide planning and representation, and they marked the first time that the field offices had strayed far beyond technical functions. NSAEUR continued to augment the staff in Paris and in 1963 moved its office there, leaving behind in Frankfurt the technical support staff to deal with internal cryptologic issues. Included in the 1963 move was a new organization, NSA Europe Intelligence Support Section (NSAEUR/ISS), an element that had been set up to interpret SIGINT product. It was the first Cryptologic Support Group (CSG).⁴³

AFSS and the Development of Second-Echelon Reporting

A parallel development produced profound changes in theater reporting. Ultimately, it was to lead to the revolution in SIGINT reporting which resulted in the creation of the National SIGINT Operations Center (NSOC). It started with the [REDACTED]

AFSS understood at its birth that airplanes move faster than almost anything and that to conduct a COMINT support function for the Air Force, it would have to create an extremely rapid reporting system. At first this led to negotiations with Canine over field site reporting authorities. But AFSS had bigger plans. Keeping track [REDACTED] would involve networking all its theater collection sites, and this would require the creation of a theater-level center. [REDACTED] The plans for this were on the drawing board even before the demise of AFSA.⁴⁴

NSA and AFSS went back and forth during the early 1950s over what organization should handle this responsibility and where it should be located. By 1955, however, they had resolved their differences. [REDACTED]

The [REDACTED] as it was called, would have considerable power. It would "direct the intercept and analysis of foreign communications" and would "exercise routine operational control . . . of all COMINT, ELINT, and [REDACTED] matters. . . ." It would collect traffic forwarded from field sites under its control and would forward raw and semiprocessed traffic back to the States. It also had its own independent reporting authority.⁴⁶

(b) (1)
 (b) (3)-P.L. 86-36
 (b) (3)-50 USC 403
 (b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

This was not unique. ASAEUR exercised similar responsibilities at its processing center in [redacted] differed by the way that it evolved. A key figure in the evolution of [redacted] was a young Air Force captain named Benjamin Ardisana.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36



Benjamin Ardisana shown as a lieutenant, with his wife Betty, in the early 1950s

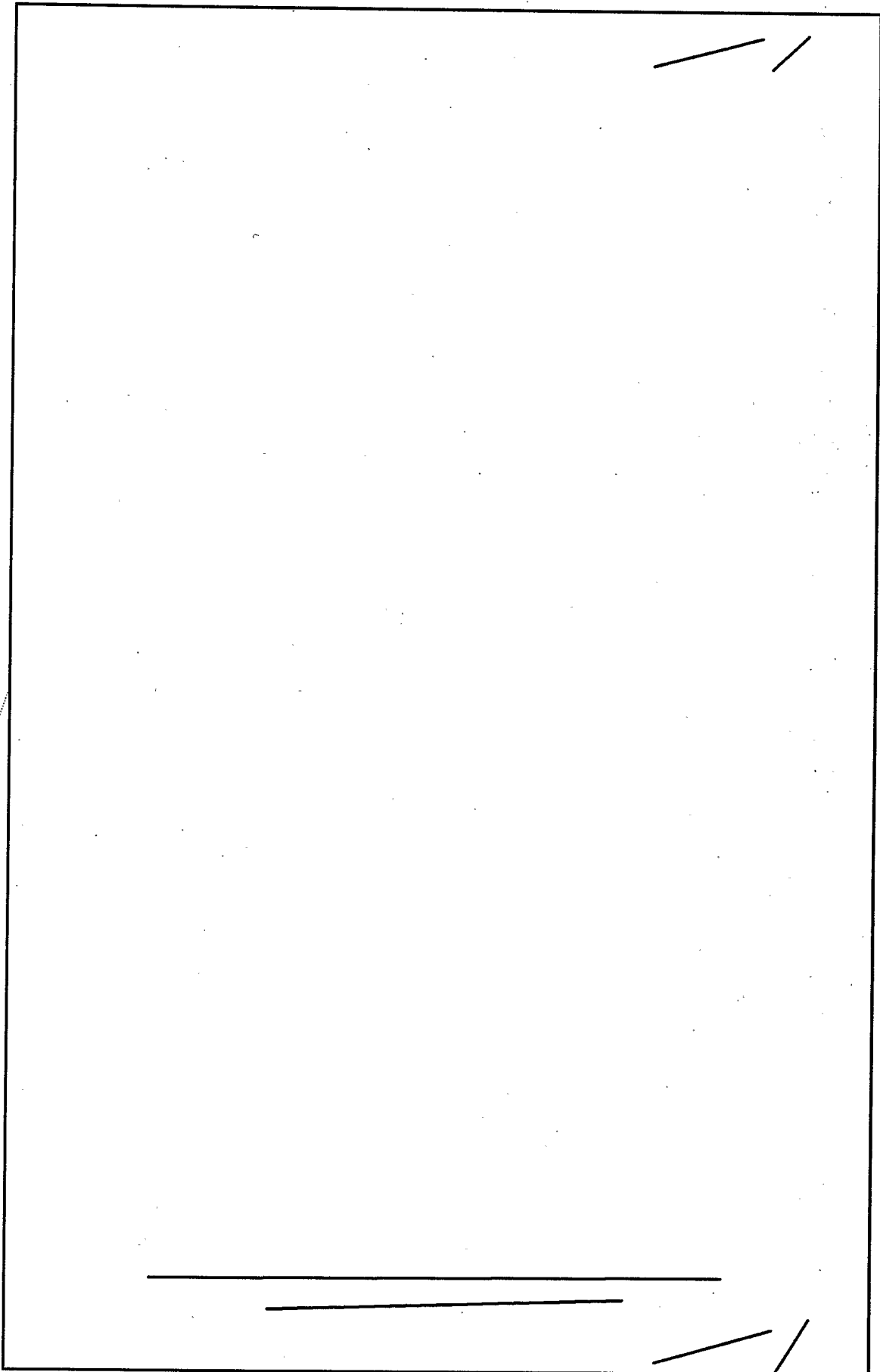
Ardisana had begun his service career in the Army Signal Corps during World War II. He had entered the cryptologic business in 1952, and after a series of assignments with AFSS units in the Far East, where he had shown an exceptional talent for innovation and initiative, he arrived in [redacted] in July 1958.⁴⁷

Less than a year later (May 1959), Ardisana set up the first European field Opscomm circuit, between [redacted] to coordinate the [redacted] between the two organizations. (Some claim that this was the first Opscomm in the community; the strength of that claim rests on the date that SMAC first set one up, a date which is less well documented.) At the same time, Ardisana established an around-the-clock surveillance and warning center to watch the [redacted] as it was being reported from subordinate sites.⁴⁸

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~



(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~TOP SECRET UMBRA~~

All this emanated from four massive stone buildings left over from World War II. The reporting operation was on the fourth floor of one of them, under the very eaves of the building, in a room filled with up to twenty-six Opscomm machines (Teletype Mod 19s and 28s) all clattering away together.

51

The Struggle for Control in the Pacific

The Pacific theater was very different from Europe, and it developed in a very different way. Unimaginably huge and far-flung, it was made to order for fragmentation. In World War II it suffered from two different and competing commands employing different lines of attack - MacArthur in the southwest and Nimitz in Hawaii. Supporting each was a separate and unique cryptologic system. When, in 1945, the two commanders went into garrison, their cryptologic organizations followed them.

In Japan, MacArthur's cryptologists centered on Tokyo. NSA Far East (NSAFE), the cryptologic flagship in the Pacific, eventually came to be located on Pershing Heights in downtown Tokyo. ASAPAC and 6920th SG, the ASA and AFSS senior representatives in theater, were also posted to the Tokyo environs. Among them they controlled most of the Army and Air Force cryptologic assets in the theater.

Supporting Nimitz was NSAPAC. But the offices in Hawaii were just that - offices without dynamic functions. NSAFE had garnered all NSA's technical expertise in the theater. This was an accident of history, which resulted from the collapse of the Civop program in the mid-1950s. The program had been roundly disliked by the SCAs, but it did provide highly skilled civilian talent that they found most useful. Thus an organization which became known as PACEXFAC (Pacific Experimental Facility) developed as part of the NSAFE staff in Tokyo, and it absorbed most of the billets. Like NSAEUR Office Germany in Frankfurt, PACEXFAC was the cryptologic troubleshooter for the Pacific. It reinforced the real utility of the Tokyo office.⁵²

In 1957, Samford decided to rename the offices, but he kept the pecking order the same. NSAFE was renamed NSAPAC, but the office in Hawaii was called NSAPAC (Rear), as if it were a skiff being towed by a battleship. It was a name that grated.⁵³

This was how NSA was organized in the Pacific when the Unified and Specified Commands were created in 1958. Under the new scheme, CINCPAC in Hawaii was clearly the senior commander in the theater. When Samford's immediate superior, General Erskine, came through on a trip the following year, however, he was surprised to see that NSA had not changed to conform to the realities of the new military command structure. NSAPAC (Rear) was still in Hawaii, and its chief was the deputy to NSAPAC

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

in Tokyo. He returned to Washington complaining that NSA had it all wrong in the Pacific.⁵⁴

This unusual organizational scheme bumped along until a new director, Admiral Frost, toured the Pacific in the spring of 1962. Frost talked it over with the current CINCPAC, Admiral Harry Felt. When he returned to NSA, he decreed that NSAPAC would henceforth be located in Hawaii to support CINCPAC [redacted]

Samford Joins the Agency

The Canine era came to an end on 23 November 1956. His replacement was Lieutenant General John A. "Sammy" Samford. As mellow as Canine was forthright, Samford came to NSA to smooth ruffled feathers and give the Agency some room to breathe. Canine's five years (including one year as director of AFSA) had been a hectic time.

Samford was actually better prepared for the job than Canine had been. He came to NSA from the Pentagon, where he had been chief of Air Force intelligence, and served a grooming period of six months as Canine's vice-director. When he became DIRNSA, he already knew the players.



John Samford, second director of NSA

His style was fluid - Samford was as smooth as silk. A CIA official described him as "more of a pedant than a pilot, more of a philosopher than a fighter, . . . a man who understood and loved the SIGINT business."⁵⁵ He set out to calm the waters between CIA and NSA, and when he left the job in 1960, the two organizations were back on speaking terms. His relations with USAFSS, contentious under Canine, settled back down. Samford had developed a close personal relationship with Gordon Blake, who became commander of USAFSS in 1957, based on old-school ties established when they had both

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

been cadets at West Point. They both knew that the independence of AFSCC would have to end, but with as little bloodshed as possible.

In order to enshrine the new era of good feelings, Samford initiated a novel experiment in 1958, in which the chief of the Soviet Navy shop (GENS-2), a Navy captain, would actually work for the director of naval security, while continuing to respond to DIRNSA on operational matters. The next year he extended this unique arrangement to the Air Force and Army, resubordinating the chiefs of GENS-1 and GENS-3 to their parent SCA commanders. The idea was to give each SCA a stake in NSA, but it did not last long. Seeing that it had failed to sublimate service factionalism (and even in some cases making it worse), Frost scuttled the system in 1962.⁵⁷

Samford also moved quickly to resolve a long-standing dispute between Canine and Deputy Secretary of Defense Reuben Robertson. The 1956 McKinsey Study recommended that NSA be run more on private business principles. To instill a sense of corporate management, the director should appoint a civilian deputy from the business community. But Canine, having called in the McKinsey group, rejected the recommendation. Instead, he continued with his system of elevating one of his service deputies to a position called the vice-directorship, and he continued to act as his own de facto deputy. The dispute between Canine, who opted strongly for military management, and Robertson, who demanded a business approach, grew acrimonious and soured Canine's last months in office.

Samford found, on being elevated to the directorship, that Robertson already had someone in mind. That someone was Joseph H. Ream, a top CBS executive. So, only some two months into office, Samford named Ream to the new job of deputy director, just to give the idea a whirl.

It soon whirled into oblivion. Ream had no SIGINT background, and the learning curve was too steep. He had serious family problems that required extended trips to Florida and that cut into his learning time. His lack of technical qualifications for the job simply could not overcome his well-documented managerial skills. Further, he found it hard to deal with an entrenched bureaucracy that viewed him as an outsider. Ream quit in frustration only six months into the job. It was the last time anyone successfully imposed a nongovernment outsider on NSA's top-level management structure.⁵⁸

In his place, Samford hired Howard Engstrom. Engstrom's impact on cryptology had already been considerable. He was brought into the Navy from the Yale math department during World War II. He quickly became influential in the development of computers for cryptologic work, and when the war ended, he left the Navy to form Electronic Research Associates (ERA), where he was the guiding genius in the effort to develop computers for NSG, AFSA, and later NSA. In the mid-50s he left Remington Rand (which had swallowed ERA), where he was a vice-president, to join NSA's R&D organization. When he arrived at NSA, Samford elevated Engstrom to the position of associate director, which gave him and his R&D organization special status and was designed to answer DoD-level

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

concerns that NSA was not doing enough in research and development. When Ream quit, Samford moved Engstrom to the post. But he remained only a year, and in August of 1958 NSA experienced yet another change in the revolving door position of deputy director.⁵⁹

The Tordella Era Begins

In late July of 1958, Samford summoned Louis Tordella, NSA's influential representative at Office of Special Operations (OSO), to his office to talk. Tordella remembers a short chat about inconsequential matters, following which Samford asked Tordella what a deputy director should be. Tordella told the director that the deputy should be his "alter ego." That sounded good to Samford, and he offered Tordella the job on the spot. It was the last time any director would have to do that for sixteen years. The revolving door shut with a bang behind the lanky form of Louis Tordella.⁶⁰



Louis Tordella changed the deputy directorship from an office to an institution.

Like Engstrom, Tordella had been plucked from a college math department for Navy service in World War II. Originally a Hoosier, he had gone to school in Illinois. OP-20-G's Laurance Safford found him on the campus of Chicago's Loyola University through his unique program of recruiting academics with an expressed interest in cryptology. And also like Engstrom, he was, in 1958, already a cryptologic legend. Tordella had pioneered in so many areas of Navy cryptology that he was close to being a universal man, like the Army's Frank Rowlett. He joined NSA when it opened its doors and served in numerous key positions which permitted him to push his favorite projects, especially the application of computers to cryptanalysis. Tordella had been NSA's representative on numerous high-level committees. This, and his tour in the Pentagon, had given him the opportunity to get acquainted with just about everyone who counted, and when Samford proposed his name to Deputy Secretary of Defense Donald Quarles (who had replaced Reuben Robertson) in 1958, he got no opposition.⁶¹

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Tordella did indeed become the director's alter ego. Staying through the tenure of seven directors, he was the details man, the continuity. To many inside and outside the Agency, Louis Tordella was NSA.

Public Law 86-36

In 1959 Congress passed Public Law (PL) 86-36, which contained provisions permitting NSA to separate its personnel system from the regular Civil Service system, a permission which CIA had had since its inception. The problem that NSA had faced was that it had never been created by statute (only by executive order, the now-famous Truman Memorandum). There was thus no law which could keep NSA's personnel system apart from that of the rest of the federal government. Civil Service regulations straight-jacketed NSA procedures, and classification hampered NSA adherence to procedures which were intended for a completely open system. To eliminate the dilemma, PL 86-36 exempted NSA from the laws relating to the classification and grading of civilian positions from disclosing any information regarding the number of employees, the names, titles, or job descriptions. Public Law 86-36 was to have a major impact on NSA policies in both the personnel and security areas.⁶²

NSA AND THE AMERICAN PUBLIC - THE ISSUE OF LEGALITY

No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. . . .

Federal Communications Act of 1934

Cryptologic activities, which in the United States began during the early years of World War I, occupied an uncertain place in government. Early American cryptologists worked without the knowledge of the American public. They even worked without knowing if what they were doing was legal or not. It was an odd and unsettling position to be in.

Early statutes affecting cryptology were devised by Congress to protect radio, a new invention which required protection. Thus it was that a series of acts, beginning with one in 1912, was passed to protect information in radio messages from being passed to a third party to be used for commercial gain. This appeared to have a benign effect on cryptologic activities in the Army and Navy until 1927, when a revised statute stated that "no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purport, effect, or meaning of such intercepted message to any person. . . ." The aim of the legislation was the same as that of earlier statutes - to protect the information "unless legally required to do so by a court of competent jurisdiction or other

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

competent authority. . . ." Other competent authority could be the president or someone in the Army or Navy chain of command. But as the word "intercept" had crept into the statute, for the cryptologists who secretly plied their trade, this was unnerving news. It implied that what they were doing might be illegal. Further, it had the effect of shutting off liaison with the telegraph cable companies, who had in the early years supplied most of the material that the Army worked on. (But by the late 1920s the Army, like the Navy before it, was beginning to set up its own intercept stations.)⁶³

Meanwhile, the American public was blissfully unaware of any cryptologic activity at all - unaware, that is, until the publication of Yardley's *The American Black Chamber* in 1931. Worse, Yardley was hard at work on a sequel, to be called "Japanese Diplomatic Secrets." It was never published - it became, in fact, the first publication ever suppressed in the United States on the grounds of national security. To prevent any other revelations, Congress in 1933 hurried through a bill that prohibited all government employees from revealing their knowledge of American codes "or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States." The penalty would be a \$10,000 fine or ten years imprisonment, considered to be a heavy enough hammer in those days. This appeared to be a backhanded way of authorizing other black chambers. If such activity were illegal, then why protect its activities from disclosure?⁶⁴

This step forward was followed immediately by disappointment. When the Federal Communications Act was passed the following year, it contained the same clause regarding "intercept." There was a good deal of discussion about this within SIS and OP-20-G. Legal minds pointed out that the statute prohibited intercept "and divulging" of such communications. If it had said "or divulging," it would clearly have singled out the process of intercept as illegal. But the intercept activity would not be illegal unless it were accompanied by "divulging," which, once again, referred to use of the information for commercial gain. And the so-called Yardley Act the year before seemed to imply legality. But there was a lingering suspicion that they might someday be prosecuted for what they were doing on the basis of Section 605 of the Federal Communications Act of 1934. The penalties were exactly the same as they were under the Yardley Act.⁶⁵

Following the 1945 Pearl Harbor hearings, which amounted to the second public revelation of cryptologic activities, there were loud demands for legislation protecting this vital activity. Within the Army and Navy themselves, lawyers drafted protective statutes, and the Truman administration moved toward the introduction of legislation. Finally, in 1949 a draft was ready, and it was steered through the Senate by Lyndon Baines Johnson, a young senator from Texas. In 1950 the bill became law: Title 18, U.S.C. 793.⁶⁶

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The United States already had legislation. But the Espionage Act of 1917 required proof that the person revealing the secret information intended to injure the United States. The courts had required a high standard of proof, including the direct involvement of agents of a wartime enemy, in order to secure a conviction. What if no enemy agents were involved? Or what if the agents were from a "friendly" country? Or what if the person simply gave the information to a reporter who published it?

Title 18 took care of all that. It made it a crime to divulge information relating to various aspects of cryptologic activities to an unauthorized person "or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government. . . ." It cast a very broad net, was almost totally inclusive, and was legally enforceable even in the absence of intent to injure. It could thus deter, or be used against, well-meaning but misguided idealists.⁶⁷

Just as important, it implicitly authorized COMINT activities by acknowledging that they were going on and by protecting their secrecy by law. Here was an implicit voiding of Section 605 of the Federal Communications Act of 1934 and earlier statutes as they related to cryptology.

This was followed two years later by the Truman Memorandum creating NSA and describing its responsibilities. Here was the "lawful authority," even though classified, so needed in the years prior to the war. As the years rolled on and Congress appropriated money for NSA's activities, the legal status of the business became less and less debatable. The 1959 anonymity statute (Public Law 86-36) for the first time named NSA in legislation. Finally, in 1968 the Omnibus Crime Control and Safe Streets Act specifically overruled Section 605 of the Federal Communications Act of 1934. Cryptology had made the journey from a secret black chamber to an officially authorized and avowed government activity.⁶⁸

PUBLIC REVELATIONS AND CRYPTOLOGIC SECRECY

[[It is] of the essence of a secret service that it must be secret, and if you once began disclosure, it is perfectly obvious that there is no longer any secret service and that you must do without it.

Austen Chamberlain, British foreign secretary in the 1920s

Following Yardley, COMINT went underground. The Black Chamber had already been destroyed by Secretary of War Stimson in 1929 (through the device of pulling State Department funding). Its successor, Friedman's SIS, was so small (he started with a staff of six) as to be effectively invisible. The Navy had an effort of comparable size, and the entire enterprise proceeded reasonably secure from the eyes of the public.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Beginning in 1939, a series of magazine and newspaper articles trumpeted the success of the federal government in breaking up German espionage rings. Some of the articles referenced German codes and discussed U.S. intercept activities. SIS and OP-20-G officials were livid – someone was calling attention to COMINT activities in such a way that the Germans could be alerted and might take countermeasures.

The “someone” turned out to be the Federal Communications Commission (FCC). FCC revelations to the press, designed to boost its stock with the public, were at least partly responsible for the War Department’s securing Roosevelt’s order in 1942 directing that such activities be discontinued in all but the Army, Navy, and FBI. Despite the order, the FCC continued its radio monitoring and codebreaking activities throughout the war and even accompanied this with leaks to the press boasting of its COMINT effectiveness.⁶⁹

Potentially more damaging was an article in the *Chicago Tribune* immediately after the Battle of Midway alleging that the U.S. had had advance knowledge of Japanese plans. The article was bylined by Stanley Johnston, a reporter who had been with the Pacific Fleet during the battle of Coral Sea. The next month columnist and broadcaster Walter Winchell stated that this knowledge had come from the breaking of Japanese naval codes. The Navy demanded that Johnson be indicted, and the case went to a federal grand jury in Chicago in August. No indictment resulted, a blessing for an over-eager Navy legal department that would have had to reveal far more damaging information in court to secure a conviction. The glare of national publicity was mercifully diverted, but in August, far ahead of schedule, the Japanese Navy changed all its codes. (There was never any direct evidence, however, that the Japanese read the *Tribune* or changed their codes in response.)⁷⁰

Classifying Cryptologic Information

Service cryptologists were almost instinctively aware of the extreme sensitivity of their work. They began in such small organizations, though, that the process itself was easy to protect. Once they developed information that needed to go to someone, they generally distributed it on a by-name basis to those few Army, Navy, and State Department people who had an absolute need to know. Information was often taken in locked containers, and a courier stood by while the official involved read and initialed the paper.

As for a formal classification, they had to use what was available. Existing service regulations at the beginning of World War II contained only two classifications: Secret and Confidential. Another quasi-classification, called Restricted (an earlier version of For

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Official Use Only, or FOUO), was reserved primarily for information relating to military hardware.⁷¹

Their British allies had three classifications. Above Secret they added the term Most Secret. In 1944 the Army adopted the British three-tiered system, but called the highest category "Top" Secret. COMINT, being among the most sensitive items on the menu, was classified Top Secret.⁷²

When the Army obtained an agreement with GCCS in 1943, the Americans had to agree to attach a security caveat associated with COMINT. The most sensitive information (which at the time included ENIGMA and MAGIC decrypts) was now handled under a special codeword called ULTRA. Information derived from traffic analysis, DF, and plain text received codeword protection, but different codewords were used to denote lesser sensitivity - THUMB and PEARL were two which appeared during World War II. After the war the system devolved into two codeword categories: Top Secret Codeword, and everything else. That which related to COMINT but was not derived directly from communications intercepts began to receive the stamp Handle Via COMINT Channels Only (HVCCO).

Within cryptology, there were certain projects that received much more limited distributions. BOURBON, the early Soviet problem, was a good example, and VENONA got even more limited handling still. This system of ad hoc compartmentations continued into the early 1960s, when it was augmented by a more formal compartmentation system which was applied to SIGINT product reports. The most sensitive category was Gamma, A lesser category, called Delta, was often used to protect

Despite the strict secrecy applied to the trade, the number of people indoctrinated for COMINT rose steadily as its utility came to be recognized. By 1955 the number of COMINT clearances within the federal government (and to contractors) had grown to over 31,000, and the Hoover Commission expressed concern about the spread of highly sensitive information to such a large group. Of these This was a far cry from the six people that Friedman hired to carry on the Army's COMINT business in 1929 or the two people (Laurance Safford and Agnes Driscoll) who began Navy COMINT in the 1920s.⁷³

Pulling on the other end of the rope were the people who advocated an even broader dissemination of COMINT. In 1960 Lyman Kirkpatrick (who headed the Kirkpatrick Committee - see p. 263) took the Defense Department to task for over-strict rules regarding intelligence. (And by intelligence, he was clearly referring to COMINT.) Kirkpatrick wrote:

(b) (1)
(b) (3) - P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Entirely apart from the well-known tendency throughout the intelligence community to over-classify, the special handling required for a very significant portion of intelligence information has at times deprived key personnel of information vital to the successful discharge of their responsibilities.⁷⁴

The tug of war between the advocates of secrecy and dissemination was never-ending. Nor could the conflict be resolved. As SIGINT became more successful, it became an inevitable victim of its own success. Utility meant dissemination, and dissemination meant risk.

BREACHES IN THE DIKE - THE SECURITY CASES

The first significant breaches of the security system came from within rather than from without. The first two were quiet, and while they both involved significant compromise, their very obscurity minimized the damage. Neither became a cause célèbre, although one of them became public. The third, however, did major damage primarily because it became a public case.

L' Affaire Weisband

The first case did the most real damage. But it was so successfully hushed that only a few insiders knew that it had occurred. It involved an AFSA analyst named William Weisband.

Weisband was an immigrant. Born in Alexandria, Egypt, in 1908, he had entered the United States in either 1925 or 1929. (The record on this point is obscure.) He became a citizen in 1938 and, while living in New York City, was inducted into the Army. Weisband went into the Signal Corps, and he first began working with ASA in 1943, where he became a favorite of Colonel Harold Hayes (who headed the Army's cryptologic activities in the Mediterranean). As an accomplished linguist, he was an ASA natural and received a transfer from North Africa to Arlington Hall in 1944. The end of the war found him still working there, and he hired on as a civilian. ASA needed all the help it could get in 1945, and getting a linguist like Weisband was a good day's work.⁷⁵

Unfortunately for ASA, Weisband was a Communist and suspected of being a spy. He had handled other agents passing defense information to the Soviets even before he entered the Army. He apparently gave up handling agents once he entered the service, but after he arrived at Arlington Hall he probably resumed his old avocation.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

At the Hall he had a reputation as a stroller. He wandered around, chatting and picking up bits of gossip. He was also adept at getting himself on distribution for documents that did not directly concern the work of his section. Highly gregarious, Weisband had a wide circle of friends, and he entertained some of the top officers and civilians in ASA. His postwar wedding party was talked about as a who's who of Army cryptology.⁷⁶

Although Weisband had been on an FBI list of suspected Communists since 1948, he was first tagged as a possible spy through the VENONA project. In 1949 a Soviet agent identified in VENONA traffic led the FBI to another agent, who led them to another, who finally implicated Weisband as a "handler." The FBI began piecing together information on this new identity and was aghast to learn in 1950 that Weisband was employed at Arlington Hall, the very place whence the VENONA decrypts were coming. In April 1950 Wesley Reynolds of the FBI went to Carter Clarke, commanding general of ASA, to report the news. Clarke told Reynolds that Weisband had transferred to AFSA. They went to Admiral Stone.

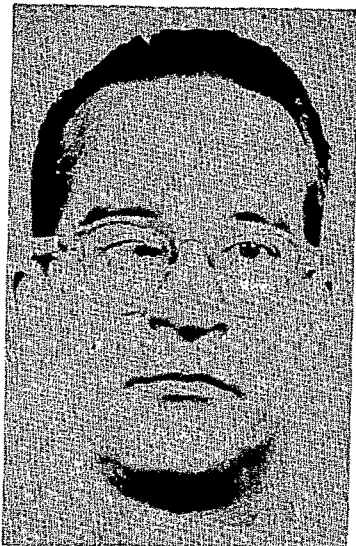
At the time, Weisband was working as a section chief on the Soviet problem. Co-workers had already reported him as a possible security risk, and he had been removed from access to some of the more sensitive projects while security looked into it. He was immediately suspended and interrogated. He denied everything. But the walls were falling in on him even as he spoke. In August, as the subject of an unrelated investigation, he appeared before a federal grand jury in Los Angeles investigating West Coast Communism. Ordered to return for further testimony, he did not comply, was arrested and was convicted of contempt, for which he served a year in a federal prison.

He never returned to AFSA, and in 1951 he was mustered out of federal employment by a loyalty-security board in San Francisco, which, not surprisingly, found that removal from federal employment was in the best interest of national security.⁷⁷ He remained in the Washington area, working as a car dealer and apartment manager, and died in 1967 in Fairfax. He never admitted anything.

The FBI never found out what, if anything, Weisband passed to the Soviets. But his close involvement with the Soviet problem argued suggested some of the tightening up of Soviet communications was a result of Weisband's activities. Many AFSA employees believed, rightly or wrongly, that he was single-handedly responsible for "Black Friday." His case instilled a certain paranoia within the profession, and accounted to some degree for NSA's extremely close guarding of COMINT.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~**The Petersen Case**

Joseph Sydney Petersen, Jr.

The second security breach involved an NSA analyst named Joseph Sydney Petersen, Jr. Petersen had served with ASA in the South Pacific in World War II and had formed a close liaison with Dutch cryptologists with whom the United States was exchanging information. After the war this liaison came to an end, but Petersen decided on his own to become a one-man Third Party office to the Dutch intelligence service. He collected documents at his home and periodically passed them on to Dutch intelligence people from the embassy. This apparently went on for several years.

(b) (6)

Petersen's espionage might never have come to light had it not been for an unrelated naval security case involving an officer who had been separated from the service for [redacted]. He implicated Petersen as a [redacted] and an investigation was launched. But when NSA learned that Petersen had close friends at the Dutch embassy, the investigators forgot about the [redacted] charge and called in the FBI. In September 1953 the FBI began questioning Petersen, and he began revealing his story. A search of his apartment uncovered a large number of classified documents, and the FBI reckoned that it had enough to prosecute.⁷⁸

The joint NSA-FBI team consulted with Canine in his quarters. The options were to try to prosecute or to be satisfied with a simple resignation on his part. This would be the first prosecution under Title 18, and a hearing in open court might bring to light information that would be more damaging than just giving Petersen his walking papers. But Canine decided to go for prosecution, and he later overrode objections by USCIB that the resulting publicity would seriously damage NSA.

When Petersen's lawyer found out that the government had opted for prosecution, he began negotiating a plea bargain. On the day the trial was to begin, he told the judge that Petersen was pleading guilty to a violation of Title 18. Petersen fully cooperated with the FBI and in return was sentenced to seven years in prison. He was paroled after four years.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The Petersen case was similar to that of a much more notorious case years later, the espionage of Jonathan Jay Pollard. He passed cryptologic documents to an ally who he felt had been left in the lurch. Along with technical information regarding the establishment of cryptanalysis courses, Petersen also informed the Dutch [redacted]

[redacted] When the FBI searched his house, they found cryptologic documents dealing with several COMINT targets, among them Korea and Communist China. The NSA damage assessment found that the number of documents passed to the Dutch was "very large."⁷⁹

When Petersen was indicted, the Associated Press ran a dispatch which was printed in many newspapers across the country. It was the first time the new agency had ever fallen under the klieglights. The dispatch described NSA as "essentially a radio monitoring service. It has a network of radio receiving stations and other equipment, some of which are based overseas. It listens in on the world's radio traffic, both conventional messages and coded material . . . secrecy even tighter than that shrouding the Central Intelligence Agency surrounds the National Security Agency. It is not listed by name either in the Washington directory or in the Pentagon phone directory."⁸⁰

A number of other details about NSA appeared to bring about a focus on the Agency's anonymity. NSA's obscurity had been so perfect that Richard Russell, the chairman of the Senate Armed Services Committee, once asked, "What does the NSA do?"⁸¹ The job description appearing in the *U.S. Government Organization Manual* was a marvel of obfuscation: "The National Security Agency performs highly specialized technical and coordinating functions related to the national security." The Petersen case was the first to pry open the lid of anonymity.

Martin and Mitchell

On 1 August 1960, a small story appeared in the local Washington newspapers. Two Department of Defense employees of the National Security Agency had failed to return from vacation and were still missing.

The story did not stay small very long. NSA's reputation for secrecy guaranteed that any news would be big news, and by the next day it was on the front page. On 5 August the Department of Defense issued a brief statement that it was now known that the two employees, Bernon F. Mitchell and William Martin, had flown to Mexico City and thence to Cuba. It was assumed that they were behind the Iron Curtain.⁸²

(b) (1)
 (b) (3)-P.L. 86-36
 (b) (3)-50 USC 403
 (b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Martin and Mitchell during their press conference in Moscow
(from the *New York Mirror*)

But the most shattering blow came on 7 September. Listeners to Radio Moscow tuned in on one of the most remarkable press conferences of the century. Now in Moscow, Martin and Mitchell were introduced by the Soviet announcer and proceeded to tell their story in exquisite detail. They related how they had become analysts at NSA, full of confidence in the integrity of their government. They described how the U.S. government was intercepting and breaking communications of its allies (Turkey was named specifically), about intentional violations of Soviet airspace to collect intelligence, about alleged American plans for a nuclear first strike, and how NSA was trying to exploit Soviet communications. They exposed NSA's organization (PROD does this and ADVA does that,

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

etc.). They described the arrangements between NSA, GCHQ, and Canada. They spent a good deal of time on the RC-130 shootdown in 1958. It was marvelous theater for Khrushchev, who had launched a diplomatic and press offensive against the United States in May following the U-2 shootdown.⁸³

Martin and Mitchell were young mathematicians. Both had gone into NSG and had been assigned together at [redacted] Mitchell, who was from California originally, was quite bright and had been something of a prodigy in high school. But he was extremely immature socially and had a great deal of difficulty adjusting. While he was at [redacted] Martin was his only close friend. Martin was from Columbus, Georgia. He, too, had been labeled as very bright and, compared with Mitchell, was more gregarious. Certain questions about their psychological health came up on the polygraph and background investigation but were not regarded as serious impediments to employment. Once out of the Navy, both pursued college degrees in mathematics, and upon graduation both were approached for employment by NSA. They entered on duty as GS-7s in 1957.⁸⁴

In 1959 Martin was sent to the University of Illinois for graduate study. While there he established Communist associations, and in his private conversations became more and more critical of the U.S. government. (He expressed special distaste for the U-2 overflights and other reconnaissance activities, and this was reflected in the statements of both men to the press in Moscow.)

At the time, Mitchell was having his own problems and finally sought psychiatric advice. The private psychiatrist concluded that Mitchell was in all probability a homosexual with serious personality disorders. But the psychiatrist felt that this sexual orientation was not the root of his problems. More serious was his poor relationship with his own family.⁸⁵

It has been alleged that in 1959, in violation of standing rules for government employees, Martin and Mitchell visited Cuba. Despite this, there was no evidence that they actually established an espionage relationship with any Communist country prior to the defection.

In June of 1960, just after Martin returned from Illinois, they both applied for annual leave. They stated that they were going to visit family on the West Coast. Instead, they departed for Mexico City and from there flew to Cuba. Apparently they proceeded from there via Soviet trawler to the Soviet Union.

Back at the office, no one thought to question their absence until they were a week overdue. When their supervisor failed to reach them either in their Laurel apartments or at their families' homes, the FBI was called in, and there began an intensive investigation. The security people concluded that the defections were impulsive and self-initiated.⁸⁶

There was no evidence that they carried off any documents, which argued for the theory that they made their decision after going on leave. Still, the route they took

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

required considerable planning, and they left a defection note in a safe deposit box in a Laurel bank, to which they referred during the Radio Moscow broadcast. So the whole idea had been evidently a long time abuilding.⁸⁷

The defection precipitated a storm of criticism of NSA. The secretary of defense initiated an investigation of NSA security practices. Not to be outdone, the House Un-American Activities Committee, chaired by Representative Francis E. Walter of Pennsylvania, launched its own investigation. Finally, President Eisenhower directed that the FBI initiate an investigation to determine if there were any more potential Martins and Mitchells in the ranks at NSA.⁸⁸

All three investigations lambasted the current practice at NSA of granting interim security clearances upon successful completion of the polygraph. Canine had authorized this procedure as an emergency measure during the Korean War, and it had come into routine use. After Martin and Mitchell the practice was terminated, and every employee had to have a complete background check in addition to the polygraph before performing any sort of classified work at NSA.⁸⁹

The Walter Committee investigation was exhaustive. It spanned thirteen months, took two thousand man-hours, covered fifteen states, and resulted in sixteen separate hearings. Thirty-four present or former NSA employees testified in closed session. NSA and the Department of Defense began by opposing committee access to NSA records, but eventually a compromise was worked out, and NSA and the committee finished on reasonably good terms. Still, the Agency could not keep the process from being sensationalized, and it was stung by a charge by Walter that NSA was a "nest of sexual deviates."⁹⁰

The legislative result of the Martin and Mitchell affair was a law which set up the legislative authority for NSA's security system. Among other things, it established that employment at NSA was appropriate only when it was "clearly consistent with the national security." It required a full field investigation prior to employment (i.e., no interim clearances) and gave the secretary of defense additional authority to fire NSA employees "when such action is deemed necessary in the interest of the United States..."⁹¹

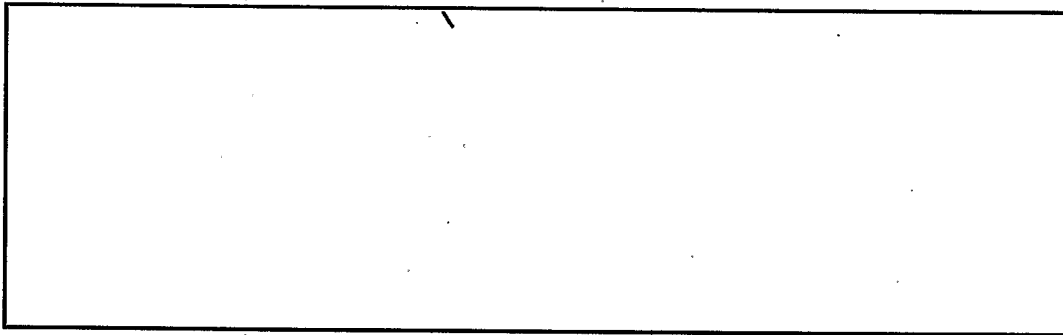
In addition, the committee made certain recommendations concerning NSA's administrative practices - for instance, making professional psychological and psychiatric services available in assessing applicants and employees who revealed instability. But almost all the committee's recommendations had already been implemented, and in its final report the committee gave NSA credit for this. The most far-reaching of the changes related to the termination of the procedure of granting routine interim clearances, and the institution of the so-called three-hour rule, which required that employees three hours overdue for work would be reported to the security office. These and a long list of other changes became a permanent part of NSA's way of doing business.⁹²

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

(b) (6)



As the Walter Committee proceeded, the FBI investigation was winding down. An intensive screening of on-board employees had turned up a small number of people whose sexual conduct, in light of the sexual mores of the time, might be questioned, and of these some twenty-six had been terminated. The proceedings were not all that a civil libertarian might have wanted, but they calmed the waters long enough for NSA to begin functioning again.⁹⁴

The damage to NSA's public image was so severe that it overshadowed the cryptologic damage that had been done. Because it appeared that the two defectors had not carried away documents and that they had not had a previous relationship with the Soviets, just what the Soviets did know as a result was speculative. Martin and Mitchell had known about [redacted] the Soviet problem, but they were in a position to give away information [redacted] on certain Soviet cipher systems, especially a system called [redacted]

[redacted] NSA employees blamed Martin and Mitchell. But no one ever had proof. And unlike Weisband, their defection was not coincident with any sort of "Black Friday." This, the most famous (or infamous) of NSA's security cases, was not the most damaging.

Notes

1. Max Davidson, "The Criticomm System," *Cryptologic Spectrum*, Spring 1975, 11-14.
2. "NSA's Telecommunications Problems, 1952-1968," CCH Series X.H.4.
3. "Report of the Secretary's Ad Hoc committee on COMINT/COMSEC" (the Robertson Report), June 1958, in CCH Series VI.C.1.11.
4. "NSA's Telecommunications Problems. . ."
5. "NSA's Telecommunications Problems. . ."; Tordella oral interview; Eisenhower Library papers in CCH Series XVI.
6. NSCID 7.
7. Tordella interview.

(b) (1)
 (b) (3) - P.L. 86-36
 (b) (3) - 50 USC 403
 (b) (3) - 18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

8. Davidson.
9. "NSA's Telecommunications problems..." [redacted] 108.
10. Eisenhower Library papers, "Report of the Joint Study Group on Foreign Intelligence Activities," 15 December 1960, in CCH Series VI.C.1.32.
11. "The Baker Panel Report and Associated Correspondence," in CCH Series VI.X.1.9.
12. Ibid.; Eisenhower Library papers.
13. Baker Panel Report, ACC 16667, CBRF 51.
14. Baker Panel; Eisenhower Library.
15. Baker Panel; Eisenhower Library.
16. Baker Panel.
17. NSA/CSS Archives, ACC 16667, CBRF 51.
18. Eisenhower Library papers.
19. Eisenhower Library papers; David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: MacMillan, 1967), 677; History of IDA/CRD by Richard Leibler, in CCH Series VI.A.1.6.2.
20. Baker Panel.
21. Howe, draft history of the Robertson report, in CCH Series VI.C.1.12.
22. Robertson report.
23. Ibid.
24. Ibid.
25. Ibid.
26. Ibid.
27. Memo for Mr. [redacted] Subject: Oversight of the National Security Agency by the Department of Defense, 9 Nov 1967, in CCH Series VI.C.1.27.
28. "History of the Electronic Intelligence Coordinating Group, 1955-1958," in CCH Series VI.O.1.6.; Collins, V. III, 12.; Tordella interview.
29. CCH Series VI.O.1.3.; VI.B.2.6.
30. CCH Series VI.O.1.3. [redacted] study, 16-17; interview with Dr. Robert Hermann, NSA OH 45-94, 2 Sept 1994, Charles Baker and Tam Johnson.
31. CCH Series VI.O.1.3.; VI.O.1.2.
32. NSA/CSS Archives, ACC 39471, H03-0311-4 [redacted] study, 16-26.
33. CCH Series VI.O.1.3.; NSA/CSS Archives, ACC 39471, H03-0311-4.
34. Melville J. Boucher, "Talomatry [sic] and How it Grew," Part I, *Spectrum*, Fall 1971, 13; CCH Series VI.O.1.3.; ACC 39471, H03-0311-4.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

35. NSA/CSS Archives, ACC 39741, H03-0311-4; [redacted] "The Soviet Land-based Ballistic Missile Program, 1945-1972: An Historical Overview," manuscript in CCH.
36. NSA/CSS Archives, ACC 39741, H03-0311-4.
37. CCH Series VI.O.1.13.
38. Eisenhower Library papers.
39. "Report of the Joint Study Group on Foreign Intelligence Activities," [The Kirkpatrick Report], 15 Dec. 1960, in CCH Series VI.C.1.32.
40. Ibid.
41. NSA/CSS Archives, ACC 26115, CBNE 48.
42. Informal correspondence between Gary Winch and Mel Boucher, 1977.
43. CCH Series VI.I.1.9.
44. Bob Rush, "AFSCC Tasking: The Development of the Three-Echelon Reporting Concept, 1949-1952," USAFSS history available at AIA, Kelly AFB, Texas.
45. "History of the USAF Security Service; Fiscal Year 1955," AIA, Kelly AFB, Texas.
46. Ibid.
47. Official USAF biography, Oct 1977.
48. Historical Data Report for the 6901st SCG, Semi-Annual, 1956-1964, available at AIA, Kelly AFB; Oral interview with [redacted] 25 March 1993, by Tom Johnson and Jim Pierson, NSA OH 15-93.
- [redacted]
50. Ibid.
51. Ellerson oral history; 6901 SCG Semi-Annual histories.
52. [redacted] "A Look at the Pacific Experimental Facility," *Spectrum*, Winter 1974, 18-21.
53. Howe, "Narrative History..." Part V, Ch. XXVI-XXX.
54. Howe, "Narrative History."
55. CCH Series VI.HH.12.10.
56. Collins, V. III, 40-41.
57. Transcript of videotapes of five former directors; [redacted] study, 16; CCH Series VI.NN.1.1.
58. Ibid.; Tordella interview.
59. CCH Series VI.D.1.1.; Stone interview; Kahn, *The Codebreakers*, 705.
60. Tordella interview.
61. Tordella biography in CCH Series VI.D.3.4; Tordella interview.
62. Summary of Statutes Which Relate Specifically to NSA and the Cryptologic Activities of the Government, available in CCH.
63. Ibid.

(b) (1)
 (b) (3)-P.L. 86-36
 (b) (3)-50 USC 403
 (b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

64. Ibid.
65. Ibid.
66. Ibid.
67. Ibid.
68. Church Committee Hearings, V. 5, 7-8, ACC 25958-25959, H0-02-0405.
69. John V. Connorton (LTJG) and Floyd W. Tompkins (LT), "The Need for New Legislation Against Unauthorized Disclosures of Communication Intelligence Activities," June 1944, SRH 016.
70. Ibid.
71. CCH Series V.C.2.8.
72. Ibid.
73. Hoover Commission report.
74. Kirkpatrick Committee report.
75. Benson and Phillips, V. I, 155.
76. Ibid., V I, 158.
77. Ibid., V. I.
78. Dr. Theodore W. Bauer, "Historical Study: The Security Program of AFSA and NSA, 1949-1962," unpublished manuscript available in CCH.
79. Bauer; Kahn, *The Codebreakers*, 690-92.
80. NSACSS Archives, ACC 2146, CBOI 37.
81. Quoted fm Thomas Powers, *The Man Who Kept the Secrets: Richard Helms and the CIA* (New York: Knopf, 1979), 276.
82. Wayne Barker, *The Anatomy of Two Traitors: The Defection of Bernon F. Mitchell and William H. Martin* (Laguna Hills, California: Aegean Park Press, 1981).
83. Press statement; copy available in ACC 27147, CBOI 37.
84. NSA/CSS Archives, ACC 24399, G11-0502.
85. Ibid.
86. Bauer.
87. Barker, CCH Series X.H.5.
88. Bauer; Eisenhower Library papers.
89. Bauer.
90. ACC 45399, G11-0502.
91. "Summary of Statutes . . ."; NSA/CSS Archives, ACC 24399, G11-0502.
92. Ibid.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

93. Ibid.

94. Ibid.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~