DOCID: 3188691

~~TOP SECRET~~ American Cryptology during the Cold War, 1945–1989 – Book I ~~TOP SECRET~~

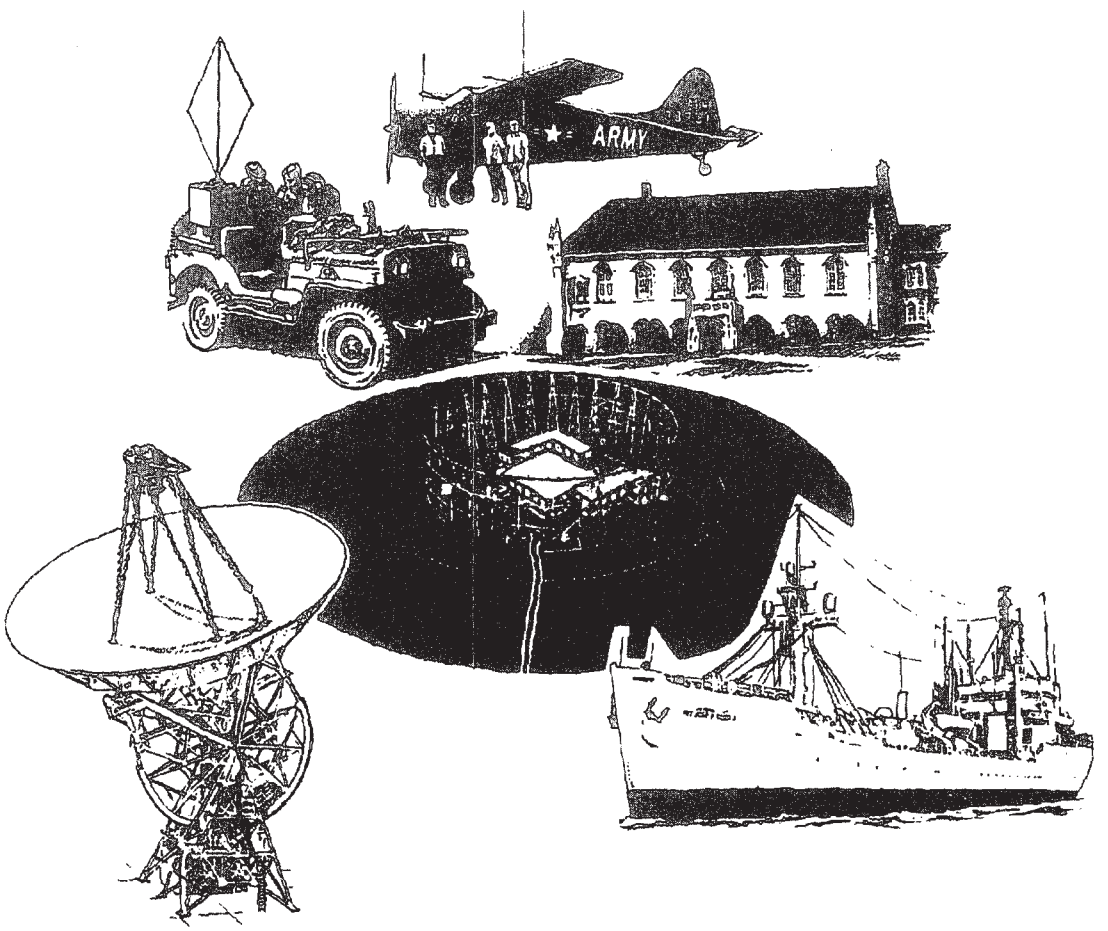
series VI
volume 5

book I

national security agency
central security service

~~TOP SECRET~~ NO. 903

UNITED STATES CRYPTOLOGIC HISTORY



American Cryptology during the Cold War, 1945–1989

Book I: *The Struggle for Centralization 1945–1960*

HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
THIS DOCUMENT CONTAINS CODEWORD MATERIAL
NOT RELEASABLE TO FOREIGN NATIONALS

Classified by NSA/CSSM 123–2
Declassify on: Originating Agency's Determination Required

~~TOP SECRET~~

CCH–E32–95–03
TCS–54649–95

Approved for Release by NSA on 07-31-2007, FOIA Case # 40186

This monograph is a product of the National Security Agency history program. Its contents and conclusions are those of the author, based on original research, and do not necessarily represent the official views of the National Security Agency. Please address divergent opinion or additional detail to the Center for Cryptologic History (E322).

This document is not to be used as a source for derivative classification decisions.

~~TOP SECRET UMBRA~~

UNITED STATES CRYPTOLOGIC HISTORY

Series VI
The NSA Period
1952 – Present
Volume 5

American Cryptology during the Cold War, 1945–1989

Book I: The Struggle for Centralization, 1945–1960

Thomas R. Johnson

CENTER FOR CRYPTOLOGIC HISTORY

NATIONAL SECURITY AGENCY

1995

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

~~TOP SECRET UMBRA~~

Table of Contents

Page

Foreword xi
Preface xiii
Acknowledgements xv

BOOK I: THE STRUGGLE FOR CENTRALIZATION, 1945–1960

Chapter 1: Cryptologic Triumph and Reorganization, 1941–1949

World War II and the Intelligence Revolution 1
The Way COMINT Was Organized at the End of the War 7
The CJO 11
The Cryptologic Allies 13

Chapter 2: AFSA and the Creation of NSA

The Stone Board 23
AFSA 26
The Brownell Committee 33
Korea 36
The Country 36
The Asia Dilemma 38
The Invasion 40
The Murray Mission 41
Counterattack 43
China 43
AFSA and ASA Operations 46
White Horse Mountain 48
AFSS Introduces Tactical Warning 48
The Navy 51
The AFSA Factor 52
Relations with ROK COMSEC and COMINT 52
Korea – an Assessment 54

Chapter 3: Cryptology under New Management

Canine and the New Organization 62
The Early Work Force 63
Fielding the Field Offices 67
Civilians in the Trenches – the Civop Program 69
COMINT Reporting in Transition 69

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

NSA Training – the Early Years 71
Setting Up Security 73
NSA and the U.S. Intelligence System 75
Consumer Groups Come to NSA 75
The Struggle for Technical Control 76
The Decentralization Plan 78
Relations with the SCAs 80
The SCAs Create Second Echelons 83
Watching the Watchers 85
NSA and CIA – the Early Years 86
CIA Enters the COMINT Business 89
[redacted] 90
[redacted] 91
CIA and Cryptographic Materials 92
The [redacted] Business 93
[redacted] 94
[redacted] 95
[redacted] 96
[redacted] 97
[redacted] 98
[redacted] 99
The Third Parties in the Early Years 100
CIA in the NSA Trenches 101
[redacted] 102
[redacted] 103
NSA's Other Competitors 107
ELINT and NSA 108
Building the Overt Collection System 111
[redacted] 112
The United Kingdom 118
[redacted] 121
[redacted] 121
[redacted] 125
[redacted] 126
[redacted] 126
[redacted] 127
[redacted] 127
The Far North 131
[redacted] 132
What It Was Like 132
[redacted] 138
SIGINT Goes Airborne 139
BLUE SKY 140
Peripheral Reconnaissance 140
The Origins of Advisory Warning 143
The RC-130 Shootdown 144
Advisory Warning Is Implemented 147
The RB-47 Shootdown 148

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

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

Chapter 4: The Soviet Problem

The Early Days 157
The Advent of BOURBON 158
VENONA 160
"Black Friday" 168
ASA and AFSA Turn to Radioprinter 169
The Soviet Strategic Threat 170
How It Began 171
The American Response 174
The Soviet Atomic Bomb Project 176
The Chinese Threat 178
The Early Days of Overhead 179
The Attack on Soviet Cipher Systems 184
Tracking Submarines - [redacted] 187
[redacted] 188
[redacted] 189

Chapter 5: Building the Internal Mechanism

Cryptology is Automated – The Story of Early Computerization 195
Antecedents 195
Postwar Developments 197
NSA Communications in the Pre-Criticomm Era 205
The COMINT Comnet 207
Securing American Communications 211
The Era of the Wired Rotor 211
The Early Years of Secure Speech 214
Organizing for COMSEC in the Postwar World 215
AFSAM-7 217
The Push for On-line Encipherment 218
From SIGSALY to Modern Voice Encryption 220
TEMPEST 221

Chapter 6: Cryptology at Mid-decade

The Early Assessments 227
The Robertson Committee 227
The Hoover Commission 228
The Killian Board 229
The Jackson Report 231
1956 232
Suez 232
Hungary 235
[redacted] 236
Lebanon, 1958 237
1956 in History 239

The Reorganization 239
The Move 241

Chapter 7: The Eisenhower Reforms

The Post-crisis Centralization of the SIGINT system 253
Criticomm 253
The Baker Panel 256
The Reuben Robertson Report 259
The marriage of ELINT and NSA 260
The Kirkpatrick Committee 263
NSA Centralizes the Field System 264
AFSS and the Development of Second-Echelon Reporting 265
The Struggle for Control in the Pacific 268
Samford Joins the Agency 269
The Tordella Era Begins 271
Public Law 86-36 272
NSA and the American Public – The Issue of Legality 272
Public Revelations and Cryptologic Secrecy 274
Classifying Cryptologic Information 275
Breaches in the Dike – The Security Cases 277
L' Affaire Weisband 277
The Petersen Case 279
Martin and Mitchell 280

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

~~TOP SECRET UMBRA~~

Non - Responsive

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

Foreword

(U) The Center for Cryptologic History (CCH) and its predecessors have published thirty-seven volumes – monographs, crisis studies, source documents, bibliographies – concerning the history of signals intelligence and information systems security, the *yin* and *yang* of modern cryptology. These publications have treated specific events, organizational issues, and technical developments in peace and war; most have been pioneering efforts, based on original documentation, and, in many cases, are the first history of their particular topic in any venue.

(U) There has been a strong need, however, for a single work to undertake the full sweep of cryptologic history, providing a context into which the more specialized studies may be placed. Such a cryptologic Cook's tour should incorporate the military-political events of our time and the history of interaction between cryptologic organizations and other components of the intelligence community – access to SIGINT and INFOSEC is limited to "insiders," but it is clear that cryptologic operations do not occur in a vacuum.

(U) Thomas R. Johnson's *American Cryptology during the Cold War, 1945–1989* meets these requirements admirably. Drawing on over a decade of study and reflection on cryptologic history, Dr. Johnson deals with three facets of cryptologic history: first he explains how cryptology responded to the landmark events and challenges of the post-World War II era. He next provides profound analysis of how events and personalities affected the development of cryptology institutionally and professionally. Finally, and even better, Dr. Johnson spins a fascinating tale of the success or failure of cryptologic operations in the various crises that have challenged the SIGINT system.

(U) With Books One and Two of this projected four-book work now available, *American Cryptology during the Cold War* is "must reading" for the cryptologic professional. The narrative and analysis in these first two books are essential background for understanding how the cryptologic community progressed to its present configuration. This is the definitive work on American cryptology after World War II.

(U) For readers who may wish to explore American cryptology prior to the modern period, I recommend as a companion piece to the present book, Dr. Ralph E. Weber's *Masked Dispatches: Cryptograms and Cryptology in*

American History, 1775–1900 (CCH, 1993). Two more useful books with background on pre-World War and World War II cryptology are Frederick D. Parker's *Pearl Harbor Revisited: United States Navy Communications Intelligence, 1924–1941* (CCH, 1994) and Thomas L. Burns's *The Origins of the National Security Agency, 1940–1952* (CCH, 1990).

David A. Hatch
Director,
Center for Cryptologic History

Preface

What It Is and What It Is Not

This book is intended to be a general overview of U.S. government cryptology since the end of World War II. It is projected to be a four-book study carrying the story to the end of the Cold War, symbolized by the fall of the Berlin Wall.

I have attempted to include the entire effort, which includes the Service Cryptologic Agencies (as they were once called), as well as certain CIA programs. These organizations comprised almost the totality of the cryptologic efforts of the federal government, although other organizations (FBI is a good example) have occasionally dabbled in the discipline. Because it is comprehensive rather than strictly organizational, it contains information about the field sites, intermediate headquarters and the SCA headquarters themselves. It does not cover in detail the organizational aspects of the creation of the National Security Agency. That is covered in good detail in Thomas L. Burns's book, *The Origins of the National Security Agency: 1940-1952*, published in 1990. Thus the coverage of events between 1945 and 1952 is sketchy and simply tries to fill in blanks in the record that the Burns book did not cover.

This is not a history of private or nongovernmental cryptology. Although it covers relationships with our Second and Third Party partners, it does not focus on that aspect either, except as it contributed to the development of our own effort. Our long-standing debt to the British cryptologic effort at GCHQ should not go unnoticed, however. It deserves a separate book.

If you are looking for a history of your specific organization, you will not find it. This is a history of events, not organizations. The importance of the cryptologic contribution to American security is so broad as to obscure individual organizations and, often, the specific people involved. In certain cases, however, I have identified major individual contributors to cryptologic history or those who were, by chance, thrown into momentous events.

Two overarching themes characterized American cryptology from the end of World War II to the end of the first Nixon administration: centralization and expansion. The SIGINT system underwent a period of almost unbroken expansion from 1945 to the American retreat from Southeast Asia. These themes dominate the first two books in the set.

The end of the Vietnam War and the era of the Watergate scandals that followed marked a watershed, and new themes of retrenchment and decentralization marked the period that followed. These will be the themes that open Book III.

THOMAS R. JOHNSON

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

Acknowledgements

My debt to others begins with the staff of the NSA Archives, who dropped whatever they were doing whenever I needed material. [redacted] in the Archives helped with photographs, and the staff in L32 produced hundreds of black and white prints to go into the publication. [redacted] in E31 (Geographics) did most of the map work. My debt also includes the CIA staff historians, especially [redacted] and [redacted] who guided my work and opened doors to CIA material.

My thanks also go to the editorial staff of Barry Carleen [redacted] and [redacted] who, for days on end, did nothing but edit this history. It was the longest work that the Center for Cryptologic History has attempted, and I am sure it taxed their patience, although they never said so. Also owing to the unusual length and complexity of the book, the NSA photo laboratory (E23) and NSA's printing services (Y19), which did the photo reproduction and printing of this book, should be recognized for their major efforts to get out the publication. [redacted] deserves praise for the cover graphics.

In the Service Cryptologic Agencies, James Gilbert and Jack Finnegan, the INSCOM historians, were very responsive to my need for Army cryptologic materials. A special debt is also owed the historical staff at the Air Intelligence Agency. Everyone on the staff, from James Pierson (now retired) to Jo Ann Himes to Joyce Homs to Juan Jimenez, responded almost instantly to my many requests for information. Their help resulted in a rather more thorough treatment of Air Force cryptology than would have been possible otherwise.

The history itself has had a large number of "readers" who plowed through the various drafts and revisions offering helpful comments and additional information. Everyone in the Center for Cryptologic History (CCH) had a hand in its improvement, as well as a list of other readers who critiqued various portions. Among them, David Gaddy and [redacted] deserve special note for their help with the chapter on Vietnam.

The history also had a group of "general readers," senior Agency officials who agreed to read the entire work in draft state. Milton Zaslow, Cecil Phillips, Donald Parsons, Eugene Becker, and David Boak spent long hours poring over various drafts, offering comments and encouragement and correcting information.

Finally, I wish to thank all those who, over the years, volunteered their time to sit for oral history interviews. NSA owes them all a debt of gratitude for their contributions to retrieving otherwise vanished information.

THOMAS R. JOHNSON

Footnotes

The text is footnoted throughout with short, abbreviated citations. More complete information can be obtained in the Bibliography. However, a few comments on certain footnote abbreviations are in order.

The largest number of citations is from the Cryptologic History Collection, which is the working file of the Center for Cryptologic History. This collection is organized into sixteen series, and citations to that collection begin with the series number and a series of numbers, e.g., CCH Series V.A.29.

Citations from the NSA Archives vary depending on whether the document was part of an archived collection or was still in the Retired Records collection when researched. The former begins with the accession number, followed by a location, e.g., ACC 16824,CBTB 26. The latter begins with a box number, followed by a shelf location, e.g., 28791-2, 80-079.

A general bibliography and an index are included at the end of Book II.

Chapter 1
Cryptologic Triumph and Reorganization, 1941–1949

The combined U.S.-U.K. COMINT operation of World War II was perhaps the most successful large-scale intelligence operation in history.

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

[redacted] CIA, 1971

WORLD WAR II AND THE INTELLIGENCE REVOLUTION

The Second World War began a true "revolution" in intelligence. The impact of intelligence on the strategy and tactics of the Allies (and to a somewhat lesser extent on the Germans and Japanese) was truly revolutionary, and it is just now coming to be recognized for what it was. Through the publication of books like Frederick Winterbotham's *The Ultra Secret* and John Masterman's *The Double Cross System* and by the massive declassification of war records begun by the British and Americans in 1977, the true extent of this influence is now emerging.

No other intelligence source had the revolutionary impact of SIGINT. World War II was, in the words of historian Walter Laqueur, "a SIGINT war." The influence of SIGINT was so pervasive that it is now hard to imagine how we might have fought the war without it. Even prior to the direct engagement of American and British forces against the Germans and Japanese, two of their most complex ciphers were broken. The British effort at Bletchley Park first produced plaintext reports from the German ENIGMA system in September 1940, the same month that a small Army team under William F. Friedman broke the Japanese diplomatic cipher machine called PURPLE. By February of 1942 the Navy had broken the Japanese Fleet Operational Code, called JN25. In 1943 the Army broke the Water Transport Code, while in 1944 a lucky battlefield retrieval of cipher material allowed the Army to read the Japanese Army codes. When combined with successes in direction finding, traffic analysis, and the exploitation of plaintext communications, SIGINT yielded a torrent of useful information.

British achievements have come in for the most scrutiny (and praise). We know that Churchill "revelled" in his ability to read Hitler's mail and spent hours pondering on Nazi strategy as revealed in the decrypted messages. The British set up a very efficient and secure system for disseminating SIGINT, the precursor of our SSO (Special Security Officer) system. Always wary of the "blabbermouth" Americans, they insisted that we adopt their system before they would share everything in the SIGINT larder with us. As the Combined Chiefs prepared for Overlord, they knew precisely how the Germans were reacting to the invasion plans and where they were positioning their units for the expected blow.

Moreover, once the invasion was launched, they knew what the Germans were doing and were able to adjust accordingly. As Allied troops moved across France, they moved in sync with the gold mine of intelligence which detailed most of the important German military movements. Their intelligence officers must have looked like geniuses – they were able to predict German moves before they happened and could advise commanders how to react. If every dog has its day, this was the day of the G-2, the military intelligence officer. The product of breaking high-grade ciphers was called ULTRA, and it was so good that when it was not available, as it was not at the Battle of the Bulge, the G2 corps scarcely knew what to do. A few predicted the German offensive, but most did not. They were wedded to the SSO and the bonanza of information that he could provide.

The Pacific was the American theater, and the U.S. was as successful there as the British were in Europe. Navy cryptanalysts broke JN25 in time for Admiral Nimitz to use it in the Battle of Coral Sea in May of 1942. The success of strategic SIGINT was so important that Nimitz had become a permanent convert. When the cryptologists at Pearl Harbor came to Nimitz with information outlining a much bigger battle shaping up in the central Pacific, the admiral was quick to believe and quick to act. To his dying day he credited SIGINT with the key to the victory at Midway. This turned the war in the Pacific completely around and launched Nimitz on his Central Pacific campaign which took him to Okinawa. He considered SIGINT as an absolutely critical component, and he learned to use information from both the high-grade cipher traffic and the plaintext messages and operator chatter. Some of his subordinates were as successful as Nimitz in the use of this intelligence, some were not. But it is hard to argue with results.

SIGINT and MacArthur had a turbulent marriage. The commander in the Southwest Pacific had outstanding success in using SIGINT on some occasions, the most conspicuous success coming in his 1944 New Guinea campaign. There were also some failures resulting from several causes. His staff never came to trust SIGINT as did that of Nimitz. When they did use it, it was sometimes hard to get it melded into the battle plan, as MacArthur was a classical intuitive decision maker. Jurisdictional disputes between MacArthur and the War Department in Washington caused him to come to distrust this strange SSO lash-up which he could not control because it did not work for him.

In the battle for the sea lanes, SIGINT again played a decisive role. The Japanese merchant marine was devastated largely because its movements were being given away in the Water Transport Code. Sinking the defenseless and slow-moving merchant vessels was relatively easy when their movements were known beforehand. In the Atlantic, the U.S. and the British used decrypted ENIGMA messages to track German U-boats and to drive their wolf packs from the sea lanes. This was not quite as easy as going after merchantmen, and the marriage between SIGINT information and operational procedures to effect a kill represented a very high level of military and technological expertise. It may have been the most difficult and delicate use of SIGINT during the war.

One other wartime accomplishment would become significant in later years. In 1944 the British and Americans established a Target Intelligence Committee (TICOM) to interrogate captured German COMINT personnel. The major objective was COMSEC – to determine how well the German cryptologists had exploited Allied communications. The flip side of that effort was COMINT – to see how well the Germans were doing against other, and particularly Soviet, communications. TICOM was at Bletchley Park, headquarters for the British cryptologic service, Government Code and Cipher School (GC&CS). Six teams of American and British COMINTers were dispatched to the battlefields of the Continent. They sent their "take" to the Document Center at GC&CS. The original documents remained there while the microfilm copies were sent on to Washington. TICOM teams also captured equipment. One-of-a-kind equipment remained at GC&CS, while duplicates were sent to the United States.

The new system was so successful that teams were established in the Pacific, with the British taking the lead in Southeast Asia, the United States in the Central Pacific and Japan, and joint American and Australian teams in Rabaul and Borneo. Although TICOM was formally dissolved in November of 1945, American and British experts continued to exploit the material for years afterward, and TICOM was later re-created in the United States as TAREX (Target Exploitation), minus British participation.

If the strength of American SIGINT was in providing militarily useful information, its weakness was in its organization. The Army and Navy were at constant loggerheads over the control of cryptology, and at times the factional disputes were little short of catastrophic. British historian Ronald Lewin, a great admirer of American technical ingenuity which yielded the SIGINT bonanza, was frankly contemptuous of our inability to get along:

> The old antagonism and suspicion between Army and Navy persisted in a manner that may at times seem infantile, until it be remembered that tribal loyalty, narrowness of vision, and sheer egocentricity can make even the most senior and hardened officers occasionally enter a second childhood.[1]

Army and Navy cryptologic organizations had a long and inglorious history of failing to coordinate their efforts, dating back to the 1920s. In 1940, when the Army's success in breaking Japanese diplomatic cipher systems became known to the Navy, there ensued lengthy and difficult negotiations to determine how the effort was to be divided. They finally arrived at a Solomonic solution by which the Army processed Japanese diplomatic traffic originating (i.e., cipher date) on even days of the month while the Navy would process traffic from odd days. This resulted in a fair division politically, but from the standpoint of cryptanalytic continuity it was a horror. To make matters even worse, there was in those days no thought, no concept, of centralized and coordinated intelligence analysis. What little analysis and interpretation was done (and there was very little indeed) was accomplished by each service on the traffic which it had decrypted, leaving for each a checkerboard pattern of information in which every other day was left out. This

almost inconceivable situation persisted until 1942, when diplomatic traffic was, by mutual agreement, left to the Army, while the Navy concentrated on Japanese naval material.[2]

Alfred McCormack

The disaster at Pearl Harbor resulted in a thoroughgoing Army internal investigation. Secretary of War Henry Stimson picked Yale lawyer Alfred McCormack to lead the way. McCormack discovered a scandalously incompetent Army G2 and a nonexistent SIGINT analysis and dissemination system. He set up a separate system called Special Branch, Military Intelligence Division, and was picked as the first deputy. (Colonel Carter W. Clarke became the first commander.) At the same time, the Army and Navy arrived at a joint modus operandi regarding the division of overall SIGINT responsibilities. Each service was to work what we now call "counterpart" targets. Since there was little in the way of Japanese Army traffic to work, the Army took on the task of diplomatic intercept. The third partner was the FBI, which shared with the Navy the task of working Western Hemisphere agent and clandestine traffic. These three were tobe the only participants in SIGINT for the duration of the war. Roosevelt's directive of July 1942 specifically excluded the FCC (Federal Communications Commission), Office of Censorship, and the OSS (Office of Strategic Services) from SIGINT production .[3]

At the same time a standing committee of Army, Navy, and FBI COMINT officials was established. It met only a few times and had little lasting impact on organizational matters. Meetings were frequently marred by vituperative arguments, especially between Navy and FBI, which were supposed to be sharing Western Hemisphere clandestine traffic. It was not cryptology's finest hour. Meanwhile, the COMINT activities of the FCC and Censorship Bureau continued virtually unabated.[4] Only the OSS seems to have been temporarily frozen out of the COMINT community. Resurrected after the war as the CIA, it

exacted revenge over a period of many years for having been excluded from wartime cryptology.

Carter Clarke, head of Special Branch of Military Intelligence Service

The Army and Navy cryptologic organizations, Signal Security Agency (SSA) and OP-20-G, respectively, found cooperation difficult. The Army was willing to share everything it had with the Navy, but OP-20-G would not reciprocate. What finally brought matters to a head was the breaking of the Japanese Army code in early 1944. This produced information vital to the Navy in the Southwest Pacific. SSA decided to withhold information from it until the Navy agreed to expand cooperation. The Navy quickly came around, and the result was a wartime agreement signed by Army Chief of Staff General George Catlett Marshall and Chief of Naval Operations Admiral Earnest J. King. Called the Marshall-King Agreement, it provided for the total exchange of COMINT materials (but at the Washington level only).[5]

It quickly fell apart, and for a time this informal agreement seemed a dead letter. But the need to cooperate was by then so vital that the two services were driven to a more permanent solution. Thus was formed the Army-Navy Communications Intelligence Coordinating Committee (ANCICC) in April of 1944. The committee was to coordinate

and settle "such controversial matters as can be resolved without reference to higher authority," a plain attempt to keep disagreements out of the offices of Marshall and King. Although the Navy was consistently the more parochial of the two services in COMINT matters, the "godfather" of this cooperation was almost certainly Joseph Wenger, a naval commander and career cryptologist within OP-20-G. Meanwhile, coordination under the terms of the Marshall-King Agreement continued its bumpy course, now underpinned by this policy committee.[6]

Joseph Wenger

In late 1944 the Navy (probably Wenger) once again suggested improving cooperation. This time they proposed creating a new board called the Army-Navy Communications Intelligence Board (ANCIB). Representation would be of a higher level – instead of the heads of the cryptologic organizations, the members were to be the heads of intelligence and communications for the two services. The board would be formally established (ANCICC was informal) and would be approved by Marshall and King. Although the Army initially answered "No," it later changed its mind, and ANCIB became official in March 1945. ANCICC became a working committee of ANCIB, insuring that the heads of COMINT organizations would continue to meet. To keep COMINT out of the JCS arena (in

order to tighten security), ANCIB reported directly to the Chairman of the Joint Chiefs of Staff, rather than through the Joint Staff.

FBI was not invited to be a member of the board, a deliberate move which was occasioned by Navy-FBI friction over the control of clandestine intelligence. But in December 1945, the State Department was invited, and ANCIB became STANCIB. This recognized the existence of a small COMINT exploitation unit at State and implicitly acknowledged that State would have to be invited if ANCIB were to represent the United States in postwar COMINT negotiations with the British. In 1946 the board changed name once again, to USCIB (the United States Communications Intelligence Board), a lineal predecessor of today's National Foreign Intelligence Board. At virtually the same time, the newly created Central Intelligence Group, soon to change its name to CIA, accepted an invitation to join. Through all this, ANCICC changed to STANCICC and then to USCICC.[7]

No matter what the name of the board, cooperation remained purely voluntary, and all decisions required unanimity. There was no higher authority imposing central control of COMINT. The British, who had a unified COMINT service under the Government Code and Cipher School (GCCS), were scandalized. During the war they were forced to deal separately with the three organizations with COMINT interests – the Army, Navy, and FBI. British officials regarded negotiations with the Americans as a little like dealing with the former colonies after the American Revolution – disorganized and frustrating at times, but they could still play one off against another to achieve their objectives.

THE WAY COMINT WAS ORGANIZED AT THE END OF THE WAR

The cryptologic system that emerged from World War II was profoundly and tenaciously decentralized. Instead of a central control (like NSA) and Service Cryptologic Elements (SCEs) as we know them, there were only the separate COMINT organizations of the Army, Navy, and FBI. Naval COMINT was under an organization called the Supplemental Radio Branch and designated OP-20-G, part of Naval Communications. There was a headquarters in Washington called CSAW (Communications Supplementary Activity, Washington) where centralized processing functions were performed, chiefly against the German naval ENIGMA problem. For the Pacific theater there were virtually independent processing centers: one in Hawaii, called FRUPAC (Fleet Radio Unit, Pacific); one at Melbourne, Australia, called FRUMEL (Fleet Radio Unit, Melbourne) and, late in the war, one on Guam, designated RAGFOR (Radio Analysis Group, Forward).

Naval COMINT had grown through the years. From its beginnings in 1924 with one officer, Laurance Safford, and a single civilian, Agnes Driscoll, OP-20-G had by 1941 increased to 730 bodies. During the war the number of intercept sites in the Pacific increased from four to eight, and the receivers allocated to Japanese intercept increased

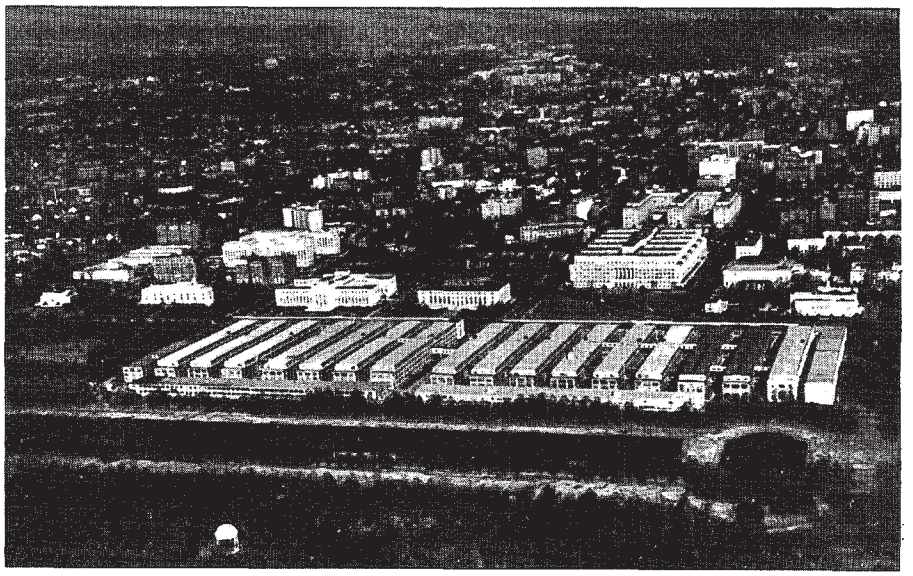
from 68 to 775. Shipborne collection began with one operator and one receiver in the Pacific in 1941, but by 1945 there were eight shipborne operator teams with 120 receivers. Yet in 1945 the entire system quickly collapsed. OP-20-G closed ten of its sixteen intercept and DF stations. When the war ended, the German cipher exploitation section went from over 2,000 to only 200.

Since its creation, OP-20-G headquarters had been in the Navy Building on Constitution Avenue in Washington. COMINT success required more people and more space to work the traffic, and the Navy began looking for a separate facility for its most secret activity. They found it in the fall of 1942, at a girl's school on Nebraska Avenue called the Mount Vernon Seminary for Women. The Navy bought it for about $1 million and began converting the ivy-covered red brick structure into a military facility. One of the first things they did was to build new barracks for the 4,000 WAVES (Women Accepted for Volunteer Emergency Service) who were brought in primarily to operate the "bombes" that deciphered ENIGMA messages from German submarines.[8]

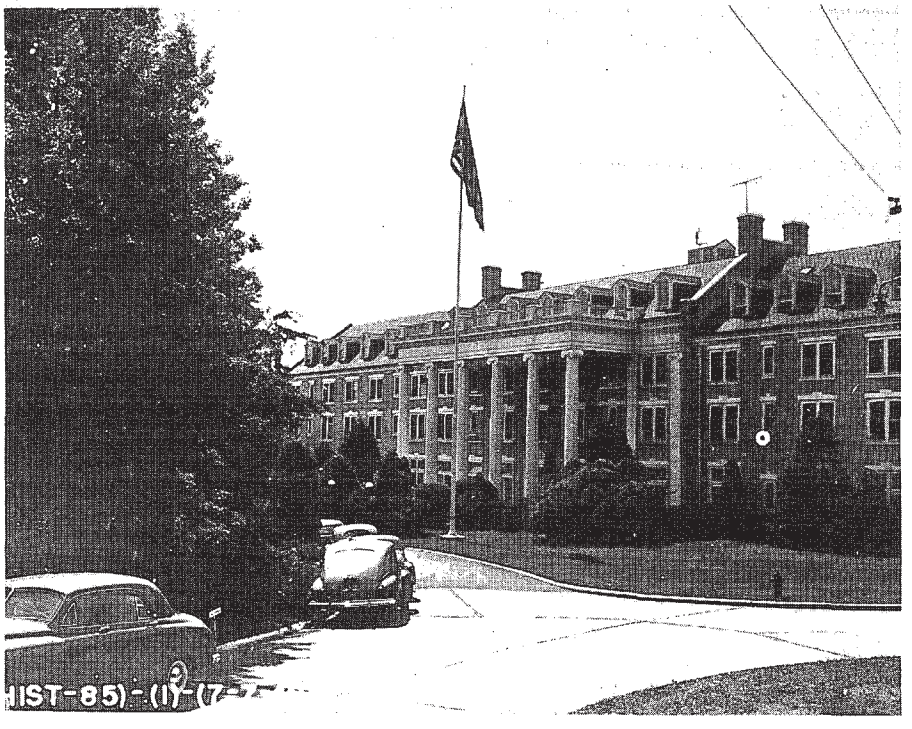
The Army, too, took over a girls' school. In 1942 Signal Intelligence Service (SIS) was, like OP-20-G, looking for a new and larger home. Then it found Arlington Hall, a junior college located in the rolling hills of suburban Arlington. The school was big on horses and equestrian pursuits but had always been short on cash. Its founder, a Dr. Martin, went bankrupt in 1929, and the school limped along on a hand-to-mouth existence until it was mercifully extinguished by the Army. Paying $650,000 for the property, SIS acquired it in June of 1942 and moved from the Munitions Building, which stood beside the Navy Building on Constitution Avenue.[9]

Organizationally, SIS was similar to OP-20-G. Although it changed its name to Signal Security Agency (SSA) in 1943, it remained part of the Signal Corps. In September 1945 it was finally severed from Army communications, attaining status as an independent command called Army Security Agency (ASA), an implicit recognition of its contributions to winning the war. Elevated status gave it a two-star command billet and an independent position in the Army hierarchy, but it now took its operational direction from Army intelligence. This placed it back in roughly the same position that it had been when, in the 1920s, it had been named MI-8 and had been under G2.[10]

For SIS, intercept work was more difficult than for OP-20-G because the Army lacked geographic access. During the early 1930s, SIS relied on the telegraph cable companies to provide it with message traffic. The earliest SIS efforts to develop intercept sites resulted in stations in Hawaii and Panama later in the decade, and by 1938 SIS had additional sites at the Presidio in San Francisco, Fort Sam Houston in Texas, and Fort Hughes in Manila. In 1942 SIS attempted to hear German transmissions from a new site (USM-1) at Vint Hill Farms in northern Virginia. By the end of the war, SSA had eleven intercept stations. The force at Arlington Hall numbered 7,848, of whom 5,661 were civilians.[11]



Government offices on the Mall
Both SIS and OP-20-G began World War II in these temporary buildings on the Mall in Washington.



Arlington Hall Station in the 1940s

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

To Army cryptology, as to the Navy, peace was devastating. Most of the work force at Arlington Hall left civilian government service, and within days the halls were almost empty. Intercept sites overseas were suddenly confronted with no Japanese or German intercept mission. One former soldier described the experience as being left stranded on Okinawa with no Japanese mission to copy and no instructions on a follow-on assignment. His unit eventually moved to Seoul, relocated to a former Japanese communications station, and there got a new mission – Soviet and Chinese Communist communications. European units tackled French and Greek missions, and by mid-1946 nearly half the Army's end product was based on the intercept of French communications.[12]

The late 1940s were a period of damaging retrenchment. The Army and Navy cryptologic organizations that began the Soviet mission had little experience, less money, and no expertise. Yet ASA was able to survive better than OP-20-G. The Army had relied historically on civilians, and many of the best, including William Friedman, Frank Rowlett, Abraham Sinkov, and Solomon Kullback, stayed on. Missing the excitement of wartime cryptology, others drifted back to Arlington Hall after brief, humdrum civilian careers. The Navy, which had relied on uniformed cryptologists, lost a far higher number to civilian life and found the transition to peacetime a difficult one.

In 1947 ASA and OP-20-G were joined by yet a third cryptologic service, that of the newly created Air Force. The Army Air Corps had actually established its SIGINT service in the Pacific in 1944. The Air Force acquired an early reputation for parochialism and interservice rivalry. The feuding led Carter Clarke, then head of Special Branch of Military Intelligence Service, to write in June 1944 that "the Air Force insists that these [redacted] operate only for the Air Force and insists further that no personnel can be attached or detached therefrom; neither should the theaters give them any operational directives in the sense that we think of it." The first Air Force unit in the Pacific was the [redacted] which began operations in 1944 in New Guinea.[13]

When the independent Air Force was created in 1947, there was no direct reference to cryptologic activities, and for a time ASA continued to provide these to the nascent Air Force. Yet the Air Force was determined to establish its own capability. Certain Air Force generals were aware of the contributions of COMINT during the war. One in particular, Hoyt S. Vandenberg, who was later to become Air Force chief of staff, was convinced that the Air Force had to have its own cryptologic service. He saw how the British controlled cryptology in Europe and felt that it was essential to get this under American, and particularly Air Force, control.[14]

In early 1948 the Air Force fashioned a transition agreement with ASA. The latter established an Air Force Security Group within its headquarters at Arlington Hall to oversee the transfer. Three [redacted] and eight COMSEC units were turned over to the Air Force. The Air Force role was defined as mobile and tactical, and ASA continued to operate all fixed sites. A set number of ASA officers (thirty-two) became blue-suiters, and this group became the "founding fathers" of Air Force cryptology. Air Force cryptologists

were to continue to train at ASA schools and were to contribute instructors and financial support as soon as the Air Force had a budget of its own. Significantly, the Air Force assumed all responsibility for "the investigation for intelligence purposes of all types of electronic emissions relating to radar, radio control of guided missiles and pilotless aircraft, proximity fuses, electronic navigation systems, infrared equipment and related subjects." In other words, the Air Force was to take the ELINT and electronic warfare missions, which were at the time too new to even have a name. Needing equipment but not yet having a budget, the Air Force arranged for the transfer of equipment from the Army, which turned out to be cast-off receivers and antennas that ASA no longer wanted.[15]

On 20 October 1948, the new Air Force cryptologic organization was officially established as the U.S. Air Force Security Service (USAFSS), still located at Arlington Hall. It was a major air command, responsible to neither intelligence nor communications. Thus from its earliest existence the Air Force accorded a loftier organizational position to its cryptologic service than did the other, more senior, services. And the Air Force did something else that was unprecedented. In May of 1949 it moved completely out of Washington. Security Service set up shop at Brooks Air Force Base outside of San Antonio, Texas. The move was calculated to remove USAFSS from geographical proximity to the central control authority for COMINT – at the time the Coordinator for Joint Operations, shortly to become the Armed Forces Security Agency. Thus USAFSS hoped to be insulated from any sort of outside control, which it regarded as bald interference in its affairs.[16]

THE CJO

The lack of central control for COMINT was the most pressing problem of the postwar years. Cooler heads recognized that the uncoordinated and fractionalized efforts that had existed since the 1920s simply had to be better controlled. They had already agreed on a committee system, at that time called STANCIB and STANCICC. The committees could and did arrive at policy decisions which, in the case of unanimity of the board, were binding on the services. What was still lacking, though, was an executive organization to carry out the routine business of central coordination.

In early 1946 the Navy proposed such an executive body. They called it the Coordinator for Joint Operations, and it was to work out routine intercept coverage and processing responsibilities between the services. The Navy got Army concurrence, and on 15 February STANCIB approved the proposal. The Coordinator for Joint Operations, or CJO, was born.[17]

The CJO was to implement general policies on allocation of joint tasks as approved by STANCIB. It was to be assisted by three groups: the Joint Intercept Control Group (JICG), the Joint Processing Allocation Group (JPAG) and the Joint Liaison Group (JLG).

The CJO agreement owed its existence to the two most influential sponsors, Joseph Wenger (who commanded OP-20-G) and Preston Corderman (chief, ASA) for the Army, and it was in those days referred to as the "Corderman-Wenger Agreement." But when the first CJO was appointed, it turned out to be Colonel Harold G. Hayes, a long-time Army COMINTer and the new chief of ASA.

The first task of the CJO was to allocate intercept tasks. This was not as easy as it appeared. Agreement was reached that counterpart targets were to be copied by the respective U.S. service cryptologic organization. All other targets, even those being intercepted entirely by a single service, were to be considered "joint." The CJO then reallocated the intercept responsibilities. This had the largest potential impact on the resources of the Navy, which during World War II, as previously discussed, completely gave up "joint" targets (with a few exceptions) to the Army.

Intercept allocations really got down to priorities. With limited resources (and in 1946 resources were constrained), the key to obtaining copy was in the priority system. In September of that year USCICC decided to hold monthly meetings to consider priority problems. By this process a standing priority list, in rather general terms, was established. The CJO then made intercept assignments to positions in the field. When the CJO assigned a joint case to a position it controlled (i.e., one which had been turned over by one of the Service Cryptologic Agencies, as they were then called) there was no problem. But occasionally the CJO assigned a joint target to a service-protected position. This invariably met with resistance, and the CJO had no enforcement authority. The Service Cryptologic Agencies (SCAs), for their part, insured that counterpart positions were manned with the best operators, that they were never left uncovered, and that technical data were always up to date. In short, if a target had to be slighted, it was likely to be the joint target. The servicemen never forgot whom they worked for.

CJO also allocated processing tasks through the JPAG. Since people and equipment for processing were in very short supply, processing on each major target was to be done in only one place – either Arlington Hall or Nebraska Avenue – no matter which service collected the traffic. In those days communications systems were mutually exclusive rather than common and interlocking, and once traffic was intercepted by one service, it had to pass vertically through those communications channels all the way to Washington. This meant that there had to be communications between Nebraska Avenue and Arlington Hall so that the traffic could be exchanged, and under CJO a teleprinter link was set up. The services had a great deal of difficulty talking to each other (electrically, not to mention in person), and it was a real effort to establish common cryptographic gear for interoperability. In the late 1940s this process was just getting started.

Communications security policy was, if possible, even more difficult to meld into a cohesive system than was COMINT. Through the war each service handled its own COMSEC matters with little reference to joint policy. In the Army, ASA was responsible for both COMINT and COMSEC, a development substantially influenced by such technicians as Frank

Rowlett and William Friedman. In the Navy, COMSEC had begun within Captain Laurance Safford's embrace, but it had eventually become part of a separate organization under Naval Communications, called OP-20-K.

After the war, COMSEC policy was allocated by an unregistered executive order to a Cryptographic Security Board consisting of the secretaries of state, war, and navy. This very high-level board quickly became moribund, and the real actor in COMSEC policy was the Joint Communications-Electronics Committee (JCEC) and its subordinate, the Joint Security and Cryptographic Panel. When COMINT was unified in 1949 under the Armed Forces Security Agency (AFSA), COMSEC was still decentralized.

The CJO was a compromise between those who wanted tight central control and those who wanted to continue a loose arrangement. It was voluntary, as had been all of its predecessors. It never resolved the conflict over joint targets, much to the dismay of the State Department, which was the principal customer for most of those targets. But the establishment of an executive organization was the first step in creating an organization to control COMINT. It didn't work, but it pointed the way toward the future.

THE CRYPTOLOGIC ALLIES

America's SIGINT relationship with Great Britain also dates to World War II. In July 1940, the British ambassador to Washington, Lord Lothian, proposed that the two nations exchange information on, among other things, technological secrets related to "submarine detection and radio traffic." This appears to have pertained generally to SIGINT, but the wording of the now famous Lothian Letter did not really say precisely what he (or Churchill) meant. It also appears that day-to-day intelligence cooperation predated the Lothian Letter, for in April of the same year President Roosevelt met Churchill's special envoy William Stephenson to discuss a plan for secret cooperation between the FBI and British secret intelligence. According to a fascinating account in the somewhat unreliable book by William Stevenson (unrelated to the wartime William Stephenson), it was at that meeting that Stephenson informed Roosevelt of British progress in breaking the German ENIGMA system. (This might have happened but was quite out of character for the security-conscious British.) This meeting did, in fact, lead to the establishment of the British Security Coordination (BSC) in Washington, with Stephenson in charge. During its early days this organization dealt primarily in HUMINT and counterintelligence.[18]

The Lothian Letter was followed in August by a visit by Sir Henry Tizard, scientific advisor to the Royal Air Force (RAF). This inaugurated a series of technical discussions on a wide variety of subjects. Tizard, not a SIGINTer, was mainly interested in discussing radar and other such technical developments. At the same time, the United States sent to Britain a delegation consisting of Brigadier General George V. Strong (Chief of War Plans), Brigadier General Delos Emmons (United States Army Air Forces –

USAAF), and Rear Admiral Robert Ghormley (Assistant Chief of Naval Operations). Though the discussions were to be general, it appears that Strong had, or thought he had, considerable latitude to discuss cryptologic intelligence. On 5 September he cabled Washington to propose a total exchange of information on SIGINT product and technical matters (i.e., cryptanalysis). Back in Washington there was a good bit of concern. The Navy said "No," while the Army vacillated. Their top cryptanalyst, William F. Friedman, was consulted. Friedman favored the exchange.

So initial hesitance was eventually converted to approval, and on the day after Christmas 1940, the Army decided once and for all to initiate a complete cryptologic exchange with the British. In February 1941, Captain Abraham Sinkov and Lieutenant Leo Rosen of the Army's SIGINT organization, along with Lieutenant Robert Weeks and Ensign Prescott Currier of the Navy, sailed to London. They brought with them a PURPLE Analog, a machine the Army was using to break the keys for the Japanese diplomatic cipher system. They had instructions to initiate a complete exchange of cryptanalytic and SIGINT information.[19]

The British appear to have been flabbergasted. Never had they anticipated that the United States would simply walk in and plunk down their most secret cryptanalytic machine. This was, indeed, an intelligence exchange worth the money. But they were cautious. They did not tell the Army and Navy emissaries everything they were doing, and they did not show them the ENIGMA operation at first. Agreed upon in principal in 1940, the complete exchange of cryptologic information and techniques progressed slowly through the war. Once again the Navy, reluctant in the beginning, produced the more beneficial exchange. This was due largely to historical circumstances. The Army was still mobilizing and clearly would not see action in Europe until at least late 1942, if not later. But the Navy was already engaging German U-boats in the North Atlantic. They and the British had worked out a convoy system, and daily cooperation in intelligence was essential to avoiding wolf packs. Thus it was that Commander Roger Winn, who headed the Operational Intelligence Center in the Admiralty, convinced the U.S. Navy that it must have something similar. Prompted by Winn, the U.S. Navy established the mysterious organization called F-21 (Atlantic Section, Combat Intelligence Division, U.S. Fleet) and its still more mysterious submarine tracking room. The latter used all sources of intelligence, including U-boat positions obtained by ENIGMA decrypts, passed to them by the British.

The arrangement worked well at first, but in February 1942 the Germans introduced the four-rotor ENIGMA, and the British at Bletchley were unable to read it. The Americans were already suspicious because the British kept the cryptanalytic techniques so closely held. So in 1942 the Navy embarked on a project to break the ENIGMA themselves, in defiance of British protests. Colonel John Tiltman, a temporary GC&CS resident in Washington, finally convinced the British that the Navy would proceed with or without British help. In June 1942, after Tiltman's intervention, the Navy sent two expert

cryptanalysts, Lieutenant R. B. Ely and Lieutenant Junior Grade Joseph Eachus, to Bletchley to learn all they could about ENIGMA processing. In September the Navy began a project to build a four-rotor ENIGMA processor (called a "bombe" by the British). When, in the summer of 1943, the Navy moved to its new headquarters on Nebraska Avenue, a major portion of the space was reserved for the bombes, which were being employed to break the keys on German submarine ENIGMA traffic. In the end, the two nations drove the U-boats from the North Atlantic, based in part on information provided by the bombe project.

Meanwhile, the Army was having its own problems on the SIGINT front. Increasingly suspicious of British reluctance to share cryptanalytic techniques, they retaliated by refusing to share information on voice ciphony equipment with Alan Turing. Since Turing was one of the top Bletchley scientists (and has been given credit for developing the first British bombe), this was a very serious breakdown in cooperation. It became the subject of a long series of exchanges between General George Marshall and Sir John Dill (chairman of the British Joint Chiefs of Staff), and at one point it seemed possible that the two sides might break COMINT relations. The dispute was resolved in 1943 when the British agreed to allow a total technical exchange. The agreement was hammered out during a series of sessions between Military Intelligence Service and Commander Sir Edward Travis, who headed GC&CS, during Travis's trip to Washington in May. The paper specified that the United States would be responsible for the COMINT problem in the Far East, while the British would worry about Europe. To implement this, it was agreed that the Americans would send a team of cryptologists to Bletchley to work side by side with the British in all aspects of COMINT, including cryptanalysis of the ENIGMA. That way the Americans would gain technical expertise on the system without mounting a competing cryptanalytic effort on the American side of the Atlantic.

To begin the new relationship, the Army sent a three-man team consisting of Colonel Alfred McCormack, William Friedman, and Lieutenant Colonel Telford Taylor to Bletchley. By mutual agreement, Taylor was left behind in London to serve as a liaison officer and to act as a funnel for British COMINT being sent to the War Department in Washington. Taylor's job was not easy, as there was a good deal of second-guessing the British forthrightness in the exchange. But as the war progressed it became smoother and eventually became a very open exchange of highly sensitive information.

With the Axis almost defeated, the thoughts of cryptologists in 1945 turned with increasing frequency to the Soviet Union. Both nations had maintained rudimentary efforts against the "Communist menace" since the 1920s, and they both kept small efforts even during the war. In June of 1945 ANCIB proposed to the British that they extend their wartime cooperation to the intercept and exploitation of their erstwhile but distrusted ally. They called the project BOURBON, and it was kept compartmented for the obvious reason that the Soviets were still officially on our side. The arrangement was largely informal and involved the exchange of liaison units on both sides of the Atlantic.

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

But in September, with the war officially over, the U.S. had a legal problem. Could it now continue to collaborate with its British allies? Clearly, the American cryptologists, good as they had become, still regarded GC&CS with a certain awe. In many cryptanalytic areas the British were still ahead of us, and their organization of the COMINT system was superb. And of course there was the problem of the Soviet Union. Already the wartime alliance had disintegrated. In September of 1945 both the Army and Navy suggested to President Truman that collaboration with the British continue for the present "in view of the disturbed conditions of the world and the necessity of keeping informed of the technical developments and possible hostile intentions of foreign nations. . . ." In reply, Truman signed a brief, single-sentence note sent to him by the Joint Chiefs of Staff:

> The Secretary of War and the Secretary of the Navy are hereby authorized to direct the Chief of Staff, U.S. Army, Commander-in-Chief, U.S. Fleet, and Chief of Naval Operations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify, or discontinue this collaboration, as determined to be in the best interests of the United States.[20]

Now that the American side was officially unleashed to collaborate with the British, it seemed necessary to write a bilateral agreement for the postwar years. After months of meetings and conferences, the two sides sat down in March 1946 to sign the British-U.S., or BRUSA, Agreement. The paper which charted the future course of both countries was only four pages long. (The policy conference at which it was signed was followed by a technical conference which wrote all the fine print appearing later as annexes and appendices.)

With the signing of the BRUSA Agreement, the BOURBON liaison offices on both sides of the Atlantic became representatives of STANCIB and LSIB, The BOURBON officer, Commander Grant Manson, was invested with the rather cumbersome title of U.S. Liaison Officer, London SIGINT Centre (LSIC, as GC&CS was then known) – or USLO LSIC. He reported to STANCIB through the deputy coordinator for Liaison, part of the new CJO structure. In early 1946 the British moved LSIC from its wartime location at Bletchley to Eastcote, outside London, and began using a new title, Government Communications Headquarters, or GCHQ. Space for Manson was provided at Eastcote. The BOURBON

liaison office had maintained an office in London, and Manson had to cover two locations, in Eastcote and London. (This situation continues to this day, with NSA holding offices in both London and Cheltenham.) USLO never controlled the TICOM group, which also found quarters at Eastcote.[21]

The British, meanwhile, had a more difficult problem. While the U.S. dealt with only one COMINT organization, GCHQ, the British had two – the Army at Arlington Hall Station and the Navy at Nebraska Avenue. Not wishing to choose, the British diplomatically located their liaison officer in the State Department building in downtown Washington. (They did, however, maintain a technical staff at Arlington Hall.) Their first liaison officer was Colonel Patrick Marr-Johnson, who had signed the BRUSA Agreement for the British side. When he retired in 1949, he was succeeded by Tiltman, who was already well known to the Americans and had served for a time as Travis's deputy at GC&CS. This began a practice, continued to this day, of assigning very senior cryptologic officials to the respective liaison offices, and the USLO eventually became SUSLO – Senior U.S. Liaison Officer.[22]

And where were the British Dominions in all this? They were mentioned in the BRUSA Agreement, and it was agreed that they would not be termed Third Parties, but they were not direct and immediate partners in 1946. Arrangements that Great Britain might make with them would be communicated to STANCIB. STANCIB, in turn, would make no arrangement with a Dominion without coordination with LSIB. Thus the now-famous UKUSA Agreement was not that at all, at least to begin with. It was a BRUSA Agreement. How it became the UKUSA Agreement was a development that spanned another eight years.

Of the three dominions with which the Americans eventually associated, the relationship with Canada began first. Canadian-American SIGINT cooperation appears to have begun in 1940, in the form of service-to-service collaboration between the respective armies and navies. These decentralized arrangements were eventually overtaken by a centralized relationship centering on the Examination Unit of the National Research Council, established in 1941 as one of those clever cover terms denoting a Canadian SIGINT organization. Its purpose was to decode traffic to and from the Vichy delegation in Ottawa. This unit's control was gradually broadened until it was the dominant force in Canadian cryptology. (It was the linear predecessor of the postwar organization Communications Branch, National Research Council [CBNRC] and its successor, Communications Security Establishment [CSE].) By 1943 it had its own submarine tracking room and was receiving plots from the British based on ENIGMA decrypts. When the British began cooperating with the U.S. in 1941, they requested that the U.S. bring the Examination Unit into the scope of the cooperation. But the Americans were leery. They knew that the Examination Unit had been established by Herbert O. Yardley, the renegade American cryptologist who had published cryptologic secrets in 1931 in *The American Black Chamber*. The Signal Intelligence Service, which had been victimized by Yardley's revelations, informed the

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

British that they were willing to cooperate only if Yardley were let go. The British, holding no brief for Yardley, had the Canadians get rid of him, and collaboration with the Americans flowered. By April of 1942 details of the Canadian-American cooperation were hammered out. Collaboration was particularly close in direction finding (DF) of German naval vessels.

[redacted] But the United States was suspicious; Canada had just been through a major spy scandal, the Gouzenko affair (chapter 4), and USCIB wanted to go slow. Making matters worse was the head of the Canadian policy committee on COMINT, a rather prickly character [redacted] refused for several years to adopt some of the security procedures which the United States and Great Britain had agreed upon at the BRUSA Conference. Moreover, while the United States wanted a formal document on COMINT cooperation, [redacted] did not. After several years of very difficult negotiations, the two countries finally agreed to exchange letters between [redacted] and USCIB chairman Major General C. P. Cabell. Thus [redacted] won the battle of the legal documentation while the United States got its way on security procedures.[23]

(b) (1)

Furthest from the mainstream were the Australians. British-Australian COMINT collaboration appears to have begun in the late 1930s when a small Australian cryptographic organization under the Director of Naval Intelligence began working with the British Far Eastern Combined Bureau (FECB) in Singapore. In early 1940 an Australian naval commander named T.E. Nave set up the nucleus of an Australian SIGINT group in Melbourne, which was the origin of the modern Australian SIGINT organization. Its most important organization was the Central Bureau, set up in April 1942 as a combined Australian-American COMINT group. When the Americans departed in 1945, the Australian remnant of Central Bureau became Defence Signals Bureau (DSB).

The British were determined that DSB should enjoy the same status on BOURBON as the Canadian, and, immediately after the war, began including the Australians in their technical exchanges. But in 1947 this procedure became embroiled in a lengthy dispute over Australian security practices. The procedures in dispute were arcane, and the origins were almost as difficult to fathom, but both apparently originated with a spy scandal.

In 1947 SIS succeeded in decrypting some KGB messages which had been sent more than a year earlier and which contained certain classified British military estimates. The messages came from the Soviet embassy in Canberra, and it was immediately assumed that an Australian was passing classified information. The British, alerted by the Americans, sent Sir Percy Sillitoe, chief of British Secret Service, to Australia to discuss this with the prime minister. Sir Percy was under instructions to conceal the origins of the information, and when the prime minister, a Laborite named Chifley, demanded proof, Sillitoe mumbled something rather lame about a possible mole. After considerable

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

discussion, Chifley agreed to establish a new Australian security organization, called the Australian Security Intelligence Organization.

With the Australian security house supposedly in order, the British prime minister, Clement Attlee, intervened with President Truman to get a new hearing of the Australian matter. Attlee complained in a letter to Truman that:

> The intermingling of American and British knowledge in all these fields is so great that to be certain of denying American classified information to the Australians, we should have to deny them the greater part of our own reports. We should thus be placed in a disagreeable dilemma of having to choose between cutting off relations with the United States in defence questions or cutting off relations with Australia.[24]

With matters at the crisis level, Attlee proposed to Truman that Sir Francis Shedden, the powerful and respected Australian defense minister, visit the United States to plead the case. Truman accepted, and Shedden visited Washington in April. But he was unable to sway USCIB, and the British were back to their dilemma – whether to choose the United States or the Commonwealth as allies. In 1949 the outcome was anything but certain.

Then one of those unexpected quirks of fate intervened which was to save the day: the Labor government under Chifley went down to defeat at the polls, and Robert Menzies formed a new Liberal-Country Party coalition in December. The conservative Menzies was able to successfully disassociate his government from the leftist elements of the Labor government. This was critical since the actual source of the leaks was known (through the VENONA project; see chapter 4) to be two leftists within the Australian diplomatic corps. With a Conservative government in power, USCIB authorized a limited resumption of cryptologic exchange with Australia. Full resumption of ties did not occur until 1953. The incident tarnished American-Australian intelligence cooperation for years and caused a serious rift with Britain which was made worse just a few years later with the Klaus Fuchs case and the Burgess and McClean defections. It also had a deleterious affect on early U.S. SIGINT efforts against the People's Republic of China (PRC).[25]

By 1953 relations had warmed to the point where Australia was reincorporated as a full COMINT partner. The foundations of the Australian participation in the UKUSA Agreement (the name BRUSA was changed at British request a year later) came at the Melbourne Tripartite Conference of September 1953.

New Zealand came in as a fifth partner, New Zealand had contributed mainly DF to the Allied cryptologic effort in World War II and had sent people to Australia to serve with the Commonwealth effort in Brisbane.

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

Notes

1. Ronald Lewin, *The American Magic: Codes, Ciphers, and the Defeat of Japan* (New York: Farrar, Straus and Giroux, 1982), 24.

2. Robert L. Benson, "A History of U.S. Communications Intelligence during World War II: Policy and Administration," manuscript pending CCH publication. Hereafter Benson "History."

3. Ibid.

4. Ibid.

5. Ibid.

6. George F. Howe, "The Narrative History of AFSA/NSA," part I, unpublished manuscript available in CCH. Hereafter Howe "Narrative."

7. Ibid.

8. USNSG, "U.S. Naval Communication Supplementary Activities in the Korean Conflict, June 1950 – August 1953," in CCH Series V.M.3.1.; Benson"History"; SRH 149, Records of the National Security Agency, Record Group 457, National Archives, Washington, D.C.; oral history interview with RADM Earl E. Stone, 9 Feb 1983, Carmel, California by Robert D. Farley, NSA OH 3-83.

9. NSA retired records, CACL 60, TVC 1317; [Edward S. Wiley] *On Watch: Profiles from the National Security Agency's Past 40 Years* (Ft. Meade: NSA/CSS, 1986), 13.

10. CCH Series VI.1.1.1.; X.H.7.5.

11. Oral history interview with Dr. Abraham Sinkov, May 1979, by Arthur J. Zoebelein, [redacted] Dale Marston, and Samuel Snyder, NSA OH 2-79; Howe, "Narrative."

12. Oral history interview with Col. (USAF Ret.) John P. Shean, 18 April 1984, by Robert D. Farley, NSA OH 16-84; memo to Chief, AFSA-90, 14 Dec 1948, in CCH Series V.C.2.12.

13. NSA/CSS Archives, ACC 26350, CBSK 32.

14. Philip S. Meilinger, *Hoyt S. Vandenberg: The Life of a General* (Bloomington, Ind.: University of Indiana Press, 1989).

15. NSA/CSS Archives, ACC 26350, CBSK 32; oral history interview with Gordon W. Sommers, Hqs ESC, January 1990, by Millard R. Ellerson and James E. Pierson; Richard R. Ferry, "A Special Historical Study of the Organizational Development of United States Air Force Security Service from 1948–1963," Hq USAFSS, 1963.

16. "An Oral History Interview: The Electronic Security Command – Its Roots; Featuring the Founder of USAFSS/ESC, Lt. Gen. Richard P. Klocko (USAF, Ret)," Hqs ESC, 20 October 1989.

17. The history of the CJO is covered in detail in Howe, "Narrative," and in Thomas L. Burns, *The Origins of the National Security Agency, 1940–1952*, United States Cryptologic History, Series V, Vol. I (Ft. Meade: CCH, 1990). Hereafter Burns, *Origins*.

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

18. NSA/CSS Archives, ACC 16824, CBTB 26; Jeffrey T. Richelson and Desmond Ball, *The Ties that Bind* (Boston: Allen and Unwin, 1985), 136-7. Hereafter Richelson, *Ties.*

19. "A Chronology of the Cooperation Between the SSA and the London Offices of GCCS," 2 June 1945, CCH Series VI.V.7.2. In addition, the entire Army-British and Navy-British relationships during the war are covered in detail in Benson, "History."

20. CCH Series V.A.29. The early collaboration with the British on the Soviet problem is covered in George F. Howe and [redacted] "Historical Study of COMINT Production Under the Joint Operating Plan, 1946–1949," in CCH Series V.E.1.1., and in Michael Peterson, "Early BOURBON – 1945. The First Year of Allied Collaborative COMINT Effort against the Soviet Union," *Cryptologic Quarterly* (Spring 1994).

21. See Howe, "Narrative"; Burns, *Origins*; Benson, "History"; Peterson, "Early BOURBON"; and CCH Series VI.J.1.2.

22. "Origins of the SUSLOs," in CCH Series X.H.8.

23. "Historical Summary of U.S.-Canadian COMINT Relations," 12 April 1949, in CCH Series V.J.3.; NSA/CSS Archives, ACC 16824, CBTB 26; Richelson, *Ties*; oral history interview with Frank B. Rowlett, various dates, by Henry F. Schorreck and [redacted] NSA OH 14-81. See also Howe, *Narrative*, and Benson, "History."

24. Copies of papers from the Harry S. Truman Presidential Library in Independence, Missouri, in CCH Series XVI.

25. The early problems between the U.S. and Australia in COMINT cooperation is covered in Richelson, *Ties*; Howe, "Narrative"; Benson, "History"; copies of papers from the Dwight David Eisenhower Presidential Library in Abilene, Kansas, contained in CCH Series XVI. Specific information about the Australian spy scandal and its impact on COMINT collaboration is covered in Christopher Andrew, "The Growth of the Australian Intelligence Community and the Anglo-American Connection," *Intelligence and National Security* (April 1989), V. 4, # 2: 213-256; Robert Manne, *The Petrov Affair: Politics and Espionage* (Sydney: Pergamon, 1987); and Desmond Ball and David Horner, "To Catch a Spy: Signals Intelligence and Counter-espionage in Australia, 1944–1949" (Canberra: Strategic and Defence Studies Centre, Australian National University, 1993), pending publication.

26. Vincent Las Casas, *NSA's Involvement in U.S. Foreign SIGINT Relationships through 1993*, United States Cryptologic History, Series VI, Vol. 4 (Ft. Meade: CCH, 1995).

Chapter 2
AFSA and the Creation of NSA

The formation of AFSA resulted from both technical and budgetary causes. The technical concerns were first surfaced within the Army Security Agency (ASA) over the conclusions of a study on World War II German SIGINT done by the Target Intelligence Committee (TICOM – see chapter 1). TICOM had studied the German failure to crack high-grade Allied codes and ciphers and concluded that it resulted from a badly fragmented effort. The Germans mounted at least five different cryptanalytic efforts. Each competed for resources and attention, and each jealously guarded its resources and techniques from outside encroachment.[1]

The result was failure. As Frank Rowlett, perhaps the leading ASA cryptanalyst in 1948, said, "they all skimmed the cream off and they did the easy ones and nobody, none of them, were [*sic*] ever able to concentrate on the more important and more secure systems and bring them under control."

THE STONE BOARD

The disastrous results of German cryptologic competition spurred Rowlett and his associates to press for unification of the American effort. In 1948, under the direction of Brigadier General Carter Clarke, Rowlett chaired a committee to write a paper proposing cryptologic unification. The committee included some of the leading names in subsequent American cryptology, including Herbert Conley, Benson Buffham and Gordon Sommers. Rowlett's concerns were mainly technical. With so many good cryptanalysts leaving the services, there was a greater need than ever to concentrate resources. Fragmentation would guarantee the same fate that had met the Germans. This technical argument had been supported in 1946 by the results of the Congressional Pearl Harbor Committee, which, as part of its final report, recommended cryptologic unification.[2]

Army secretary Kenneth Royall was persuaded to support unification, but at his level the concerns were mainly financial. Royall was concerned that the formation of the new U.S. Air Force Security Service (USAFSS or simply AFSS) would mean a smaller slice of the monetary pie for ASA. His report convinced Secretary of Defense James Forrestal, who in August of 1948 established a DoD-level committee to look into the matter of cryptologic unification. Although the committee contained members of the intelligence establishments of all three services, it became known as the Stone Board, after its chairman, Rear Admiral Earl E. Stone, the director of Naval Communications.

Rear Admiral Earl E. Stone, Director, Naval Communications

The Stone Board was anything but harmonious. The Navy was dead set against unification, and Stone was the "chief arguer" (in his own words) against the concept. He got the Air Force behind him, and the result was a majority report arguing against the very concept it had been set up to consider. That report agreed to certain reforms in the current CJO (Chief of Joint Operations; see chapter 1) set-up, but refused to endorse any sort of thoroughgoing restructuring. The Army report favored cryptologic unification under a single agency, but it was only a minority report. The two documents were sent to Forrestal. Since the majority report favored a sit-tight approach, nothing happened, and the results of the Stone Board languished in a desk drawer until after the death of Forrestal in March of 1949.[3]

It is important to understand what was going on at that time. The interservice rivalry which had characterized American conduct of World War II had led to calls for service unification. The first step toward a reform of the U.S. military structure was the National Security Act of 1947, which established the Secretary of Defense, the National Security Council, and the CIA. Although all three institutions have become very powerful, in the early years they were not, and gaining control of their respective domains was a process marked by fierce rivalry and bitter infighting.[4]

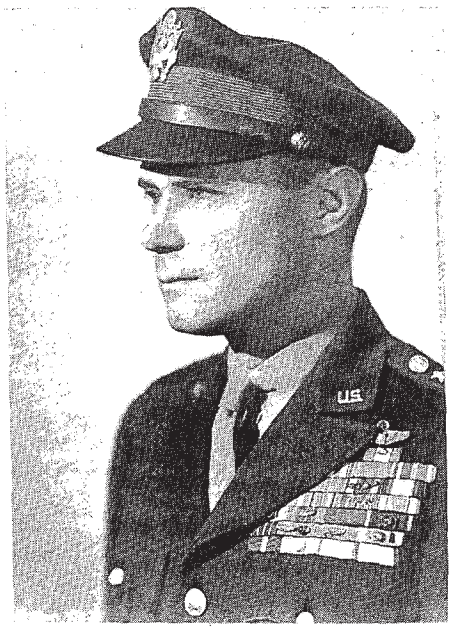
The new secretary of defense, Louis P. Johnson, arrived at the Pentagon during the worst of these interservice clashes. Cryptologic unification was one of the most hotly contested issues. The protagonists did not leave him alone very long. Carter Clarke pushed Johnson hard on the issue. According to Clarke's own description, he approached one of Johnson's top aides, General Alfred Gruenther, to resurrect the Stone Board documents. Clarke argued that lack of unification was partly responsible for the failure at Pearl Harbor. Johnson, apparently impressed by this, called in General Joseph T. McNarney, a known supporter of unification. McNarney wrote a report which recommended creation of a central organization, called the Armed Forces Security

Louis A. Johnson, secretary of defense in 1949

Agency, but which retained the separate cryptologic organizations of the three services. The report was then discussed at a JCS meeting on 18 May 1949. At this meeting the Air Force chief of staff, General Hoyt S. Vandenberg, changed the Air Force vote to pro-unification. The minority had suddenly become the majority, and it was clear that unification was to be forced through. The Navy quickly reversed its vote, too, and the decision to create AFSA was unanimous.

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

Why did Vandenberg change the Air Force vote? He may have seen the creation of AFSA as an essential ingredient in better intelligence, but he may also have felt that he could keep the fledgling USAF Security Service effectively independent. Vandenberg's central concern in those days was to establish a strategic strike force (Strategic Air Command, or SAC) which would be supported by an all-Air Force intelligence center. He regarded SIGINT as the key ingredient in such a creation and wanted to place a SIGINT analysis center within USAFSS which would be beyond the control of AFSA. It is possible that he changed the Air Force vote after assurances that USAFSS would be permitted to establish such a center. (This center, called the Air Force Special Communications Center, was actually created, and it resided at Kelly Air Force Base, home of USAFSS, for many years.) The later creation of the [redacted] a device to keep intercept facilities independent of AFSA, might also have been part of such a plan. Vandenberg's thinking was probably also influenced by log-rolling in other areas, and may have represented an attempt to obtain Army support for other Air Force programs by yielding on the cryptologic issue.[5]



Hoyt S. Vandenberg
Provided the "swing vote"
that created AFSA

AFSA

And so the Armed Forces Security Agency was created on 20 May 1949. It was promulgated by JCS directive 2010. AFSA was thoroughly military, and, because it answered to the JCS, its central concerns were all military. Organizations outside the JCS got short shrift in the collection of intelligence. State Department and CIA were intensely

unhappy with this development, but they lacked the power to wrench AFSA out of the military chain of command.

AFSA began life in borrowed quarters. Its people, just over 5,000 in the beginning, occupied spaces in Arlington Hall and the Naval Security Station on Nebraska Avenue, sharing space with the Army Security Agency and Naval Security Group from which the space was obtained. Admiral Stone decided that the Naval Security Station would be used by AFSA for COMSEC, while the COMINT mission would be done at Arlington Hall. This decision began a historic physical separation between SIGINT and COMSEC which has never been completely bridged, despite the later move to Fort Meade. It was logical, though. Naval Security Group (NSG; formerly OP-20-G) was strong in the COMSEC discipline. Moreover, the Naval Security Station (NSS) at Nebraska Avenue had only about one-fourth the space available that Arlington Hall did, and this disparity in size meant that NSS was about the right size for COMSEC, while the larger spaces at Arlington Hall would be ideal for COMINT. There was a certain amount of shuffling back and forth as COMINTers from NSS moved their desks to Arlington Hall and COMSEC people from Arlington Hall transferred to NSS. But when it was finished, all the COMSEC people were housed in almost 214,000 square feet of office space at NSS, while the COMINT operations were lodged in 360,000 square feet at Arlington Hall. Including administrative, storage and machine space, there were only 79 square feet per worker at the Hall, but about 98 square feet at NSS.

Workers often sat at tables rather than desks, in large warehouse-like rooms, cheek-by-jowl, as they worked complex code or callsign systems. Floors were tiled and the noise level was high. There was practically no air conditioning, and in the summertime it was common to close down for the day when the ratio of temperature to humidity got too high.

AFSA owned two other facilities. The cryptologic school, a rudimentary training ground used originally to keep newly hired workers busy before their clearances came through (see p. 71), reposed in a structure on U Street Northwest in the District of Columbia. The Agency also maintained a courier facility at National Airport, then called Congressional Airport.[6]

The impact of AFSA on the services was immediate and severe. Besides turning over more than 600,000 square feet of space to the new organization, the Army and Navy had to donate about 80 percent of their existing Washington-area billets – 79 percent for ASA and 86 percent for NSG. Although ASA kept many of its uniformed service people, its corps of over 2,500 civilian experts was turned over to AFSA virtually intact. This made the Service Cryptologic Agencies little more than collection organizations, with practically no central processing – all arms and legs, but no body. This revolution was accomplished virtually overnight with only minimal dissension and was AFSA's most noteworthy success.

Analytic section,
Arlington Hall Station

The sole exception to this trend was USAFSS. The Air Force cryptologic agency practically seceded, opening its first headquarters at Brooks AFB, Texas, 1,600 miles away from the menace of centralization. Even more startling, it was required to donate only thirty officers, twenty civilians, and eighty enlisted billets to AFSA. So when USAFSS opened its processing center, it had plenty of billets to do it with. If this was what Vandenberg had in mind, it was working.[7]

AFSA organization reflected service competition. The director was to be chosen from among the three services on a rotating basis, and its first director was its most ardent opponent, Earl Stone. Assisting him were three deputy directors, one for each service. Below them were four major divisions, which have survived to this day – Operations,

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

Research and Development, COMSEC, and Administration. The office designator system was numerical, so that Operations was AFSA 02, R&D was 03, COMSEC was 04, and Administration was 05. Each of the military deputy directors also had a sphere of influence. The Navy deputy director, Captain Joseph Wenger, controlled COMINT, while the Army deputy, Colonel Samuel P. Collins, supervised COMSEC, and the Air Force deputy, Colonel Roy Lynn, handled administrative matters.[8]

The field collection effort consisted of the intercept sites which had survived the budget cuts after World War II. Army Security Agency had seven sites: Vint Hill, Virginia; Petaluma, California; [redacted] Helemano, Hawaii; [redacted] Fairbanks, Alaska; and Clark AFB in the Philippines. The Navy had twelve: [redacted] Adak, Alaska; [redacted] Dupont, South Carolina; [redacted] Skaggs Island, California; Cheltenham, Maryland; [redacted] The Air Force had ten mobile units, whose status and location were somewhat vague. Finally, ASA had six SHAMROCK units, whose task was to screen commercial cable messages turned over to ASA by the cable companies under an arrangement which had existed since World War II.[9]

Field intercept was the rock that sank AFSA. In theory all the intercept positions were to be under AFSA control. In fact, some were not. Of the 763 intercept positions existing at the time AFSA was dissolved, 671, including all the Army positions, were under some form of AFSA control. Just over 100 were reserved by the Navy for fleet support and were thus completely beyond AFSA tasking authority. But even the positions under AFSA control could be tasked only by treading a complex paper mill by which tasking was routed through the SCAs, rather than being levied directly. This was true especially in the Navy and Air Force – the Army was more accommodating and permitted some form of direct tasking.

Completely beyond AFSA purview, however, were the mobile intercept stations. In theory, these were small mobile efforts for direct tactical support. But AFSS flouted AFSA control by simply designating all their stations as "mobile." Thus even the most permanent and sedentary station was designated as a "radio group mobile" or a [redacted]" beyond AFSA control. The Army and Navy quickly caught on, and by 1952 ASA had seven mobile units, while the Navy had three.

AFSA's lack of tasking authority over Air Force positions was intolerable, and late in 1950 Major General C. P. Cabell, Air Force director of intelligence, and Rear Admiral Stone signed an agreement granting AFSA the authority to task automatic Morse and radioprinter positions, while USAFSS retained control over voice. The Morse positions

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

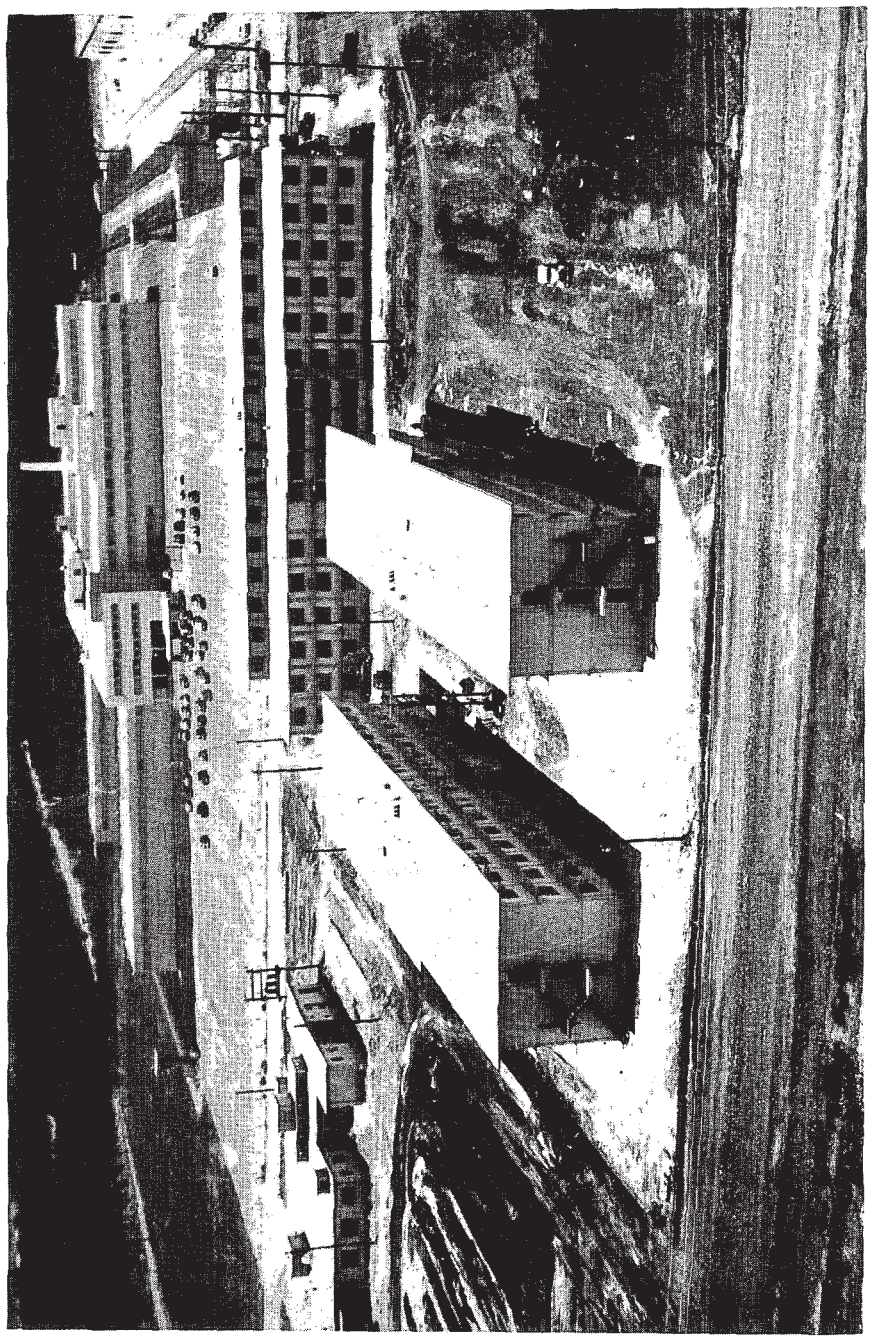
(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

were split 50/50. Still later, in 1951, this arrangement was changed when the new director of AFSA, Lieutenant General Canine, and Colonel Lynn of USAFSS signed an agreement dividing the Air Force positions down the middle, regardless of mode of intercept.

Meanwhile, USAFSS established its headquarters in San Antonio – first at Brooks AFB and later at nearby Kelly AFB, on a low rise west of the runway which is now known as Security Hill. Within its headquarters it proceeded to establish a Stateside COMINT processing center, Air Force Special Communications Center (AFSCC). This was done despite direct orders by Canine that it not be established. AFSA also directed that USAFSS not establish third-echelon processing on the [redacted] target, but USAFSS did it anyway. Air Force defiance fragmented the processing effort and had much to do with the demise of AFSA. Despite this, AFSCC continued to process on the [redacted] target until the late 1960s, when it was finally turned into an electronic warfare center.[10]

Service rivalry led to duplication. During the early days of the Korean War, for instance, both ASA and USAFSS covered the Soviet and Chinese air problems in the Korean area, and ASA did not discontinue its coverage until March of 1952, after many months of AFSA mediation. Likewise in the DF area, AFSA was unable to force a common DF net control for the Korean problem for more than a year. Ultimately the Navy kept its DF system separate. All three SCAs established second-echelon processing centers in the Pacific with or without AFSA blessing. Without firm control of SIGINT, there was simply no way to organize effectively. This lack of control attracted unfavorable reviews from the generals trying to fight the Korean War and played a part in the COMINT reorganization of 1952.[11]

The final blow to AFSA was the development of a policy mechanism outside of AFSA itself. It was called the Armed Forces Security Advisory Committee (AFSAC), and it was created by the same JCS directive that established AFSA. The original plan was for an advisory committee composed of nine members – three from each service – chaired by the director of AFSA. But the JCS gradually changed AFSAC's charter from advisory to directive. Had AFSAC possessed a proper decision-making mechanism, the conversion of its role to that of direction might have worked after a fashion. But the rules required unanimity on all substantive matters.[12] AFSAC was immediately immobilized by interservice disputes and was ineffective from the start. AFSA had become a body with no head.



USAFSS Headquarters, Kelly AFB, as it appeared in July 1953

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

One small success during these early years was the development of customer liaison organizations. By 1949 both the Army G2 and the Office of Naval Intelligence had established informal liaison offices with their cryptologic counterparts at Arlington Hall and NSS. When AFSA was established, these arrangements continued undisturbed. Both the Army and Navy groups developed a very close relationship with AFSA, and their people often worked in an intelligence production role. By the end of the Korean War, the Army organization, which called itself SRB (Special Research Branch), had some fifty people. Air Force Intelligence had a similar group, which was gradually subsumed by AFSS into a large organization of over sixty people performing both a customer (for Air Force Intelligence) and producer (for AFSS) role. Thus the Air Force group performed both as a producer and consumer, while the Army and Navy acted only as producers.

Both CIA and State maintained small offices within AFSA, under a USCIB edict of 1948. Although AFSA regulations permitted them to see semiprocessed intelligence, they never participated in the production process, maintaining their offices for liaison purposes only. FBI's refusal to establish any office at all reflected J. Edgar Hoover's adamant opposition to COMINT centralization.[13]

While COMINT was fractious, COMSEC was relatively serene. During World War II there had been a single authority for joint service communications matters, the U.S. Joint Communications Board, established in July of 1942. Its principal members were the chiefs of communications for the Army, Navy, and Air Force. In 1948 it gave way to a new organization, the Joint Communications-Electronics Committee (JCEC), which reigned supreme in this area for many years thereafter. The JCEC was concerned with communications planning, standards, and interoperability, but its charter by implication gave it a determining voice in COMSEC policy as well.

When AFSA was created, JCEC effectively transferred central COMSEC functions to it. The charter did not extend to non-JCS organizations, but the State Department and other civilian agencies with communications security concerns had for years relied on the Army and Navy for COMSEC support, and this reliance was transferred to AFSA. AFSA began producing codes and ciphers for all the armed services and many of the non-DoD agencies. In addition, it undertook centralized COMSEC R&D functions, planning and programming, setting of security standards, and technical supervision of the communications security activities of the armed services. The SCAs retained many residual functions, such as distribution of AFSA-produced codes, security monitoring of transmissions, and the like.[14]

While AFSA successfully controlled the highly technical function of COMSEC, it was never able to control COMINT. This lack of control made powerful enemies. The State Department was upset because, under AFSA, the number of positions allocated to [redacted] actually declined in the three years of AFSA existence, from 64 to 51, and from almost 17 percent of the total to only 6.5 percent.

~~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

THE BROWNELL COMMITTEE

The entire intelligence community was concerned over performance of the COMINT system in Korea. AFSA had not predicted the outbreak of war. A watch committee established under the wing of CIA in early 1950 listed Korea fifth on the list of world trouble spots, but this was not translated into action, and when the war began AFSA still had no positions allocated to Korean military.

15

Walter Bedell Smith
Director of Central Intelligence

AFSA had no more dangerous opponent than Walter Bedell Smith, director of Central Intelligence. In 1950 the wartime feud between the COMINT empire and Smith's HUMINT organization boiled over. On 10 December of that year Smith wrote a memorandum recommending that a committee be established to "survey" COMINT. Smith was "gravely concerned as to the security and effectiveness with which Communications Intelligence activities . . . are being conducted." He pointed to "the system of divided authorities and multiple responsibilities" which was endangering national security. The National Security Council in turn forwarded the recommendation to President Truman, who directed that a committee be formed.

The JCS could not take heart from the composition of the comittee. Its chairman was George A. Brownell, a New York lawyer and layman in intelligence matters. The members were Charles Bohlen, a prominent State Department official; William H. Jackson, special assistant to the DCI; and Brigadier General John Magruder, special assistant to the secretary of defense. Thus the Joint Chiefs, who owned the COMINT organizations, had no one on the committee. It was composed of "enemies," representatives from State and CIA – the two most vocal opponents of the existing system.

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

George A. Brownell

The Brownell Committee held fourteen days of formal sessions, which were backed up by many days of research and data-gathering. Its report was a scathing indictment of the old ways of doing business. Its bottom line stated bluntly that

> [redacted] The added difficulty of the problem under attack places a greater premium than ever on the quantity and quality of the physical and intellectual resources available, and on the efficiency and clarity of the organization charged with the task. While much has recently been done to provide adequate physical resources for the job, the Committee is convinced that the present organization of our COMINT activities seriously impedes the efficiency of the operation, and prevents us from attracting and retaining as much top quality scientific management manpower as this country ought to be investing in so important a field. It is highly significant to the Committee that the return of many of the best wartime COMINT brains to more attractive [redacted]

The committee concluded that the creation of AFSA, coinciding as it had with the creation of USAFSS, had resulted in four COMINT agencies where there had formerly been two. It criticized AFSAC for obstructionism and requested that it be abolished. It attacked USAFSS as a virtually autonomous organization not operating under joint control at all.

The positive recommendations of the Brownell Committee are worth studying, because they encompass the present-day structure of SIGINT in the United States. AFSA should be greatly strengthened, especially in its ability to control tasking at SCA collection sites. AFSA or its successor should be removed from JCS control and should be placed under USCIB, whose membership should be revised, and whose procedures should be governed by a vote of four, rather than unanimity, as had been the case with AFSAC. AFSA should centralize and consolidate processing operations wherever possible to increase the resources brought to bear on intractable cryptanalytic problems. The director should be upgraded to three-star rank, and should be appointed by the president to a four-year term. He should have a civilian deputy. Civilian career development should be encouraged to a much greater extent than formerly.

The next several months were spent putting the Brownell report into directive language. The result was the Truman Memorandum, issued on 24 October 1952. This memo directed a complete restructuring of COMINT along the lines that Brownell recommended. It resolved an on-going dispute about how to change AFSA by abolishing it and creating in its place a new organization called NSA. Its director would work for the secretary of defense, who would become the "executive agent" for COMINT for the entire government. On the same date the National Security Council issued a revised NSCID 9, almost a verbatim quote of the Truman Memorandum. Both documents were classified Top Secret, thus hiding the official creation of NSA from the American public for many years.

All that remained was for the secretary of defense to issue a memorandum establishing the new agency. He did so on 4 November the day that Dwight Eisenhower defeated Adlai Stevenson for the presidency. The creation of NSA was one of the last historical legacies of twenty years of Democratic governance.

The Truman Memorandum, on the advice of Lieutenant General Canine, had excluded COMSEC. Despite his belief that NSA should have both a COMINT and a COMSEC role, Canine recommended against mixing both in the same document. Lovett's memorandum on 4 November did mention that NSA would inherit the COMSEC functions formerly performed by AFSA. A memo in December spelled out those functions in more detail, and this marked NSA's first formal COMSEC charter.[17]

KOREA

> It has become apparent . . . that during the between-wars interim we have lost, through neglect, disinterest and possibly jealousy, much of the effectiveness in intelligence work that we acquired so painfully in World War II. Today, our intelligence operations in Korea have not yet approached the standards that we reached in the final year of the last war.
>
> General A. James Van Fleet, Commanding General 8th Army, June 1952

The Country

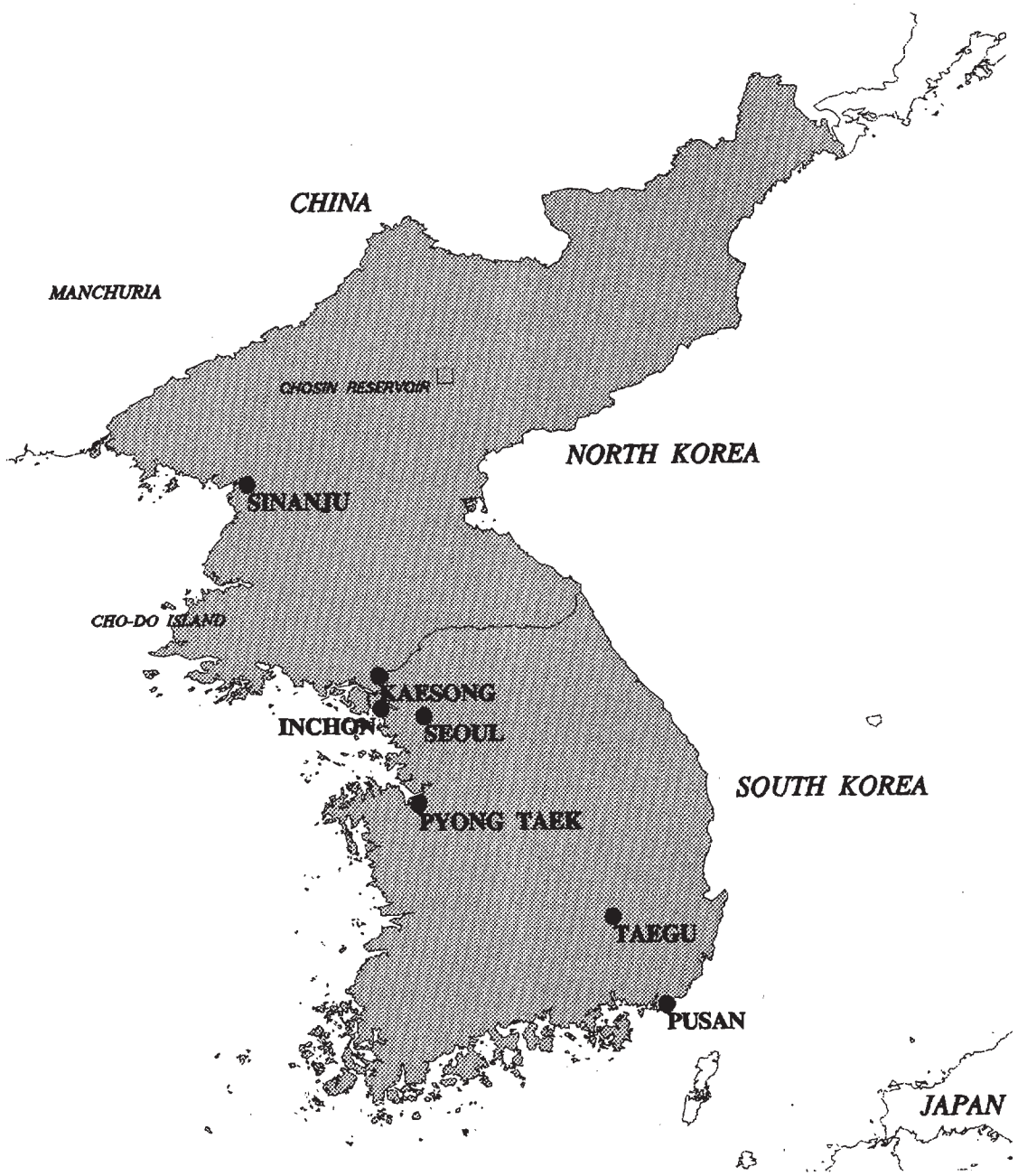
American intelligence interest and attention, so painfully refocused on the Soviet threat after World War II, were not to be rewarded. The next war occurred not in Europe, where allies and commitments were, but in Korea, a remote Asian peninsula whose name many Americans had never heard in 1950.

Korea had, throughout its recorded history, been a battleground between China, Japan, and Russia. Frequently invaded and occupied, its primary purpose seemed to be as a strategic buffer among three conflicting imperial ambitions. The most recent change of ownership had come after the Russo-Japanese War of 1904–05. Russia, the loser, was forced to cede its influence. Korea became forcibly Japanese.

The Allied powers recognized during World War II that Korea was one of those geopolitical oddities whose status had to be resolved. It obviously could not remain Japanese, and so at the Cairo Conference of 1943 Roosevelt endorsed a policy that would ensure a "free and independent Korea." At Yalta in April of 1945, the Big Three (the United States, the USSR, and Britain) agreed to an Allied trusteeship, to be administered by the three plus China.

Nothing further happened until the USSR declared war on Japan on 8 August 1945, simultaneously invading Manchuria and Korea. The sudden movement of Soviet troops onto the peninsula appeared to portend Soviet occupation, and MacArthur was directed to rush troops to the southern end of Korea. The United States proposed a division of military occupation on the 38th Parallel, splitting the peninsula roughly in half. Moscow unexpectedly agreed, and still more unexpectedly, complied.

American forces dwindled down to about 30,000 by 1948. In March of that year President Harry Truman, following the country's mood of dedicated military budget-cutting, decided that America would simply have to abandon Korea to the United Nations,


CHINA
MANCHURIA
CHOSIN RESERVOIR
NORTH KOREA
SINANJU
CHO-DO ISLAND
KAESONG
INCHON
SEOUL
SOUTH KOREA
PYONG TAEK
TAEGU
PUSAN
JAPAN

Korea, 1950

to sink or swim on its own. He decided to end the American trusteeship and sponsor free elections. So in the spring of 1948 American forces marched out of Korea. The South boycotted the elections, which led to a new National Assembly and a government headed by Syngman Rhee, a seventy-three-year-old militant anti-Communist who had spent forty years in exile in the United States waiting for the liberation of his homeland. The North formed its own government, the Democratic People's Republic of Korea (DPRK), headed by a young thirty-six-year-old Communist named Kim Il-sung. The peninsula was divided at the waist.

Syngman Rhee

Kim Il-sung

The Asia Dilemma

In 1949 catastrophe struck in the Far East. The corrupt and despotic Chiang Kai-shek and his Nationalists were ousted by the Communist forces of Mao Tse-tung. As the Communists marched into Beijing, Chiang fled to the island of Formosa (Taiwan), some 100 miles off the coast, followed by as much of his army as could flee with him. By the end of the year, Mao was making confident proclamations about his intent to invade Formosa and drive Chiang and his army into the sea.

In Washington, the administration was convulsed over whether the United States should support Chiang and the Nationalists. In the end the anti-Chiang faction won, and Truman, on 5 January 1950, issued a public statement that the United States had adopted a "hands off Formosa" policy. Ambiguity about which side of the line Korea stood on was

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

resolved a week later when Secretary of State Dean Acheson, at a press conference, described an American sphere of interest in the Pacific that implicitly excluded Korea.

By June 1950 the United States had boxed itself into a very weak position in Korea. From a full army corps, it was reduced to a 500-man Korean Military Aid Group (KMAG). The U.S. had left behind plans and equipment for a 50,000-man ROK (Republic of Korea) "constabulary" (rather than a real army) but devoid of heavy equipment, as the U.S. was afraid that the militant Rhee would use it to invade the North. Rhee drew up plans for a real army of 100,000, and he succeeded in extracting additional American commitments of weapons (but still no heavy, mobile offensive weapons). On the other side of the 38th Parallel stood a DPRK army and air force of about 135,000 men, equipped by the Soviets with much of the heavy equipment that the Americans had denied to Rhee.

American military forces, overall, in 1950 were in a weakened state. Defense budgets had continued to decline from their World War II peak, and the defense budget for 1950 was only $12.3 billion, with an authorized Army strength of 630,000 (but an actual strength of only 591,000). Of these, only 108,500 were in the Far East, almost all of them in Japan. In line with administration policy, the Pentagon had no plans to defend Korea and no one there to do it. The American contingency plan for the peninsula was basically to evacuate all dependents to Japan.[18]

Parallel to the national lack of interest in Korea was AFSA's neglect of the problem. There were no documented high-priority national intelligence requirements on Korea, and the only requirement that related at all was couched in terms of keeping track of Soviet interest in the peninsula. At the time AFSA had "no person or group of persons working on a North Korean problem." During the previous year, SCA intercept sites had stumbled onto some [redacted] North Korean messages which were originally collected as suspected [redacted] When in May 1949 these messages were identified as North Korean, two intercept positions at [redacted] and a tactical unit not under AFSA control, were tasked with follow-up copy. AFSA had no Korean linguists, no Korean dictionaries, no traffic analytic aids, and no Korean typewriters.[19]

No one really expected an invasion in Korea. There was fragmentary HUMINT reporting, generally disbelieved by all, that there could be an invasion by North Korea in 1950. In March an Army organization called the Intelligence Indications Steering Committee cited the possibility of military activity in Korea sometime in 1950. But this was set against a general disbelief in the intelligence community that Korea presented a real problem.

After the war broke out, there was the usual scramble by intelligence agencies to find the indicators that had been missed. AFSA, for instance, discovered traffic indicating that there had been large shipments of medical supplies going from the USSR to Korea beginning in February. A Soviet naval DF net in the Vladivostok area had undergone a

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

dramatic switch to South Korean DF tasks beginning in February.[20] This did not quiet the critics.

The Invasion

About 0330 on Sunday morning, 25 June 1950, Captain Joseph Darrigo, a KMAG military advisor to the ROK posted near Kaesong, was jarred awake by the roar of artillery. Darrigo, the only American on the 38th Parallel, was in the middle of an invasion of North Korean ground forces into South Korea. He managed to make it to the ROK 1st Division headquarters at Munsan just ahead of the advancing North Korean forces, and he spread the alarm.

There appears to have been no tactical intelligence warning. A reporter in Seoul got word of an invasion and rushed to the American embassy for confirmation. At the same time that he got off a wire to New York, the American ambassador was cabling Washington. His cable had to be encrypted and decrypted, and it got there late. The Americans learned of the invasion from the reporter in Seoul.[21]

ASA decided to support the fighting with a communications reconnaisance battalion at Army level and three battalions to serve each of the three corps. The 60th Signal Service Company at Fort Lewis, Washington, appeared to be closest to being ready for deployment of any ASA tactical asset, so that organization was selected. But it took time to get ready, and in the meantime ASA Pacific (ASAPAC) in Hawaii rushed a signal collection unit to the Korean peninsula, arriving there on 18 September. The Fort Lewis unit did not arrive until 9 October.[22]

Meanwhile, the Truman administration had decided to help the fledgling ROK army and got UN backing for the deployment of a multinational defensive force to Korea. Truman directed MacArthur to rush the 8th Army from Japan to Korea, and the first American troops reentered Korea by air on 1 July. But it took time to get enough troops into the country, and the DPRK army charged ahead, pushing ROK defensive units ahead of it pell-mell. By mid-August, ROK defenders had been shoved into a perimeter around the port city of Pusan, the last remaining large city still under the control of the Rhee government. When the first ASA unit arrived in September, the ROK army, bolstered by newly arrived American divisions (the 24th Infantry, 25th Infantry and 1st Cavalry), was desperately hanging onto this slice of the Korean landmass, and the American and Korean defenders were in the middle of a fierce struggle to retain the town of Taegu.[23]

ASA's primary concern was to get linguists. Perhaps the only two first-rate Army Korean linguists were Y.P. Kim and Richard Chun, who were both instructors at the Army Language School in Monterey in 1950. Chun had been cleared in World War II, but Kim had never been in the COMINT business. ASA needed linguists at Monterey to train what was expected to be a sudden flood of Korean language students, but they also needed someone in Korea who could translate Korean. ASA hesitated just a brief moment, and

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

then Kim and Chun, neither as yet actually cleared for COMINT, were on their way to Korea to assist the newly arrived ASA tactical COMINT unit. Until their clearances came through, they worked in a locked and guarded room every day. Intercepted messages were brought in periodically. They would translate the traffic and then pass it through a slot in the wall to the communications center.[24]

The Air Force Security Service likewise had one unit in the Korean area in 1950 – the 1st Radio Squadron Mobile (RSM) at Johnson Air Force Base outside Tokyo. This unit had been created in 1942, and it had supported 5th Air Force through MacArthur's Pacific campaign from New Guinea to Japan. In 1950 it was still engaged in support to 5th Air Force, but by then had changed its mission to [redacted] In late June it scrambled to change over to Korean targets. It had no cryptanalytic capability, and so began with a traffic analytic attack against North Korean air targets. It likewise had no cleared Korean linguists, so it could do little against readable voice communications.[25]

The Murray Mission

The Air Force Security Service actually beat ASA to Korea – their first representative, First Lieutenant Edward Murray, arrived in Taegu on 19 July. But Murray's mission quickly became entangled in one of the most bizzare incidents in the history of American cryptology.

When Murray arrived, 5th Air Force already had a COMINT service. The origins of that organization are very murky but appear to go back to the days after the end of World War II. At the time a civilian named Nichols, who also had a reserve commission as an Air Force major, headed the local Air Force Office of Special Investigations. Nichols, whose background and training in COMINT are completely unknown, decided that Korea needed a COMINT service. The South Korean government under Syngman Rhee did not appear interested, so Nichols proceeded on his own, seeking out the assistance of some Koreans with COMINT experience.

Among his recruits was one Cho Yong Il, who had come from North Korea, where he had been a radio operator and cryptanalyst with the North Korean Army. Joining Cho was Kim Se Won, a captain in the ROK navy. Kim had served as a COMINTer with the Japanese army in World War II and, owing to having been interned by the U.S. Army in Hawaii, spoke excellent English. Cho, Kim, and those who worked for them did intercept and translation work for Nichols; the source of funding has never been discovered. In 1949 Cho, with Nichols's assistance, obtained a commission in the Korean air force (ROKAF), and his group dual-hatted as a private group working for Nichols and as the ROKAF COMINT service. At about the same time the ROK navy set up Kim and some colleagues from the Nichols group as their COMINT service, so they, too, were dual-hatted.

When the ROK army retreated south in July of 1950, Nichols and his COMINT group retreated with them. As they fled south, fissures developed between Cho and Kim, and in late July or early August the Kim group seceded. Cho stayed with Nichols to supply COMINT to the Air Force, while Kim eventually hooked up with ASA units entering Korea. Nichols was reporting directly to 5th Air Force, which was releasing his reports into USAF intelligence channels at the noncodeword level.

Meanwhile, AFSS had sent Murray to Johnson Air Force Base to put together a direct support package. Murray assembled some vans and other equipment from 1st RSM, and on 15 July he flew to Korea to set up a mobile COMINT effort. AFSS was operating under a misty-eyed concept of COMINT as covert operations, and 1st RSM was directed to expunge its identifications from the equipment, and to insure that Murray could not be indentified as a COMINTer. The direct support went under the codename Project WILLY.

Murray's first concern on arriving in Korea was linguists. Fifth Air Force offered him eight of them, straight from the Nichols pool. The only problem was that Nichols still controlled them, and the upshot was that Nichols wound up with 1st RSM's equipment for use by his own operators. As for 5th Air Force, they were quite happy with the support they were getting from Nichols and informed Murray that he was no longer needed. First Lieutenant Murray returned to Japan on 1 August, having utterly failed to set up a Security Service unit in Korea and having lost his equipment to boot.

The breathless nature of Nichols's coup left USAFSS spinning. A severe jurisdictional battle ensued, encompassing command organizations in the United States, Japan, and Korea. Security Service appeared to carry the day, and Murray was ordered back to Korea on 12 August, armed with a letter of authority from General Banfill (Deputy for Intelligence, Far East Air Force). But the struggle was far from over. Nichols was still unwilling to relinquish control of his COMINT organization, and he had the backing of 5th Air Force. Nichols was a local asset under their complete control, was publishing COMINT without the restrictive codewords that limited dissemination, and already had the expertise that Murray lacked. On 17 August, 5th Air Force ordered Murray to catch the next plane out of Korea. AFSS was again out of the picture.

The Nichols effort was limited by its lack of national-level technical support from AFSA and USAFSS, and 5th Air Force eventually realized this. On 20 November, 5th Air Force reversed its earlier position and asked for the deployment of a radio squadron mobile to Korea to provide support. Cho's group became Detachment 3 of the 1st RSM, and Nichols disappeared from the scene.

Meanwhile, back in Tokyo 1st RSM was trying to mobilize an effort against the North Korean air force. When Murray returned to Japan the first time he carried with him some captured North Korean code books turned over to him by Nichols. Lacking Korean translators, the unit came upon a Catholic priest named Father Harold Henry, who had spent a number of years in Korea as an Army chaplain. AFSS agreed to give him access to

intercepted materials but did not agree to give him an SI clearance. He began applying the code books to the traffic, and he turned out to be a pretty good cryptanalyst, even though he was doing the work without benefit of formal clearance. Father Henry produced the first decrypts of enciphered North Korean air traffic.[26]

Counterattack

While ASA and AFSS were having trouble getting organized tactically, AFSA pushed rapidly ahead. Despite an almost total lack of expertise and resources to work the unfamiliar Korean target, codebreakers in Washington succeeded in penetrating North Korean communications by late July. At the time, DPRK troops were being readied for their all-out assault on Taegu, which, if successful, might have caused the collapse of the Pusan perimeter and American defeat. Three divisions of Lieutenant General Walton Walker's 8th Army were on line with the remnants of five ROK divisions; opposing them were fourteen battle-tested DPRK infantry divisions. On 26 July AFSA decrypted a North Korean message which contained much of the battle plan for the assault on the 30th. The information reached Walker on the 29th, and he shifted his forces to meet the attack, thus saving Taegu and the Pusan perimeter.[27] It was one of AFSA's most conspicuous successes.

On 15 September MacArthur launched the spectacular Inchon invasion, the second largest amphibious landing in history, near Seoul. North Korean troops suddenly had a large American force in the rear of their operations. On 19 September 8th Army began its breakout from the Pusan perimeter, and in a brief month they had pushed DPRK forces back north of Seoul. Syngman Rhee's government formally returned to the capital on 29 September. But the dynamic and committed Rhee wanted to push the fighting into North Korea, and on 30 September, ROK troops crossed the 38th Parallel. Washington viewed this development with anxiety. But MacArthur was confident that Chinese and Soviet forces would not intervene and, like Rhee, lobbied for authority to go all the way to the Yalu River. The CIA issued an assessment that MacArthur was right. The risks of invading North Korea appeared minimal, and in the end the Truman administration backed MacArthur. American forces crossed the 38th Parallel on 9 October, heading north.

China

The Chinese problem which MacArthur was so blithely underestimating had been building for years. The postwar COMINT effort against Chinese communications began officially in 1945 during the mission of General George Marshall to try to get Chiang Kai-shek and Mao Tse-tung to the bargaining table. Marshall, familiar with what COMINT had

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

done during World War II, requested COMINT information from both Communist and Nationalist communications.

ASA mounted a small effort against both the Nationalists and Communists. [redacted] ASA could still report that the two sides were far apart, and it was obvious from the COMINT traffic that they were determined to settle their differences on the battlefield. The Marshall mission was withdrawn in 1946, and in October of 1949 Mao triumphed.

Following the withdrawal of the Marshall mission, the COMINT mission against China suffered, as ASA employed all available resources against the Soviet target. [redacted] ASA kept only a small section against Chinese civil communications, [redacted] Collection resources were concentrated at [redacted] security problems.[28]

When American and South Korean troops crossed the 38th Parallel, the Chinese had already decided to intervene in North Korea. The decision was taken at a meeting in Beijing from 3 to 7 October 1950. On the first day of the conference, Chinese foreign minister Chou En-Lai called Indian ambassador Panikkar to tell him of the decision, and Panikkar relayed this news to the West. But Indians were regarded as pathologically left-leaning, and Panikkar's communique was disbelieved. Chou's warning was followed up by Chinese radio broadcasts, but these, too, were disregarded.[29]

Historian Clay Blair asserts that "when MacArthur returned to Tokyo from Wake Island [in mid-October] he had no inkling of the CCF armies gathering in North Korea."[30] This was wrong. AFSA had clear and convincing evidence of the massing of Chinese troops north of the Yalu and had published it in product reports available to the JCS, the White House, and to MacArthur. As early as July, AFSA began noting references in Chinese civil communications to army units moving north. Rail hubs in central China were jammed with soldiers on their way to Manchuria. By September AFSA had identified six of the nine field armies that were later involved in the fighting in North Korea and had located them in Manchuria, near the Korean border. Ferries at Anshan (on the Yalu River) were being reserved for military use. Maps of Korea were being ordered in large quantities. On 7 November, in voice communications intercepted and published by the COMINT community, [redacted] stated, "We are already at war here."[31]

Douglas MacArthur with President Truman on Wake Island, 1951

That was not news to the ROK army. On 25 October a ROK division had been badly mauled by elements of the Chinese 40th Army, already reported by AFSA to be close to Korea. Five days later MacArthur's chief of staff, Lieutenant General Ned Almond, reported that he had seen Chinese POWs being held by a ROK unit. On the first of November, a Chinese force attacked a U.S. unit for the first time. But Charles Willoughby, MacArthur's G2, preferred to believe that these encounters represented isolated PRC volunteers rather than division-strength regular army units confronting UN troops.[32]

AFSA reports continued to document the presence of major Chinese forces on the Yalu, but the reporting was subtle. AFSA was regarded as a collection and processing agency, not as a producer of intelligence. There were no dramatic wrap-ups, no peppery conclusions – just the facts, strung through a flood of intelligence reports. The COMINT community had almost the only hard information about the status of Chinese forces.[33]

Intelligence agencies were beginning to pay attention. The Watch Committee of the JIIC, which began noting Chinese troop movements as early as June, concluded by September (probably on the basis of AFSA reporting) that these troops were moving north rather than to the coastal provinces near Formosa. By mid-October, influenced perhaps by MacArthur's opinions, the Watch Committee had concluded that, though there was convincing evidence that startling numbers of Chinese forces were in Manchuria, the time for intervention had passed – they assessed that the Chinese would not intervene.

However, encounters with Chinese ground and air forces in late October and early November caused the committee to take another look. Admiral Arleigh Burke, who commanded naval forces in the region, was convinced that Chinese intervention was imminent and brought up the subject twice to Willoughby, who summoned his very large staff to try to dissuade Burke.[34]

MacArthur continued to press ahead with offensive operations to reach the Yalu and get the boys home by Christmas. But on the snapping cold night of 25 November with trumpets braying, thousands of Chinese soldiers fell on unsuspecting units of the 8th Army. The American offensive turned quickly into a defensive, and a defense into a rout. The American and ROK armies were overwhelmed, and some units were virtually wiped out. Weeks later the front stabilized near Seoul, and the war settled down to grim trench warfare for almost three more years.

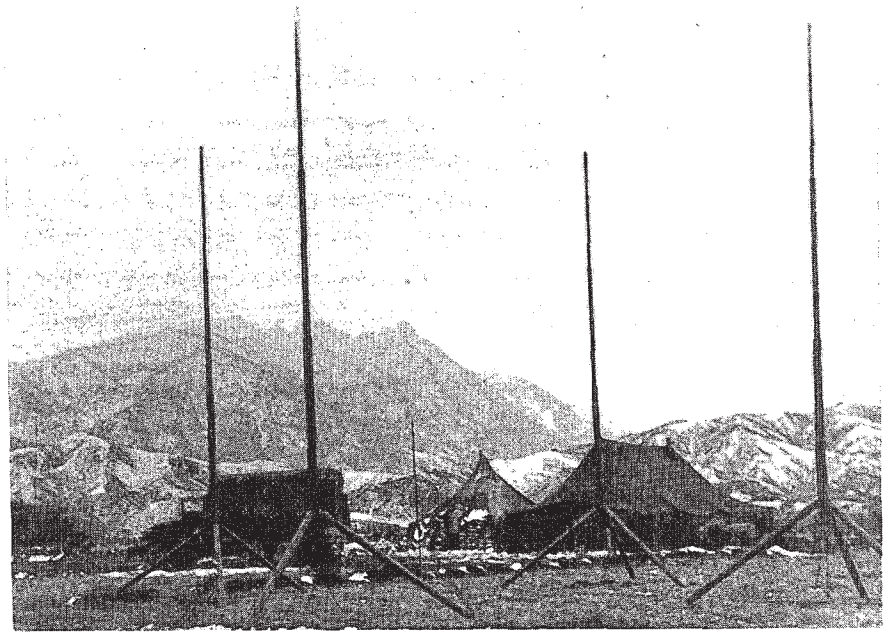
AFSS and ASA Operations

AFSS operations in Korea continued their harrowing path. The decision in November to send regular AFSS units occurred just prior to the Chinese invasion. Two locations were envisioned: one in Sinanju to intercept North Korean targets in the battle zone and a rear detachment in Pyongyang to intercept related Soviet and Chinese communications. But even as the two detachments were in the air on their way to Korea on 28 November, the Chinese had attacked, and Sinanju was not safe. The unit destined for Sinanju was diverted to Pyongyang, much further south, while the detachment commander was flown to Sinanju to assume command of the troops on the ground (the Cho detachment) and to get them to safety farther south. AFSS in Korea operated as Detachment Charlie of 1st RSM until 1951, when the 15th RSM was activated to control all AFSS Korean operations.[35] The Cho group made it safely back to Allied lines, and by February of 1951 the front had stabilized just south of Seoul.

ASA tactical units dug in for the winter. ASA manual Morse intercept efforts in Korea were having very modest success. Most intercepted material was [redacted] providing little of tactical value. But sometime in February reports began to filter to ASA that UN front-line troops were hearing Chinese voice communications. ASAPAC (Advance) sent an investigating officer to IX Corps, and he reported that there was a good volume of spoken Chinese interceptable.

ASA already had some Chinese linguists, but what they needed to exploit this type of nonstereotyped communications was native linguists. An arrangement was made with a former Nationalist Chinese general working for the U.S. in Tokyo to begin hiring former Nationalist officers from Formosa. They were enticed to Korea by the promise of earning GS-6 pay as Department of the Army civilians, and they were to enjoy officer status while in Korea. Competition was keen, and by the summer of 1951, Chinese linguists were flocking to ASA units in Korea.

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



DF operations – an ASA DF unit in the mountains of Korea

The linguists were formed into Low-Level Voice Intercept (LLVI) teams and were positioned as close to the front lines as possible. The effort was expanded to include Korean LLVI, although that part of the program got off to a slower start because of the difficulty of getting good linguists in a cleared status. Low-level voice quickly became the prime producer of COMINT in Korea, and the demand for LLVI teams overwhelmed ASA's ability to provide enough good linguists. The program expanded from one unit, to seven, to ten, and by the end of the war there were twenty-two LLVI teams, including two teams dedicated to tactical voice intercept.[36]

In September of 1952 the 25th Infantry Division began picking up Chinese telephone communications from their tactical landline telephones. This was accidental, of course, and apparently originated from a sound detecting device normally used to indicate the approach of enemy troops. When the unit moved off line, they passed on the technique to the relieving 40th Infantry Division. The 40th improved the equipment but did no analysis. In November, an ASA liaision officer at division headquarters was notified, and ASA proceeded to develop the technique on other sectors, supporting it with LLVI teams

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

consisting of either Korean or Chinese linguists, depending on which type of unit was on the other side of the line. The Americans had accidentally rediscovered a technique for gathering intelligence which had originally been developed during World War I and which had been a prime producer of tactical information.

These LLVI teams were quite small, consisting only of an ASA officer, a couple of enlisted men for analysis, and two or three native linguists. Their value to front-line commanders, however, far outran their cost, and LLVI was hailed as one of the most important producers of tactical intelligence during the war.

White Horse Mountain

As the conflict settled down to unremitting trench warfare, highlights were few, and peace talks gradually replaced warfare in American newspapers. But the front lines continued to shift imperceptibly as the two sides bludgeoned each other in a series of bloody encounters to take high ground. One of those, the battle for White Horse Mountain, illustrated the use of COMINT in a tactical situation.

The action was originally tipped off by a Chinese Communist military message that was in the hands of the tactical commander before the battle took place. ASA set up a special effort and tactical communications to report information that might bear on the battle.

True to the intelligence prediction, the Chinese launched a massive infantry assault on American and ROK troops at White Horse on 6 October and persisted until 15 October. Throughout the battle, LLVI teams kept the American commander informed of the position and activities of Chinese units. In a precursor to Vietnam, the American units were able to call artillery fire on Chinese positions on the basis of the LLVI-provided information.[38] The Chinese suffered nearly 10,000 casualties out of some 23,000 committed to the battle.[39]

AFSS Introduces Tactical Warning

Like ASA units, AFSS operations in Korea depended increasingly on intercept of low-level voice communications, using this for tactical warning. The concept relied on the Joint Training Directive for Air-Ground Operations published in 1949, which stated that the primary purpose of radio squadrons mobile for tactical support was to collocate with the Tactical Air Control Center (TACC) so that direct tactical warning could be supplied. (This followed World War II COMINT doctrine used effectively by Lieutenant General Kenney at 5th Air Force.)

Because of the lack of linguists, AFSS was slow to set up this service in Korea. However, in the early spring of 1951 AFSS units began intercepting Soviet ground-controlled intercept (GCI) communications, and this spurred Far East Air Force (FEAF) into requesting AFSS tactical support. Fortunately, AFSS did have some Russian linguists, and eight of them were on their way to Korea in April to form the first linguist team. They originally set up a mobile intercept and processing hut at Pyongtaek in central Korea, and communicated with the TACC by landline. No one in the tactical air operation was cleared for COMINT, so it was disguised using a simple substitution code to identify enemy aircraft and ground checkpoints. Arrangements were made for the TACC controller to pass relevant COMINT, intermixed with radar plots, to fighter pilots. The operation was nicknamed "YOKE," and became highly successful because it significantly expanded the range of control of the TACC and improved the air controllers' ability to warn pilots of impending threats.

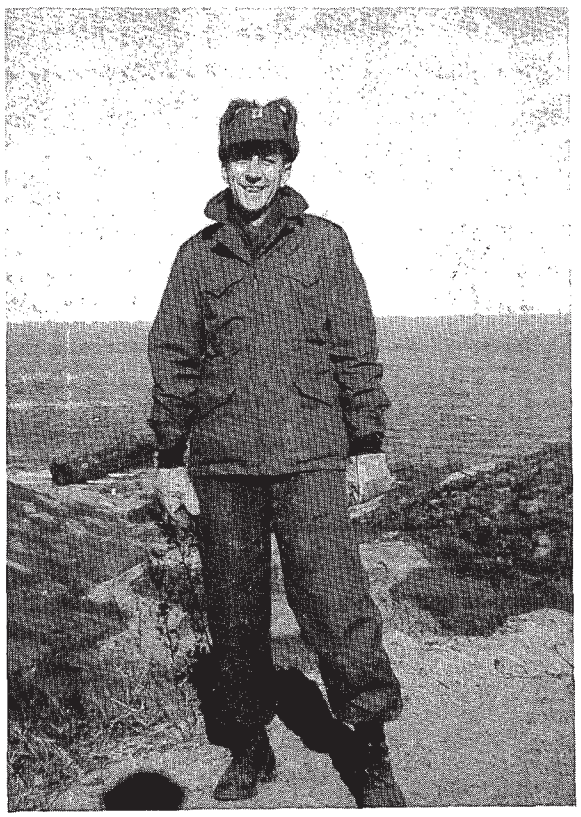
As the front advanced north of Seoul, so did the air control operations. In June of 1951, the entire air control operation moved forward to a hill four miles northeast of Kimpo Airport near Seoul. But in August hearability deteriorated, and the operation, including the TACC and Security Serice operations, migrated by LST to Pyong-Yong-Do island. Only six miles from enemy lines, "P-Y-Do" (as it was called) was in an ideal location. The site at Kimpo was kept open, and linguists were split between the two sites.

Soon AFSS was finding tactical voice communications in Chinese and Korean as well as Russian. Two more voice teams were established for the additional languages. The Korean voice team consisted of the Cho contingent of the Nichols group. The Chinese team set up shop on the campus of Chosen Christian College in Seoul (today, Yansei University). AFSS acquired its Chinese linguists in Korea basically the same way that ASA did – they hired foreign-born linguists. In this case, they did business with one General Hirota, a former chief of the Japanese army COMINT agency during World War II. Hirota hired twelve Japanese linguists who were fluent in Chinese.

With so many languages involved, the tactical support operation was unusually complex. The AFSS facility at Kimpo correlated Chinese early warning voice, Chinese GCI voice, Soviet GCI voice, Chinese air defense Morse and Korean GCI voice. Each input was produced by a separate team, and each team was in a different location for security purposes.[40]

In September of 1951 the P-Y-Do operation was closed down and moved back to Kimpo, and that fall all AFSS operations were consolidated at Chosen Christian. This was the first time that all components of the operation were collocated, which made correlation of activity easier. According to one officer involved in the operation, "the present top-heavy success of the F-86s against MIG-15s dates almost from the day of the inception of the new integrated voice-CW-YOKE service."[41]

In early 1952 much of the GCI traffic that AFSS had been intercepting began to dry up, and AFSS became convinced that it had gone to VHF. Moreover, about that time the Chinese stopped tracking Communist aircraft, and they tracked only "hostiles." These twin changes spelled potential disaster for AFSS tactical operations. From a practical standpoint, the lack of tracking would force AFSS to rely almost entirely on intercepting GCI communications. But since these communications were disappearing, probably to VHF, that source of information was also drying up. The changes also generated a security problem, since the positions of Communist aircraft had been disguised as radar plots when being passed to the TACC. If there were no more radar position reports, disguise of the origin of the information would be much more difficult.



Delmar Lang on Cho-Do Island in 1952

These developments roughly coincided with the arrival of the first batch of school-trained American Chinese linguists, headed by Lieutenant Delmar "Del" Lang, in mid-1952. At the time the unit was located in Seoul, where VHF intercept was hardly possible, while the TACC had moved to Cho-Do Island, near the North Korean harbor of Wonsan. Information had to be relayed from the AFSS unit to Kimpo and from Kimpo to Cho-Do. Lang moved the operation to Cho-Do Island and collocated it with the TACC. Tests on Cho-Do in August of 1952 confirmed that both the Soviets and Chinese were now using VHF for their GCI control activities.

To solve the security problems and to make sure that the TACC controller got the best possible support, Lang positioned an AFSS linguist in the TACC in March of 1953, sitting next to the controller. The linguist had a field phone on his desk, the other end of which was attached to the output of a receiver at the Security Service intercept unit three-fourths of a mile away. In an era when no one knew much about TEMPEST (see chapter 5), such a wireline was regarded as secure simply because it was a landline.[42]

Combined with improved hearability, the new lash-up at Cho-Do Island provided the best support that AFSS mustered during the entire war. In one day, which Lang described as the "great Korean turkey shoot," American F-86s downed fifteen MIGs without a loss, even though none of the MIGs was ever seen on radar. The information came, of course, from the COMINT operation at Cho-Do. A visiting ASA colonel commented that "it was just like shooting ducks in a rain barrel." It was a model for tactical COMINT operations and was resurrected by the same Del Lang years later in Vietnam. (See chapter 12.)[43]

The Navy

Naval cryptology was a bit player in Korea. The DPRK had no blue-water navy, and it was so weak that the Inchon invasion went unopposed from the naval standpoint. The naval COMINT unit in the region was [redacted] But [redacted] was not concerned with the small collection of DPRK coastal patrol craft. The organization concentrated instead almost entirely on the Soviet navy in the Pacific, to determine what moves, if any, the Soviets would make toward the U.S. presence on the Korean peninsula.

The unit was housed in cramped quarters in a former Japanese artillery training school, entirely too small and inadequate for the purpose. NSG found an old Japanese ammunition storage building about ten miles from [redacted] Rehabilitation began in 1951, and in November 1952 [redacted] moved to [redacted] where it remained for many years.

Most of the NSG support to the war effort came from its afloat detachments. Originating out of Hawaii, detachments were placed aboard 7th Fleet vessels beginning in August 1951, and at the end of the war, 7th Fleet had three such units.[44]

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