

series VI
volume 5

book I

~~TOP SECRET~~

American Cryptology during the Cold War, 1945-1989 - Book I

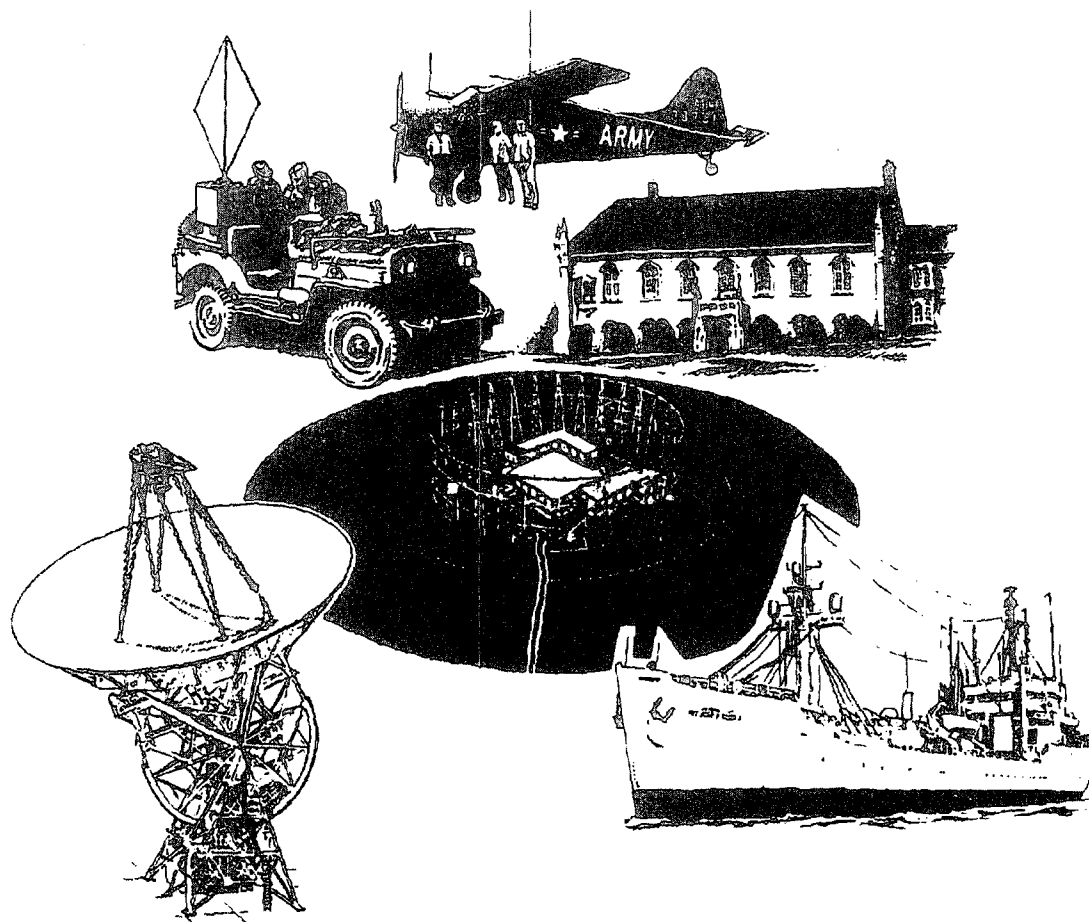
~~TOP SECRET~~

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



CCH-E32-95-03
TCS-54649-95

~~TOP SECRET~~

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.**

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~~

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 |

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

~~TOP SECRET UMBRA~~

| | |
|--|-----|
| 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

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

~~TOP SECRET UMBRA~~

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

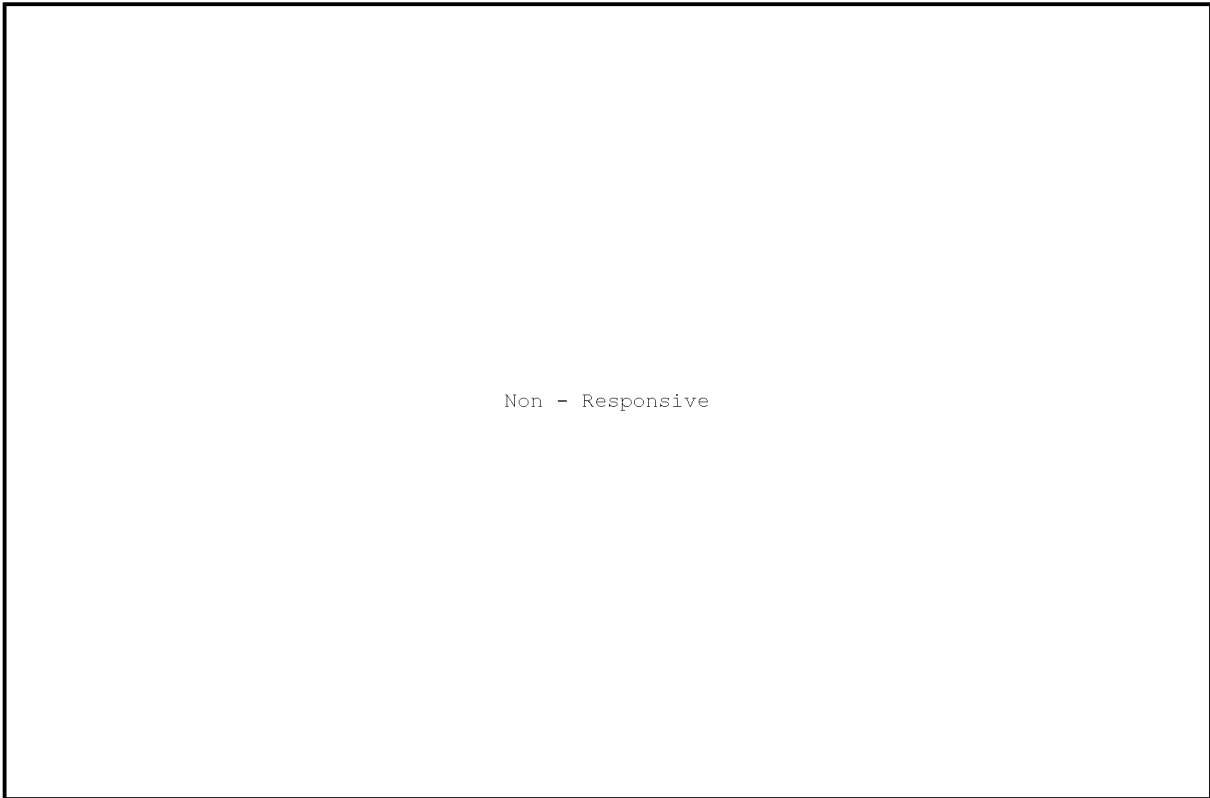
| | |
|-------------------------------|-----|
| The Early Assessments | 227 |
| The Robertson Committee | 227 |
| The Hoover Commission | 228 |
| The Killian Board | 229 |
| The Jackson Report | 231 |
| 1956 | 232 |
| Suez | 232 |
| Hungary | 235 |
| [REDACTED] | 236 |
| Lebanon, 1958 | 237 |
| 1956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

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

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

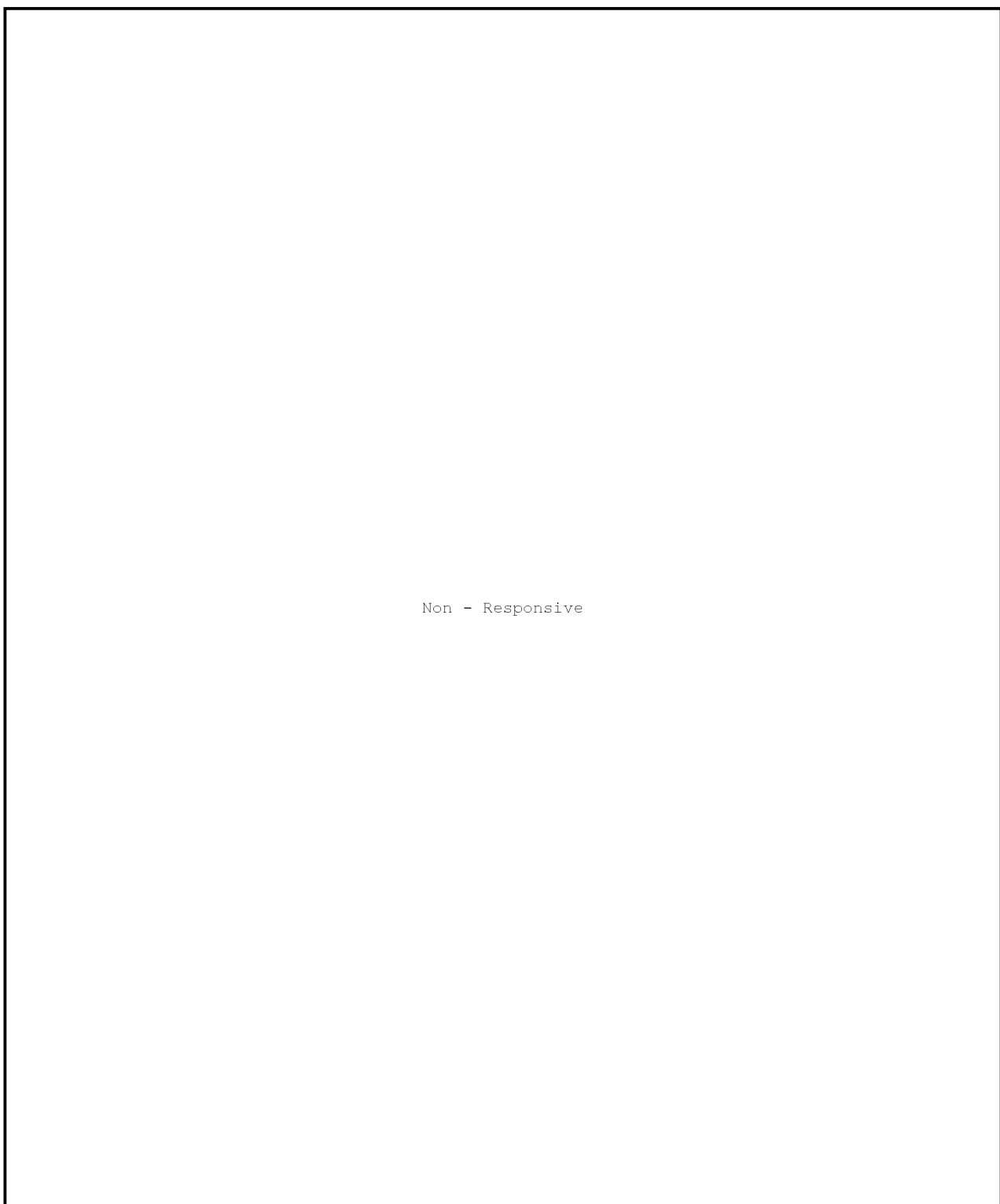


~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~



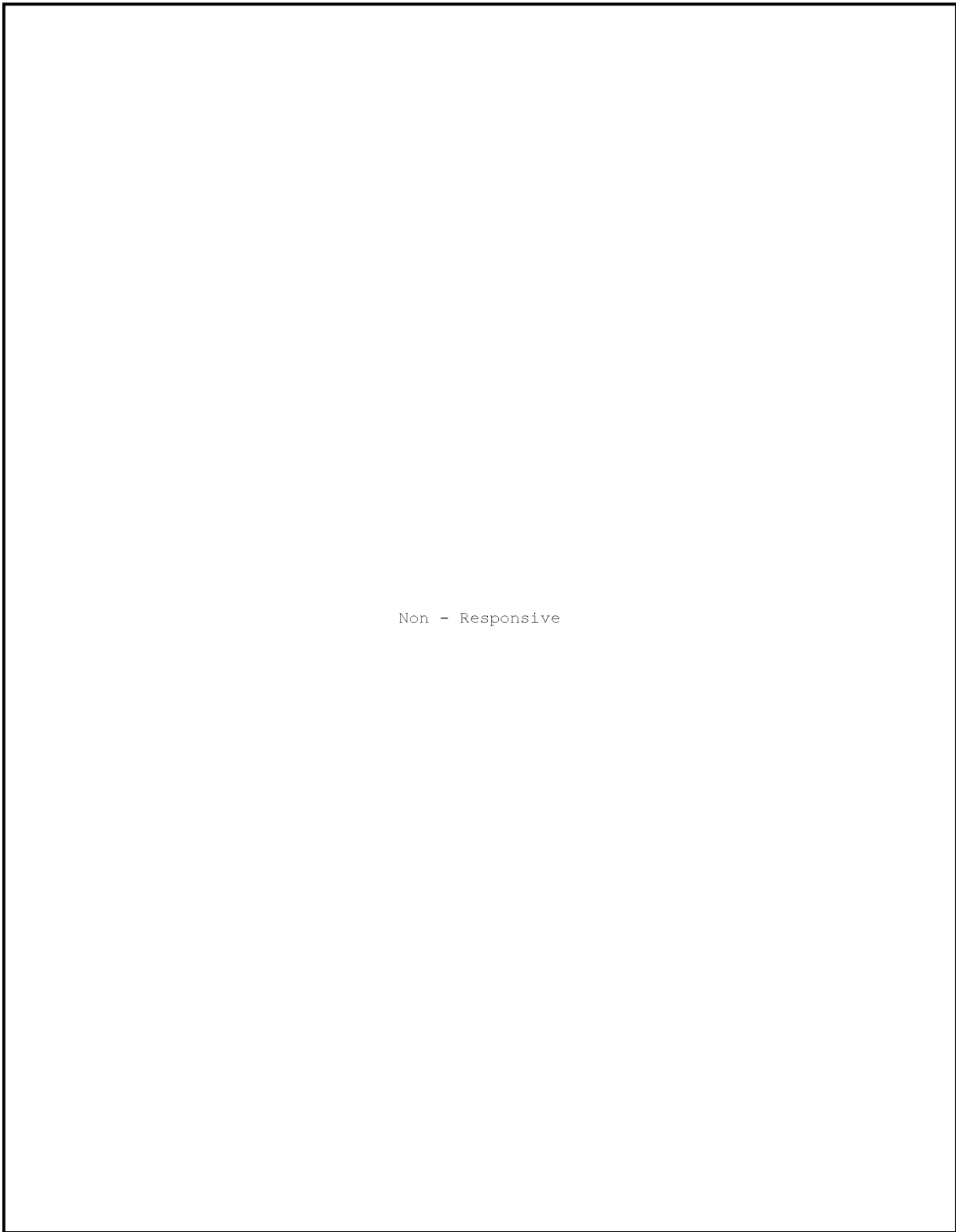
Non - Responsive

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



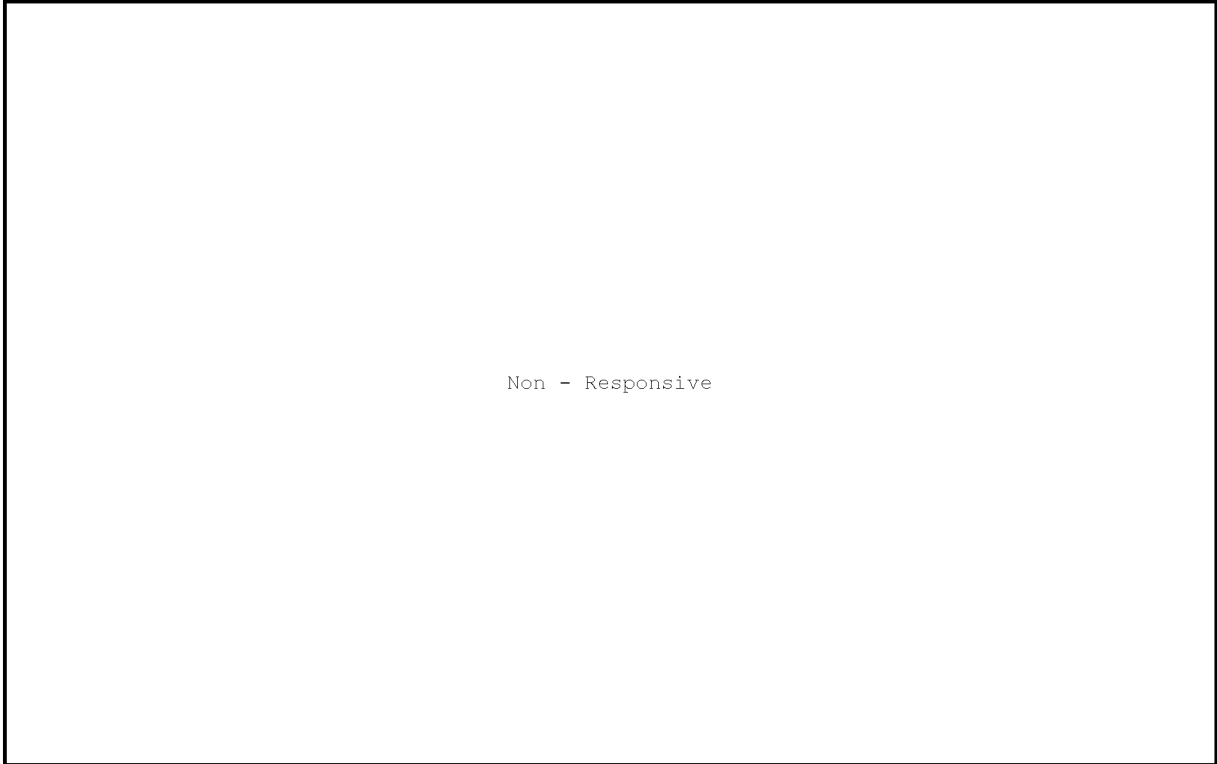
Non - Responsive

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



Non - Responsive

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



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

~~TOP SECRET UMBRA~~

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

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

~~TOP SECRET UMBRA~~

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

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

~~TOP SECRET UMBRA~~

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

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] [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

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

~~TOP SECRET UMBRA~~

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.

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

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.

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

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.

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

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

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

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

Western Hemisphere agent and clandestine traffic. These three were to be 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

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

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

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

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

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

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

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

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

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

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



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

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

~~TOP SECRET UMBRA~~

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

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

~~TOP SECRET UMBRA~~

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 COMINT 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

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

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

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

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.

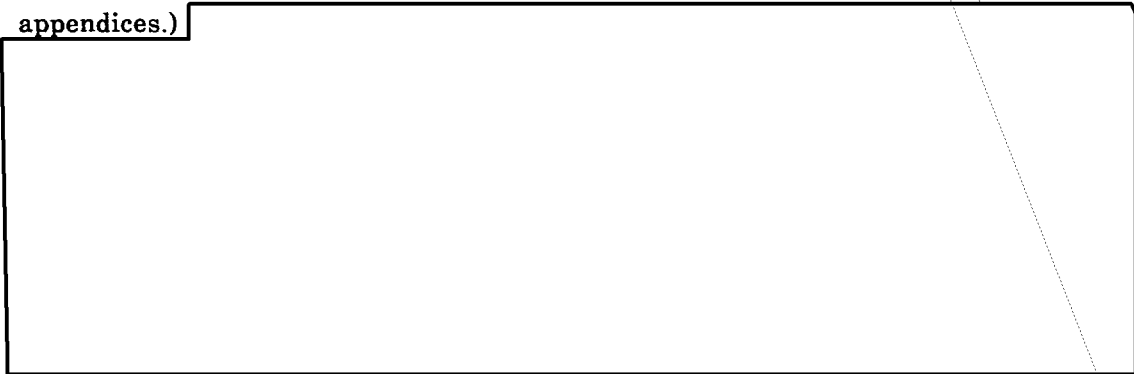
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

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

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

~~TOP SECRET UMBRA~~

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

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

~~TOP SECRET UMBRA~~

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]

[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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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. [REDACTED]

New Zealand came in as a fifth partner, [REDACTED] 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. [REDACTED]

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

~~TOP SECRET UMBRA~~



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. Zobebelein, 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*.

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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).

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

~~TOP SECRET UMBRA~~

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.

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



Rear Admiral Earl E. Stone, Director, Naval Communications

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

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



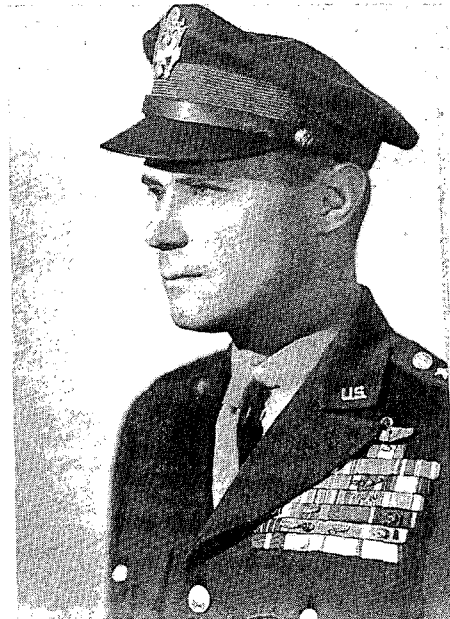
Louis A. Johnson,
secretary of defense in 1949

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

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.

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]

[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

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

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

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.

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

~~NOT RELEASABLE TO FOREIGN NATIONALS~~



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,

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

~~TOP SECRET UMBRA~~

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.⁹

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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 [] 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 [] 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.

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

~~TOP SECRET UMBRA~~



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

~~TOP SECRET UMBRA~~

~~HANDLE VIA PATENT KEYHOLE GOVINT CONTROL SYSTEMS ONLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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 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~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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.



Walter Bedell Smith
Director of Central Intelligence

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.

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 committee. Its chairman was George A. Brownell, a New York lawyer

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

~~TOP SECRET UMBRA~~



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]

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

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

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

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.

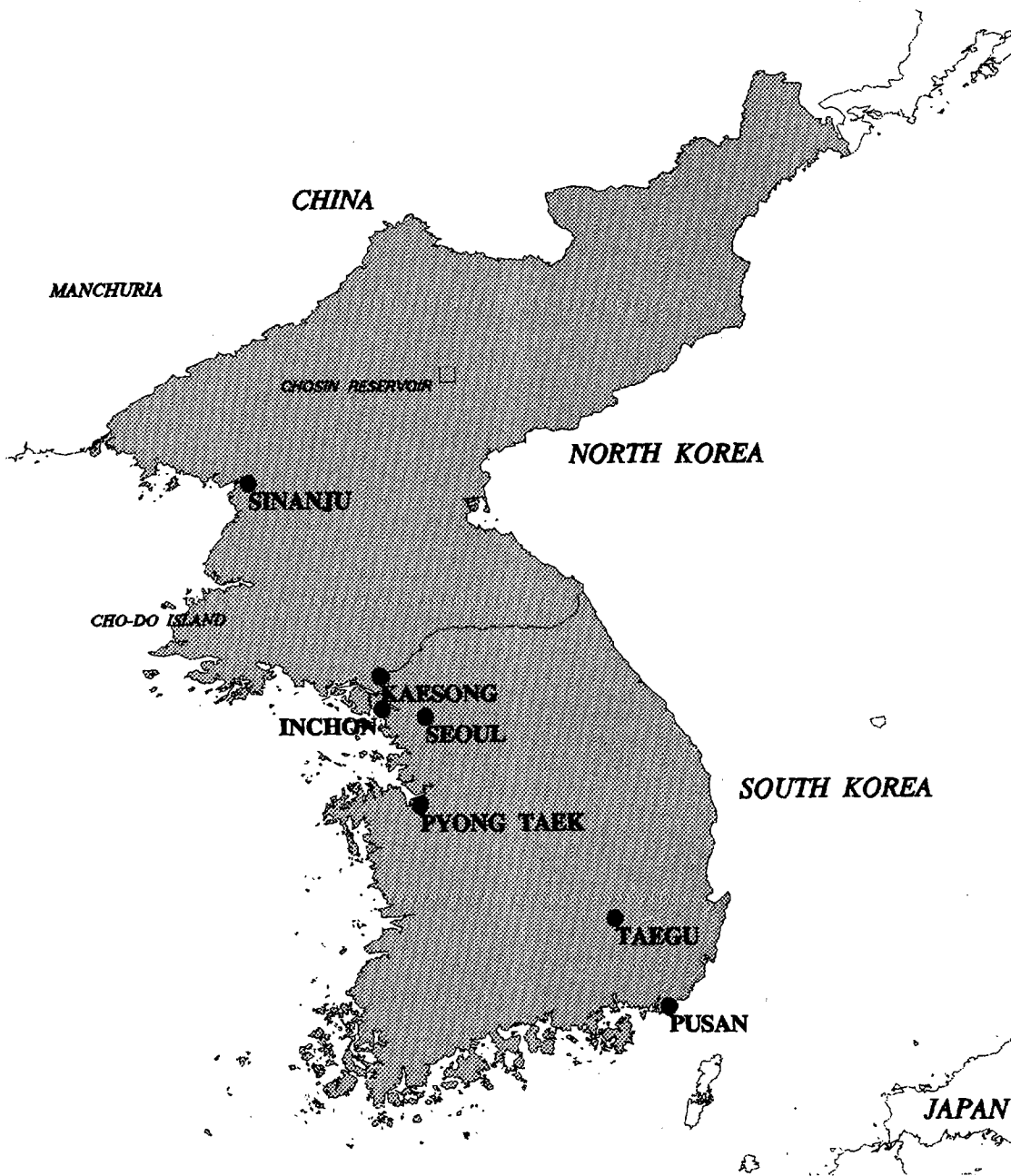
Korea had, throughout its recorded history, been a battleground between China, Japan, and Russia. Frequently invaded and occupied, its primary purpose seemed to be as a strategic buffer among three conflicting imperial ambitions. The most recent change of ownership had come after the Russo-Japanese War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

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



Korea, 1950

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

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

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

~~TOP SECRET UMBRA~~

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

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

~~TOP SECRET UMBRA~~

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 reconnaissance 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

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

~~TOP SECRET UMBRA~~

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]

[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 bizarre 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.

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

~~TOP SECRET UMBRA~~

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

~~TOP SECRET UMBRA~~

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] [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]

[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

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

~~TOP SECRET UMBRA~~



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.

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

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.

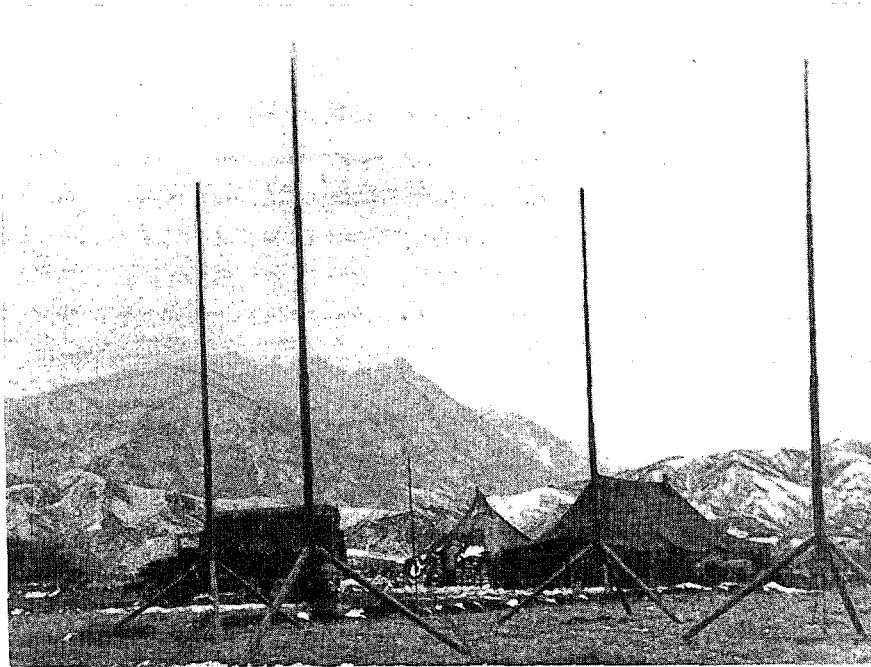
ASA tactical units dug in for the winter. ASA manual Morse intercept efforts in Korea were having very modest success. Most intercepted material was [redacted] providing little of tactical value. But sometime in February reports began to filter to ASA that UN front-line troops were hearing Chinese voice 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

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

~~NOT RELEASABLE TO FOREIGN NATIONALS~~



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 liaison officer at division headquarters was notified, and ASA proceeded to develop the technique on other sectors, supporting it with LLVI teams

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

~~TOP SECRET UMBRA~~

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. [REDACTED]

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 [REDACTED] a Chinese Communist military message that was in the hands of the tactical commander before the battle took place. ASA set up a special [REDACTED] effort and tactical communications to report information that might bear on the battle. [REDACTED]

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.)

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

~~TOP SECRET UMBRA~~

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.

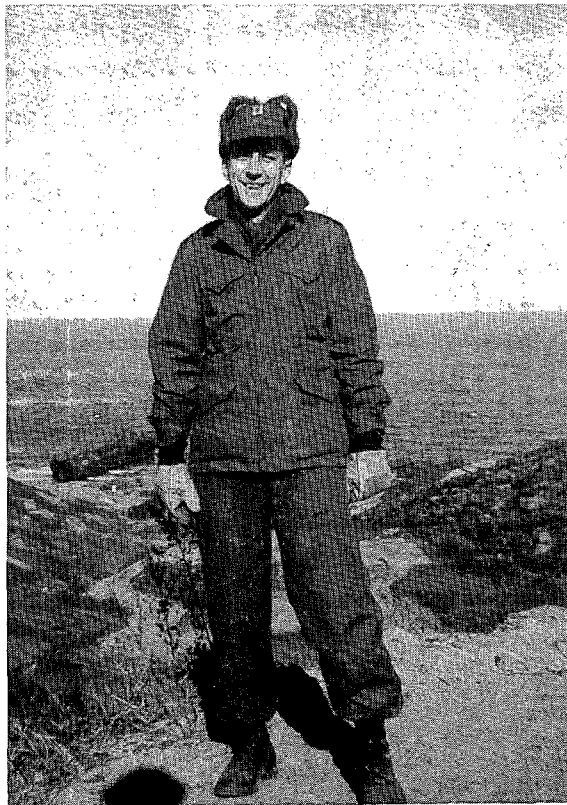
As the front advanced north of Seoul, so did the air control operations. In June of 1951, the entire air control operation moved forward to a hill four miles northeast of Kimpo Airport near Seoul. But in August hearability deteriorated, and the operation, including the TACC and Security Service operations, 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

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

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

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

The AFSA Factor

On the home front, AFSA provided significant help to battlefield commanders. AFSA's quick work [redacted] in time to turn the tide at Taegu appeared to portend the same kind of COMINT effectiveness that the U.S. had enjoyed during World War II. But it was not to be. [redacted]

In November 1950, with Chinese Communist troops flooding into North Korea, AFSA turned its attention to Chinese communications. [redacted]

In 1952 the painfully slow progress on traffic analysis of Chinese army nets finally began to bear fruit. There were indications through traffic analysis that the 46th Army was moving northward. The army eventually arrived in Manchuria and crossed the border into Korea. As it did so, AFSA began exploiting People's Volunteer Army (PVA) nets from a traffic analytic standpoint, and it achieved a level of competence on PVA nets that allowed extremely accurate order of battle determinations, unavailable through any other intelligence source. Through traffic analysis AFSA noted the build-up of PVA units on the eastern front, and this allowed 8th Army to reinforce its right side prior to a major PVA assault on 15 July 1953.⁴⁸

Relations with ROK COMSEC and COMINT

COMSEC assistance to ROK forces began almost as early as COMINT collaboration. In September 1950 ASA was asked to furnish low-level cryptographic assistance for use by the ROK army. After conferring with AFSA, ASA shipped some strip ciphers and Playfair squares. It was soon found, however, that these very time-intensive systems would not be fast enough, and in 1953 ASA provided the first electromechanical cipher equipment, the BACCHUS system. Later in the year ASA also released the DIANA one-time-pad system.⁴⁹

Cryptologic cooperation with the ROK COMINT organizations continued throughout the war. USAFSS continued its relationship with the Cho group, while ASA continued to do business with the Kim group. In November 1951 ASAPAC proposed the consolidation

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

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

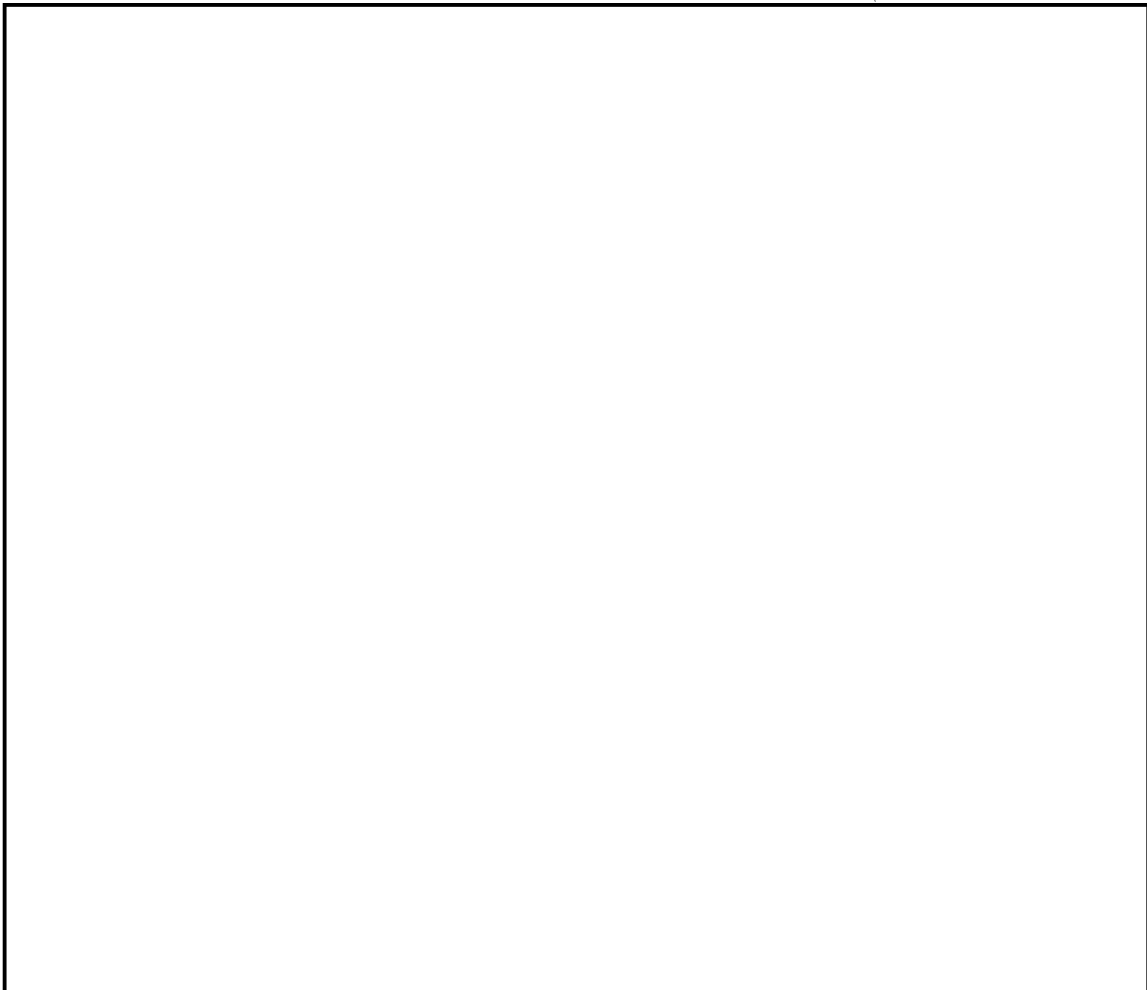
~~TOP SECRET UMBRA~~

of the two efforts, but AFSS firmly rejected the overture. This was probably based on Air Force fear that ASA would dominate the relationship and get back into the business of copying North Korean air targets, but this may also have been based on the very realistic appraisal that the animosity between Kim and Cho was unbridgeable.⁵⁰

The situation continued unchanged, and late the next year an official for the newly created NSA/



By charter (NSCID 5), CIA had control of all foreign intelligence relationships. But the "battlefield marriage" between the American and South Korean COMINT organizations represented a significant exception to the general rule. Korea was JCS turf, and military commanders were cool to CIA participation in their arena.



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


~~TOP SECRET UMBRA~~


~~TOP SECRET UMBRA~~

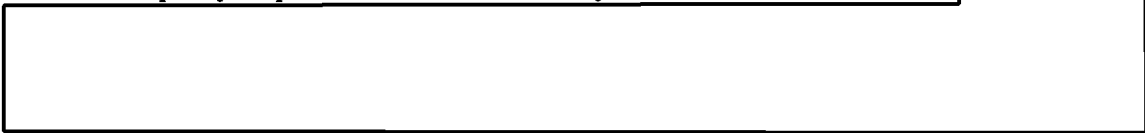


Korea - An Assessment

The Korean War occurred during a period of struggle in the cryptologic community. It began a year after the formation of AFSA and concluded after the AFSA ship had been finally scuttled in favor of a new vessel, the National Security Agency. The demands of war highlighted the fissures in the structure, and those fissures in turn made prosecution of the war more difficult. AFSA wrestled with the SCAs over control of intercept positions and targets throughout its existence, and many of those battles were related to the war effort. The Brownell Committee was convened in part because of complaints by organizations outside the Department of Defense over degraded cryptologic support resulting from the war. The committee stressed in its final report that the cryptologic community had been shown deficient in its effort during the war. NSA replaced AFSA partly because of what was happening (or not happening) in Korea.

But after forty years the picture does not look quite so bleak. Actually, AFSA and the SCAs provided good support to the war effort. Although AFSA (along with everyone else) was looking the other way when the war started, it did a remarkable about-face, and within a month it was producing large volumes of decrypted information from North Korean communications. Its accomplishments during the battle for the Pusan perimeter,  and using the information to support tactical commanders, were considerable and important. The reporting program, although hampered by restrictions on AFSA's production of "intelligence" as opposed to "intelligence information," was farsighted and effective. AFSA, almost alone among intelligence agencies, foresaw the Chinese intervention. The development of Chinese and Korean order of battle owed much to AFSA's high-powered traffic analytic effort.

After a slow start occasioned by lack of mobility, tactical resources, linguists, and working aids, ASA and USAFSS put together highly credible battlefield COMINT organizations. ASA's LLVI program produced more valuable information for ground commanders than any other source. AFSS put together a system for warning fighter pilots which was partly responsible for the much-ballyhooed kill ratio in that war. 



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

~~TOP SECRET UMBRA~~

[REDACTED]

AFSA's quick start was not sustained. Beginning in July of 1951, the North Koreans began a total changeover of their communications procedures

[REDACTED]

In the first month of the war, AFSA read more than one third of all North Korean cipher messages received, and by December AFSA was reading more than 90 percent.

[REDACTED]

The new North Korean security measures were evidently inspired by the Soviet Union, whose communications had in 1948 undergone a similar transformation in the face of possible American and British exploitation efforts. (See chapter 4.) It was accompanied by a decline in North Korean radio messages incident to the beginnings of static trench warfare roughly at the 38th Parallel, which gave the enemy a chance to divert radio communications to landline.

[REDACTED]

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

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

~~TOP SECRET UMBRA~~

[REDACTED]

Security was a problem in Korea, as it has been during all wars. Occasional press releases exposed COMINT support to battlefield commanders. The release of information about AFSS exploitation of GCI communications became so serious that in October 1951 Detachment 3 of 1st RSM took the extraordinary step of suspending operations for a few days until they got the attention of key officers in 5th Air Force.⁵⁶ The employment of tactical GCI voice and tracking information in the air war caused AFSS to devise new measures to cover the information, and it set a precedent for use of similar information during the war in Vietnam.

When NSA was created in November 1952, immediate steps were taken to sort out the effort in Korea. NSA's recommendations amounted to a classic "lessons learned" about war. Most pressing was a program which would allow the use of indigenous personnel with native language capability. Almost as urgent was the need to sort out the tangled relationships with the various ROK COMINT efforts. It would also be necessary to increase NSA representation in the field and to expand existing field offices with technical experts assisting the SCAs. Finally there was a call to develop new special identification techniques that would allow NSA and the SCAs to track target transmitters [REDACTED] [REDACTED] NSA sponsored these themes for years, until they became tantamount to COMINT doctrine on warfighting.

One beneficial effect of the Korean conflict was to begin a rapid rise in cryptologic resources. In July 1950 USCIB recommended to the National Security Council that COMINT receive a hiring jolt. The NSC approved this on 27 July in a meeting attended by the president himself.⁵⁸

Korea was America's first stalemated war, and recriminations resounded for years later. But even an acerbic CIA critic of the cryptologic community had to admit that "COMINT remained the principal source of intelligence for threat until 27 July 1953, when the armistice was signed at Panmunjom."⁵⁹

Notes

1. Rowlett interview, OH 14-81.
2. Sinkov interview, OH 2-79; oral history interview with Herbert L. Conley, 5 March 1984, by Robert D. Farley, NSA OH 1-84.
3. See both Burns, *Origins*, and Howe, "Narrative."
4. William L. O'Neill, *American High: The Years of Confidence, 1945-1960* (New York: Free Press, 1988.)
5. See Burns. *Origins*, 65.
6. CCH Series V.F.5.1.

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

7. Howe, "Narrative."
8. Burns, *Origins*, 70-71.
9. Howe, "Narrative."
10. Burns, *Origins*, 75-77; "Report to the Secretary of State and the Secretary of Defense by a Special Committee Appointed Pursuant to Letter of 28 December 1951 [Brownell Report]," in CCH Series V.F.7.13; NSA Archives, ACC 26350, CBSK 32; "Analysis of AFSS Effort in the Korean Action," unpublished draft, USAFSS, n.d., in CCH Series V.M.4.1.; A Reference Guide to Selected Historical Documents Relating to the National Security Agency/Central Security Service, 1931-1985, *Source Documents in Cryptologic History*, V. I (Ft. Meade: NSA, 1986), 36, 38.
11. Wenger comments on Howe draft history in CCH Series V.A.13.
12. Burns, *Origins*, 59-96.
13. Burns, *Origins*, 89; [redacted] "Consumer Liaison Units, 1949-1957," in NSA/CSS Archives ACC 10684, CBRI 52.
14. Howe, "Narrative"; "JCEC Memo for Information No. 1, Charters," in CCH Series V.G.2.; Brownell Report.
15. Brownell Report.
16. Ibid.
17. Ibid. See also Howe "Narrative"; Burns, 107-108.
18. An excellent account of the diplomatic background to the invasion of Korea can be found in Clay Blair, *The Forgotten War: America in Korea, 1950-1953* (New York: Times Books, 1987); and Joseph Goulden, *Korea: The Untold Story of the War* (New York: Times Books, 1982).
19. See [redacted] "The U.S. COMINT Effort during the Korean Conflict - June 1950-August 1953," pub. on 6 Jan. 1954, an unpublished manuscript in CCH collection, series V.M.1.1. See also Howe, "COMINT Production . . ." and The 'Brownell Committee Report', 13 June 1952, in CCH series VI.C.1.3.
20. [AFSA 235] no title [report on significant activity connected with the entry of Chinese Communists into the Korean conflict], 25 March 1952, in CCH Series V.M.7.1.; and [redacted] "The U.S. COMINT Effort. . ."
21. William L. O'Neill, *American High: The Years of Confidence, 1945-1960*.
22. Howe, "COMINT Production . . ."; Dick Scobey (NSA), draft study of ROK SIGINT Effort, no date, in CCH series V.M.6.1.; Assistant Chief of Staff, G2, "COMINT Operations of the Army Security Agency during the Korean Conflict, June 1950-December 1953," in CCH Series V.M.2.1.
23. Blair, *Forgotten War*, Ch. 2-4.
24. Interview Youn P. Kim, 22 February 1982, by Robert D. Farley, OH 2-82, NSA.
25. Hq USAFSS, "Analysis of AFSS Effort in the Korean Action," unpublished draft manuscript in CCH series V.M.4.1.
26. Summaries of Project WILLY can be found in the following sources: Hqs USAFSS, "Analysis of AFSS Effort . . .," Dick Scobey, "Draft Study of ROK SIGINT Effort"; ["Hop" Harriger], "A Historical Study of the Air Force Security Service and Korea, June 1950-October 1952," on file at Hqs AIA in San Antonio.
27. Manuscript entitled "SIGINT in the Defense of the Pusan Perimeter: Korea, 1950," (SC) in CCH series V.M.1.10. See also Clay Blair, *The Forgotten War*, 240.

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

28. Guy Vanderpool, "COMINT and the PRC Intervention in the Korean War," paper available in CCH.
29. Roy E. Appleman, *Disaster in Korea: The Chinese Confront MacArthur* (College Station, Texas: Texas A and M Press, 1989).
30. Blair, *Forgotten War*, 350.
31. [Drake, Robert, and others] "The COMINT Role in the Korean War," unpublished manuscript in CCH series V.M.1.9. See also Howe, "COMINT Production in the Korean War . . ."; oral history interview Milton Zaslow, 14 May 1993 by Charles Baker and Guy Vanderpool, NSA OH 17-93; oral history interview Robert Drake, 5 December 1985 by Robert D. Farley and Tom Johnson, NSA OH 18-85; oral history interview Samuel S. K. Hong, 9 December 1986 by Robert D. Farley, NSA OH 40-86.
32. Blair, *Forgotten War*, 375-78.
33. Zaslow interview; Drake interview.
34. Department of the Army G2, "Indications of Chinese Communist Intentions to Intervene in Korea," 7 May 1954, in CCH series V.M.7.4.; oral history interview Admiral Arleigh Burke, 9 December 1981, by Robert D. Farley and Henry F. Schorreck, NSA OH 13-81.
35. "Analysis of AFSS Effort . . ."; George Howe, "COMINT Production in the Korean War . . ."
36. Assistant Chief of Staff, G-2, "COMINT Operations . . .," contains the best summary of LLVI operations.
37. See Assistant Chief of Staff, "COMINT Operations . . .," 56-57.
38. Assistant Chief of Staff, G-2, "COMINT Operations . . ." See also oral history interview 24 April 1982 by Robert Farley, NSA Oral History 9-82, 122.
39. For a description of the action, see Walter G. Hermes, *Truce Tent and Fighting Front*, United States Army in the Korean War (Washington, D.C.: Office of the Chief of Military History, United States Army, 1966), 303-08.
40. Summaries of AFSS tactical operations can be found in the following: USAFSS, "Analysis of AFSS Effort in the Korean Action," unpublished draft in CCH Series V.M.2.1.; NSA, "Review of U.S. Cryptologic Effort, 1952-54," in CCH series VI EE.1.3.; and [Hop Harriger] "A Historical Study . . ." The latter document contains the fullest explanation of the Yoke operation.
41. [Hop Harriger] "A Historical Study . . .," 72.
42. The new operation is described in USAFSS, "Analysis of AFSS Effort . . ."; "Historical Data Report for the 6920 SG, 1 January 1953,"; interview with Delmar Lang [undated], in CCH Series VI, AFSS section; and Major Chancel T. French, "Deadly Advantage: Signals Intelligence in Combat, V. II," Air University Research Report # AU-ARI-84-1, 1984.
43. French, "Deadly Advantage . . ."; oral history interview Col (USA, Ret.) Russell H. Horton, 14 March 1982 by Robert D. Farley, NSA Oral History 6-82.
44. U.S. Naval Security Group, "U.S. Naval Communications Supplementary Activities in the Korean Conflict, June 1950-August 1953," in CCH Series V.H.3.1.
45. Richard Chun, unpublished manuscript in CCH Series V.M.1.11.
46. Drake and others, "The COMINT Role in the Korean War."
47. Assistant Chief of Staff, G-2, "COMINT Operations . . ."
48. [Drake and others] "The COMINT Role in the Korean War."

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

~~TOP SECRET UMBRA~~

49. "U.S. Cryptographic Assistance and COMINT Collaboration with the ROK," 24 February 1955, in CCH Series V.M.6.5.
50. File of memos related to the history of AFSA/NSA communications center, in CCH Series VI.H.1.2.
51. NSA, "Study of the COMINT Situation in Korea," undated memo (probably December 1952) in CCH Series V.M.1.14.
52. "Agreement on COMINT activities between the U.S. and the Republic of Korea, 1956," in CCH Series V.M.6.3.
53. Brownell Committee Report, G-1-G-2; see also Mary E. Holub, Joyce M. Homs and SSgt Kay B. Grice, "A Chronology of Significant Events in the History of Electronic Security Command, 1948-1988," 1 March 1990, in CCH Series X.J.6.
54. CCH Series VI.A.1.3.
55. "Study of the COMINT Situation in Korea."
56. "Analysis of AFSS Effort in the Korean Action."
57. "Study of the COMINT Situation in Korea."
58. USCIB memorandum, 20 July 1950, and NSC memorandum dated 27 July, in Harry S. Truman Library, Independence, Missouri (contained in CCH Series XVI).
59. "The History of SIGINT in the Central Intelligence Agency, 1947-1970," October 1971, V. I., 86 in CIA history collection, Ames Building, Rosslyn, Virginia.

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

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

~~TOP SECRET UMBRA~~

Chapter 3

Cryptology under New Management

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

There is something about cryptologic work that gets into the hide. . . .

Ralph Canine, 1968

NSA began life under a pall. The Brownell Committee had declared its predecessor to have been a failure. Outside the cryptologic community there was a common feeling that COMINT was broken and in serious need of repair. According to [redacted] who was appointed by Allen Dulles to ride herd on the cryptologic effort,

The early 1950s were the dark ages for communications intelligence. Intelligence officers who had been accustomed to providing information not only on the capabilities but also on the intentions of the enemy during World War II were reduced to providing the government with estimates based on frail fragments of information rather than factual foreknowledge. [redacted]

The creation of NSA was an attempt to address the problems of cryptology as the Brownell Committee saw them. (As we saw in the section on Korea, that perception was not 100 percent accurate.) That is, it attempted to institute a firm control mechanism that would unify the system and create an organization which was, in and of itself, responsible for getting the job done. No longer would consumers have to go to four different organizations to get answers or to fix blame for the lack of answers. It did not give the organization resources, improve its personnel situation, or give it adequate working space.

When NSA began life, it simply inherited its resources from its predecessor. It got the AFSA billets and the people in them, the AFSA spaces at Arlington Hall, and the AFSA rooms at the Naval Security Station. And it inherited an idea, that unification worked better than division. The difficulty was in trying to implement the solutions that the Truman Memorandum imposed. AFSA, despite its failings, had been a step in the right direction. NSA now had to take the next step.

To the AFSA population, the name change must have seemed more for appearance than for any practical value. There was no immediate change in their condition. They stayed where they were - if they were COMINTers, they remained at Arlington Hall, and if they were COMSECers, they stayed at Nebraska Avenue. Lieutenant General Canine, who had replaced Admiral Stone as AFSA director, stayed on as director of NSA. When Canine first gathered the NSA work force together on 25 November 1952, he alluded to the conflicts which had preceded the establishment of NSA, but they must have seemed remote to those who listened. It looked like business as usual.

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

~~TOP SECRET UMBRA~~



Lieutenant General Ralph J. Canine went to bat for the new organization at a time when its existence was challenged and its longevity was far from certain.

Canine and the New Organization

But it was not to be business as usual, largely because of the personality of the first director. Lieutenant General Ralph Canine, who dominated early NSA policies and stamped his character on the Agency, had been a line Army officer with no intelligence experience until he became deputy assistant chief of staff for army intelligence in 1949. Prior to that he had been an artillery officer, with wide experience in combat (both world wars, serving under Patton in World War II) as well as logistics. Although he brought no technical education to cryptology, he exerted his influence through a hands-on management style. He was forceful and determined and tenaciously enforced the Brownell recommendations on the reluctant SCAs. His whimsical personality produced legions of "Canine stories," which simply embellished his reputation as a maverick. Collins proclaimed him a "fortunate choice," and said that "he . . . raised the National Security Agency from a second-rate to a first-rate organization."² Canine was no diplomat,

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

and he might have failed had he come along ten years later. In 1952, however, he was the right man for the job.

One of the first things Canine did was to get rid of the triumvirate of service deputies who, under AFSA, had represented their own service interests rather than the interests of the central organization. He replaced them with a single vice-director, and named Joseph Wenger to fill the position. But Wenger was probably not very happy as the vice-director. By all contemporary accounts, Canine served as his own vice-director. He tended to make all key decisions himself. He had no patience with long vertical lines of control, and when he wanted an answer, he went directly to the person involved. He relied on his staff to keep others in the chain of command informed of his comings and goings but did not feel bound, himself, to use the chain. The system smacked of paternalism, and one of Canine's subordinates once said, "Whenever I see him nowadays, I expect him to pat me on the head."³

Canine organized NSA rather like AFSA had been structured, with Production, COMSEC, and R&D being the major divisions. But he broke Administration into its component pieces (security, personnel, training, logistics, and plans and policy) and placed them on his "special staff," a classically army way of doing things. The office designation system was a trigraph, NSA followed by a dinome: for instance, NSA-02 was the Office of Operations.

In February 1953 Canine changed Operations to Production, or NSA-06. Production was structured much like a factory, in which the parts of the cryptologic process were organized functionally rather than geographically. The major divisions within Production were Collection (NSA-60), Analysis (NSA-70), Machine Processing (NSA-80), and Exploitation (NSA-90). Although NSA has since changed over to a more geographical approach, the original organization more closely corresponded to how cryptologists viewed their profession at the time - as part of a complex process suitable primarily for highly skilled factory technicians. What made cryptology different from other intelligence disciplines was both the intricate technical challenge and the assembly-line processing system. It also represented NSA's way of conceptualizing the process of intelligence - as underlying data revealed through mathematical attack rather than as cognitive insight arrived at through inspiration.⁴

The Early Work Force

The Korean War had ushered in a period of explosive growth in the cryptologic population. This was followed by a long period of fairly steady personnel growth, as Table 1 shows.

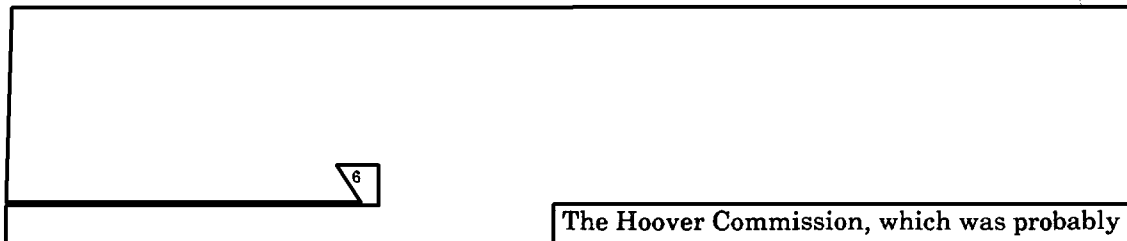
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

Table 1
Cryptologic Population, 1949-1960⁵

| Year | AFSA | NSA | Totals (includes SCAs) |
|-------------|-------------|------------|-------------------------------|
| Dec 1949 | 4,139 | | 10,745 |
| Dec 1952 | | 8,760 | 33,010 |
| Nov 1956 | | 10,380 | 50,550 |
| Nov 1960 | | 12,120 | 72,560 |

The work force in 1952 was double what it had been under AFSA, but it was still smaller than either ASA or USAFSS and larger only than NSG.



The Hoover Commission, which was probably the most extensive investigation of the federal bureaucracy ever, estimated that cryptologic costs amounted to about half a billion dollars.⁷

In the early days, the work force was about one-third military and two-thirds civilian. A snapshot of NSA's work force in 1956 (Table 2) showed most of the population working in Production.

Pay tables were not quite as generous in those days, as Table 3 clearly shows. A grade 5 employee (the most numerous group of NSA employees) started out making \$3,410, which smacks of impoverishment. But with houses costing below \$10,000, and frequently below \$5,000, employees may have been just as well off in real terms then.

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

~~TOP SECRET UMBRA~~

Table 2
NSA's Work Force by Organization, 1956

Element
Production
R&D
COMSEC
Communications
Training
Directorate,
admin, overseas
Totals

[Redacted Table Content]

Table 3
Pay grade allocations and salary (basic level) 1952 and 1993⁸

| Grade | Salary 1952 | 1993 | Grade Alloc 1952 | 1993 |
|-------|-------------|----------|------------------|--------|
| 1 | \$2,500 | \$11,903 | (0.2%) | (0%) |
| 2 | 2,750 | 13,382 | (0.7) | (0.07) |
| 3 | 2,950 | 14,603 | (6.5) | (0.5) |
| 4 | 3,175 | 16,393 | (13) | (0.7) |
| 5 | 3,410 | 18,340 | (26) | (1.9) |
| 6 | 3,795 | 20,443 | (7) | (1.6) |
| 7 | 4,205 | 22,717 | (18) | (4.9) |
| 8 | 4,620 | 25,259 | (1.5) | (1) |
| 9 | 5,060 | 27,789 | (12) | (6.8) |
| 10 | 5,500 | 30,603 | (0.5) | (0.2) |
| 11 | 5,940 | 33,623 | (7) | (12.1) |
| 12 | 7,040 | 40,298 | (4) | (22.1) |
| 13 | 8,360 | 47,920 | (2) | (26) |
| 14 | 9,600 | 56,627 | (0.8) | (11.5) |
| 15 | 10,800 | 66,609 | (0.6) | (6) |
| 16 | 12,000 | - | (.02) | |
| 17 | 13,000 | - | (.02) | (2) |
| 18 | 14,800 | - | (.02) | |

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

Included in Table 3 are the grade allocations in 1952 compared with those in 1993. This is a striking illustration of grade creep – more of a gallop than a creep. In 1952 the average grade was 6.7, while in 1993 it was 11.7, a grade inflation averaging fully five General Schedule grades over a period of forty-one years. This followed the trends in the general federal work force: in 1952, the average grade was GS-5.5, while in 1993 it was GS-9.

The conditions under which NSA employees labored were not much different from the AFSA days. Offices were badly overcrowded, especially at Arlington Hall. In 1954 approximately 30 percent of the work force worked the evening shift to relieve overcrowding on days. Air conditioning in the Washington area was still virtually unknown, and the NSA hot weather policy permitted relief from work only when conditions became fairly unbearable, as the temperature versus humidity chart (Table 4) shows. On really hot days the man whirling the hygrometer was the most popular person at the station.

Table 4
NSA Employees Could be Released When

| Temperature reached | And humidity reached |
|---------------------|----------------------|
| 95 | 55 |
| 96 | 52 |
| 97 | 49 |
| 98 | 45 |
| 99 | 42 |
| 100 | 38 |

There was a view, widely held in 1952, that the expertise of the civilian work force had declined since 1945. This was to some extent true. Not only had ASA and NSG lost some of their best minds at the end of the war, but the structure of the central organization created built-in problems for the civilian promotion system. The Navy had always run its cryptologic service with military officers, while the Army, believing that military officers rotated too frequently, had let its civilian work force run the cryptologic effort. By 1949, when AFSA was formed, NSG had a number of very senior officers involved in the business, and many of those people transferred into AFSA. Admiral Stone placed them in the key leadership positions, and the Army civilians were often shunted aside. Moreover, Stone took no steps to create a senior civilian work force, and when he departed in favor of Canine, there were no civilians above grade 15.

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

In 1953 a committee chaired by H. P. Robertson of California Institute of Technology (more commonly referred to simply as Cal Tech; see p. 227) looked at NSA's future and concluded that there was no future if the Agency was unable to obtain and retain outstanding civilians in various technical fields. This, according to Robertson, would require the establishment of a cryptologic career management program within NSA, with regular progression through the grade ranks and supergrade promotions to the top performers. The Robertson Committee also concluded that the services would have to improve their own cryptologic career advancement programs to attract and retain good uniformed people to COMINT. Robertson noted the lack of such a program in the Army and the lack of a stateside rotational base. (At the time, fully 66 percent of all ASAers were overseas.)⁹

Canine met this problem head-on. Soon after the Robertson Report was released, he directed the personnel office to begin working on a cryptologic career system, with technical specialties and a system of regular advancement. This work was well under way by early 1954 and eventually led to the structuring of the current cryptologic career program for civilians. Canine was credited personally with getting NSA's first three supergrades: William Friedman, Abraham Sinkov, and Solomon Kullback. (Frank Rowlett, hired in 1930 with Sinkov and Kullback, had joined CIA and so was not on the list.) Even more significant, in 1953 he obtained for NSA the authority to hire under the so-called Civil Service Rule Schedule A, which permitted NSA to hire without obtaining permission from the Civil Service Commission. Rather than having NSA applicants take the standard Civil Service test and then having a board interview the top three scorers NSA devised its own peculiar aptitude tests, and hired without outside interference.¹⁰

Under Canine, NSA moved in many directions at once to strengthen its civilian work force. The director got NSA a slot at the National War College in 1953, and Louis Tordella was the first appointment, Abraham Sinkov the second.¹¹ The Training Division initiated a presupervisory training program, which was curtailed in 1955 in favor of an intern training program oriented more toward technical education.¹² NSA began local recruiting in the Baltimore and Washington areas by 1954.¹³

Fielding the Field Offices

Canine moved very aggressively to establish field offices. Under Stone, AFSA had had no field organization, and the censorial AFSAC appeared to guarantee continuation of the situation. But as soon as he became AFSA director, Canine made an end-run around AFSAC. On a trip to the Far East in September of 1951, he got the concurrence of the theater commander for an AFSA field office and returned to Washington with a fait accompli. Early objections by NSG were muffled when Canine named Captain Wesley A. ("Ham") Wright, one of the most senior naval cryptologists, to head the newly formed AFSA Far East office in Tokyo. By the time AFSAC got around to considering this

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

~~TOP SECRET UMBRA~~

surreptitious move in January of 1952, the office already existed (official date: 1 January 1952) with Wright and a staff of six. When AFSAC approved a formal charter, it stripped Wright of any direct control over SCA field operations, but Canine had the nucleus of a field organization and awaited only the creation of NSA to augment the authorities of the chief.

In Europe, Canine began by sending a top civilian, Hugh Erskine, on a survey trip, the result of which, as in the Far East, was theater command concurrence with an AFSA branch office. This time Canine submitted his plan to AFSAC before officially establishing the office. AFSAC approved, and Erskine began work formally on 1 September 1952 in offices in the I.G. Farben building in Frankfurt.¹⁴ NSAEUR competed for a time with an office titled NSAUK (NSA United Kingdom), located in London, and the two shared responsibility for some of the continental COMINT functions - for instance, [redacted] This lasted until 1956, when NSAUK was abruptly disestablished.

When CINCEUR shifted to Paris in 1954, NSAEUR stayed in Frankfurt but finally shifted to Camp des Loges, outside Paris, in 1963. While the policy and liaison functions resided there, [redacted]

Once NSA was officially established, Canine moved swiftly to create more field offices. NSA Alaska (NSAAL) was created in July 1953, NSAUK on 26 August 1953, and NSAPAC, established to advise CINCPAC, on 16 August 1954. He also created at home an office to monitor field operations.¹⁶

Backed by the authority of NSCID 9 (the predecessor of the present-day NSCID 6), Canine imposed on the reluctant SCAs a group of field offices that had basically the same power as he himself within their geographic spheres. They had two functions - liaison with theater commanders and technical control of the theater COMINT system. Their main reason for existence was to impose order on the chaotic growth of the field sites, and they established large and active technical staffs which worked directly with the sites. NSA field offices could task SCA field sites directly (although they customarily did not do so). NSA's theater chiefs strove to create a cooperative atmosphere with the SCAs, but everyone involved recognized the implied threat that they represented as personal emissaries of the feared Canine. The SCA field chiefs fought this "encroachment" into their territory with every resource at their disposal.¹⁷

During and after World War II, American military organization in the Atlantic and Pacific theaters contained inherent turf conflicts. In Europe, for instance, the main power resided with CINCEUR (originally in Frankfurt), but there was also a military organization in Great Britain that competed with it for power. In the Pacific the competition between CINC Far East (MacArthur) and CINCPAC (Nimitz) was even more stark. And so it was with NSA organizations. In Europe, the latent competition between

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

the NSA offices in Great Britain and Germany was resolved in 1956, but in the Far East the competition between the offices in Tokyo and Hawaii continued for many years.

[REDACTED]

Civilians in the Trenches – the Civop Program

In the early 1950s NSA turned to the problem of field site collection. Military operator turnover was high, some years as high as 85 percent. The long-range expansion of intercept positions set by JCS during the Korean War appeared to be a dead letter unless a stable manpower pool could be established. NSA liked what it had seen of the GCHQ program of hiring civilian operators because of the exceptionally long retention rates and

[REDACTED] NSA was also aware that CIA was hiring civilian operators for

[REDACTED] Negotiations were begun with ASA, and in 1954 an agreement was hammered out which would start with a pool of one hundred civilian operators at four ASA field sites: [REDACTED]

[REDACTED] NSA would recruit and train the operators, who would be under the control of the field site commander. For the initial group, rotation at all four bases was set at two years, and the grade ranges for the program were 5 through 11. The NSA planning group waxed a little poetic, formulating long-range plans for thousands of operators and an eventual NSA field site of its own.

The trial group was duly recruited, trained, and deployed. But even as things were moving ahead, the services' attitudes were beginning to cool. NSA promised to recruit only operators who had retired from service, but ASA and USAFSS foresaw keen competition for their first-term operators contemplating better salaries doing the same job for NSA. By 1957 the services had turned against the program, and it was quietly discontinued. It had long-lasting beneficial results, however. It yielded, in later years, a cadre of experienced civilian operators who performed well in crisis after crisis.¹⁸

COMINT Reporting in Transition

The reporting legacy of World War II was translations. ASA and NSG issued thousands of translations per month, a reflection of the huge volume of readable traffic. Once the cryptanalyst had finished his or her job, and the translator had put the message into readable English, the verbatim transcript was released to either G2 or the theater commander (in the case of the Army) or Office of Naval Intelligence or the appropriate naval commander (in the case of the Navy). The mechanism for this was to hand the information in raw form to an intelligence analyst collocated with the cryptologic organization. Traffic analytic information was also passed in bulk to the appropriate

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

~~TOP SECRET UMBRA~~

intelligence organization, which would put it into readable intelligence. In other words, the COMINT factory simply passed raw information to the organization, which would itself put it in context.

The postwar cryptologic community continued to produce primarily translations, accompanied by all the COMINT technical information [redacted] [redacted] necessary for the service intelligence analyst to analyze it. NSA was not supposed to analyze. The information (it could not be dignified with the term "report") lacked a serialization resembling the modern system. [redacted]

19

AFSA began to evolve a similar system. Releases tended more and more toward reporting rather than translations, [redacted] Reports were more formal and had wider distribution. AFSA devised its own primitive serialization system: an example would be [redacted] followed by a date. [redacted] was the subject matter [redacted] and 13-50 indicated this was the thirteenth report produced in 1950 by that section. But reports still contained [redacted] and other sorts of technical data later prohibited in COMINT reporting, and narrative portions were often very heavy on discussion of details of [redacted] rather than on higher-level information like unit movements. The distribution was still very limited by modern standards. Collocated organizations (ASA, USAFSS, and NSG representatives, for example) decided who in their services should see the information and made further distribution from there.²⁰

Early NSA reporting was more formal still. [redacted]

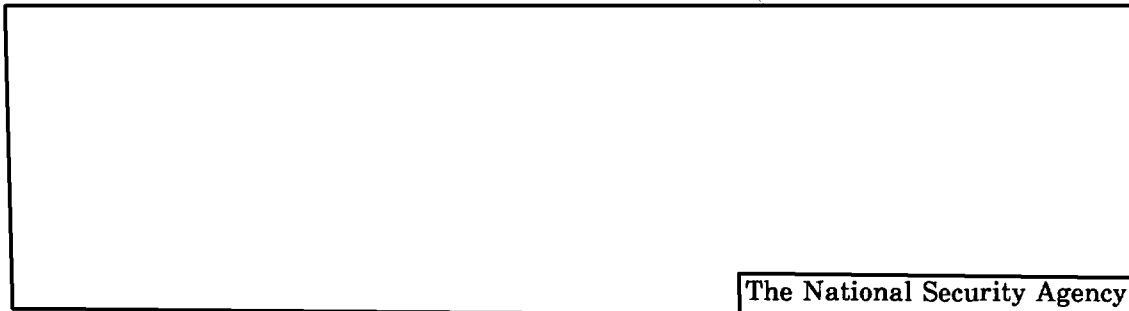
Distribution was broader as NSA ceased to rely on the SCA and service intelligence collocated liaison offices to distribute further. Reports in 1953 still contained [redacted] [redacted] had finally been expunged. There was still much information [redacted] but analytical conclusions were now separated into a "Comments" section at the end of the report.²¹ Later in 1953 NSA excluded "COMINT technical data" from product reports completely and formed an Operational Management Control Group to enforce discipline. Collateral information could be used when necessary.²²

The COMINT reporter was often bedeviled by the same problems then as today. Periodically NSA organizations would chastise reporters for overusing qualifiers like "possibly" and "probably." A 1953 memo found NSA reporting "generally so cluttered with qualifying expressions as to virtually preclude their use by a consumer."²³

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

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

~~TOP SECRET UMBRA~~



was a term shop.²⁴

The National Security Agency

In 1955 the Hoover Commission declared that NSA, while producing some very valuable information, was not an official member of the intelligence community. But the commission undercut this general statement by noting that the volume of COMINT was so huge that it could never all be turned over to consumers, and by the very act of selecting individual pieces for dissemination, NSA made analytic judgments about value and applicability.²⁵

This trend was to continue and intensify. Key NSA executives knew that the organization had to move away from translations and into true intelligence reporting. Various sources of COMINT had to be synthesized, and the results must be packaged into a meaningful explanation of the situation. If possible, the reporter should make comments as to meaning and, on occasion, should make conclusions based on COMINT. This was a higher level of analysis than the rest of the intelligence community foresaw for NSA, and it would get the organization into trouble with consumers who resented what they regarded as turf encroachment. But it was the wave of the future.

NSA Training - The Early Years

Training had been the "bastard child" of AFSA. Originally the training school had been a section of the personnel office, a way station for new and uncleared personnel. New recruits were given unclassified Army traffic analysis and communications manuals to read until their clearances came through. The training was good - many of the manuals were written by Friedman himself - but the way AFSA treated the problem was all wrong. The staff was miniscule, facilities practically nonexistent, and the function was almost totally ignored. The real training concept was on-the-job training in the duty section. Almost all operations training was conducted in Production, with little centralized control and practically no classroom instruction. There was a training staff that tried to coordinate all this, but it did not work in the same organization as the cryptologic school, which was still part of personnel.²⁶

When the Korean War began, the training school was still in languid decay, with one hundred uncleared recruits reading musty traffic analysis manuals in the training spaces at Nebraska Avenue, supervised by a staff of six people. By the end of the year all was

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

~~TOP SECRET UMBRA~~

chaos. There were 1,100 trainees jammed into the same spaces, still with a staff of 6. Canine was aware of the problem, and AFSA went to work to improve the situation. In April of 1951 the school was moved to larger quarters at 1436 U Street, N.W., designated Tempo R. In June 1954 the school moved to another World War II building – Tempo X – located on the north side of East Capitol Street, in the area that is now part of the RFK Stadium parking lot. When, in the mid-1950s, NSA moved to Fort Meade, the training school moved to a former hospital a couple of miles from the main NSA complex.

Canine later separated training from the Office of Personnel and elevated it to the level of Office of Training. Its chief was named commandant of the NSA School. Canine was also a proponent of management training, which was begun in 1952, and he placed the first NSA students in service war colleges in 1953.

AFSA also began paying more attention to formal classroom instruction. Instead of the "sit in the corner and read a book" approach, it began offering a selection of classroom traffic analysis, cryptanalysis, mathematics, language, and technical training. By 1952 the school was offering training (at some level, at least) in eighteen different languages. Secretaries got instruction in clerical and stenographic skills, and there was a four-week teletype operators course for those assigned to communications. There was also a one-week indoctrination course for all new hires, with follow-on instruction for certain specialties.²⁷ By mid-1952 AFSA was also offering three levels of management training – junior (presupervisory), supervisor, and executive. Classes were very small, but at least a rudimentary program existed.

NSA also began using education as inducement. Begun under AFSA, the College Contract Program began with a contract with George Washington University and amounted to NSA payment of tuition to qualifiers. Classes were held at Arlington Hall, Nebraska Avenue in the District, and at Thomas Jefferson Junior High School in Virginia. There was also a program for graduate students and, for a select few, a fellowship program which offered full-time study away from NSA.

NSA's role in broader cryptologic training within the services was less certain. Both AFSA and NSA enjoyed a theoretical technical control of cryptologic standards, which included training, but AFSA never exercised its review function. An early AFSA proposal to create a consolidated cryptologic training school was scuttled by Brigadier General Roy Lynn, an AFSA deputy director, who was concerned about retaining USAF Security Service independence.

After 1952, things began to change as NSA became active in reviewing SCA cryptologic courses. The Agency was especially active in providing technical assistance for language training and at one time took responsibility for all language training beyond the basic level. It did not, however, try to take on COMSEC training, preferring to leave that to the SCAs.

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

Canine continued to strengthen the organizational position of the training function. As it migrated up from branch to division level, it took on added responsibilities and acquired more resources. The people who were involved in training in those early days were first rate - Lambros D. Callimahos (a close protégé of Friedman) and Navy captain Thomas "Tommy" Dyer (one of the Navy's great pioneers in codebreaking) were especially notable examples. William Friedman, who had personally built the Army's cryptanalytic system, spent much of his career as a teacher and authored many textbooks on cryptanalysis. With such talent and influence, it was only a matter of time before NSA's training system became a model.

Setting Up Security

Security was one area with which Canine had experience, and he tackled it very early. Under AFSA, perimeter guards at Arlington Hall and Nebraska Avenue had been uncleared. Interior guard duty was pulled on a rotating basis by reluctant uniformed cryptologists, each division taking its turn for a month at a time. Canine eliminated the interior guard duty in early 1952 by bringing in cleared, uniformed security police. Later he decided to add some prestige to the NSA guard force and convinced the Navy to give up a detachment of Marine guards to begin guarding the new temporary NSA facilities at Fort Meade in 1955. Normally reserved for embassy duty, the Marine guard detachment became a fixture and source of pride at NSA for many years.²⁸

Given the size of the cryptologic complex in Washington, some sort of universal personnel identification system became necessary. The Army appears to have begun using personnel badges during World War II. Their badges in those days were round metal tabs with a picture overlaid with plastic - fully cleared people had red badges, opposite the system of today. After a costly experiment with glass badges, AFSA settled on a plastic badge. Color coding identified organization, with seven colors total. In 1956 the organizational affiliation began to fade as NSA reduced the number of colors for cleared people to four and began using green badges for fully cleared employees. Metal badges returned in 1959 and were standard until the late 1970s. NSA employees found them ideal for scraping ice off windshields.²⁹

Along with a badge system, NSA began restricting area access. By 1953 the security division had devised three work area designations: restricted, secure, and exclusion. The "red seal" and "blue seal" tabs used for so many years to designate compartmented areas did not, however, come into use until NSA moved to its new quarters at Fort Meade in 1957.³⁰

NSA's controversial experiment in polygraph screening was rooted in the Korean War. As new employees flooded into the training school at Nebraska Avenue, the security system was overwhelmed with clearance requirements. Then, as now, employees were cleared through a combination of the National Agency Check and background

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

investigations, conducted by the services. By December 1950 the system was so inundated that 39 percent of AFSA employees were uncleared. NSA security people began casting about for a quick way to process clearances and fastened their attention on the polygraph, long used by law enforcement agencies in criminal investigations. Although polygraphs were not admissible in court, AFSA discovered that CIA had begun using them for people being indoctrinated for COMINT as early as 1948 and only two months earlier, had broadened testing to include the entire CIA work force.³¹ Studies showed it to be a more reliable indicator of loyalty than the background investigation, and it was proposed that the polygraph be tried as a way to get an "interim" clearance. Canine approved a trial program in January 1951, but implementation was tricky. AFSA had to buy the equipment, recruit polygraph examiners from the police departments and private detective agencies around the country, build soundproof rooms for the interviews, and become experienced in interpreting results in this new and experimental area of loyalty verification.

The new polygraph procedures began on a trial basis at the U Street location in May of 1951. Soon examiners were working from seven in the morning to eleven at night. By the end of September, they had cleared the backlog and went back to regular hours. AFSA had suddenly acquired hundreds of employees with something called a "temporary" clearance, who still required completion of the background investigation to become "permanent." But in the helter-skelter time of war, no one paid the slightest attention to the difference, and on the day NSA was created a large portion of the work force worked with a temporary clearance. This situation would come back to haunt NSA in 1960 when Martin and Mitchell fled to Moscow and NSA's clearance practices were called into question. (See p. 280.)

In the rush to clear people, there was considerable breakage. Examiners were used to dealing with criminal investigations, and some of them had trouble making the transition. Hostile questions elicited emotional responses, and the rate of unresolved interviews approached 25 percent. The incredibly long hours added to the stress, and by the end of the first summer it was hard to tell who was more stressed, the examiners or the examinees. But after a very bumpy start, things smoothed out, and the security organization claimed to have cleared up lingering administrative problems by 1953.

When first begun, the polygraph was "voluntary," but Canine declared that if an applicant did not volunteer, the application went no further. The fiction of optional polygraphs continued until 6 December 1953, after that historic date all applicants were polygraphed. But there were always exceptions to the general rule that all employees were polygraphed. No requirement was established to include existing employees in the system, and the military, amid much controversy, refused to allow its people to be polygraphed.³²

The modern (and usually functional, if somewhat cranky) classified waste disposal system of the 1990s was a good deal less high-tech in 1952. Early destruction at both

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

Arlington Hall and Nebraska Avenue was by incineration. Burnbags were stapled shut, as they are today, were marked with the originators' organization, and were placed in central collection locations. Once picked up, they were pitched into the fire by a military detail, and destruction was certified by a commissioned officer.

In late 1951 AFSA, determined to modernize the procedure, ordered two Somat machines, which AFSA officials had seen in operation at CIA. The machines operated much like the present destruction facility but on a much smaller scale. There was a whirling tub resembling a cement mixer, into which the burnbags were thrown. The door was then closed, water was injected, and the tub churned. But the early models did not work very well, and the whole process was as dirty as a paper mill. NSA later returned to the old standby incinerator until something better could be devised.³³

NSA AND THE U.S. INTELLIGENCE SYSTEM

NSA and its director were coping with the problems – technical, organizational, and fiscal – in establishing a truly global SIGINT system, which at one and the same time would serve national and parochial interests. This required a strong central institution and considerable adjustment of the old ways of doing business. When Canine tried to make the adjustments, he ran into opposition from every direction. His attempts to impose uniformity were opposed by the SCAs, while his SIGINT turf was simultaneously being invaded by the CIA.

Consumer Groups Come to NSA

The modern method of marketing SIGINT is primarily through Cryptologic Support Groups (CSGs) accredited to consumer organizations. Many NSAers are surprised that it was not always such. But in fact, the system began exactly opposite. In the beginning, consumers established liaison detachments (sometimes referred to as "beachheads") within NSA. Indeed, NSCID 9 codified what already existed in AFSA when it stated that "the Director shall make provision for participation by representatives of each of the departments and agencies eligible to receive COMINT products in those offices of NSA where priorities of intercept and processing are finally planned." The motivating force appears to have been to give customers a voice in setting COMINT collection and reporting priorities. But the customers did not limit themselves to expressing requirements. All of them sifted COMINT information and interpreted the meaning back to their parent organizations. Some of them actually produced their own report series and distributed them to their home offices.

In the beginning, many of these organizations were quite large and robust: in 1954 both Army and Office of Naval Intelligence had fifty-two analysts at NSA, CIA had

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

[redacted] and State had four. Air Force Security Service, however, had by far the largest, a total of eighty-one analysts working in an outfit called AFSSOP (Air Force Security Service Office of Production), which produced COMINT summaries digested from the mass of technical information available only at NSA headquarters.

NSA did not like the system, and over the years it made moves to cut off the flow of technical information that kept the consumer groups alive. These attempts were initially unsuccessful, but the beachheads gradually became smaller and finally faded out of existence, victims of an aggressive NSA external reporting program that made them unnecessary. By the end of the 1950s they were gone, except for liaison detachments that had no production or interpretive responsibilities.³⁴

The Struggle for Technical Control

NSCID 9 gave NSA "operational and technical control" of all U.S. COMINT operations. This revolutionary authority proved to be the glue that knit the COMINT community together.

Those who have lived within a unified system all their working lives cannot appreciate the technical problems that confronted NSA in November 1952. For instance, among the British, Army, and Navy, there were in the 1940s seven different naming conventions for Soviet codes and ciphers.

- The Navy began the Second World War using [redacted]
- The British began with [redacted]
- The Army began with [redacted]
- The Navy copied Soviet intercept [redacted] while the Army used an [redacted]
- The British were copying things [redacted]

Each organization had its own traffic formats. When the traffic came into NSA, it all had to be hand-massaged to make it suitable for any sort of processing. A coordinated attack on high-grade systems would be too time-intensive without standardization.³⁵ Someone had to dictate formats.

The impetus behind standardization was processing. Raw traffic and digested extracts (called TECSUMs, or technical summaries) cascaded into NSA headquarters in unmanageable volumes. An NSA Technical Management Board created soon after NSA

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

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

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

itself was established concluded that collection, and thus collection equipment, would have to be homogenized to permit NSA to process the traffic.

The original vehicle for securing compliance was a program of NSA circulars. They covered procedures for intercept, traffic forwarding, end product reporting, and services and facilities. In addition, NSA published Unit Operations Orders describing in general terms the mission of each unit authorized to produce COMINT. These publications, when taken together, constituted the NSA Field Operating Manual, a device borrowed directly from Army usage. Canine regarded them as directive, and he tenaciously enforced compliance, but the SCAs resisted. They initially regarded NSA directives as voluntary suggestions.³⁶

By 1956 the SCA units were having trouble distinguishing operating policy from technical guidance, which had over the preceding four years become hopelessly scrambled between the two categories of documents. So NSA created a new system that looked a lot less like an Army directive, called MUSCO (Manual of U.S. COMINT Operations). Within two years ELINT had been added to the national cryptologic mission, and MUSCO was changed again, to MUSSO (Manual of U.S. SIGINT operations). On those occasions when a consumer needed to know how SIGINT was produced or what NSA's operating policy was, a special series of MUSSO documents called INFOCONS was issued.³⁷

In April 1954, Canine unceremoniously yanked control of field site placement away from the SCAs. Henceforth, the establishment of field sites would be done only with the permission of the director. Even site surveys had to be coordinated with NSA first. Canine relented to the extent of allowing SCAs to place small (less than ten-position) sites during peacetime without his direct "chop." The important message, however, was that DIRNSA had now delegated this authority, implying rather directly that what he delegated he could rescind.³⁸

And while he was at it, the director pushed the concept, completely foreign to the SCAs, of cross-servicing, whereby targets would be collected by the most technically capable intercept site regardless of service affiliation. During the Korean War, for instance, ASA sites collected a good deal of North Korean air force communications under the cross-servicing concept (and to the loudly voiced complaints of USAFSS).³⁹

NSCID 9 gave the director untrammelled authority over COMINT direct support resources. A theater commander could request such support, but it was entirely up to DIRNSA whether the request was honored or not. Canine's directive on control of direct support assets narrowly defined the conditions under which the director would delegate control. When and if he did, it would normally be to the SCA chief, not an "unlettered" field commander. There were no provisions for appeal should DIRNSA deny the request. This provision of DIRNSA's authority stood basically unchallenged through the 1950s, a time when there was very little direct tactical support to be done, anyway. It did not become an issue until the advent of the war in Vietnam.

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

~~TOP SECRET UMBRA~~

Having destroyed the prerogatives of the armed services, Canine, barely a month later, released control of two ASA tactical units, [redacted] to the commanding general of ASA. He made it plain, however, that these units were being released solely at his sufferance and pointedly reserved the right to task them temporarily or withdraw them completely for national tasking, at any time.⁴⁰

In 1955, Canine decreed that new types of field site equipment would henceforth require NSA coordination. In a letter to the three SCA chiefs, he stated that NSA would establish standards for facilities and equipment, manning and staffing factors, site surveys, and operational procedures. NSA set up a large and aggressive R&D program to work out equipment and facility standards. The people and equipment for this effort had been inherited from ASA and NSG, though in San Antonio AFSS clung to its own R&D organization and was more independent in this respect than the other two services.⁴¹

The Decentralization Plan

While Canine moved to secure unchallenged authority over COMINT, he began, almost simultaneously, a parallel and apparently opposite program called "decentralization." The objective of the program was to improve the speed of delivery of COMINT information to consumers. [redacted]

42

43

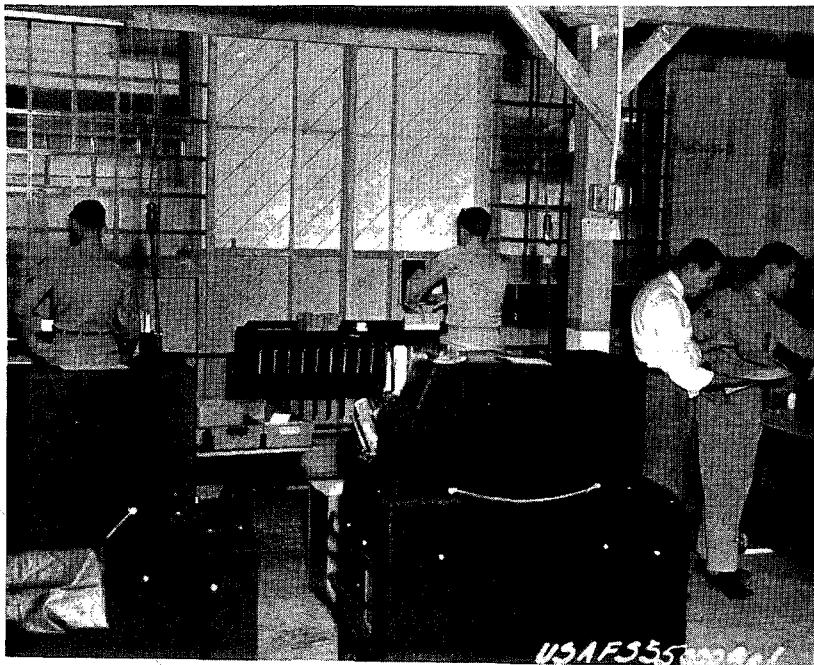
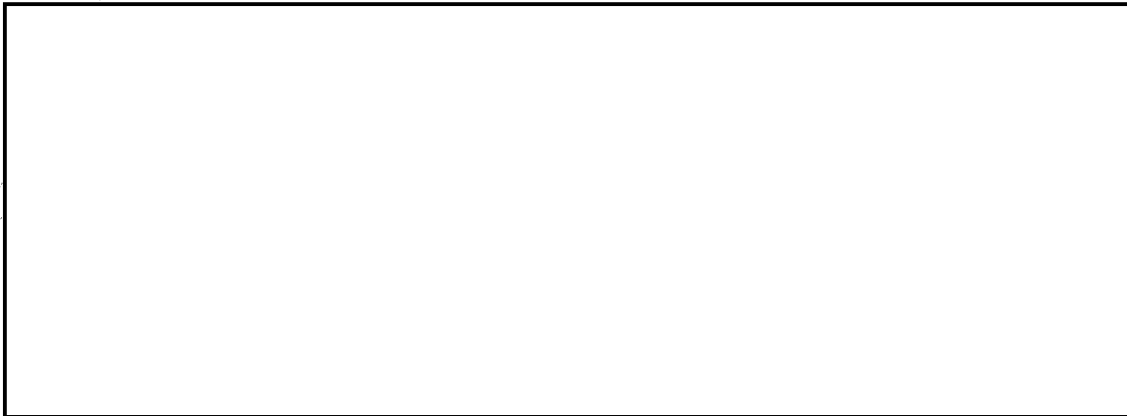
[redacted] The issue had been pushed hard by General Hoyt Vandenberg when he had been Chief of Staff of the Air Force. Vandenberg had wanted to make COMINT the basis for an independent Air Force intelligence component to back up the strategic force. Security Service and Air Force intelligence officials insisted on direct support and, in a series of conferences with NSA in the summer and fall of 1953,

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

~~TOP SECRET UMBRA~~

hammered out an agreement which resulted in NSA turning on a flow of high-precedence reports to both commands. This first included reporting from NSA but soon devolved on both field units and AFSCC. By 1954 NSA had reluctantly delegated analysis and reporting on the [redacted] problem to AFSCC, and it became the key player in COMINT warning to Air Force commands, a virtual third echelon competitor to NSA.⁴⁴

When the decentralization plan was officially launched in August 1954, it looked like planned engine thrust reversal. Under it, NSA assigned specific COMINT problems to specified field sites. The criteria for assignment were perishability, collectability, and



AFSCC, Brooks, AFB, 1950

AFSCC began 3rd echelon [redacted] using IBM punched card equipment

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

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



Relations with the SCAs

By the mid-1950s, Canine basically had what he wanted – unrestrained authority over the entire Defense COMINT system (with a single exception which will be discussed below). But it had not been a cost-free victory. Relations with all three SCAs were strained to a greater or lesser degree.

The relationship with ASA was probably the best. ASA and NSA came to agreement on key issues such as decentralization and release of operational control to direct support resources somewhat earlier than the other two services. ASA was of a mind to play the centralization game with NSA “straight up” and gained considerable good will as a result, occasional complaints from ASA field offices about “meddling” by NSA field offices notwithstanding.



Regarding naval COMINT, Canine and the Navy were speaking a different language. That they did not get into as many battles as NSA and the Air Force one can probably ascribe to the fact that most of the time they were simply speaking past each other.

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

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

Canine thought that Navy COMINT was organized like Army and Air Force COMINT, but this was not the case. The Navy had no integral cryptologic command akin to ASA or AFSS. Navy COMINT came under naval communications (OP-20), and fixed field sites were generally assigned to naval communications organizations for administrative and organizational matters. Naval afloat detachments were instruments of the fleet commander, not NSG. Certain central functions were performed at Nebraska Avenue by Naval Security Group, but it did not have the same authorities as its counterparts at Arlington Hall and Kelly AFB. In 1955, a frustrated Captain Jack Holtwick penned a lengthy memo bemoaning the difficulty that Canine was having with naval COMINT.



Captain Jack Holtwick
A highly influential naval cryptanalyst, Holtwick occupied key positions in the early NSA organization.

For more than ten years, people . . . have been talking about something which has never really existed as an entity, namely the Navy Cryptologic Agency. . . . These organizations [speaking of all Navy COMINT organizations] were an entity only insofar as they were engaged in the same trade and mutually complemented one another in it. They have never had a legal cryptologic organizational head, let alone a functional commander. Their lowest common superior was and is the Chief of Naval Operations. . . .⁴⁸

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



49

By 1956, however, Canine apparently understood enough of Navy COMINT organization to object to its entire philosophy. He took aim at the subordination of NSG detachment commanders to naval communications: "This is an unsatisfactory arrangement; there is always a conflict of basic interests in the direction of the units. The superior officers in the chain of command . . . are primarily concerned with general service communications; they are generally inexperienced in COMINT functions. . . ." He related the submersion of Navy COMINT to Navy communications with SCA position totals, in that from 1953 to 1956 NSG grew by only 7 percent, while ASA expanded by 380 percent and AFSS by 410 percent. This, he contended, resulted from deficient naval COMINT organization.⁵⁰

In contrast to NSG, AFSS growth was breathtaking. From a tiny cadre of 156 people in 1948, AFSS grew to 23,128 people by the end of 1960. The command had over 1,000 positions, a budget of more than \$26 million, and it had surged ahead of both ASA and NSG on all counts in only twelve years.⁵¹

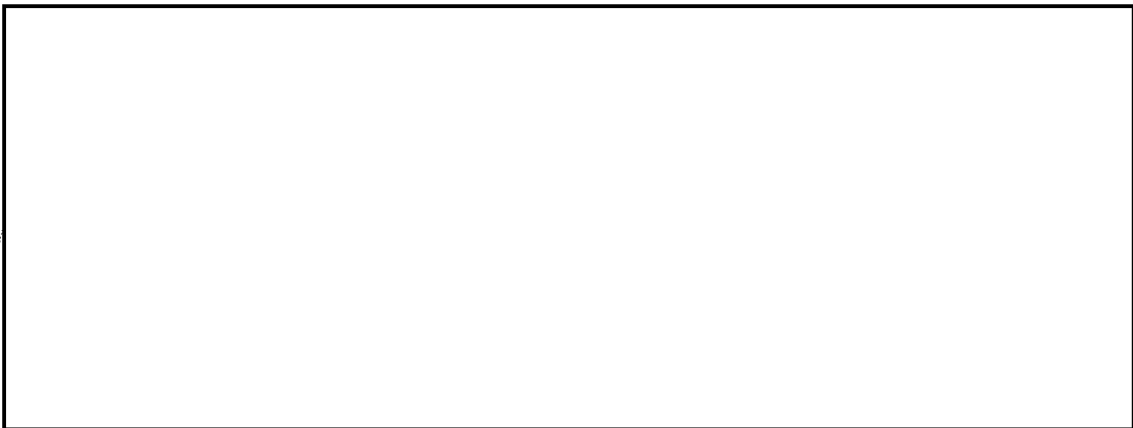
NSA's relations with AFSS, however, were the worst of the three. Although COMSEC relations were smooth, COMINT was not. Under the hollow gaze of AFSA, AFSS had virtually seceded from the COMINT community, carrying its entire field site list with it. It had called the field sites [redacted] so as to exempt them from AFSA tasking. (Major General John Morrison [USAF], a former NSA assistant director for production, once said that [redacted] with very isolated exceptions, were about as [redacted] as the Eifel Tower.")⁵² Canine's dicta on operational and technical control were intended largely to corral the errant AFSS resources. This was effective but did not make AFSS very happy.

The biggest row of the decade was over the Air Force Special Communications Center (AFSCC). Officially created in July 1953 as the 6901st Special Communications Center, AFSCC was intended as a third echelon processing center to satisfy Air Force desires for an indigenous Air Force COMINT center. The organization picked up such miscellaneous functions as the SSO system and the USAFSS training school but was intended all along as an analytical center and began functioning as one from its very first day of existence. Canine had said "No" to the Air Force plan but lost the battle. In January 1954 he gave up and, under the aegis of the decentralization plan, AFSCC acquired the mission of processing and reporting on the [redacted]. To this nucleus was added, over the years, virtually the entire [redacted] as well as, beginning in 1961, the [redacted].⁵³ Relationships continued to deteriorate, and by the end

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

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

of his term as DIRNSA, it was rumored that Canine was barely on speaking terms with the AFSS commander, Major General Hunt Bassett.⁵⁴



The SCAs Create Second Echelons

The decentralization plan spawned a second concept, [redacted] frequently wound up controlling related intercept positions at smaller units. The arrangement amounted to a de facto layering system in which large units controlled operations at smaller units, and in some cases the smaller units were officially subordinated to the larger ones. The intermediate tier came to be known as "second-echelon," while NSA (and in the Air Force, AFSCC) operations were called "third echelon."



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

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

~~TOP SECRET UMBRA~~

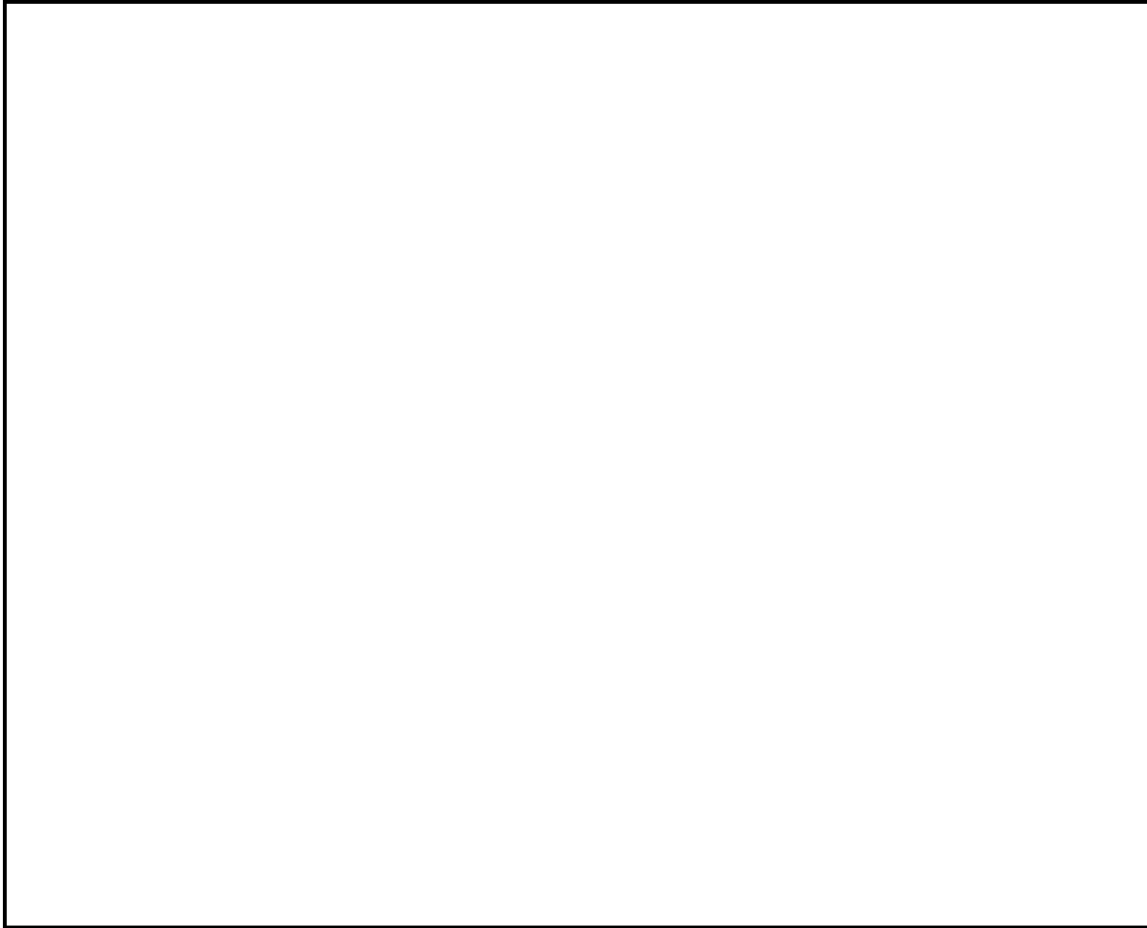


I.G. Farben Building

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



All three services created administrative units to supervise theater intercept sites, and to serve a liaison function with the supported commander(s). However, they all showed a disinclination to combine operational and administrative functions in the same organization, believing those to be separate tasks.⁵⁸

Watching the Watchers

DIRNSA's supervisor was not really the secretary of defense, despite what the Truman Memorandum said. In 1953 the secretary of defense assigned that job to General Graves B. Erskine, a Marine Corps four-star who was already assigned to his staff as head of the Office of Special Operations. Erskine monitored the CIA budget, which was hidden in the DoD budget, and after July 1953 he also monitored NSA. His deputy, Air Force colonel Edward Lansdale, later became famous as the author of covert actions projects in both the Philippines and Vietnam.

The monitoring that Erskine did was rather loose. He always retained professional cryptologists on his staff to work the details of cryptologic money, and under such a

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

~~TOP SECRET UMBRA~~

system, oversight was not detailed. Occasionally a big-ticket item would come up, like LIGHTNING (see p. 204), and Erskine's office would become involved. But Congress had not yet instituted an effective review of the intelligence agencies (and did not until the mid-1970s), and CIA did not yet have the authority to ride herd on the finances of the DoD intelligence organizations. So by the standards of later days, no one was really paying much attention to the intricacies of NSA's money.⁵⁹

NSA AND CIA - THE EARLY YEARS

Will you please have the proper instructions issued discontinuing the cryptanalytical units in the offices of the Director of Censorship, the Federal Communications Commission and the Strategic Services. If you are aware of any other agencies having services of this character, will you please have them discontinued also.

Franklin D. Roosevelt, Memorandum for Director of Budget, 8 July 1942

The origins of CIA were rooted in World War II. Roosevelt, under the pressure of wartime exigency, created an espionage agency in 1942, called the Office of Strategic Services (OSS), under New York lawyer and World War I battlefield hero (winner of the Medal of Honor in France) William Donovan. Donovan's agency both collected and produced intelligence and mounted covert operations around the world. It was a mission that CIA was to inherit several years later.

NSA's difficulties with CIA stemmed from decisions made in the 1940s, almost all of them bad. JCS, which owned most of America's intelligence assets, opposed OSS from the beginning and did everything in its power to deny to OSS the resources to do its job. The Joint Chiefs failed to keep OSS out of the HUMINT business, but in one area they succeeded almost totally: COMINT was denied.

Roosevelt's order (above) resulted in the closure of a small OSS COMINT organization. Even worse, it was used by the JCS to deny to OSS access to ULTRA. Thus OSS reporting was crippled from the beginning. It had access to agent reports, photoreconnaissance, POW and defector reports - everything, in short, but the most useful and reliable information. If World War II was, as has been claimed, a COMINT war, OSS remained on the intelligence sidelines.⁶⁰

And it rankled. OSS seniors who later served in the higher ranks of CIA never accepted the JCS policy. The British intelligence services, which dealt closely with OSS, were appalled. Their own intelligence community was unified, and HUMINT was routinely integrated with COMINT in highly specialized offices, in order to reap full value from both. (For instance, Ian Fleming, a British naval officer and later author of some note, was responsible for the integration of Bletchley-produced ULTRA with the Navy's HUMINT and

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

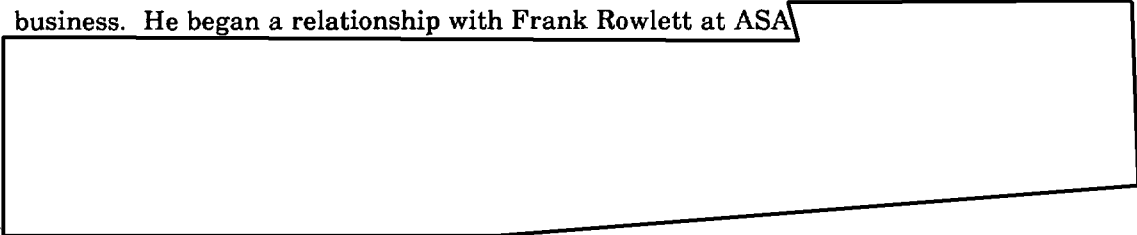
special operations.) JCS had used security as justification for the denial of ULTRA to OSS, but the British were at least as security conscious as the Americans, and they seemed able to get COMINT of the highest sensitivity to those in the HUMINT business who needed it. The outright denial of ULTRA to OSS just did not make sense.⁶¹

Truman discontinued OSS immediately after the end of the war, partly to rid himself of Donovan, who was not in favor with the president. But within six months Truman once again had himself an intelligence organization, called the Central Intelligence Group. CIG was bedeviled by the same problems that submerged AFSA - lack of its own budget and personnel resources (people were loaned in from other intelligence organizations), absence of a congressional mandate, and lack of firm direction from the top. But the idea was the same as that of AFSA - to establish central control of U.S. intelligence operations. When CIA was created in 1947, succeeding CIG, it got its congressional mandate, its budget, and its own personnel. It still lacked firm leadership, but that was remedied in 1950 with the appointment of General Walter Bedell Smith as DCI. Smith had been Eisenhower's chief of staff in Europe, and he knew how to run a tight ship. Tussling with "Beetle" Smith was like landing in a cactus patch.

In the early days the only high-level COMINT available to CIG was a copy of the MAGIC Summary put out by the Army, which was available in the Pentagon. In the very early days, only fifty people in CIG had a COMINT clearance. But in June of 1946 Hoyt Vandenberg became DCI. Vandenberg was fresh from a tour as chairman of USCIB and knew the value of COMINT. In December he created an organization within CIG, called the Advisory Council, to deal with what he hoped would be a flood of COMINT reports.

For a while there were few reports to disseminate. Requests for access to COMINT reports were generally denied. But in early 1947, two CIG organizations began to get involved with COMINT operations. The first was OSO (Office of Special Operations, the clandestine organization), which in March proposed to the Army and the Navy that they begin a Joint Counterintelligence Center (JCIC), using COMINT as the basic source of information. The services received this enthusiastically, and JCIC was established at Nebraska Avenue, with the understanding that it would eventually move to CIG. (It moved to CIA in 1949.)

At about the same time, Colonel Robert Schukraft, chief of the Communications Division at CIG, was establishing a relationship with ASA. Schukraft had been a key figure in wartime Army COMINT and knew many of the people involved in the COMINT business. He began a relationship with Frank Rowlett at ASA

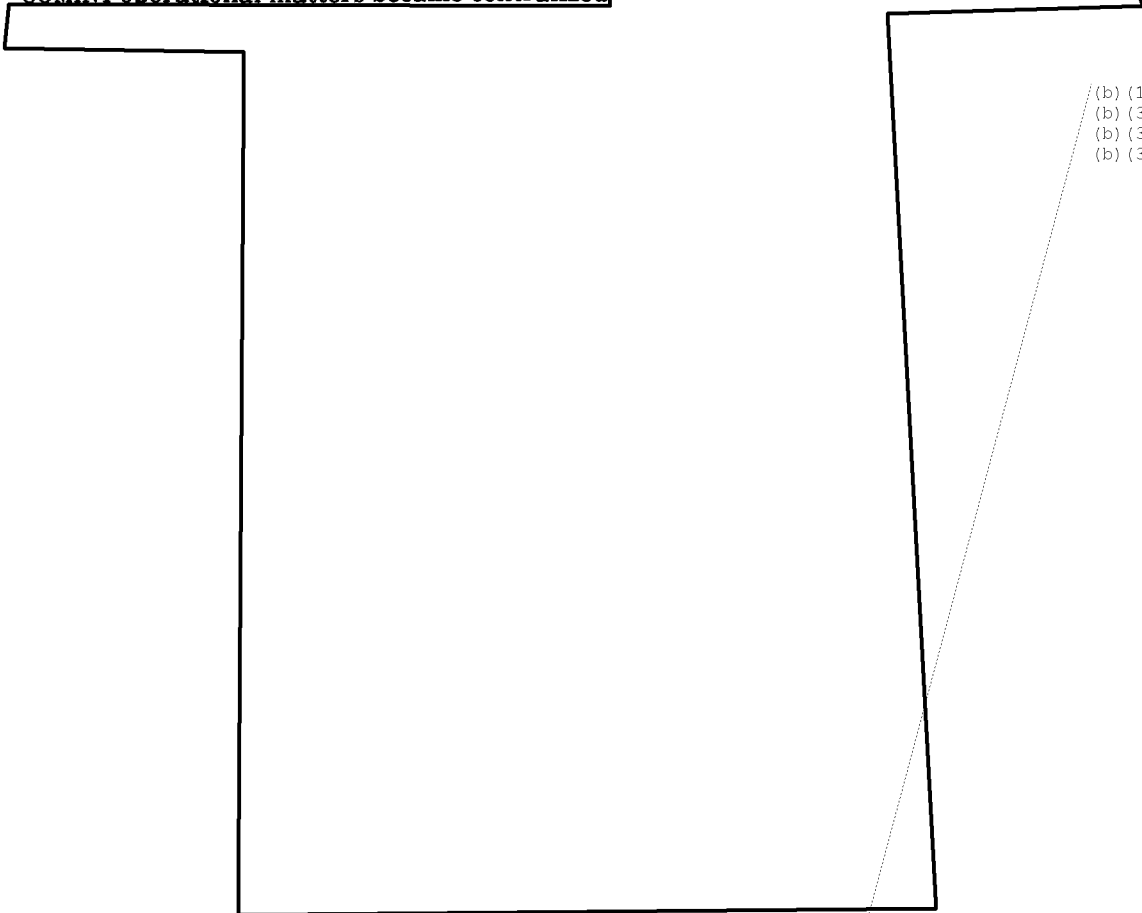


(b) (1)
(b) (3)
OGA

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

~~TOP SECRET UMBRA~~

The operational aspects of these budding relationships eventually came under the aegis of OSO, and specifically one William ("Bill") Harvey, a former FBI agent who became legendary for his clandestine operations. Under Harvey, who took over in 1950, COMINT operational matters became centralized.

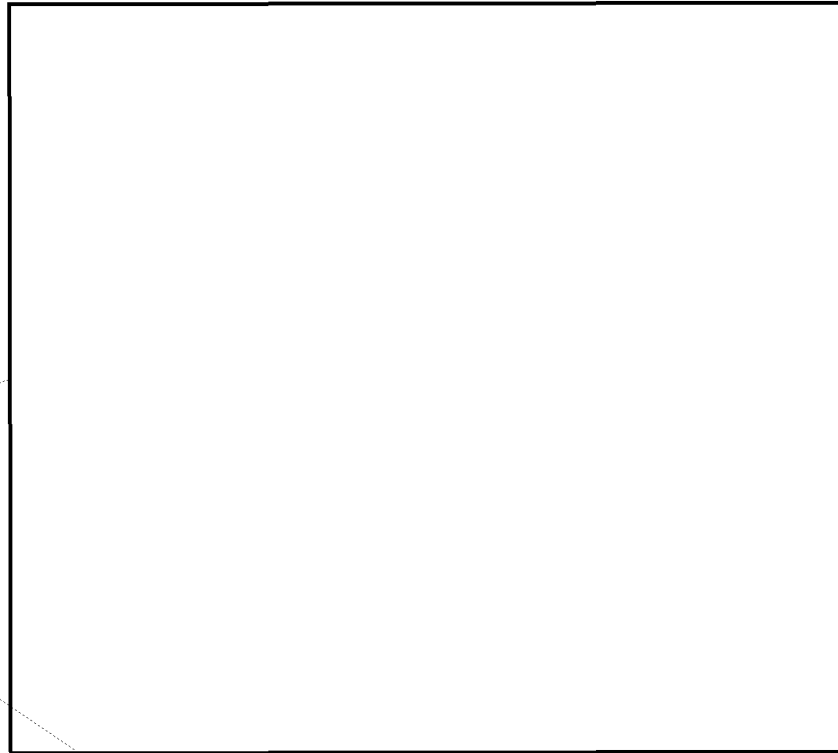


(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

Meanwhile, CIA requests for COMINT reports were still being routinely turned down. But the [redacted] contributed to breaking the logjam, and ever larger volumes of COMINT report series were forwarded to CIA. Once at CIA, the material was subdivided according to subject matter and farmed out to analysts through the auspices of the Advisory Council. CIA was determined to base reporting on all-source information, rather than to strictly segregate COMINT from all other sources. Of necessity, then, the number of CIA COMINT clearances rose rapidly, until by 1970 most intelligence analysts were cleared for the source. (See Table 5.) CIA policy stood in contrast to that of the Pentagon, which generally chose to compartment COMINT and to deal with two separate handling systems - COMINT and all other sources.

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

~~TOP SECRET UMBRA~~



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

When AFSA was created, CIA made a pitch for a more active role in COMINT. Then-DCI Roscoe Hillenkoetter proposed that he should be given the chairmanship of USCIB, but this was quickly overruled. CIA [redacted] [redacted] but was being told in unmistakable fashion that they would remain on the sidelines when it came to the policy aspects of COMINT. That was still the domain of the JCS.

CIA remained a major critic of COMINT throughout the AFSA period, and Hillenkoetter's successor, Walter Bedell Smith, played an important role in getting the president to appoint the Brownell Committee. CIA was determined to get a bigger stake in the game.

Smith got much of what he wanted from Brownell. He was made chairman of USCIB and, as such, could play a large role in COMINT policy. The results of the Brownell Report also gave CIA the chance to lean on the new NSA to get its own requirements satisfied. No longer would the civilians have to take a perpetual backseat to military requirements.⁶³

CIA Enters the COMINT Business

In the beginning, CIA probably did not intend to build its own cryptologic organization. Two very senior NSA officials, Louis Tordella and [redacted] both

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

~~TOP SECRET UMBRA~~

closely involved in the NSA-CIA relationship, categorically deny that this was the intent. [redacted] himself described his first interview with Allen Dulles when he transferred from NSA to CIA: "I mean Dulles put it flatly, we were not going into competition with NSA. We've got enough to do in CIA and we're not going to fragmentize [sic] our efforts by going over there and starting a . . . COMINT organization. . . ."64 But CIA needed certain information, and as long as cryptology remained the province of the Department of Defense, he felt it could not get its requirements satisfied. Smith decided to change things.

The CIA Act of 1949 gave the espionage agency the authority to expend what were called "discretionary funds." [redacted]

[redacted] for which the director would not have to answer to Congress in any detail.

According to Tordella, the DCI first used these moneys [redacted]

[redacted] 85

To a great extent this developed out of on-going CIA operations. [redacted]

[redacted]

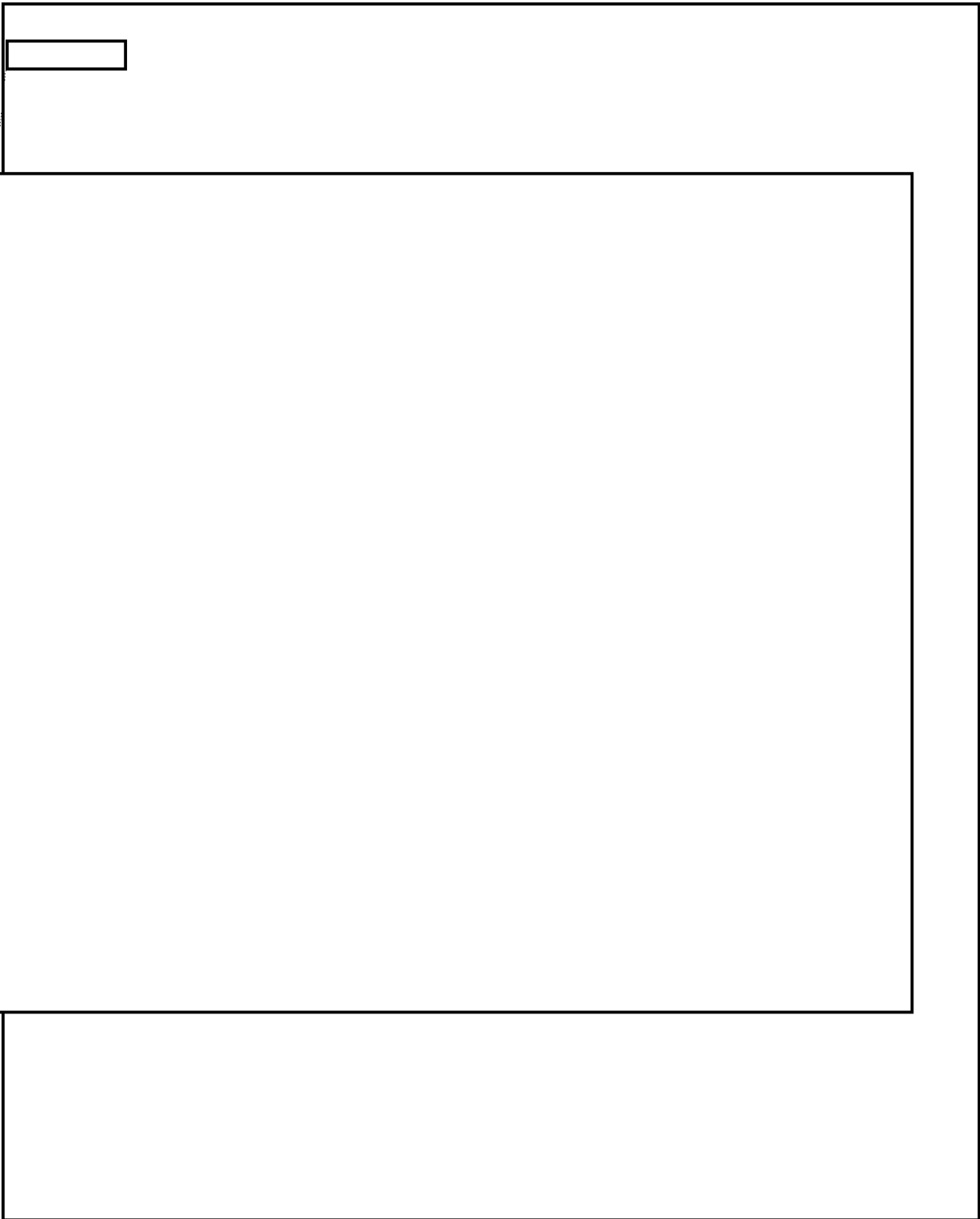
[Large redacted block]

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

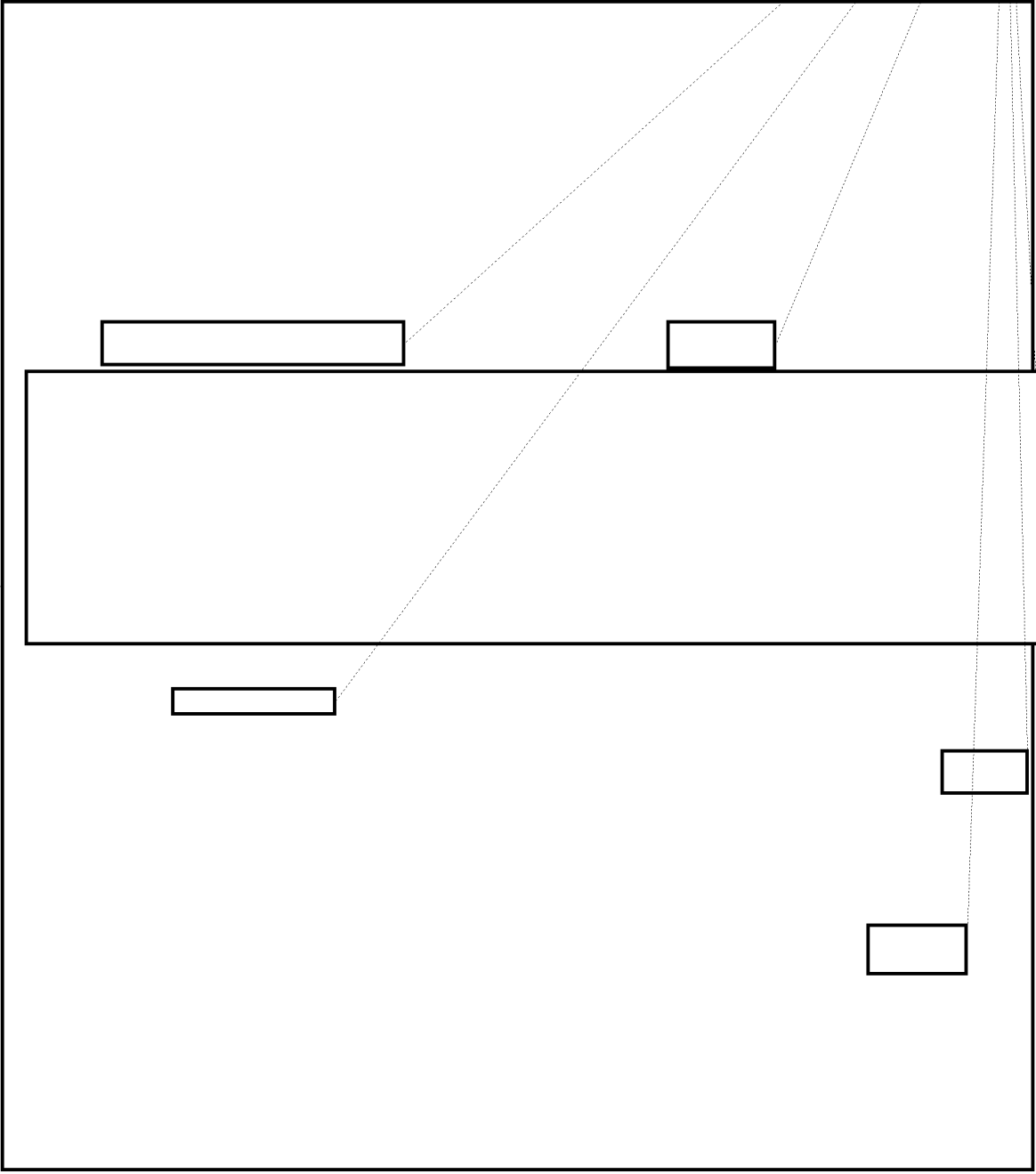


(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



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

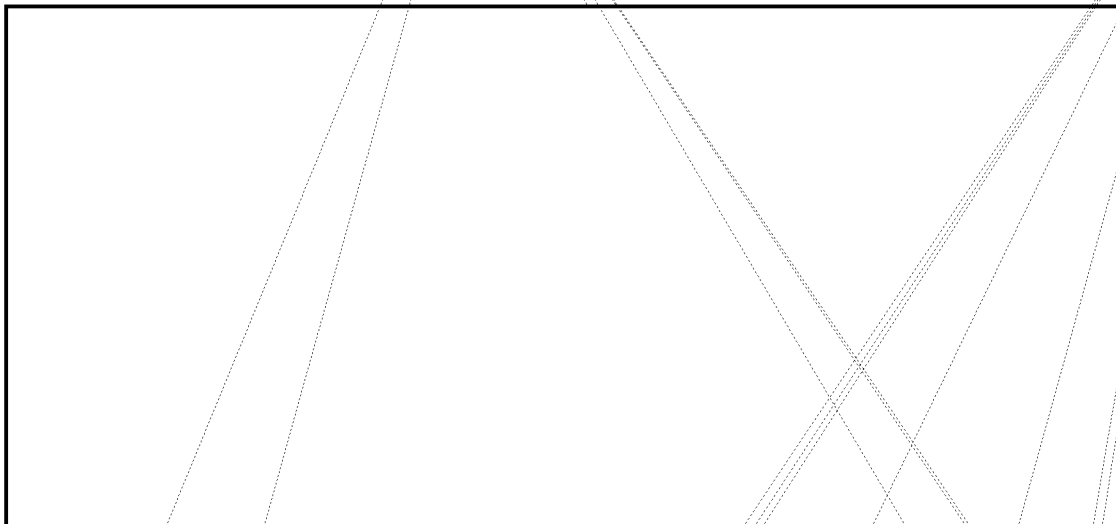
CIA and Cryptographic Materials



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

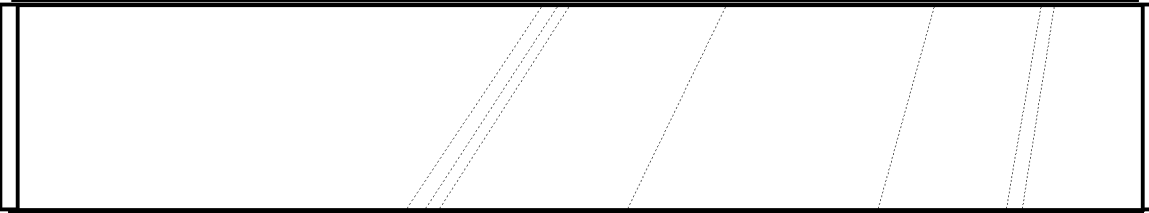
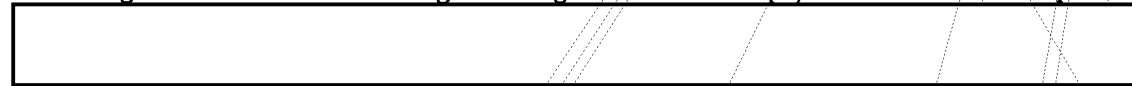
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



The [redacted] Business

In no area did NSA and CIA clash more frequently and with as much vigor as in [redacted] matters. There, NSCID 5 was in direct conflict with the BRUSA Agreement. The former gave CIA control of foreign intelligence relationships, while the latter required

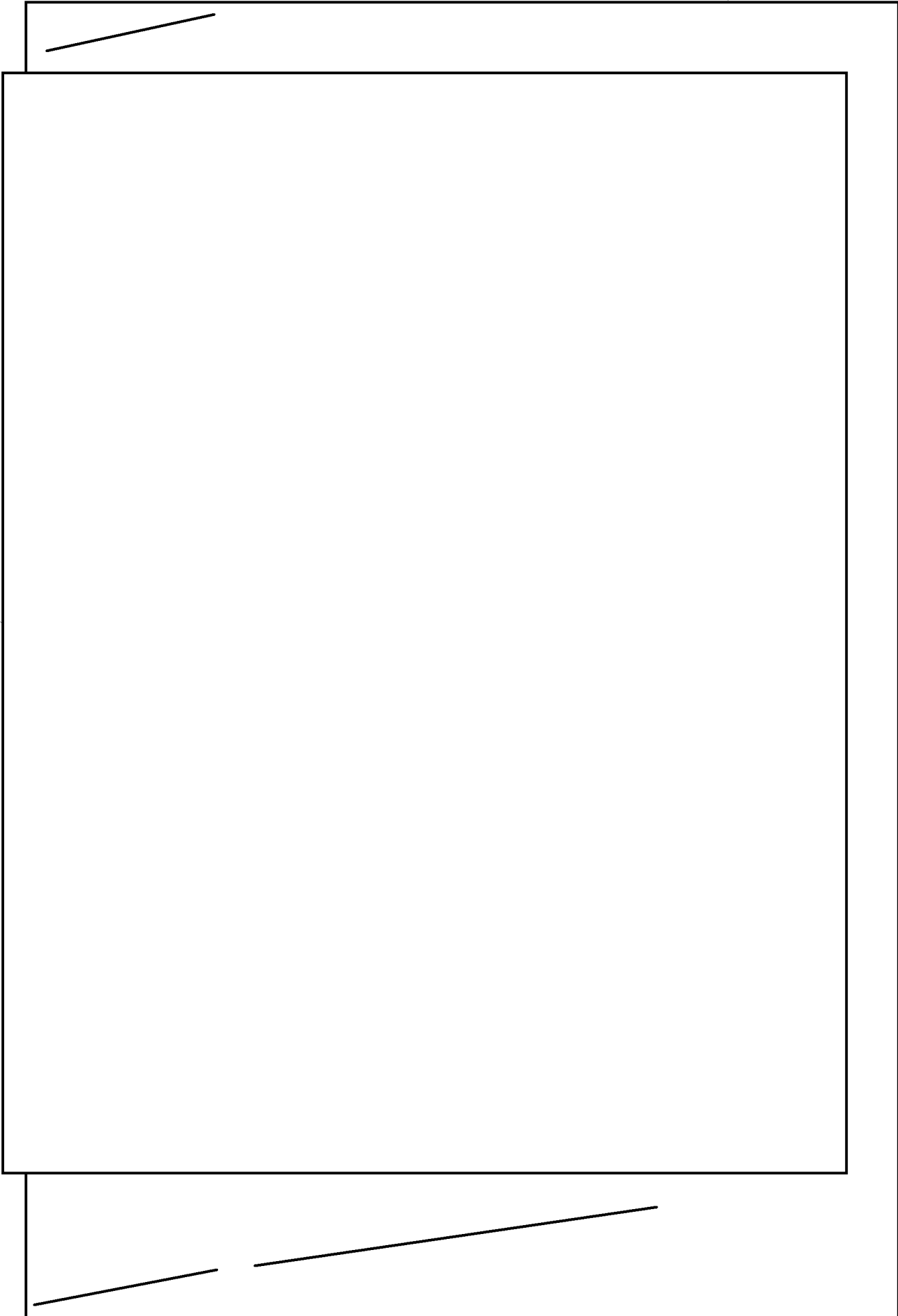


[redacted] one of the half-dozen most important cryptologists in America, had had a choppy relationship with General Canine. [redacted] felt that his own temperament was too methodical for the hip-shooting Canine, and the two were not getting along when Canine, in a mood to reorganize, decreed that all his seniors would rotate jobs in order to infuse the organization with new ideas. [redacted] who had been working in COMINT, was ordered to COMSEC. [redacted]⁷⁶

[redacted] was joined by a small but experienced group of NSAers, including [redacted] whose province was COMINT matters. [redacted]

[redacted] who was well aware of the benefits of continued collaboration with the [redacted] partners, brought some order into CIA's COMINT matters.⁷⁷

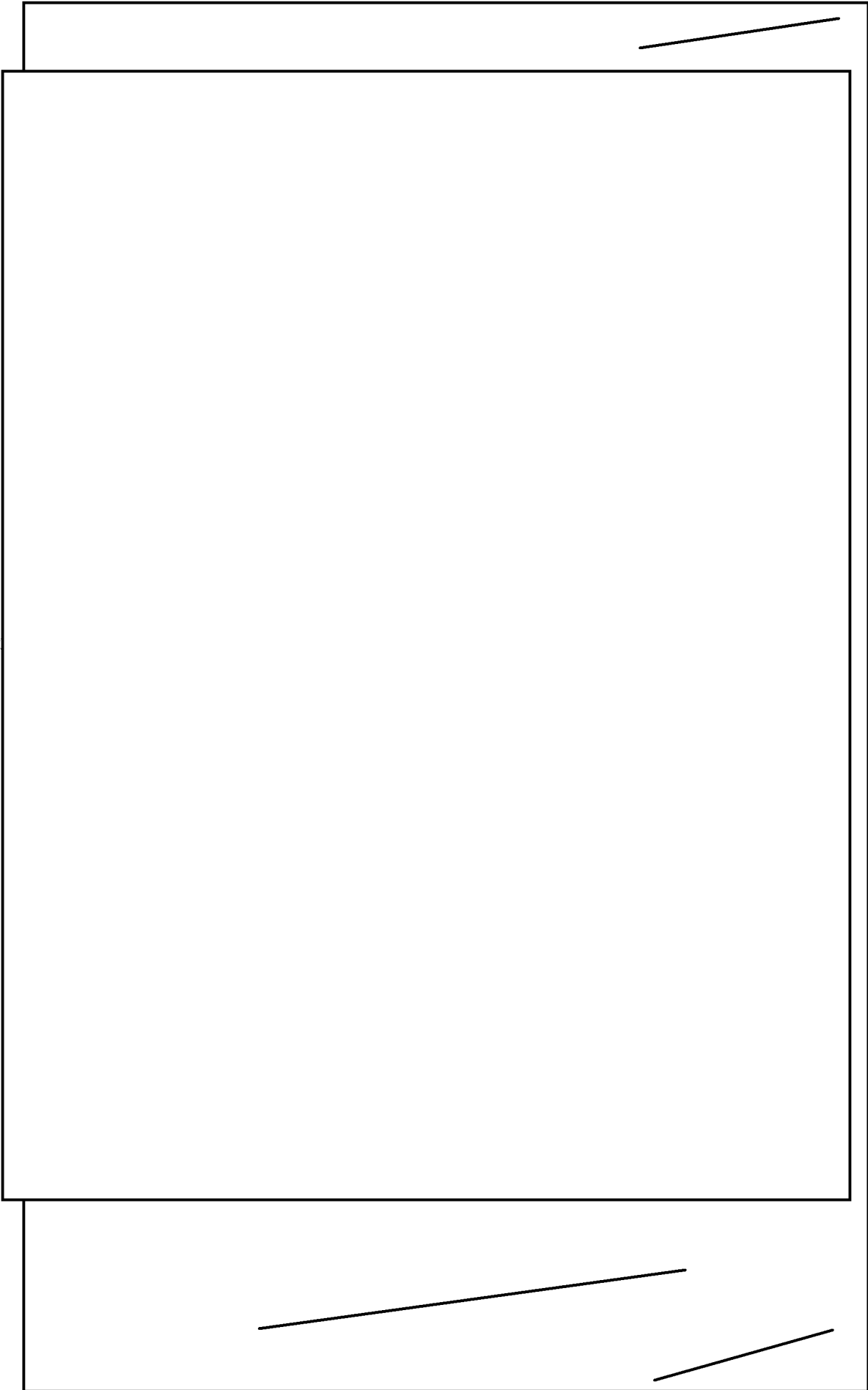
HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

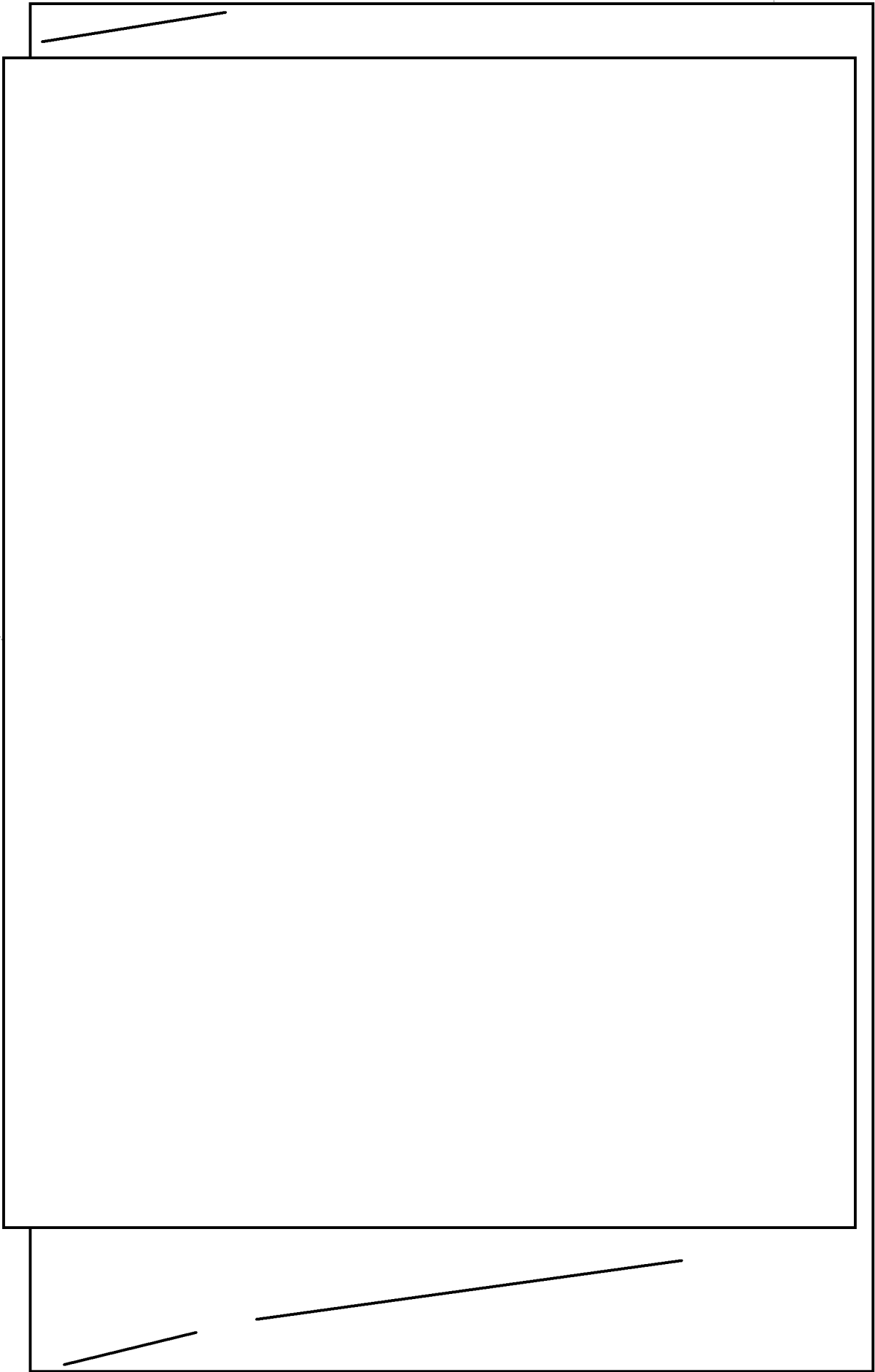


(b) (1)
(b) (3)
OGA

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

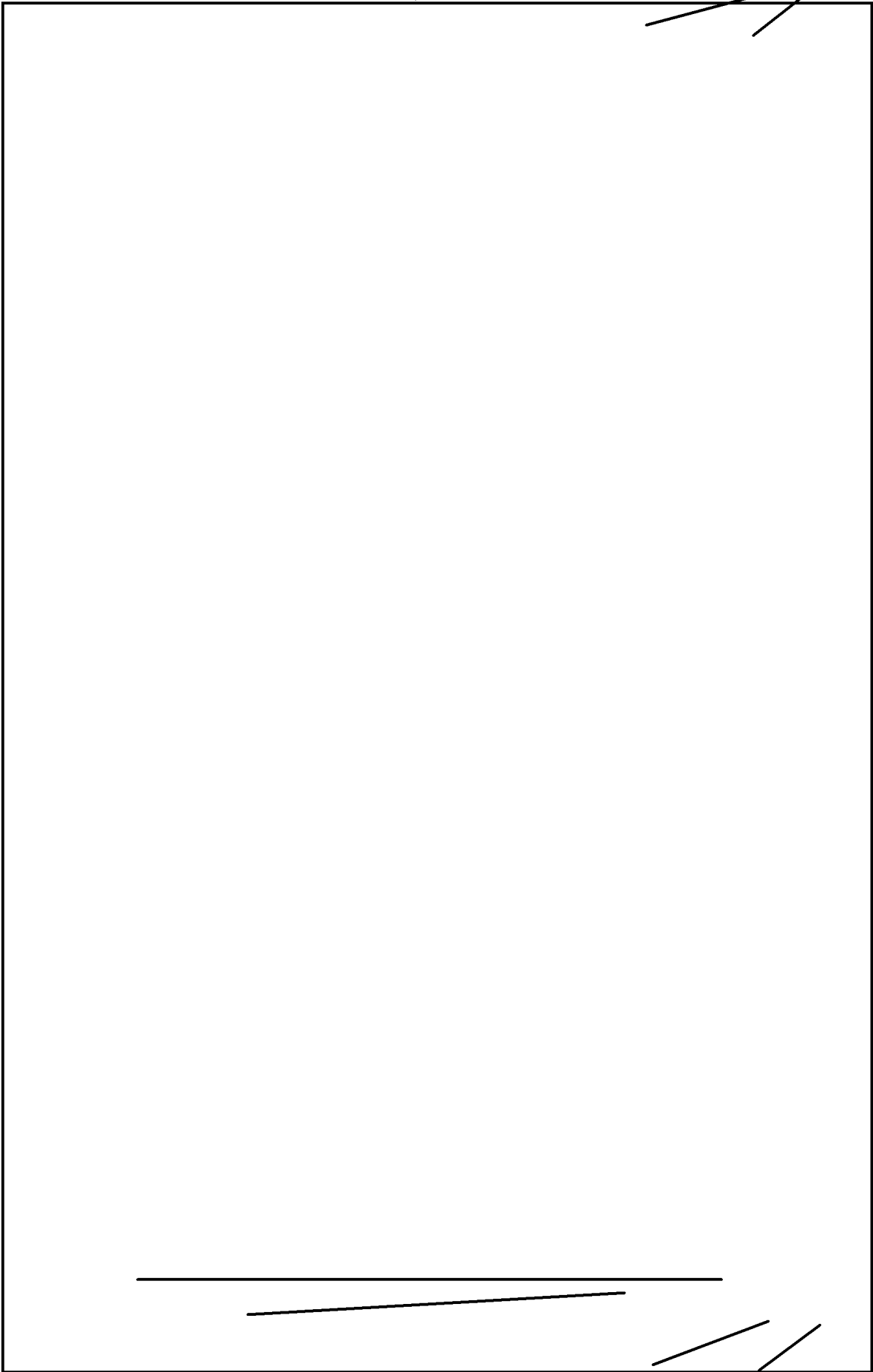
(b) (1)
(b) (3)
OGA

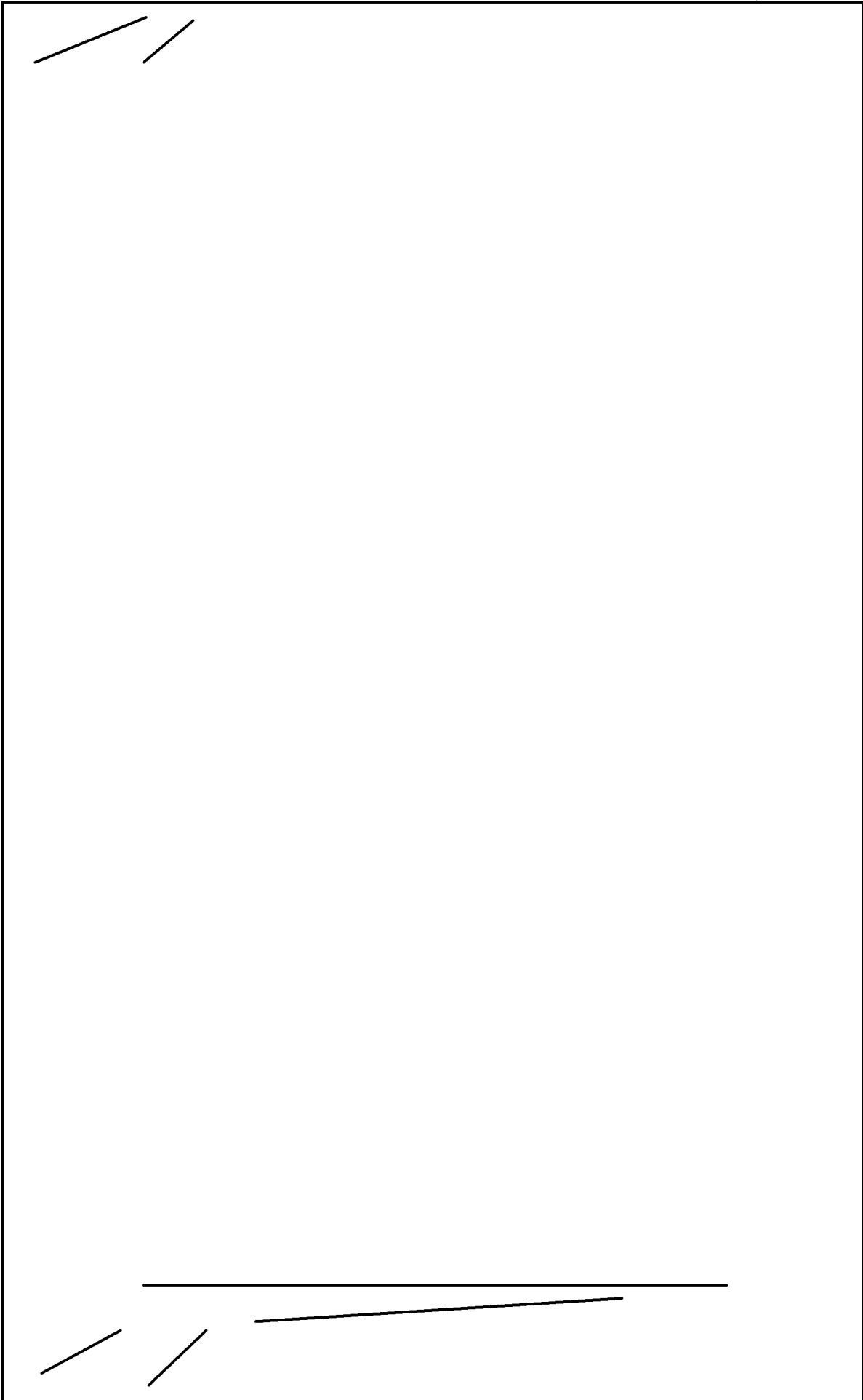


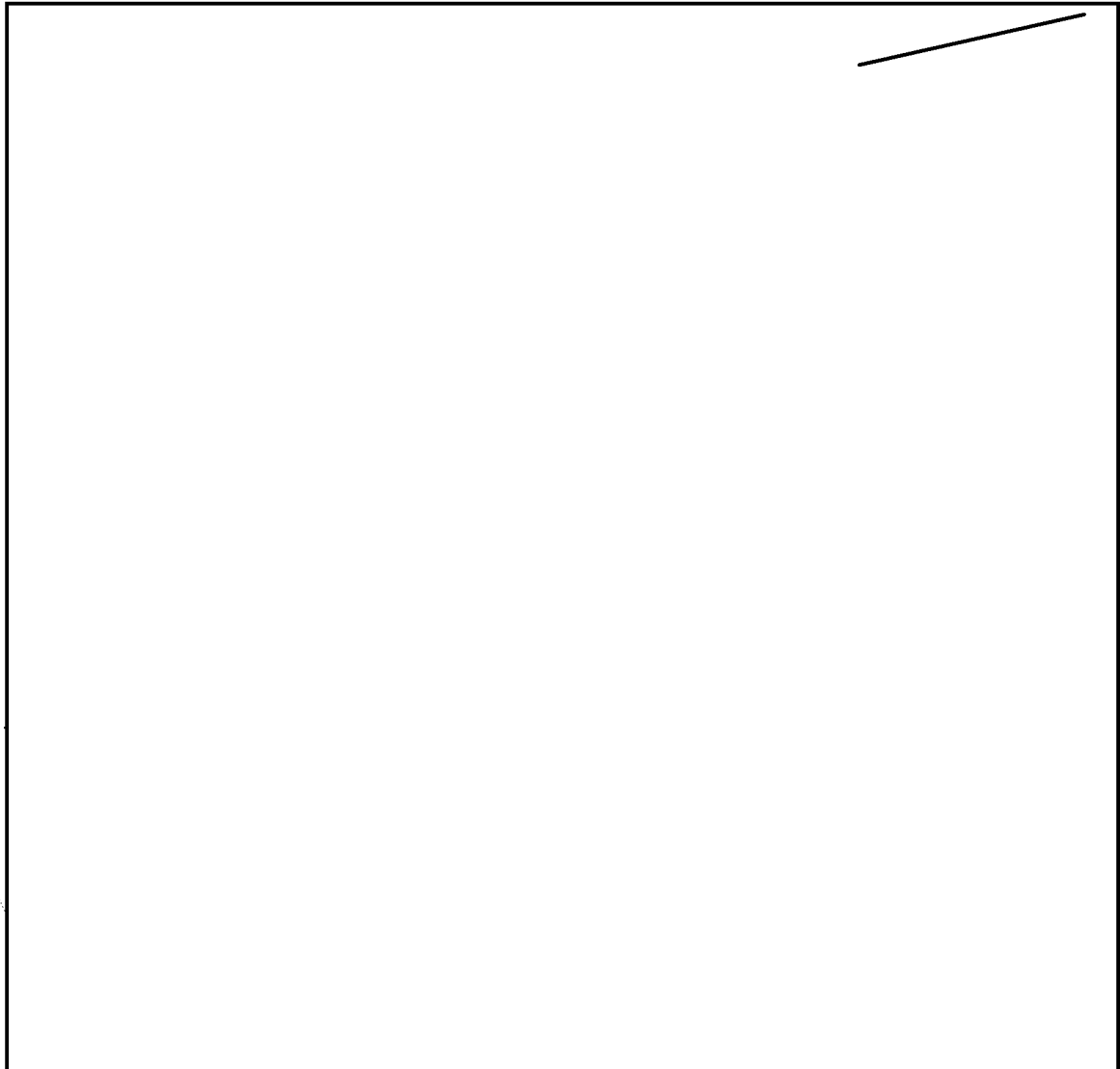


(b) (1)
(b) (3)
OGA

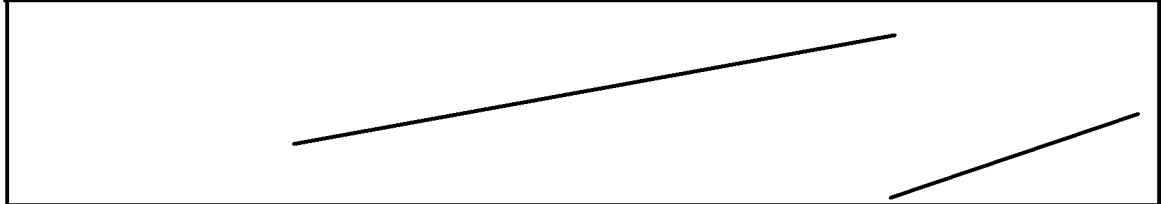
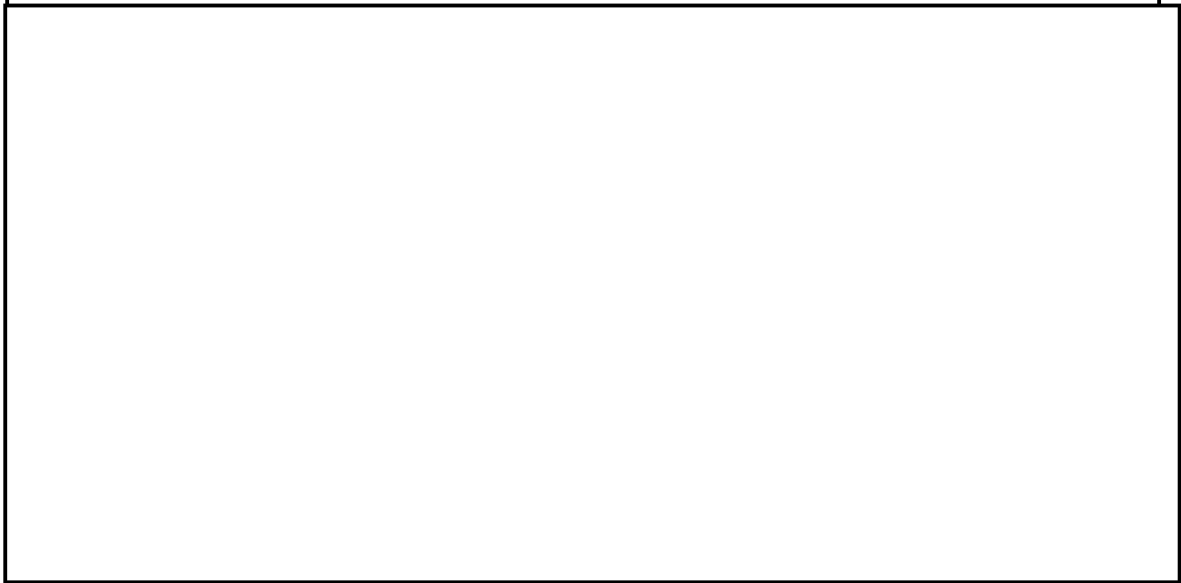
(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36



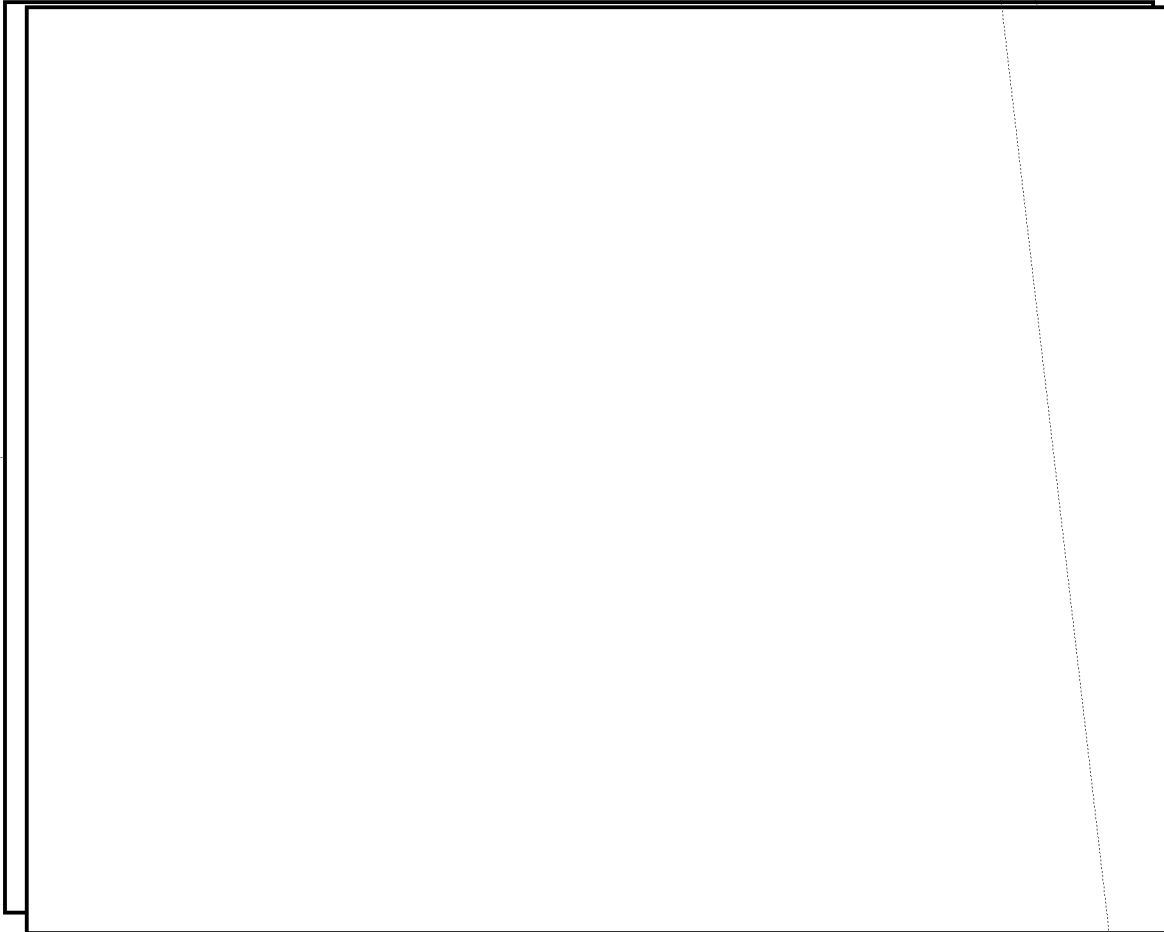




(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36



~~TOP SECRET UMBRA~~



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

The Third Parties in the Early Years



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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[redacted] On its side, however, NSA also made mistakes. The most serious was in denying technical help to some of the more advanced Third Parties. This unyielding position often reduced CIA equities in other areas and damaged NSA's relationship with its senior intelligence partner.

CIA in the NSA Trenches

The most direct CIA involvement in NSA was a CIA-controlled analysis division which existed for the better part of six years. This strange story began with the Soviet explosion of an atomic bomb.

When, in September of 1949, the Soviets exploded their first nuclear device, the eerie light from the explosion silhouetted a U.S. intelligence system in disarray. It had been CIA's job to follow Soviet nuclear technology, but JCS intelligence organizations gave CIA only lukewarm cooperation. The result was a National Intelligence Estimate (NIE), issued earlier in the year, featuring a wide variety of estimates of Soviet acquisition of effective nuclear technology, none of them even close to being accurate. [redacted]

[redacted]

As AFSA-246 became NSA-75, CIA turned more and more to direct action. In 1953, Canine and Loftus Becker, CIA's deputy director for intelligence, inked an agreement that turned management of the division over to CIA. It was captained by a CIA person, kept its own database, did its own reporting, and even forwarded raw COMINT to CIA headquarters for further analysis.

[redacted]

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[REDACTED]

In 1948 CIA, in cooperation with a Department of State organization called OPC (Office of Policy Coordination), began beaming propaganda (some would say "news") broadcasts toward the Soviet Bloc. The operation was called Voice of America, and it lived a long and healthy life during the Cold War. Predictably, however, as soon as the VOA stations went on the air, the Communist nations at which they were targetted began jamming the broadcasts. Thus ensued, in February of 1948, yet another area of intense competition between CIA and the cryptologic community.

Tackling the problem of jamming would involve radio monitoring. CIA took on the job in 1949 and immediately began preparing a plan to identify and locate the jammers and devise a solution. In June 1950 an ad hoc group of the IAC (Intelligence Advisory Committee, chaired by the DCI) approved a preliminary monitoring plan, called

[REDACTED]

Just how Admiral Stone of AFSA found out about it is not known, but it was hard to keep secrets at the IAC level. In any case, Stone contacted the Department of State (at the time OPC was still officially part of State rather than CIA) in July of 1950 to let them know that he regarded this as an AFSA responsibility under NSCID 9. Hillenkoetter justified CIA activity to AFSAC as being performed under the section of the National Security Act that permitted CIA to perform "such additional services of common concern as the National Security Council determines can be more efficiently accomplished centrally. . . ." This was a weak reed, and Hillenkoetter made his case even less plausible by stating that monitoring facilities so established could be used for other purposes in time of war. Such a direct challenge to AFSA authority in COMINT brought a predictable AFSAC response, and in November USCIB took up the issue. USCIB concluded in November that [REDACTED] was a COMINT mission and should be headed by AFSA. A USCIB study costed the problem at \$5 million and 355 people. But when the matter went before the National Security Council in early 1951, CIA won. The NSC directed that CIA be the focal point for a multi-agency attack on the jamming problem.

AFSA wrote a supporting plan but continued to insist that it be given the mission. When Canine became director, he took forceful exception to CIA encroachment in the [REDACTED] situation. But Canine was handicapped by limited resources. [REDACTED] was going to be expensive, and when the SCAs were polled, they offered only part-time DF facilities. NSA did not have the money to create a separate system just to monitor jamming, and the military services contended that they could not provide the communications to interlock a monitoring system anyway. So in February 1952 President Truman approved a plan for CIA to proceed on its own.

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

~~TOP SECRET UMBRA~~

[Redacted]

Just what was [redacted] anyway? Jammers actually produced noncommunications signals, and the Army contended that they were ELINT, not COMINT. The entire subject of ELINT was in chaos at the time, and [redacted] simply contributed to the disorder. The services also saw electronic warfare applications, and they wanted their own people in the projected NSA-controlled [redacted] sites to send EW-related information to their parent services. NSA feared this approach because it would spread COMINT-related information outside codeword channels, and the services might turn the information into EW (electronic warfare) projects that would block COMINT hearability. This prompted NSA to appoint a committee to study the matter of jamming versus COMINT requirements. The confusion in definitions foreshadowed more serious divisions during the Vietnam era.

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

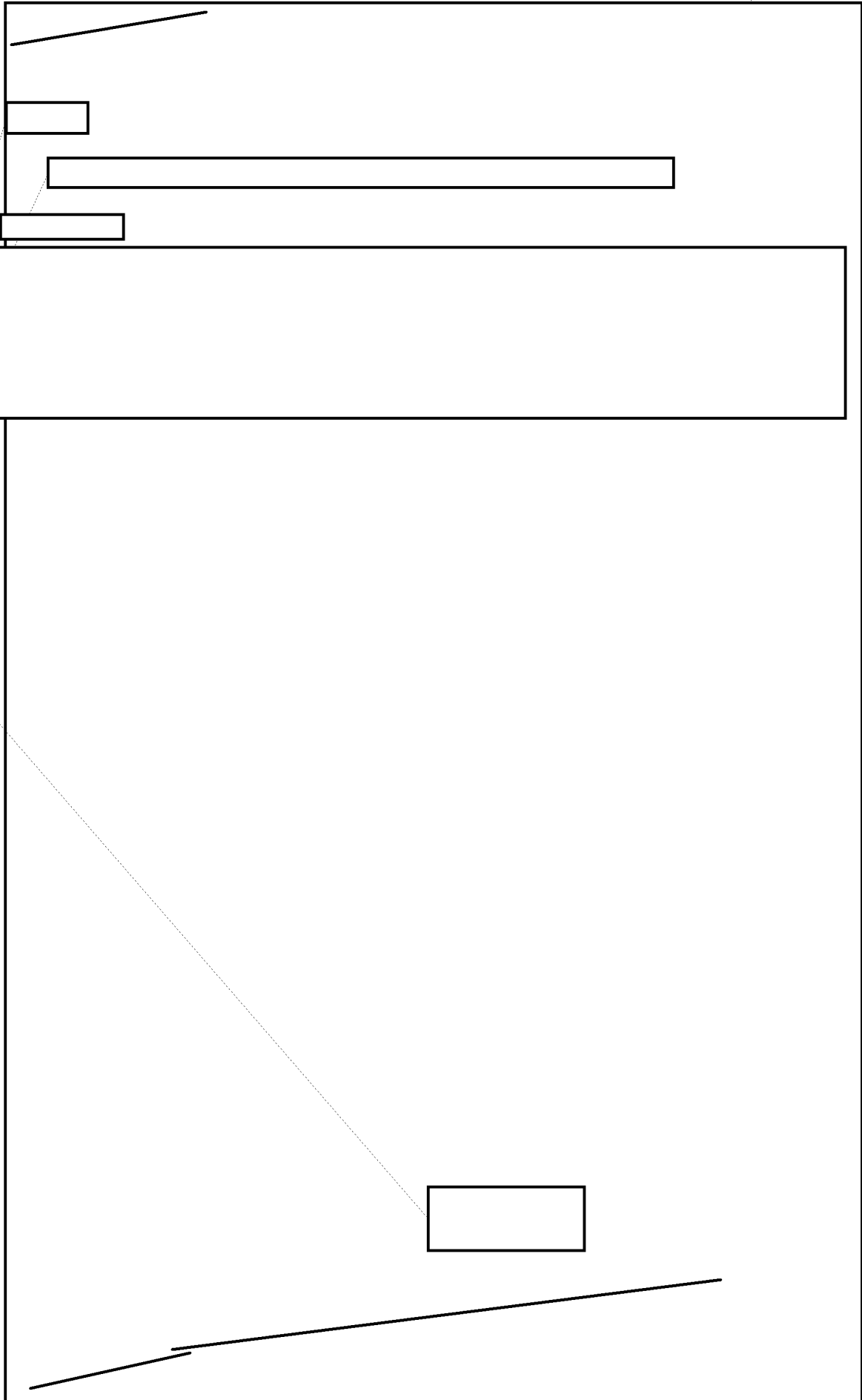
[Redacted]

This was a direct invasion of NSA's turf.

In the mid-1950s, as [redacted] continued along an inconclusive course, various schemes emerged for the eventual institutionalization of [redacted]. Most had as their central assumption that CIA would not continue in charge, and some placed NSA in control. The services wanted the mission but did not want to budget for it. One proposed plan would even have given the mission to the Federal Communications Commission. In late 1955, the secretary of defense put the matter to rest by decreeing that it was an ELINT mission and made the Air Force executive agent. The Air Force had only recently become executive agent for ELINT, and it had a central ELINT processing center. Since no resources were allocated to do [redacted] it became subsumed in the overall service ELINT mission.

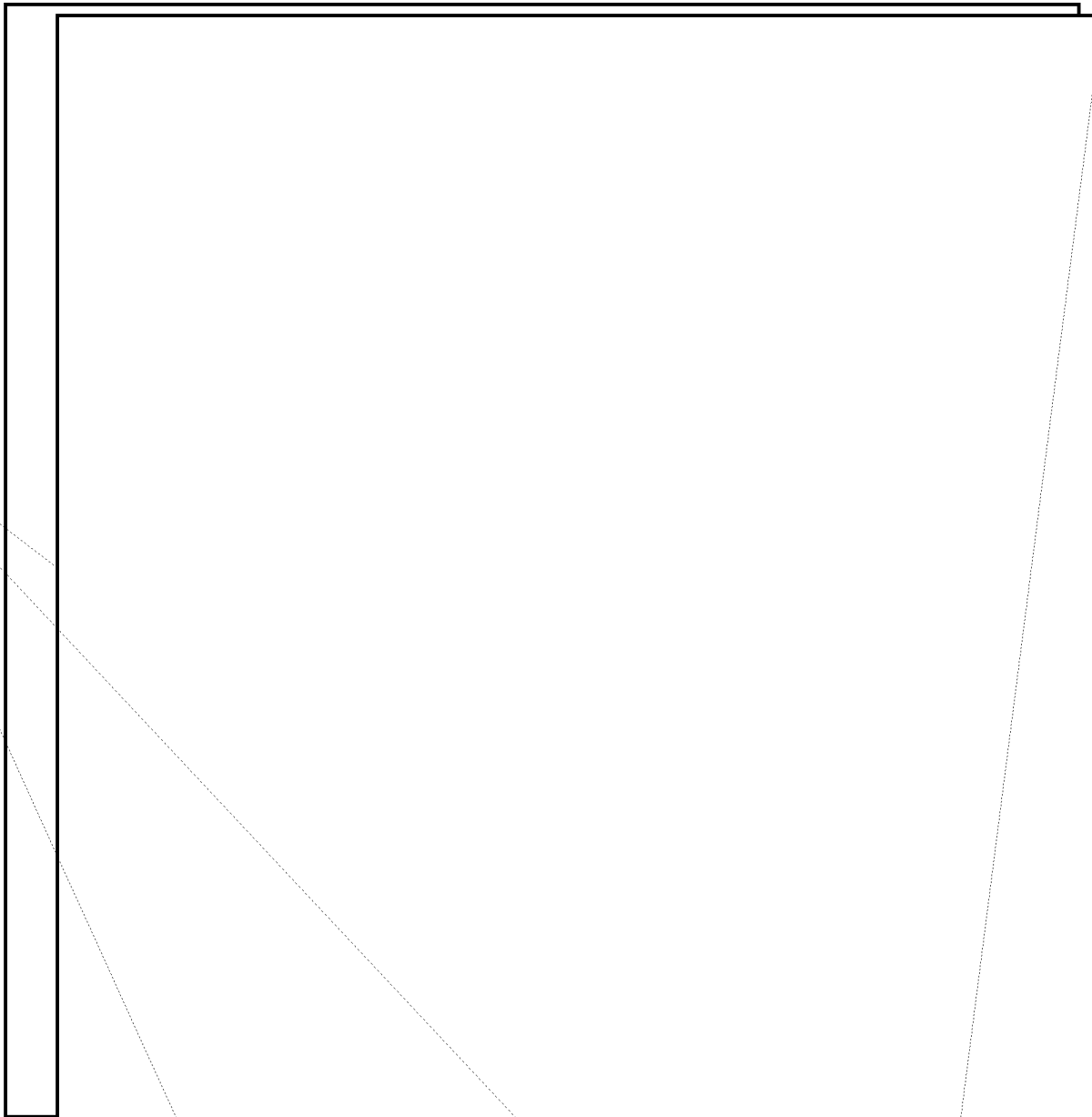
So in the end a separate monitoring system was not built. The jamming mission was handled as a corollary mission by the three SCAs, and when, in 1958, control of ELINT went to NSA, the threat posed by [redacted] vanished.⁹¹

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



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

~~TOP SECRET UMBRA~~



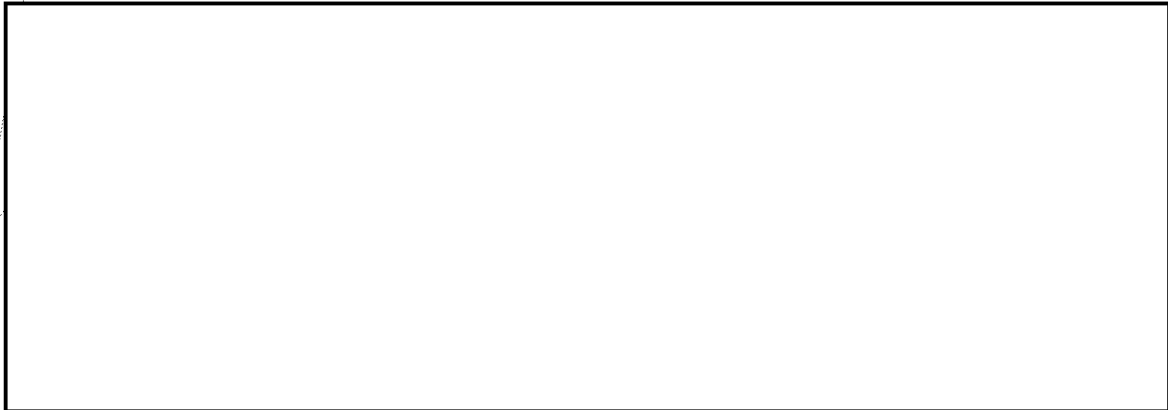
(b) (1)
(b) (3)
OGA

In April 1956, after heavy rains caused interruptions in communications service in the East Zone, East German maintenance workers discovered the taps and unearthed the entire operation. In the space of a few hours, [redacted] was shut down, and the acting commandant of the Soviet Berlin Garrison held a press conference on the site of the " 'capitalist warmongers' expensive subterranean listening post.' " Now that the whole world knew about [redacted] CIA could not continue [redacted] for security reasons. After April 1956, CIA sent an enormous volume of unprocessed channel hours

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

~~TOP SECRET UMBRA~~





Years later the "accidental" discovery of [redacted] came under serious question. In 1961 George Blake, a British MI-6 official who had been involved with the planning of [redacted] was identified as a Soviet mole by a Polish defector and was subsequently arrested and jailed. In 1970 Blake, who had escaped from a British jail and fled to Moscow, bragged to the press that he had betrayed the Berlin Tunnel operation. It was also suspected that he had blown the whistle on the [redacted] operation, too.

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



George Blake

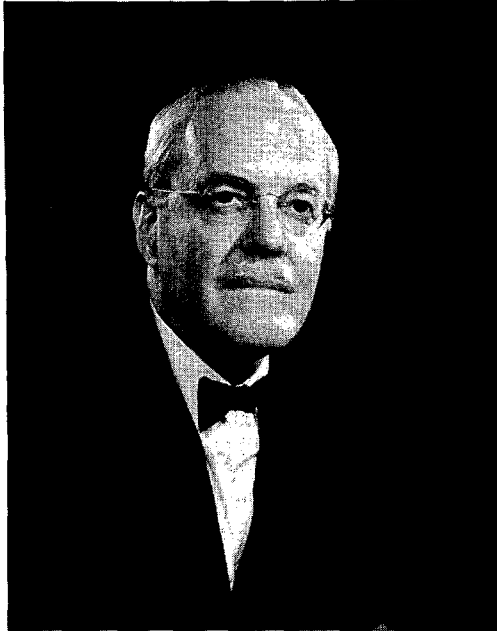
Bitterness between NSA and CIA lasted for years. Canine was understandably upset when he found that he had been bypassed and left in the dark. DCI Allen Dulles once mused that,



NSA and CIA continued to clash over a variety of issues as long as Dulles and Canine were the respective helmsmen. Yet the warfare was oddly out of place in Dulles's office. According to historian Thomas Powers, Dulles "never attempted to exercise [authority over the Defense Department intelligence components], partly in the interest of maintaining bureaucratic peace with the military, and partly because he just did not care."⁹³

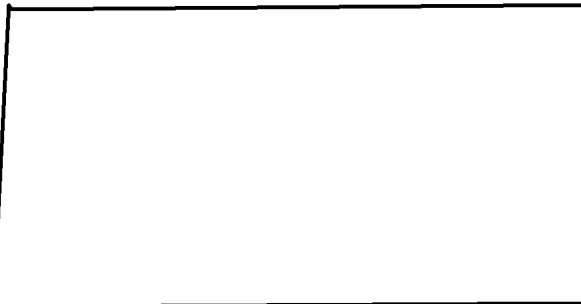
(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

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



Allen Dulles

Dulles was interested in HUMINT and covert operations, not technical intelligence. Richard Bissell, who headed the CIA's operations organization in the late 1950s, once said that "Dulles was always being encouraged by successive Presidents to exercise more direction of the whole intelligence community. And Allen always resisted that. . . . He always wanted to run his Agency and exercise a direct, unambiguous control. . . ."94



According to senior NSA officials of the time, the era of CIA's SIGINT system was already beginning to fade. They had neither the time nor the money to pursue a big SIGINT system and a big HUMINT/covert actions system simultaneously, and so SIGINT was sacrificed.

General John Samford, who replaced Canine in 1956, moved to heal the breach with Dulles and the CIA. Samford was a consummate diplomat, and he probably gained more by soft-soaping the downtown intelligence people than Canine could have done through head-on collisions.⁹⁵

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

NSA's Other Competitors

The growing size and importance of COMINT made it inevitable that the cryptologic organizations of the armed services would have other competitors from time to time. During World War II there had been several.

The Federal Communications Commission had a long history of communications monitoring to secure compliance with federal radio regulations. During the early part of World War II, the FCC published a series of magazine articles plugging their successful efforts at finding Axis agent communications. The Army and Navy cryptologists did not appreciate this glare of publicity on their secret profession, and they sought to get Roosevelt to close down FCC operations. Roosevelt's order of 1942 (cited at the beginning of this chapter) was meant to apply to the FCC and other competitors of the Army and

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

Navy, but there is evidence that the FCC continued a small intercept effort into the postwar period. At some undefined point in the 1950s, the effort was probably shut down.

The FBI represented a far stronger and potentially more dangerous foe. But J. Edgar Hoover's interests were more limited, and throughout his life the FBI displayed a certain ambivalence toward involvement in COMINT. During World War II the FBI was one of the three organizations given a COMINT role. Namely, they were responsible for monitoring of the communications of Axis agents in Latin America. This apparently simple division of effort placed the FBI in almost constant conflict with OP-20-G, which had a very similar mission. By all accounts, the FBI had a small but competent intercept and cryptanalytic section of indeterminate size. But COMINT had nothing to do with Hoover's main thrust as FBI director, and after the war the FBI COMINT effort was reduced. When FBI joined STANCIB in 1947 (which then became USCIB), Rear Admiral Thomas Inglis, the chairman of USCIB, offered COMINT resources to monitor agent communications and do the cryptanalysis. Hoover accepted, mainly because this would allow him to divert FBI resources to other matters. In 1947 FBI withdrew from USCIB, allegedly because of declining budget to do COMINT tasks.



Even more important was the AFSA-FBI liaison which led ultimately to the arrest of the atomic spies (see p. 160).⁹⁶

ELINT and NSA

ELINT as an intelligence discipline probably began during the Battle of Britain. The intercept of noncommunications signals was first attempted by one R. V. Jones, who successfully collected mysterious German navigational signals used by the Luftwaffe to steer their bombers to targets over Britain. Jones employed electronic countermeasures to divert the bombers and cause many of the bombs to fall off target. It was one of Churchill's top secrets of the war.⁹⁷

The British understood the close relationship between ELINT and COMINT, and they centralized both under GCHQ. But when they tried to deal with the United States, they found American ELINT to be frustratingly decentralized. It wasn't just that they had to deal directly with the SCAs rather than AFSA and NSA, they found that even within the individual services there was no focal point.

The SCAs did much of the ELINT collection for their respective services. Each one had a network of ELINT collection sites, often collocated with COMINT sites. But the tactical commanders also had their own ELINT assets, often airborne (and shipborne, in the case of the Navy). Once collected, the intercepted tapes were forwarded to processing centers in

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 theater and on to the United States. Some of the processing centers were joint-service operations, while some were single-service.

By 1953 the Army and Navy had established a consolidated ELINT processing center called ANEEG (Army-Navy Electronic Evaluation Group) collocated with NSG at Nebraska Avenue. The Air Force did not participate, preferring to keep a separate processing facility at AFSS headquarters, under the auspices of the Air Force Technical Intelligence Center (ATIC) at Wright-Patterson Air Force Base near Dayton, Ohio. NSA was not involved in this tangled web.

In 1953 the Robertson Committee (see p. 227) reported to Canine on the profoundly disorganized nature of American ELINT and concluded that as a source of warning information, this intelligence discipline was in danger of becoming irrelevant. The committee recommended that a focal point be found.⁹⁸

CIA, too, was unhappy with the way ELINT was being managed and in the same year conducted an internal study that indicted the Defense Department for mismanagement of ELINT. CIA pointed out that there was no central authority, no coordination of ELINT activities, and no central processing. The study opted to place central control in USCIB, but one option which the drafters seriously considered was to give NSA the job.

There being no focus in U.S. intelligence for ELINT, CIA began to take on this task also. In 1954, the deputy director, General C.P. Cabell (USAF), appointed an ELINT czar by giving H. Marshall Chadwell, the assistant director for scientific intelligence, an additional hat for ELINT.

When he received the Robertson study in November of 1953, General Erskine in the office of the secretary of defense called in Canine and requested an NSA response. On returning to Arlington Hall, Canine found his agency badly divided over what to do. The eminent logic of combining ELINT and COMINT was sometimes obscured by the evident difficulty of getting the services to heel to central authority and the dismal prospect of ever getting a charter as clear and unequivocal as NSCID 9. If COMINT, with NSCID 9 conveying absolute authority, was proving so difficult to manage, what of ELINT?

Despite this, the allure of finally getting the two pieces of the electronics puzzle together proved too strong. Under Canine's direction, NSA's Office of Plans and Policy

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

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

produced a draft report which placed operational and technical control of ELINT with DIRNSA. The battle was joined.

When the issue went to USCIB, the JCS predictably defended decentralization. Over the ensuing two years, piles of studies were completed, and hundreds of options were tossed about. The services never relented in their opposition to any sort of restriction on the latitude of the tactical commanders to collect, process, and report ELINT. All concerned recognized that there should be some sort of overall coordinating mechanism and that the government must set up a central processing facility at which all the players would be represented, including non-DoD organizations (i.e., CIA). NSA appeared to be the only organization that felt that NSA should be in charge.

The "ELINT Problem" was temporarily resolved in May of 1955 with the publication of NSCID 17. This document gave ELINT policy to USCIB and directed that a centralized ELINT processing center be set up (the National Technical Processing Center, or NTPC). However, it still allowed for separate management of DoD and CIA ELINT activities. The Air Force was given executive responsibilities for both ELINT and monitoring of jamming signals, [redacted]. Neither NSCID 17 nor the DoD implementing directive resolved the issue of where NTPC was to be located. After months of discussion, the services decided to keep it at Nebraska Avenue, where ANEEG was already located.

NTPC was comprised initially of approximately one hundred people from the three services and CIA - NSA was not even represented. Most of the billets came from ANEEG, and the SCAs exercised a predominant influence since they provided most of the expertise. CIA, however, sent a very strong delegation. An ELINT requirements group was established in 1956, comprising representatives from the services plus CIA, and later in the year a committee on [redacted] was created. This was the first NTPC organization that had any sort of NSA representation.

In 1956 NTPC was given the additional mission of processing telemetry from Soviet missiles. This problem was to grow and multiply almost geometrically as the Soviet missile problem became a national preoccupation. Sitting between COMINT and ELINT, telemetry would soon become another area of controversy between NSA and its competitors.

NSCID 17 was remarkable for what it did not do. It did not establish operational control in one organization. Nor did it rein in the propensities of the armed services to fund separate ELINT assets for nearly every operational command. It did not unify the technical aspects of the business. Instead, it consigned management to a committee which was already deeply fractured on other issues (such as the dispute between NSA and CIA over control of COMINT). It did not resolve anything at all, but it merely perpetuated an existing condition.¹⁰⁰

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

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

BUILDING THE OVERT COLLECTION SYSTEM

Few cryptologic field sites survived World War II (see map on p. 113). By 1947, the two services were operating [redacted]. The Army maintained large fixed field sites, but very few of them. The Navy tended toward small sites, many with only a DF mission, scattered throughout the world to maintain a DF baseline.

Even more striking was the geographic pattern. The United States had but one cryptologic organization on the continent of Europe. [redacted] sites were in the U.S. Of the rest, the Army collection site in [redacted] had existed since the early days of World War II. The other overseas sites were in [redacted] and they copied primarily [redacted] targets. The Navy's overseas sites were all in the [redacted]

This soon changed. The Cold War, the Communist takeover in Czechoslovakia in 1948, the Communist victory in China in 1949, and the unpleasantness in Korea, combined to force a revolution in America's cryptologic posture. The somnolent late 1940s became the go-go 1950s. Cryptologic planning was stirred to a white heat, and the collection system fairly exploded. By 1960 American's cryptologic collection system [redacted] had basically been built.

Three things typified this system:

1. The target was the Soviet Union. China, Korea, and the East European satellites were simply corollary targets. [redacted]

2. Containment of Communist expansion was the objective. The collection system became geographically arrayed to resemble Lenin's predicted "capitalistic encirclement," a figurative string of pearls beginning in [redacted]

[redacted] And despite this seemingly heedless expansion, NSA was barely able to keep up with customer requirements.

3. This was the Golden Age of HF. Long-haul HF systems dominated the world communications networks. Above-HF transmissions did exist, but in HF's Golden Age, most of the truly important messages seemed eventually to find some mode of HF expression. Propagation vagaries demanded that collection sites be placed in a wide variety of locations. But in theory, if one established enough sites and built

~~TOP SECRET UMBRA~~

[Redacted]

Expansion proceeded on two fronts. The first was ELINT, which was chaos reborn. The services embarked on a period of virtually uncontrolled site-building. ELINT was above HF, so sites tended to be located in great profusion [Redacted]

[Redacted] In this field each SCA had been given the primary collection job by its respective service, and each moved quickly to establish sites. In many, if not most, instances ELINT preceded COMINT, and again in most cases ELINT sites already existed where COMINT sites were later added. [Redacted]

[Redacted] Added to this was a burgeoning airborne collection system, fielded by USAFSS. NSA played no role in ELINT, either in collection or processing.

When it came to COMINT, though, NSA employed its guiding hand. Even before NSA was created, AFSA had a master plan for the establishment of SCA intercept sites which [Redacted] This plan was passed on to NSA, which refined it. NSA worked very closely with each SCA to determine collection requirements and determine the best candidate locations. In the early 1950s NSA asserted control over site surveys, without which no collection site could be established. NSA balanced customer requirements against existing overt [Redacted] sites, documented hearability, and Second and Third Party contributions. If the project did not make sense, DIRNSA could be counted on to oppose it.¹⁰¹

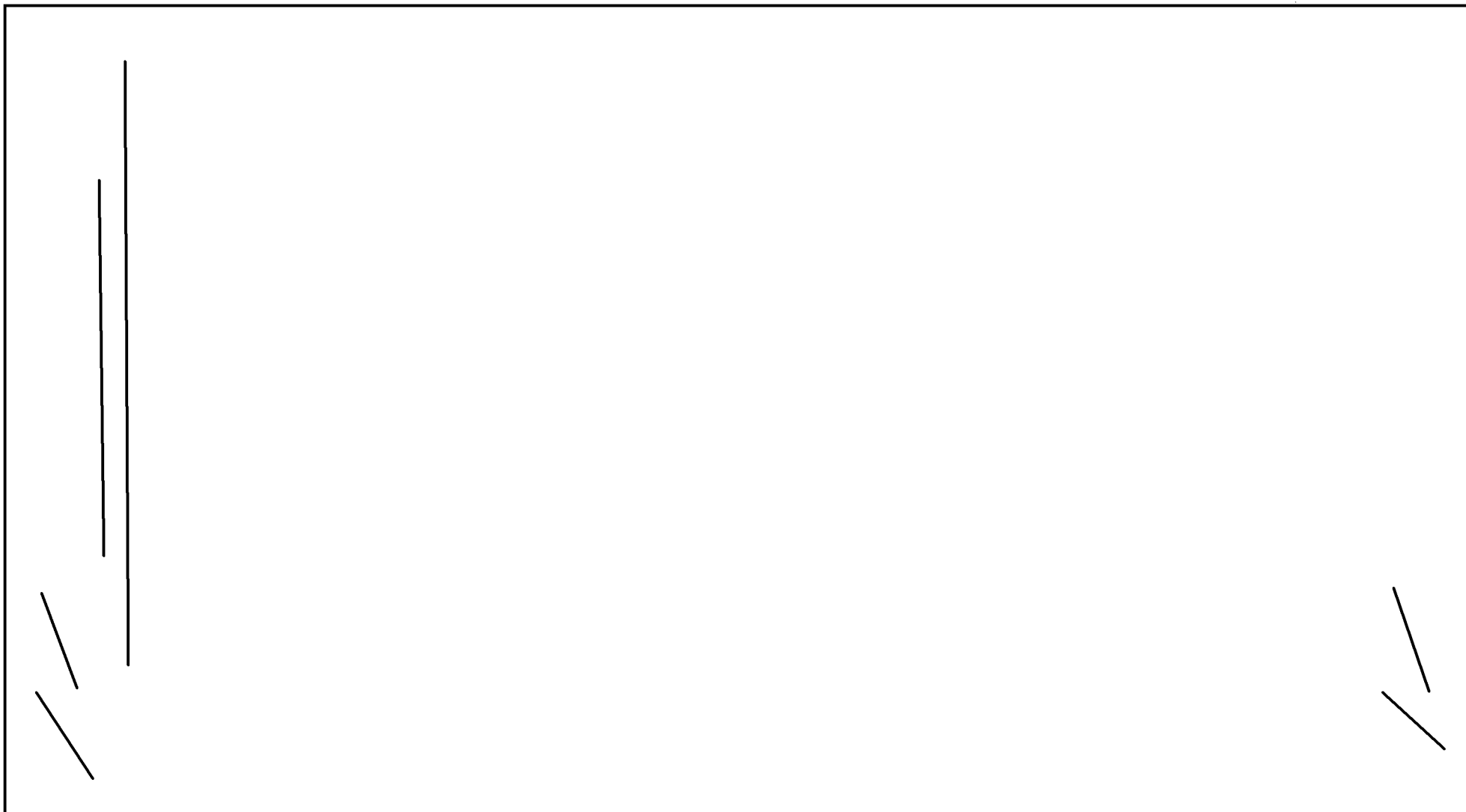
[Large Redacted Block]

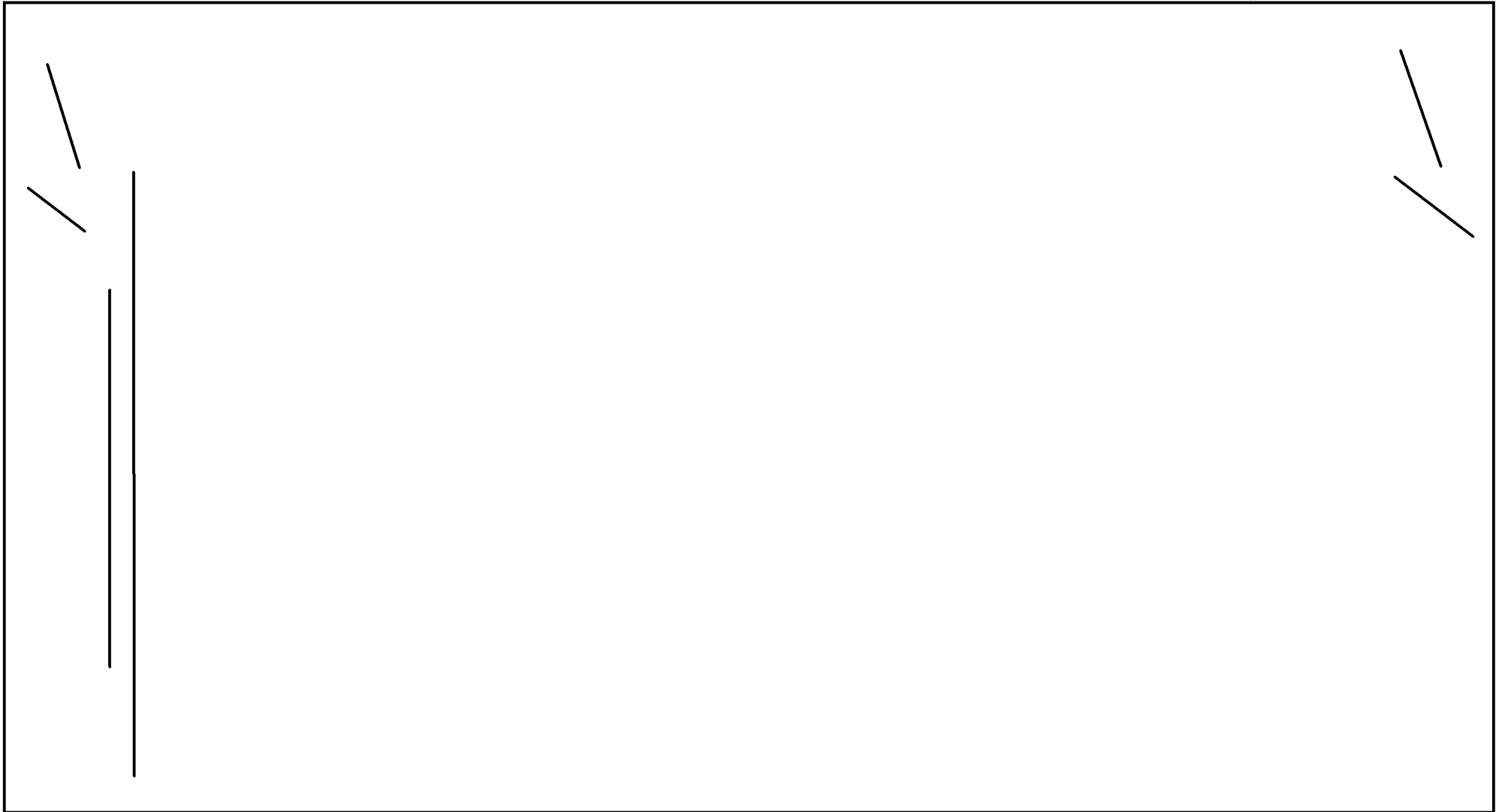
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

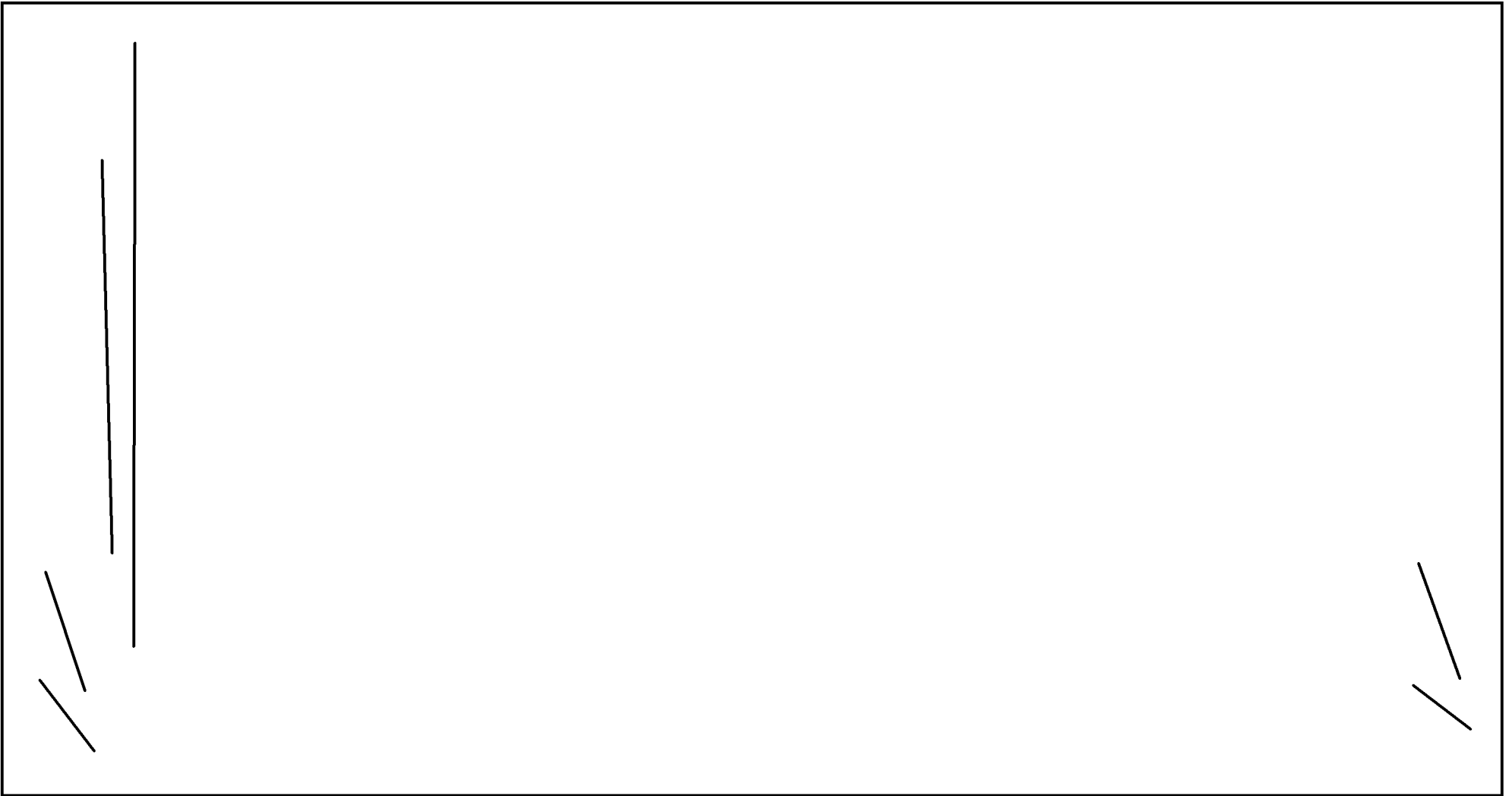
(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

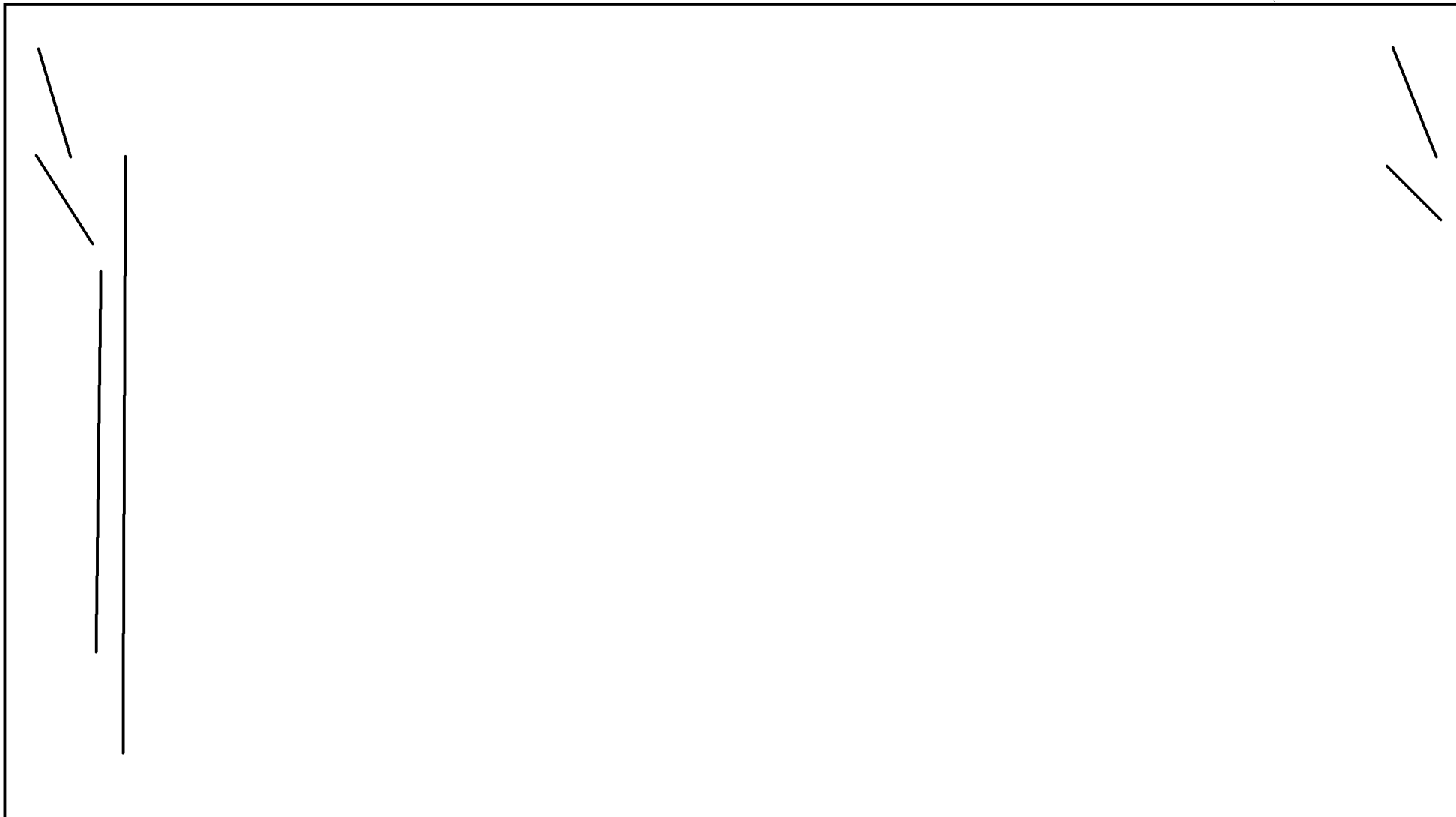
(b) (1)
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36



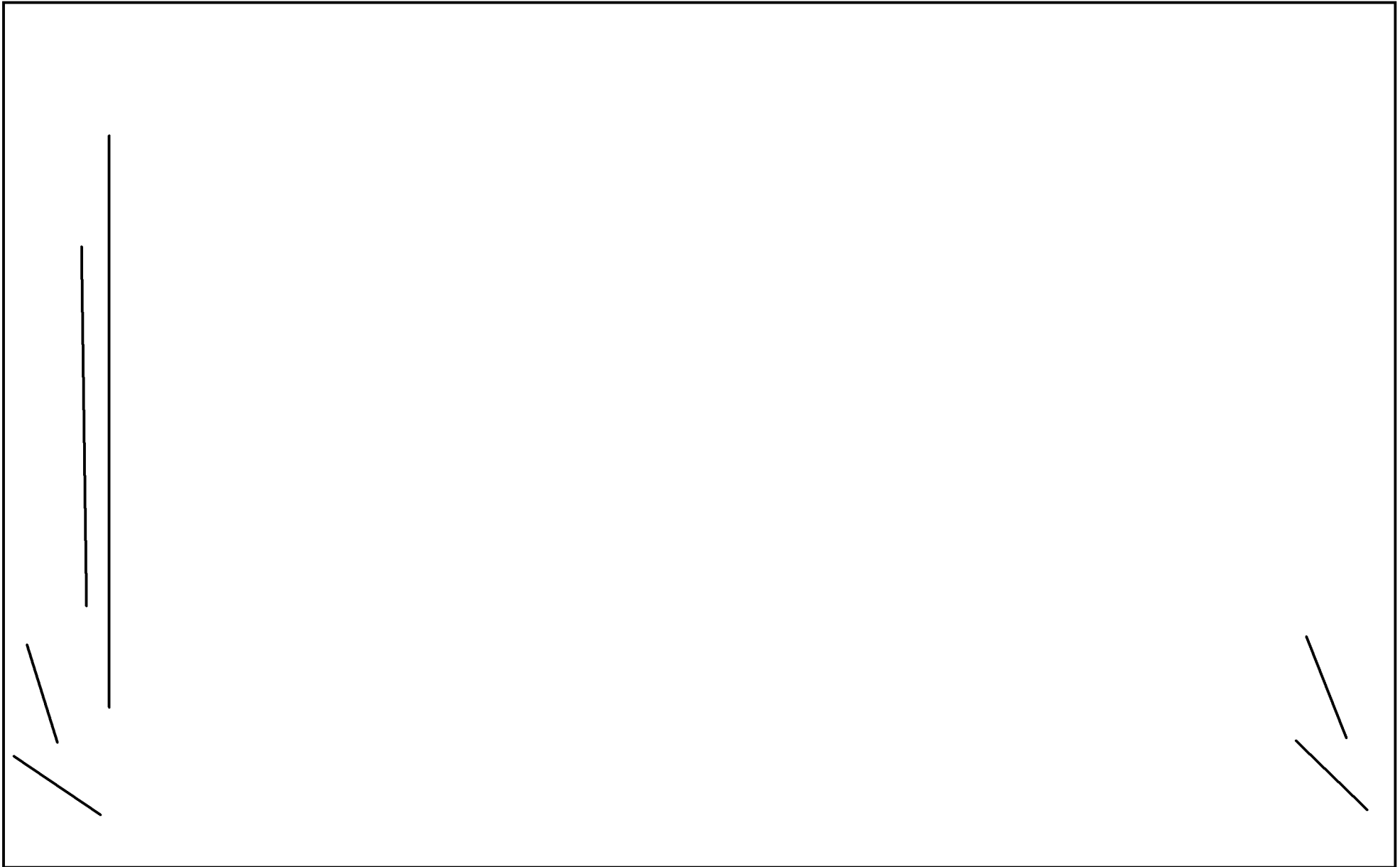


(b) (1)
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36





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

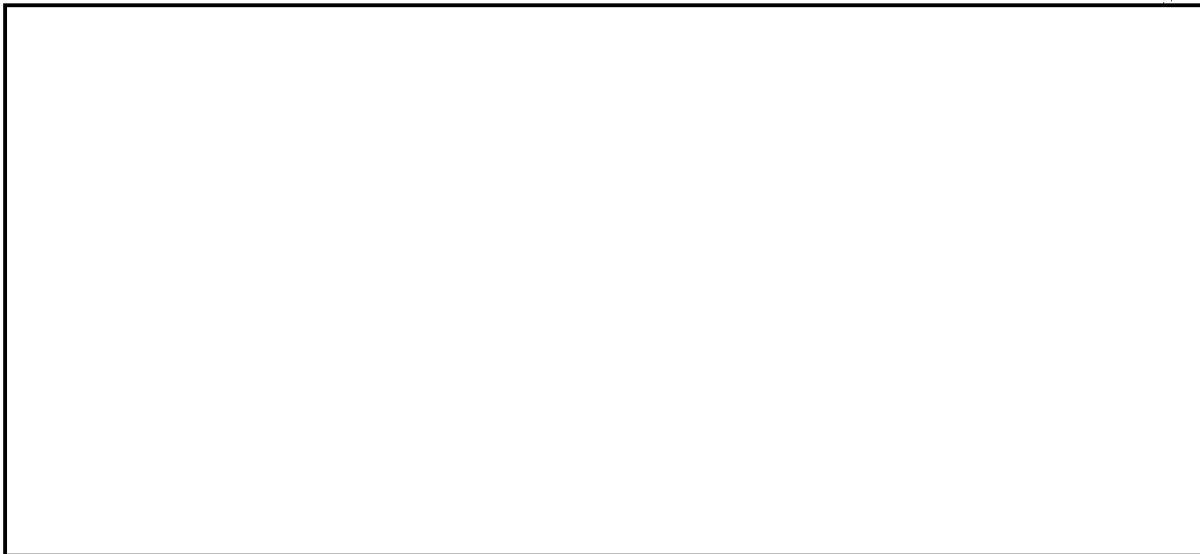


~~TOP SECRET UMBRA~~

Berlin was in an entirely different situation. Its status as a four-power occupied city meant that Soviets could walk relatively freely even in the American Sector. Stalin's attempt to squeeze the Westerners out of Berlin (resulting in the Berlin Airlift) in 1948 placed the city in a uniquely precarious position. In such circumstances the first COMINT intercept organization, a detachment of the ASA site [redacted] arrived in a covert status and stayed only a few weeks in 1951. But ASA covert detachments kept appearing in Berlin, and in the following year the command established a permanent unit there, and the troops moved from tents to covered buildings.

In 1953 the Army G-2 concluded that the results had been paltry and recommended the site be closed, a strange finding given the later reputation of Berlin as a SIGINT bonanza. Fortunately, no one listened to the G-2, and ASA continued to occupy a variety of locations [redacted] AFSS followed ASA into Berlin in 1954, beginning a presence in the city that would last until after the fall of the Berlin Wall.¹⁰²

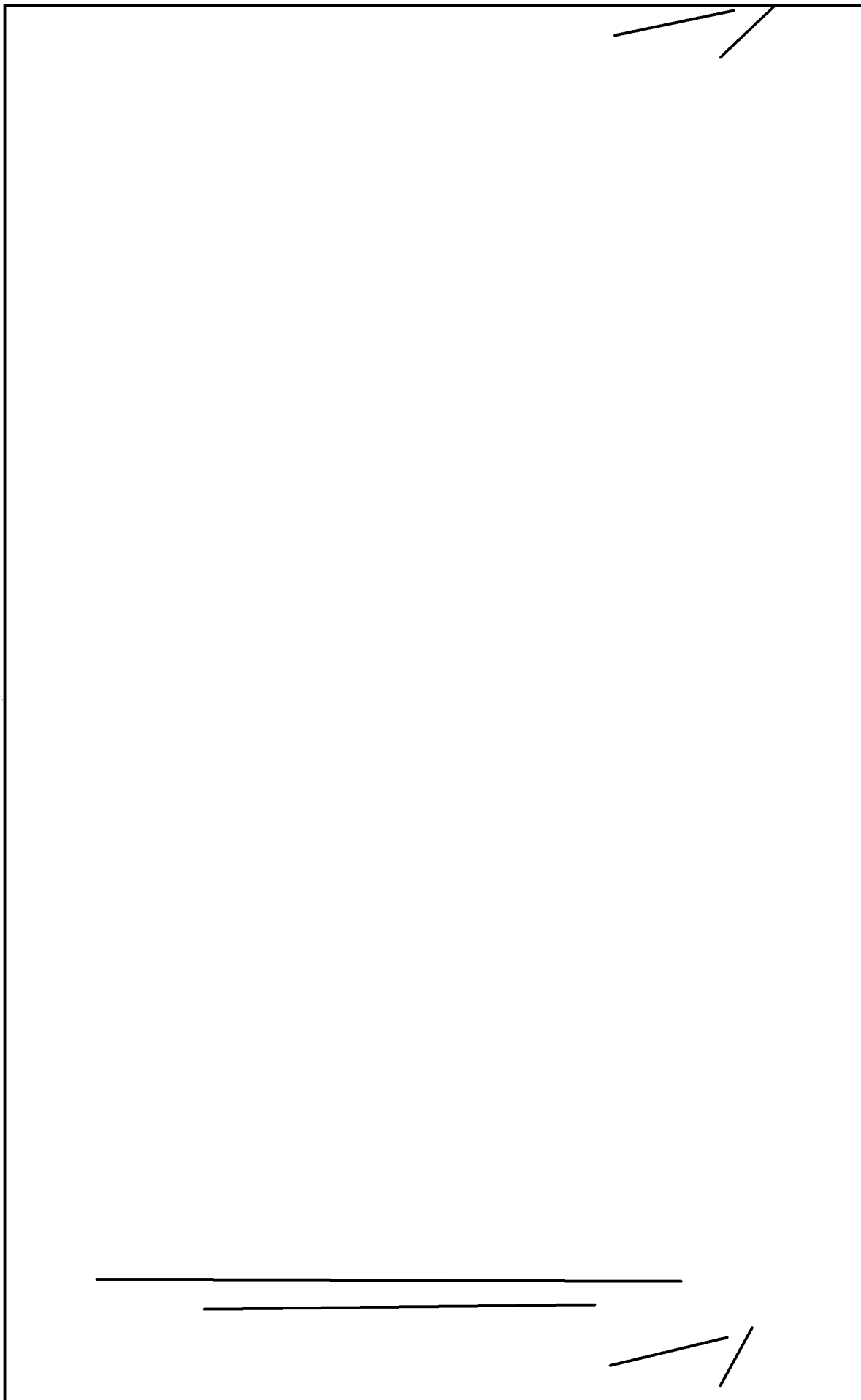
Berlin became a SIGINT gold mine, a window into the heart of the Communist Bloc military system. In the mid-1950s the collection sites began to report the existence of VHF communications, and NSA moved in to investigate. An NSA technician [redacted] discovered that Berlin was crisscrossed with above-HF communications that the West had never before intercepted, including Soviet high-capacity multichannel and microwave transmissions. The discovery was to have a profound influence on the development of the SIGINT collection system.¹⁰³



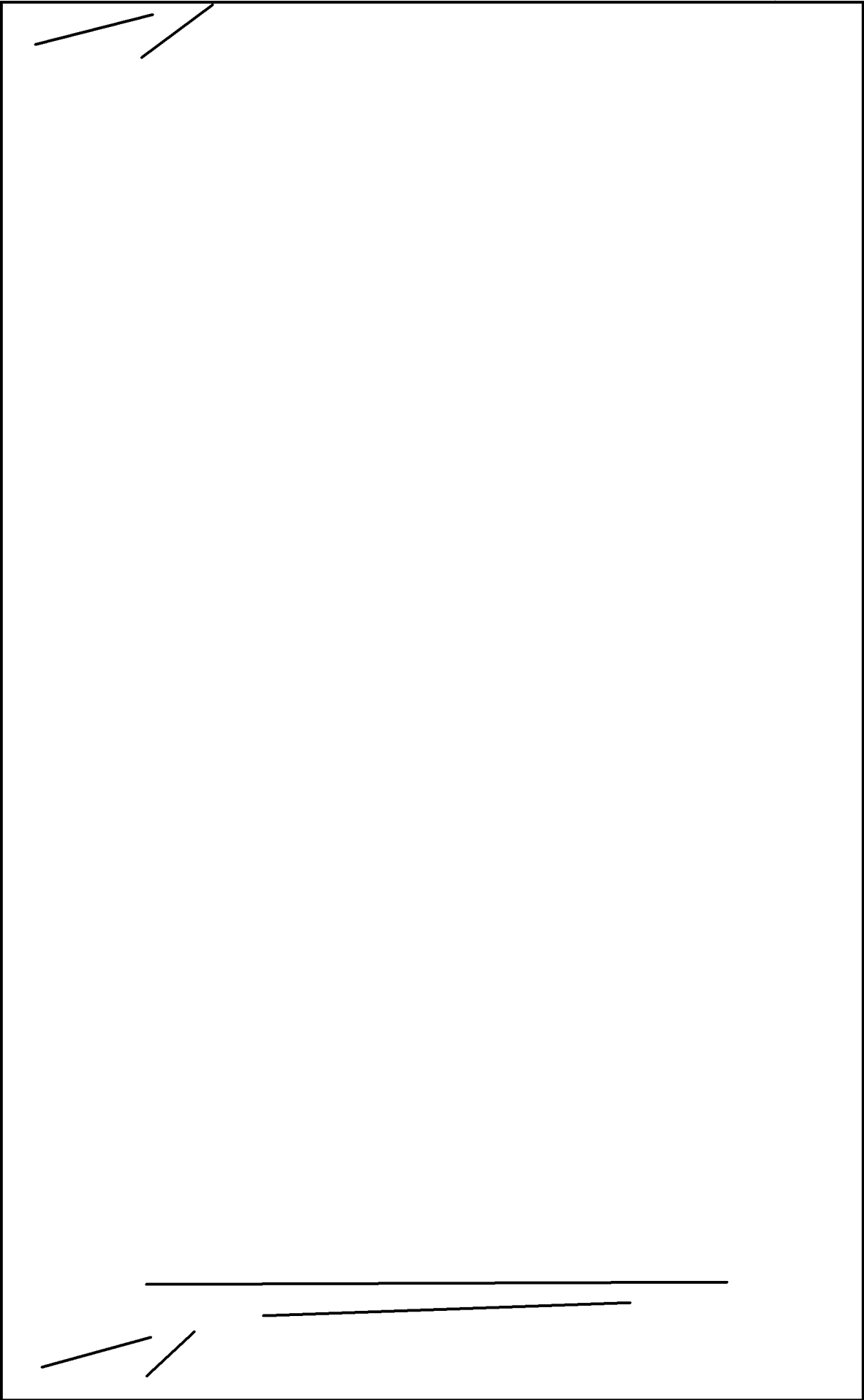
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

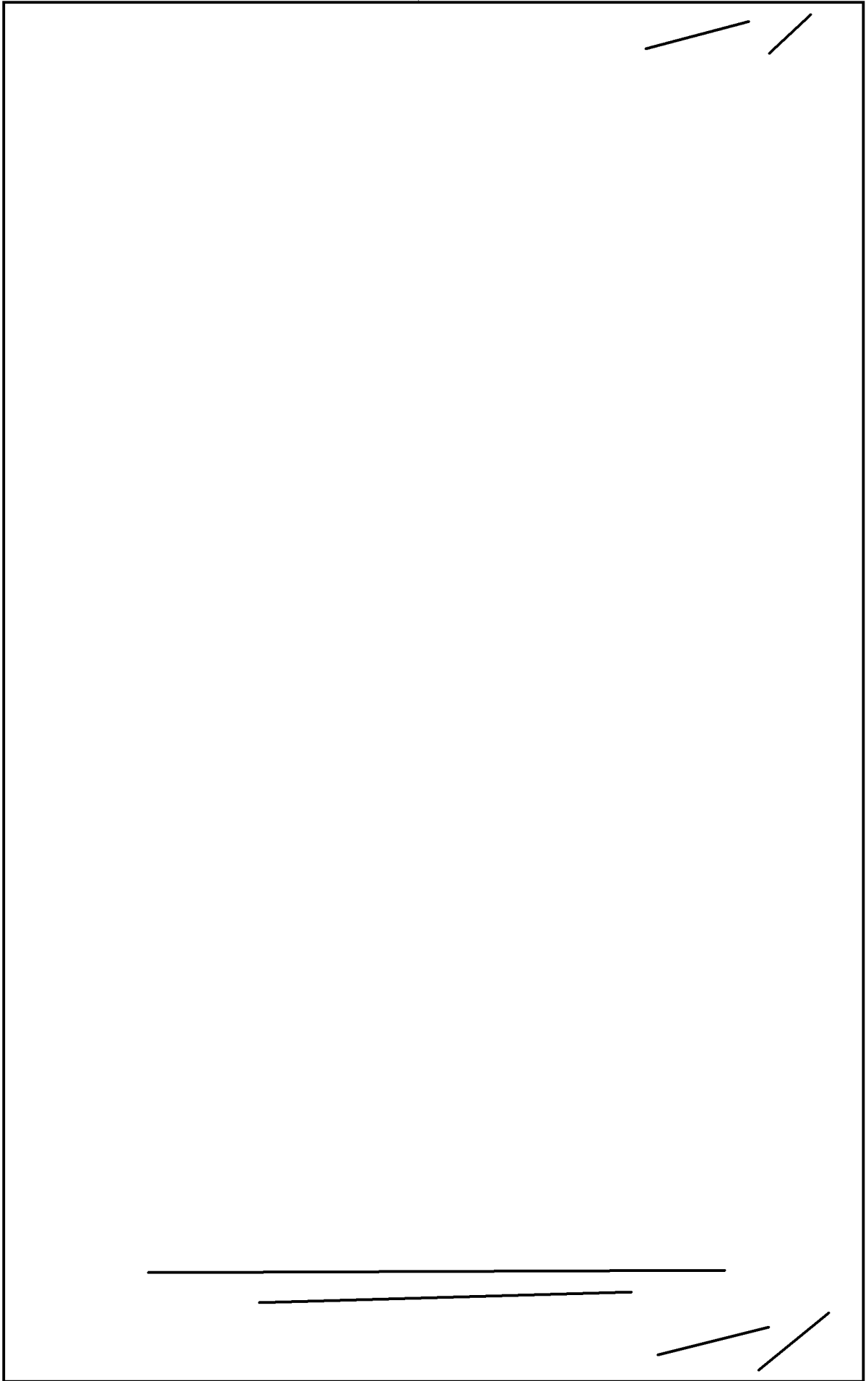
(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

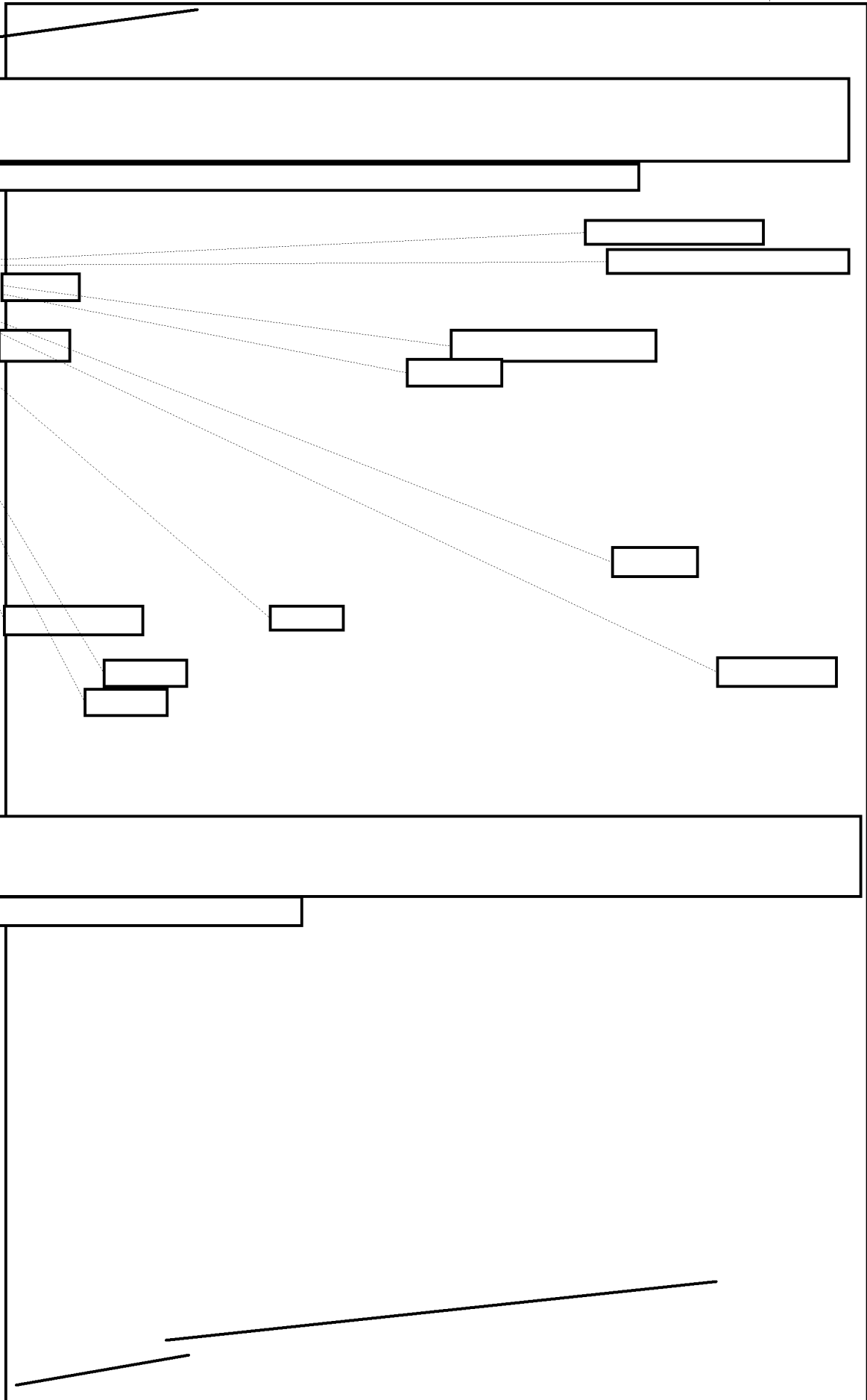


(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36



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





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

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

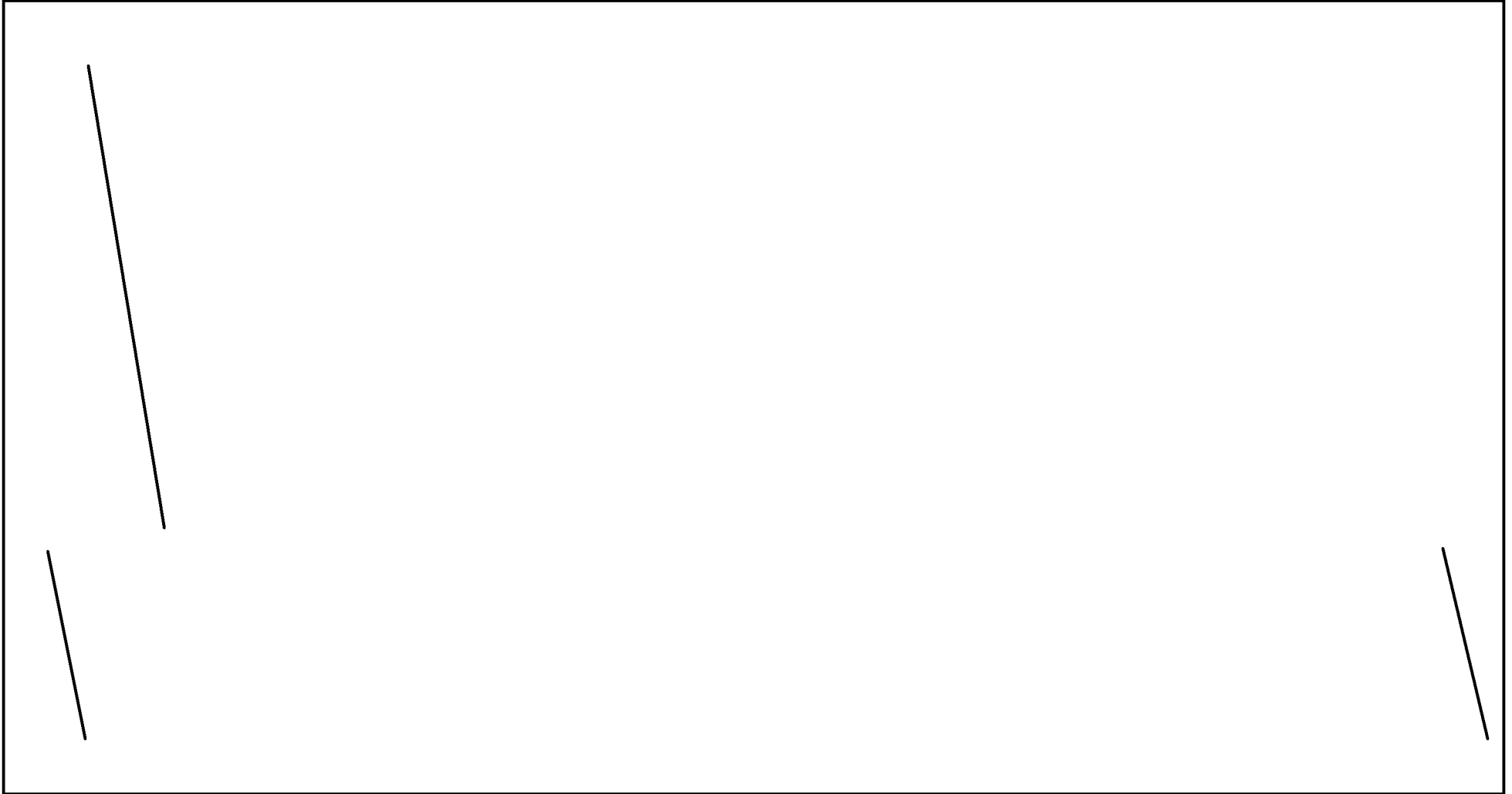
[Redacted]

[Redacted]

[Redacted]

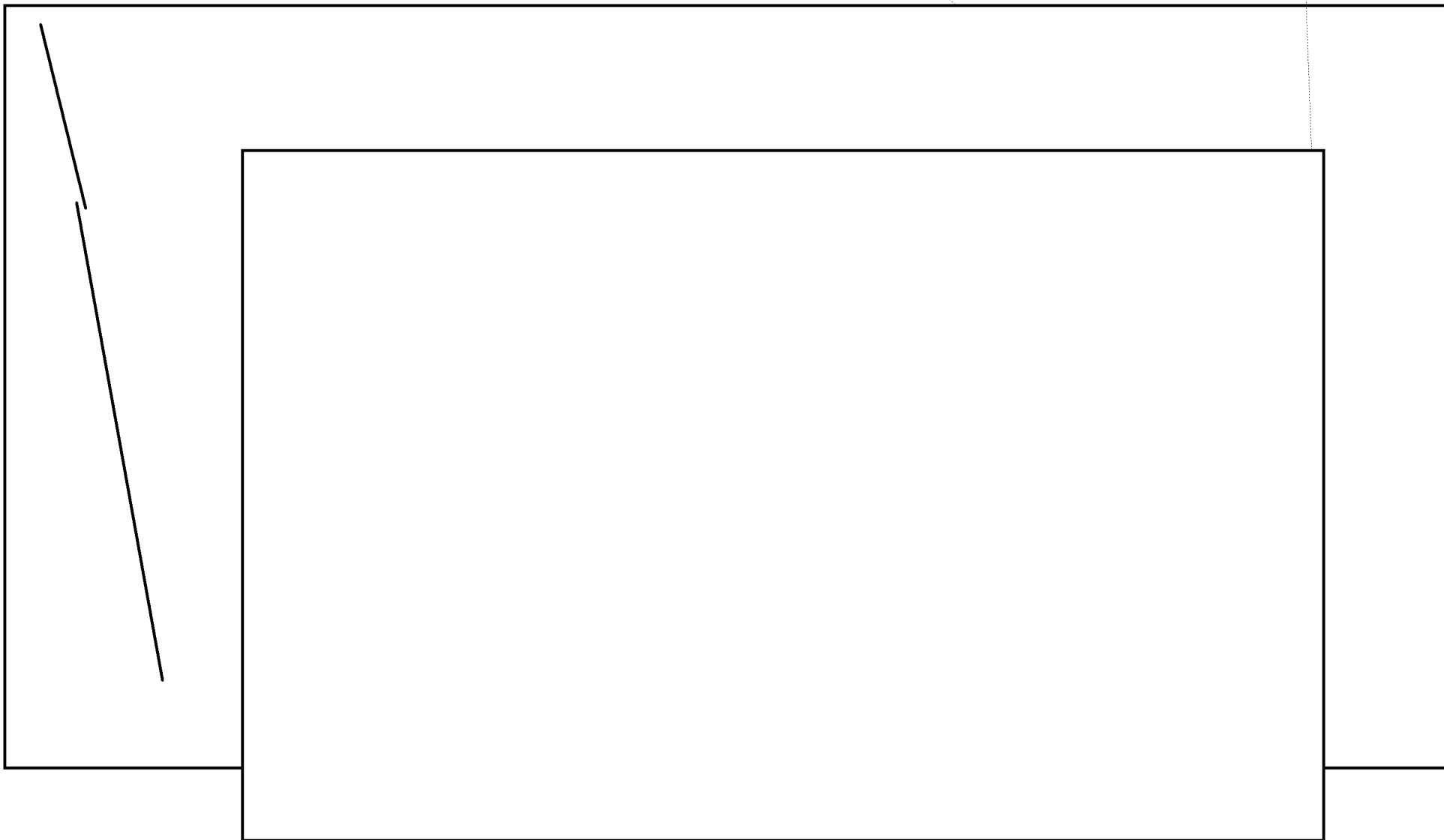
(b) (1)
(b) (3)
OGA

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



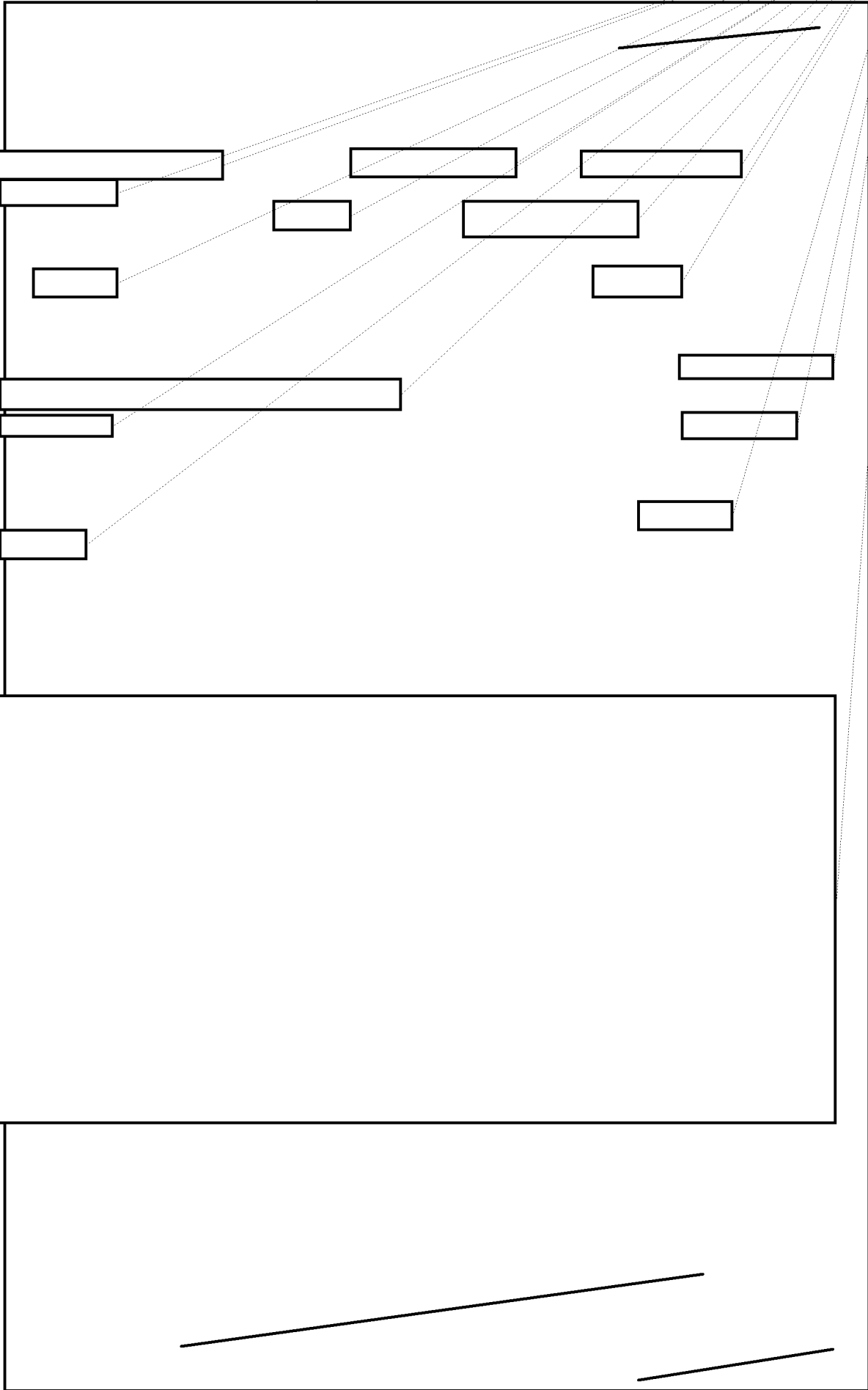
(b) (1)
(b) (3) - 50 USC 403
(b) (3) - P.L. 86-36

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



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

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



[Redacted]

[Redacted]

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

[Redacted]

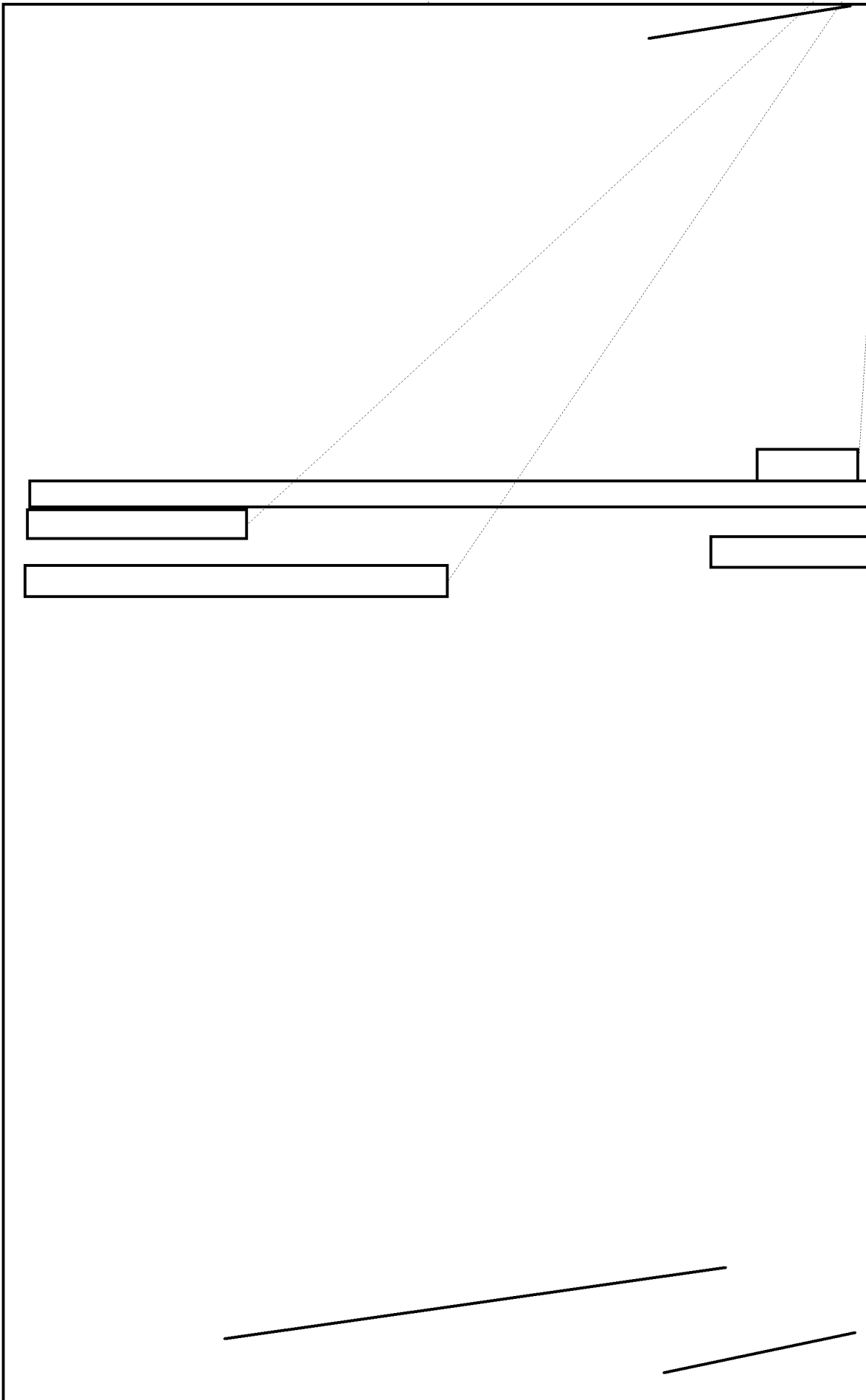
[Redacted]

[Redacted]

[Redacted]

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

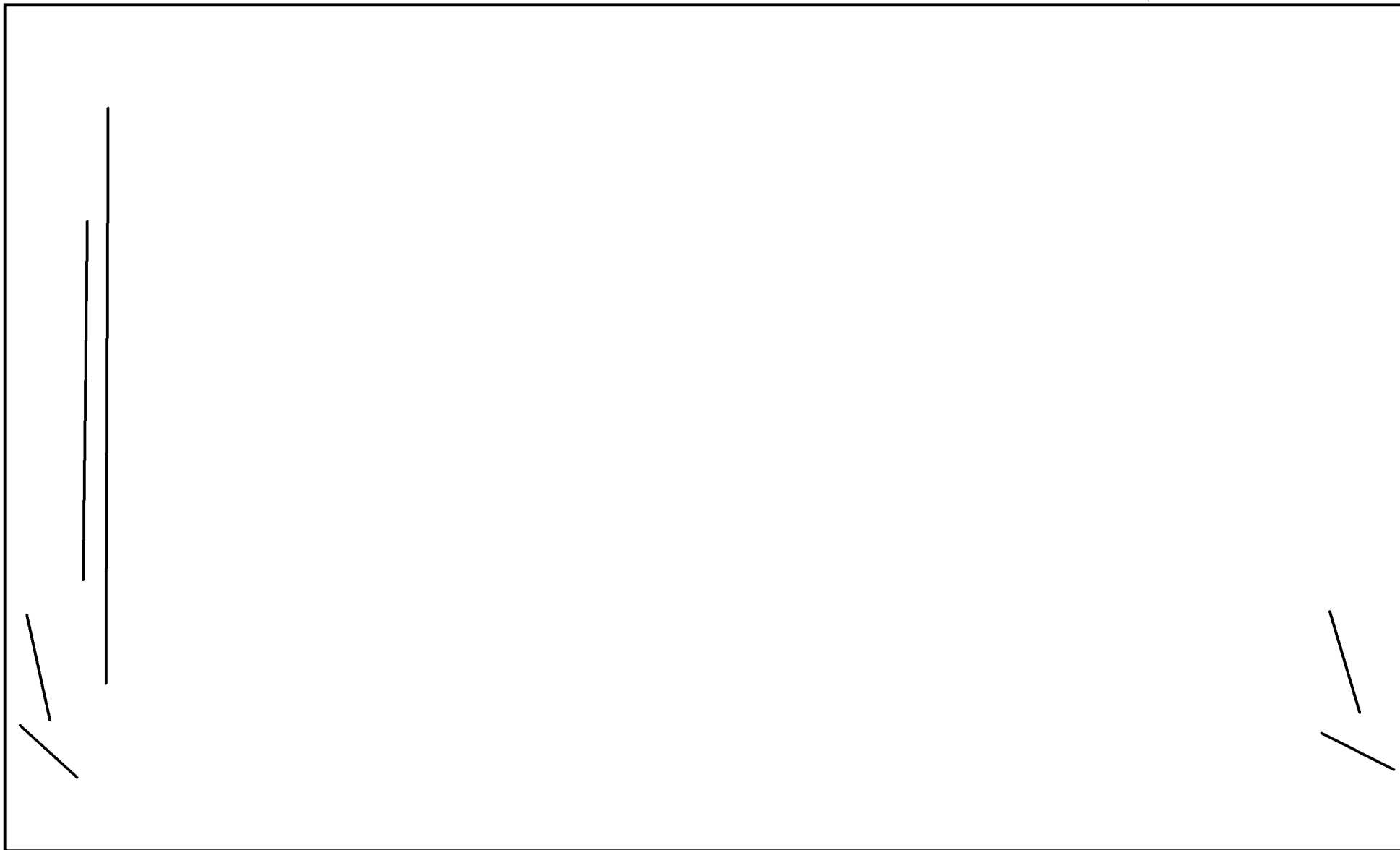
(b) (1)
(b) (3)
OGA

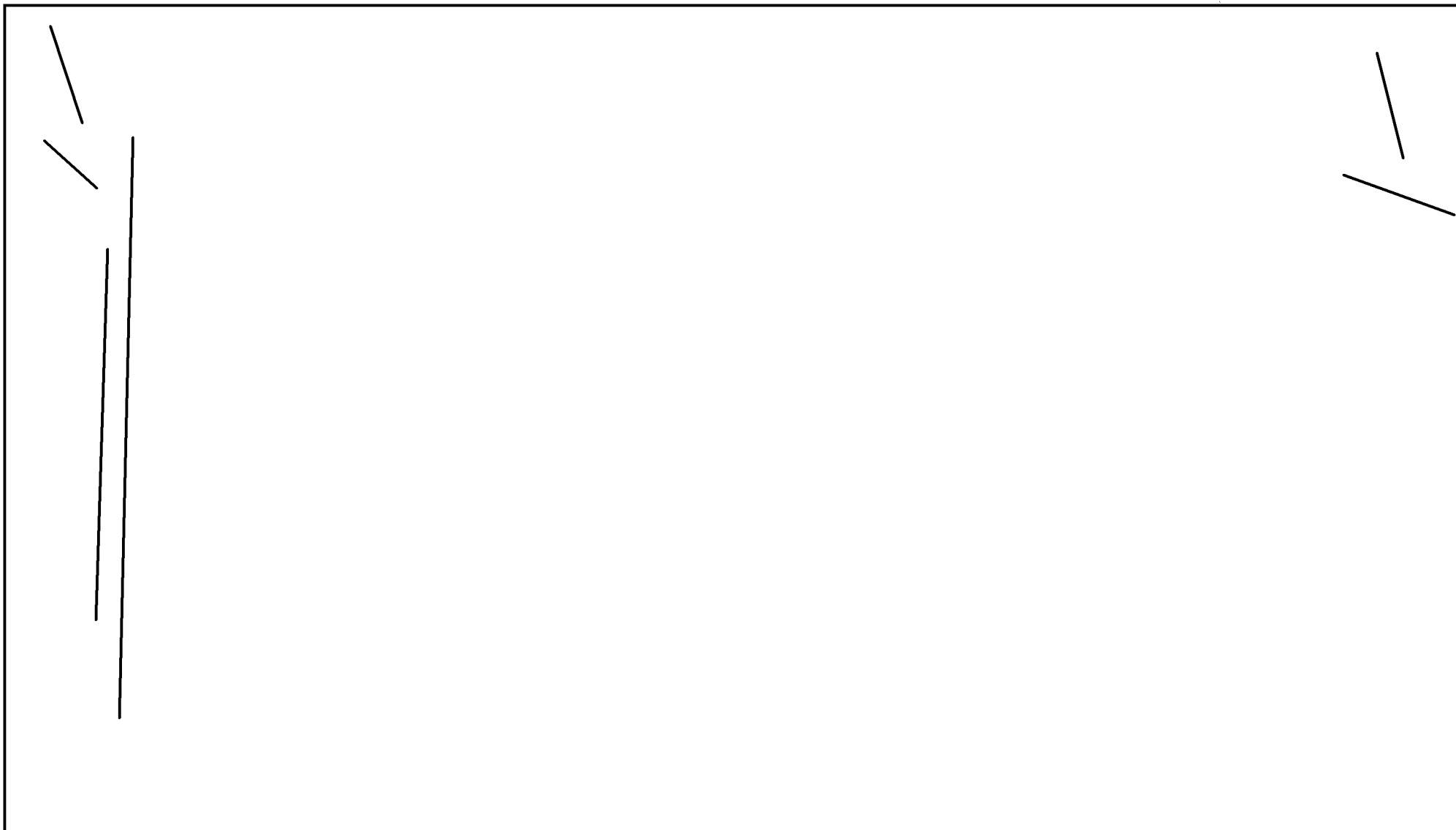


_____ /

_____ /

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





(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798



ASA PAC in the 1940s

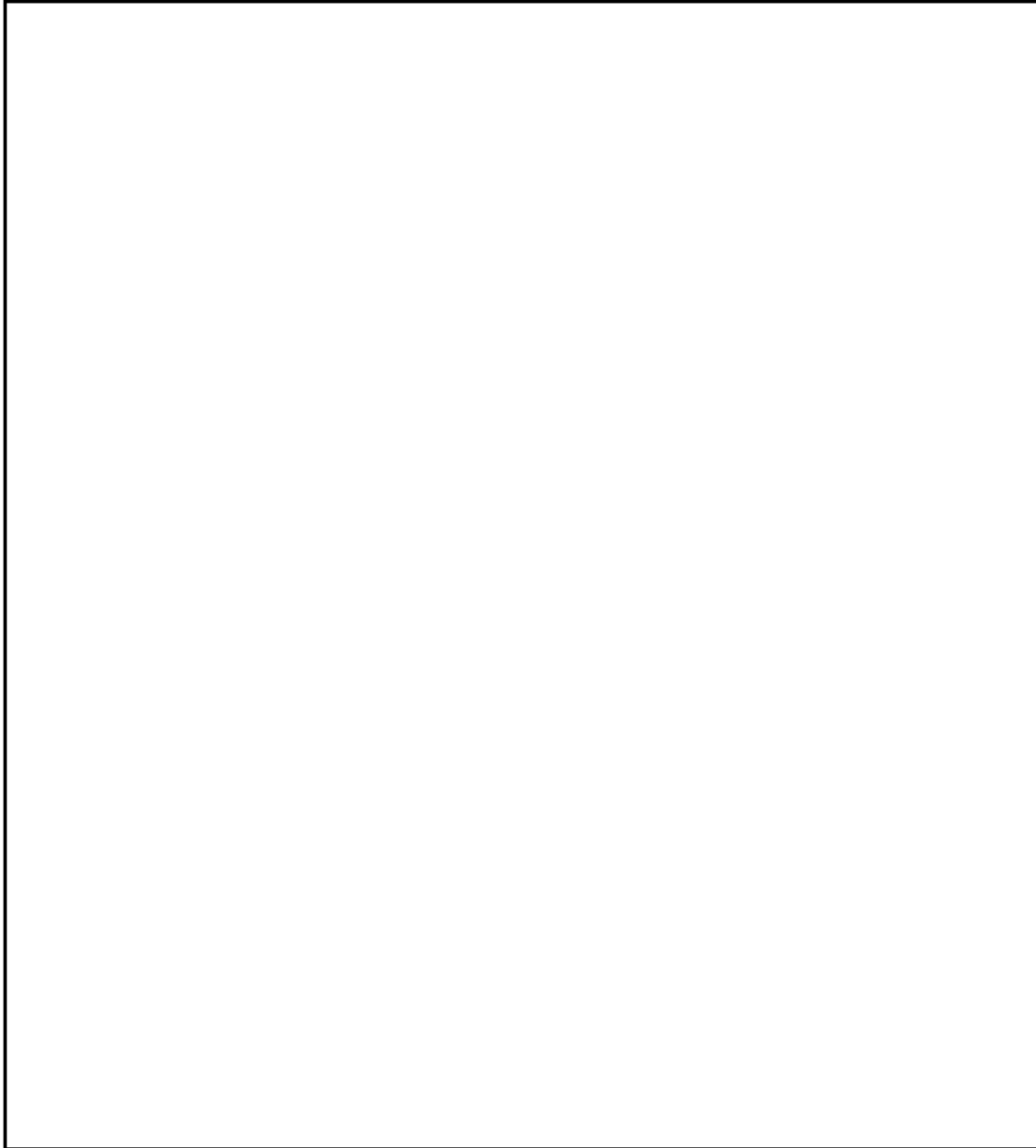
ASA's first postwar Far East headquarters was in a relatively intact building in downtown Tokyo. Japanese nationals staffed the support services.

The Far North

All three services established collection sites in Alaska. The Navy site at Adak dated back to World War II, and the Air Force and Army soon followed. The USAFSS site grew out of the [redacted] a World War II Army Air Corps asset. Security Service established its first collection site [redacted] The Army site was established near Fairbanks (1950). But AFSS soon eclipsed ASA in resources, as the [redacted] proved to be very lucrative and the predominant one in Alaska. [redacted] eventually grew to become one of the major Security Service sites, while the ASA site closed in 1959.

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

~~TOP SECRET UMBRA~~



What It Was Like

Military units tend to form around existing support organizations. Army units cluster at Army posts, Air Force organizations locate at existing Air Force bases, Navy units form at Navy bases. Cryptologic units, however, must go where they can hear targets. Where there is an existing military base, so much the better. But if there is none, one must be built specifically for the collection organization. This condition was especially true in the 1950s, when collection was done primarily to satisfy national, strategic requirements

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

~~—NOT RELEASABLE TO FOREIGN NATIONALS—~~

~~TOP SECRET UMBRA~~

rather than to support tactical commanders. In such a situation, it was not necessary for cryptologic organizations to stay with a supported commander. They could, and often did, go off on their own.

Geographically, collection sites were scattered. They tended to be small, isolated, and largely self-sufficient. Running a site required a very high level of independence and self-reliance. Even when collocated on a major military installation, the SIGINT unit was not part of the command structure. The post or base commander was generally not SI cleared and treated the cryptologic unit somewhat like a leper. Under such conditions, support was difficult to obtain.

In the late 1950s, Air Force Security Service under Major General Gordon Blake decided to solve its logistics problems itself. With the blessings of the Air Force, AFSS began managing bases at which its unit represented the major activity. Begun in July of 1958, the program eventually resulted in USAFSS's taking over [redacted] as well as their training base, Goodfellow AFB, Texas. The huge 466L building program (see chapter 8) may have been a factor, but Blake himself claimed that troop support was the driving force behind this program. It changed USAFSS into a large-scale landowner, and it was not copied by either ASA or NSG.¹¹⁹

Climate could be an enemy. Air Force and Army sites at places [redacted] would frequently be snowed in much of the winter. Roads [redacted] were often impassable. Some sites could be supplied only by helicopter. In the tropics, the lack of air conditioning at places like Clark made work almost unbearable.

Even when the weather cooperated, conditions in places [redacted] were primitive. Army troops arriving [redacted] lived in pup tents for months. There was initially no air strip, and visitors to the site had a two-day drive from [redacted] over almost nonexistent roads.

Living conditions presented further challenges. A former resident of [redacted] a relatively "plush" location [redacted] describes the site in fairly realistic terms:

The station itself was a loose cluster of small, dusty buildings perched on the cliff above the village [redacted]

[redacted] The age old strategic value of the place was shown by the fact that our work went on in the shadow of a ruined, [redacted] castle.

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

~~TOP SECRET UMBRA~~

Water had to be hauled a mile from a spring. The site produced its own electricity with diesel generators, as the local power could not be relied on. There were no barracks, and the site personnel lived in apartments [redacted] and commuted by bus and boat [redacted] to the site. Since the ferry did not run after dark, the eve and mid shifts had to report at 1600, and the off-duty watch slept in bunks in a quonset hut.¹²⁰

In the early days, intercept sites took on all manner of configuration, from squad tents to quonsets to clapboard "hootches" in Southeast Asia. (The term "hootch" derived from the Japanese word "uchi," meaning "home," and migrated from the postwar occupation forces to the jungles of Southeast Asia.) But they gradually assumed a classic appearance as systems were standardized and permanent structures built. Most permanent sites were windowless blockhouses surrounded by high chain link fences with a single, guarded aperture.

[redacted] and the base commander sometimes economized on space by building the golf course in the antenna field.

[redacted]

The intercept area was generally divided into smaller rooms. Manual Morse, radioprinter, and voice modes usually had separate rooms, and at larger sites the Morse mission was frequently subdivided into rooms by target. Operators in the early days often

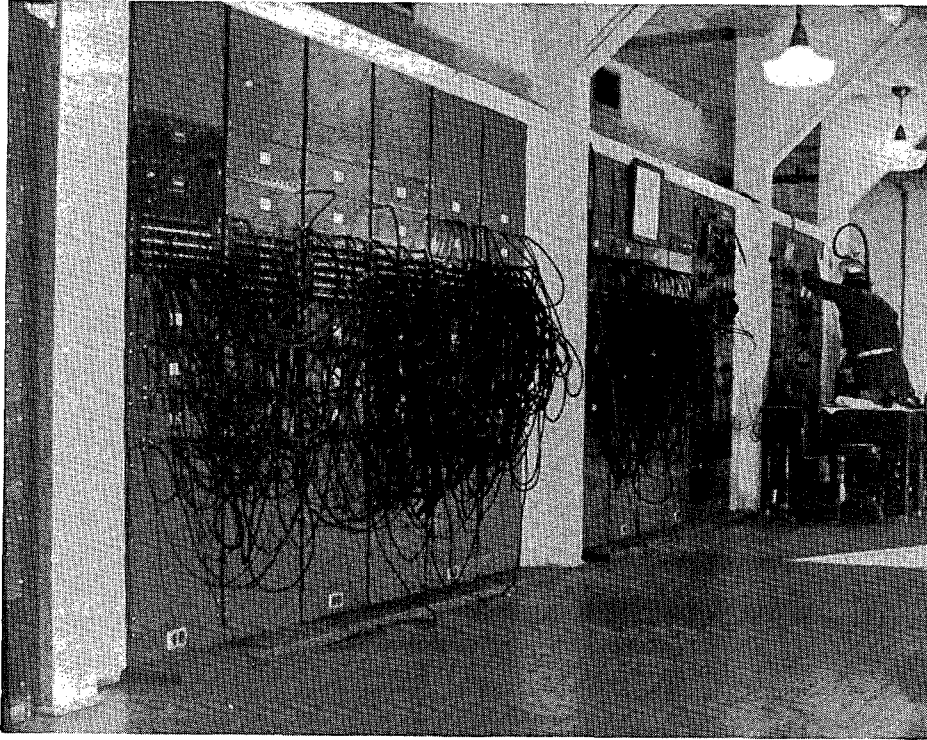
[redacted]

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

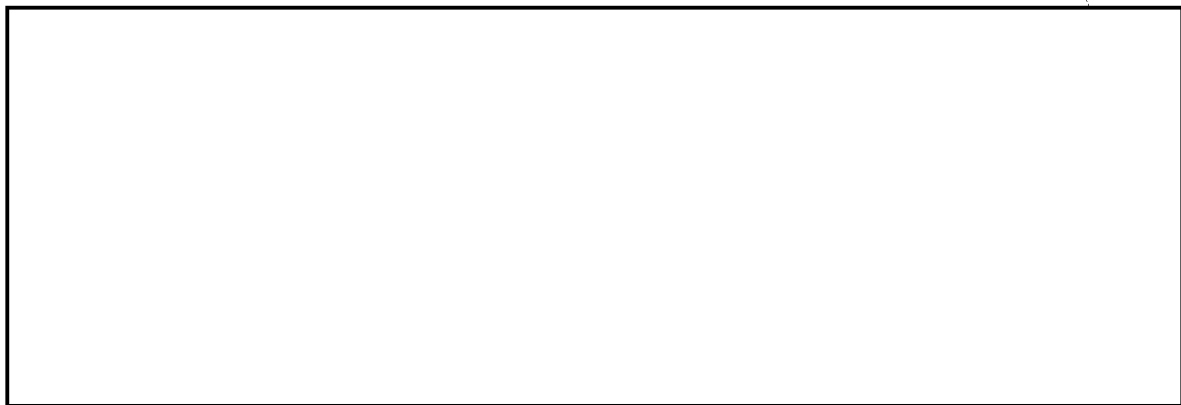
~~TOP SECRET UMBRA~~

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

~~TOP SECRET UMBRA~~

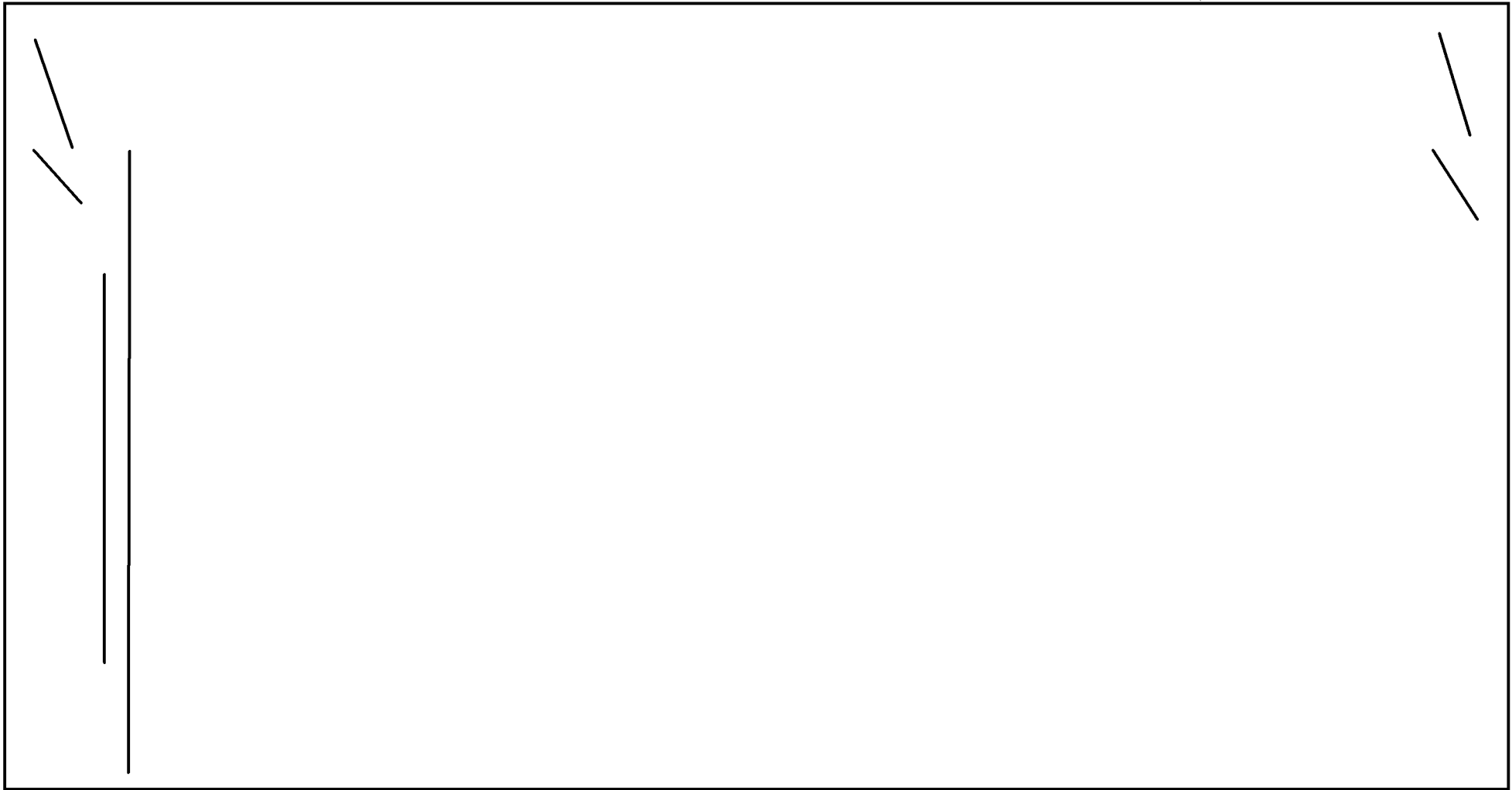


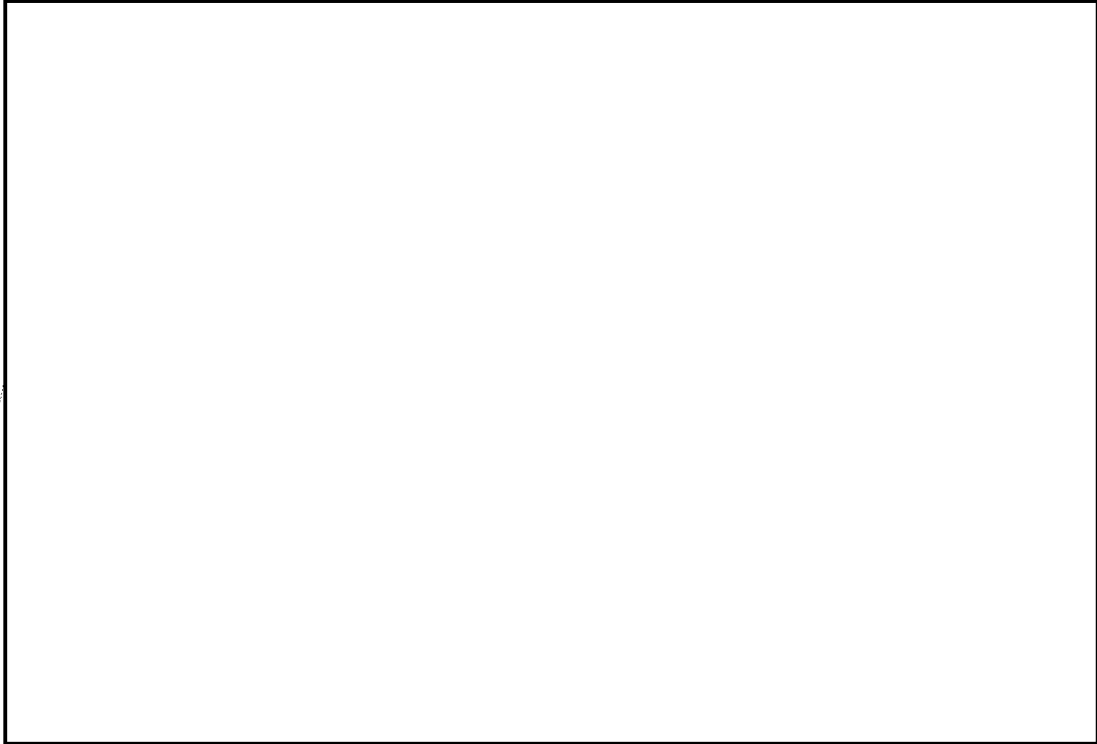
The "spaghetti panel" RF distribution room at USM-1 (Vint Hill Farms)



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

~~TOP SECRET UMBRA~~





The Navy site on Adak Island in the Aleutians survived and prospered despite the cold and snow.

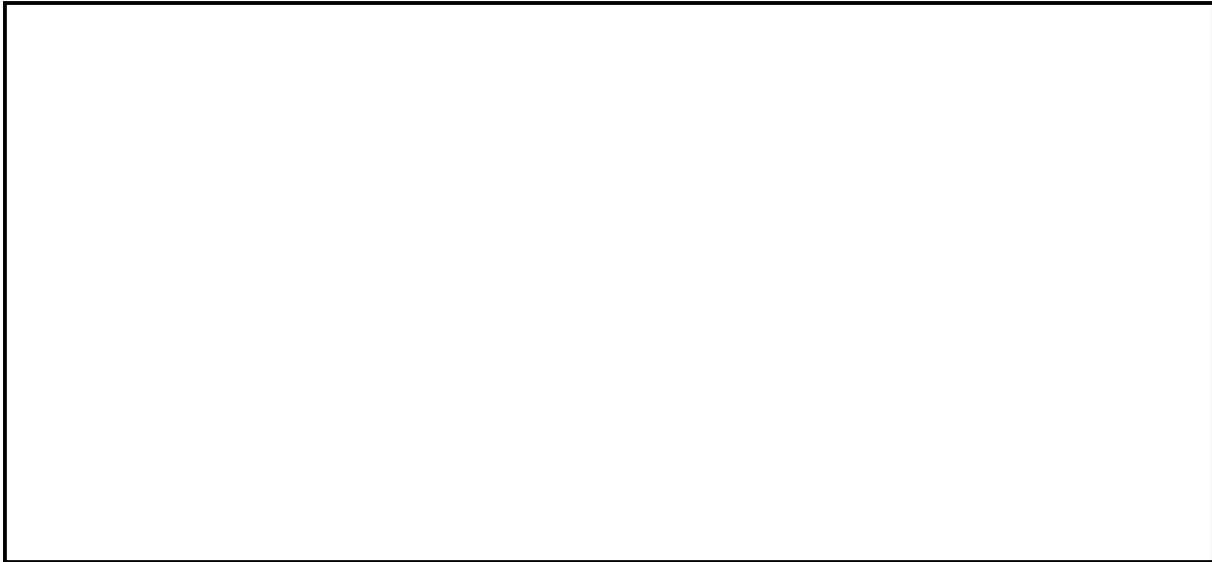
(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

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

~~TOP SECRET UMBRA~~



Barracks, USA-57, Clark AB, Philippines, early 1950s
These early "hootches" lacked air conditioning
(and just about everything else that would make them habitable).



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

~~TOP SECRET UMBRA~~

All services showed an interest in DF as a SIGINT technique, but the Navy was far ahead of the other two. The Navy had begun experimenting with DF as a navigational aid as early as 1906, and until the mid-1930s DF was developed for its short-range navigational value. But by 1935 OP-20-G had got hold of DF for intelligence purposes, and it gradually turned the Navy's primary interest toward strategic and tactical intelligence applications. By 1941 the Navy operated twenty-two strategic DF stations, organized into Atlantic, West Coast, Mid-Pacific, and Asiatic nets. In addition, the Navy had found that the British had invented effective shipboard DF systems (something the U.S. Navy had yet to accomplish) and began buying these systems from the British.



SIGINT Goes Airborne

Even by the end of World War II, the HF spectrum was becoming very crowded, and the Germans were beginning to experiment with VHF communications. Both the British and Americans flew airborne intercept missions against VHF targets during the latter stages of the war.

Eighth Air Force, concerned about the possibility of a German march into the VHF spectrum, began to install recorders and receivers set to pretuned frequencies on some of their strategic aircraft [redacted] This they referred to as their "airborne Y Service." General "Hap" Arnold of the Army Air Force directed a crash program to develop a dedicated airborne reconnaissance program, replete with special schools, dedicated aircraft (a modified B-24) and designated equipment. The AAF called the program "Ferret," and in early 1943 sent the first B-24s to Adak in the Aleutians. In March of 1943 a Ferret aircraft flying out of Adak obtained what was probably the first airborne intercept of a Japanese radar emission.¹²⁴

Spurred by the fortuitous capture of a Japanese radar on Guadalcanal in 1942, the Navy put together a seat-of-the-pants ELINT collection effort in the Pacific. The program did not have dedicated aircraft or specific units; the people involved just loaded their intercept gear on any airframe that happened to be flying in the right area. The effort paid off in June 1943, when Navy airborne intercept operators collected their first Japanese radar emission. Despite this success, however, the Navy realized that this approach was too haphazard, and in late 1943 a special reconnaissance unit was formed for the Southwest Pacific Theater. This very early effort eventually became the VQ-1 squadron.¹²⁵

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

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

~~TOP SECRET UMBRA~~

Following the war, the Air Force continued aerial reconnaissance against the [redacted]
[redacted] By 1947 the Army Air Force already had a rather elaborate postwar Ferret program in both the Far East and Europe. The AAF requested ASA assistance in placing COMINT intercept aboard, but at the time ASA displayed little interest.¹²⁶

BLUE SKY

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

Postwar COMINT airborne collection, however, developed from the Korean War rather than from the Soviet threat. In 1952 Air Force Security Service became concerned about reports that North Korean pilots were using the VHF spectrum for GCI communications. As their intercept of HF GCI communications was beginning to dry up, this seemed plausible and led to the establishment of a survey site on Cho Do Island. Cho Do definitely proved the existence of VHF GCI communications, and this finding boosted an embryonic USAFSS program to build a COMINT collection aircraft using an RB-29 as the platform.¹²⁷

But the people in the Far East were not willing to wait for a long-range fix. The commander of [redacted] working with Far East Air Force, initiated an in-theater effort which they called Project BLUE SKY. The idea was to seize whatever platform was available - this proved to be a C-47. It was modified by the addition of collection equipment and antennas formed up into a single intercept position and was launched into a series of trial orbits. Although there was plenty of VHF to be had, the orbit, because of requirements to be able to communicate with the ground station, was far from ideal, and the initial trials were only moderately successful. The Air Force adjusted the orbit, but results were still mixed because the wire recorder produced scratchy, almost unintelligible voices.

After the armistice in 1953, coverage requirements became even more pressing, and an additional VHF position was added. Results were better, but aircraft maintenance problems, equipment failures and lack of qualified transcribers on the ground prevented the program from fully realizing its potential. By 1958, however, BLUE SKY had expanded by the addition of three more C-47s, and the program continued until 1962, when all C-47s were replaced by USAFSS RC-130s.¹²⁸

Peripheral Reconnaissance

The reconnaissance program of which BLUE SKY was a part came to consist of a bewildering variety of programs operated by [redacted] American military services. Most of the missions were peripheral to the Soviet Bloc nations, and to those missions some rather strict rules applied. But some parts of the program apparently dealt with deliberate overflights. In the very early days, the penetration missions in Eastern Europe were for the purpose of unloading tons of propaganda leaflets. As time went on, however, CIA radio broadcasts substituted for more intrusive measures, and the overflights turned toward

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

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

~~TOP SECRET UMBRA~~

intelligence collection. The best known of the latter were the U-2 overflights which originated in the mid-1950s. Even when actual penetrations went out of favor, SAC continued to fly "exciter flights" along the periphery, nudging the boundaries of the Soviet air defense system to actually stimulate reactions and get them to turn on their equipment.¹²⁹

By the early 1950s the Soviet Union had built a capable air defense system. It was deficient in high-altitude aerial intercept capability, but the Soviets had an outstanding radar detection system, beginning originally with American lend-lease equipment. And as American [redacted] aircraft began playing with their borders, the Soviets began coming up after them.

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

The ensuing twenty years were marked by repeated border incidents, both aerial and naval. A study by NSA in 1986 documented 126 incidents, 81 of them occurring during the 1950s. The peak year, 1952, was marked by nineteen incidents, including the downing of an RB-29 in the Sea of Japan on 13 June, the first SIGINT aircraft shot down during the Cold War (and the first loss of life by USAFSS intercept operators).

The Soviets and their allies became hypersensitive to peripheral reconnaissance, and on occasion they acted "trigger-happy." In some cases, such as the shutdown of a USAF photo mapping mission north of Japan in 1954, Soviet radars showed the American aircraft in Soviet territory. In other cases, especially in the Berlin air corridors, Soviet pilots showed a predisposition to fire at an Allied aircraft no matter which side of the border it was on. Some missions were shot down; others were simply fired on or harassed by "buzzing."

Although there is no direct evidence for it, it appears very likely that the pattern of peripheral reconnaissance employed by the U.S. and its allies exacerbated an already touchy situation and led to more incidents. As Table 5 shows [redacted] of the incidents were clearly aerial reconnaissance, [redacted] and of the [redacted] [redacted] reconnaissance incidents, [redacted] Reconnaissance CPAs (closest point of approach) were frequently within a few miles of the twelve-mile limit and often paralleled the border at that distance for many miles. To the Soviets, this must have appeared as a taunt. The SAC exciter flights were the most provocative by far. This was made worse by the inherent inaccuracy of radar, which sometimes placed the Allied reconnaissance aircraft closer to the Soviet border than the aircraft's navigator believed to be the case. Into this volatile mix came the Soviet bloc fighter pilot, who had no way of knowing exactly where he was relative to the international boundary.

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

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

~~TOP SECRET UMBRA~~

Table 6

Summary of Incidents by Type, 1949-1985

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

| Type | Number |
|-------------------------------------|--------|
| [REDACTED] | |
| Non-SIGINT aerial reconnaissance | 22 |
| Other military | 56 |
| Commercial/private air | 18 |
| Military ship | 3 |
| [REDACTED] | |
| Commercial ship (<i>Mayaguez</i>) | 1 |

The number and pattern of peripheral reconnaissance flights over the years, and the nationalist sensitivities of the Communist nations, produced a lively time. Some of the shootdowns became international incidents which heightened the Cold War tensions and seriously affected international diplomacy.¹³⁰

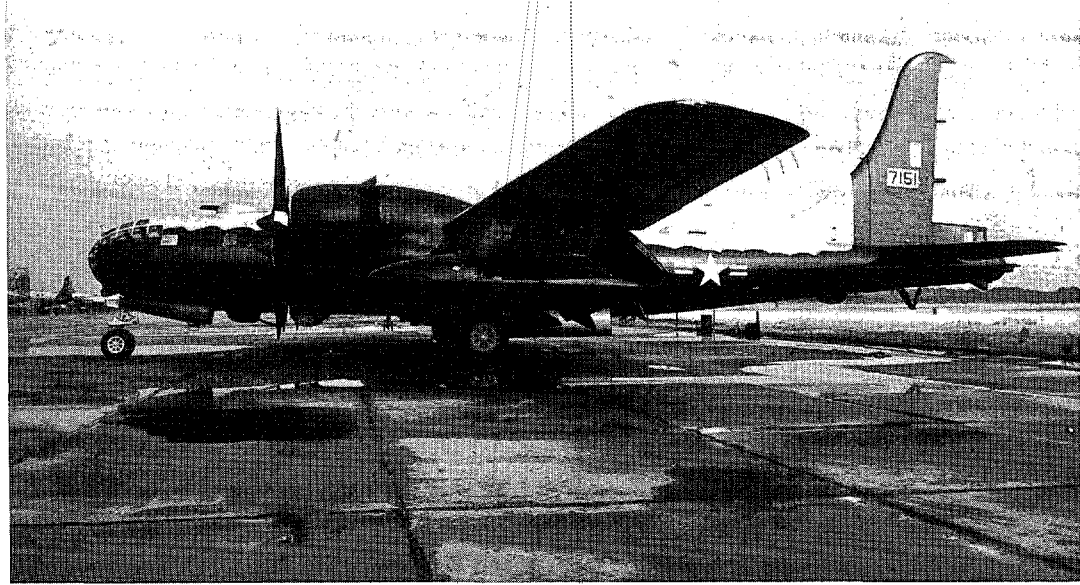
All three services developed their own aerial reconnaissance programs, each using different types of aircraft. Of the three, USAFSS had the largest program. Security Service began laying plans as early as 1948, but it was not given the go-ahead from USAF until August 1950. Originally USAFSS hoped to use the C-47 as an airframe, and it actually tested that aircraft and a C-54. USAFSS decided on the RB-50, a modification of the B-29, as its long-range airframe, but none was available, and in the early 1950s the command used an RB-29 as an interim measure. The single RB-29 went operational in the Pacific in 1954, flying out of [REDACTED] but this was never more than an experiment. AFSS finally ended up with a group of ten RB-50s in 1956, and by the fall of 1957 all ten were distributed - five to Asia and five to Europe. The program was a joint effort between AFSS and the theater commanders, who operated the front end of the planes. In the early years of the program, only the back-end crew was COMINT cleared. All positions were under local control, and tasking was done by USAFSS with little or no NSA input.¹³¹

The Navy program developed from the early VQ-1 and VQ-2 squadrons originally established in World War II. VQ-1 was originally based at Sangley Point Naval Station in the Philippines, flying P4M Mercators, P2V Neptunes, and A3D Skywarriors. In 1955 the

[REDACTED]
In Europe the SIGINT reconnaissance mission, VQ-2, evolved out of a World War II naval unit at Port Lyautey, Morocco. [REDACTED]¹³²

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

~~TOP SECRET UMBRA~~



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

RB-50

When converted for reconnaissance use, the World War II B-29 was renamed the RB-50.

The SAC Ferret program continued in the postwar years with only minimal involvement by the cryptologic community. [redacted]

[redacted]

By late summer of 1951, both AFSS and AFSA had become interested in the program, and by September the plans were expanded to include [redacted]

[redacted]

The Origins of Advisory Warning

The AFSS unit at [redacted] by now renamed [redacted] realized that they held in their hands information that could save an aircraft from being shot down. [redacted]

[redacted]

In early 1952 [redacted] worked out a plan to warn aircraft in imminent danger, by passing a coded warning to the Air Control and Warning (AC&W) sites [redacted] They wrote down their plan into a document which they

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

~~TOP SECRET UMBRA~~

called Project BITTERSWEET and sent it to USAFSS for approval. In May 1952 AFSS approved the plan for temporary implementation, [REDACTED]

[REDACTED] details of the new warning procedure were still being worked out when, on 13 June, an RB-29 SIGINT collection flight was shot down over the Sea of Japan. The two AFSS operators who were killed might have been saved had a system been in place; the event added a real sense of urgency to this, the earliest advisory warning plan in American SIGINT history.

At this point BITTERSWEET got bogged down in the tangled thicket of COMINT classifications. The problem revolved around the possible [REDACTED] [REDACTED] USCIB approved the USAFSS advisory warning plan for the Far East, but LSIB was reluctant to go along except in a war zone (i.e., Korea).

It appears that at least one version of the plan was given interim approval by USCIB, and a former USAFSS operator claims that it was actually implemented in the early 1950s for at least one mission. Various modifications were introduced to make it more palatable, such as the use of bogus messages disguised as warning messages by AC&W units.

In 1956 President Eisenhower, concerned over the number of incidents and loss of reconnaissance aircraft, directed that positive action be taken to remedy the situation. The only change that resulted was the implementation of a Navy warning program in the Far East, which contained certain safeguards, chief among these being the initiation of "blind" (unacknowledged) broadcasts. Through the summer of 1958, there existed no universal advisory warning program.¹³³

The RC-130 Shootdown

The RB-50 program lasted only a few years. The aircraft were old and difficult to maintain and had room for only five positions. The success of AFSS collection against the growing VHF problem led to a new program on the heels of RB-50s, in which the new McDonnell-Douglas C-130 would be converted to a collection platform. The C-130 had room for [REDACTED] positions, could fly longer and higher, and, being new, had few maintenance problems. AFSS planned for a fleet of [REDACTED] in each theater, to begin in 1958. The first [REDACTED] went to Europe, and in September AFSS, in association with USAFE, began to fly trial reconnaissance missions in [REDACTED] areas.¹³⁴

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

~~TOP SECRET UMBRA~~



RC-130

Then disaster struck. On 2 September 1958 an RC-130 on its initial flight out of Adana strayed over the border and was shot down. Two pairs of MIG-15s (or 17s; there was not enough evidence to determine which) attacked the reconnaissance aircraft in waves in a well-coordinated operation which left no room for doubt that their intent was destruction. The voice tapes were as dramatic as they were damning. (See p. 146.)

The Soviets said nothing, so the State Department on 6 September sent a note to the Soviet government requesting information on an unarmed C-130 carrying a crew of seventeen which had disappeared during a flight from Adana to Trabzon, Turkey. Finally, on the 12th the Soviet embassy in Washington replied that the missing transport had crashed in Soviet Armenia, killing six crew members, but that Moscow had provided no information about an additional group of eleven. An exchange of diplomatic notes over the next ten days shed no further light on the missing eleven bodies, so on 21 September the State Department admitted that they knew the aircraft had been shot down and appealed for information on the rest of the crew on humanitarian grounds. The Soviets replied that they considered the flight to have been an intentional violation of their borders but made no reference to the involvement of fighter aircraft or a shootdown.

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

| PBS | CONVERSATION |
|-----------------------|--|
| [pilot billet suffix] | |
| 582 | The target is a large one. . . . Roger |
| 201 to 218 | Attack! Attack! 218, attack. |
| 201 | I am attacking the target |
| 201 | Target speed is 3000, I am flying with it. It is turning toward the fence [i.e., border]. |
| 201 | The target is banking. . . . It is going toward the fence. Attack! |
| 218 | Yes, yes, I am attacking. |
| [missing] | The target is burning. . . . |
| [missing] | The tail assembly (b% is falling off) the target. |
| [missing] | Look at him, he will not get away, he is already falling. |
| [missing] | Yes, he is falling (b% I will finish him off) on the run. |
| [missing] | The target has lost control, it is going down. |

A crew of seventeen men, including eleven USAFSS airmen and a front-end crew of six, was lost.

In October the Soviets produced the bodies of the six members of the front-end crew, but the bodies of the eleven USAFSS airmen were never turned over; and this strange circumstance produced a spate of conspiracy theories regarding the possible capture and long-term incarceration, not to mention forceable interrogation, of the COMINT crew. The evidence of the voice tapes makes it quite clear that no one could have escaped the fiery crash in a mountainous region of the Caucasus, but what happened to the bodies remains a mystery to this day.¹³⁵

In November, after more than two months of Soviet "stonewalling," Deputy Under Secretary of State Robert Murphy summoned Soviet ambassador Mikhail Menshikov to his office, told him he had the voice tapes of the shootdown, and said he would play them immediately. Menshikov declared that he was not a technician and walked out of the office. In January of the following year, Vice President Nixon and Secretary of State

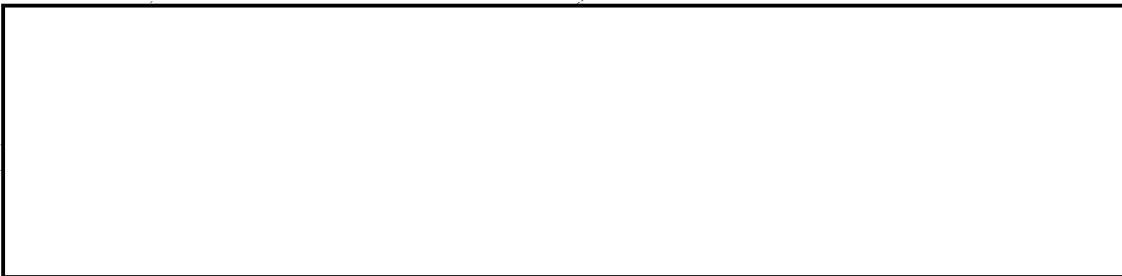
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

Dulles protested the Soviet attitude on the shutdown to First Deputy Chairman of the Council of Ministers Anastas Mikoyan, but their representations were again brushed aside. Out of patience, the administration on 5 February released copies of the tape to the *New York Times*, which published them on page one. This deliberate leak of COMINT had already been placed before USCIB, which had concurred, as had the British.¹³⁶

The downing of the RC-130 had immediate and serious consequences. USAFE grounded the entire RC-130 fleet, and Headquarters USAF requested a complete review of the ACRP program worldwide. USAFSS produced statistics designed to prove the effectiveness of the program when compared with ground collection sites, and by mid-October the flight ban had been lifted. As part of its review, USAFSS also investigated the possibility that the aircraft was meaconed (intentionally lured over the border) by Soviet navigational facilities. This possibility added to the conspiracy theories surrounding the fate of the RC-130, but it was largely contradicted by the internal evidence of the study which showed that three navigational beacons in the area, two of them in the Soviet Union, were all operating on virtually the same frequency. Thus, the aircraft very likely homed on the wrong beacon and pulled itself off course.¹³⁷ Although President Eisenhower himself believed it to have been a deliberate meaconing incident, it was more likely a navigational error on the part of the SAC crew.

Advisory Warning Is Implemented

The downing of the RC-130 decided the advisory warning issue. USAFSS gave its units immediate authorization to man the heretofore unmanned manual Morse position aboard the RC-130s for internal advisory warning. And the long-stalled plans for the provision of warning [redacted] got untracked. By 1961 USAFSS and SAC had implemented a limited advisory warning program, [redacted] applying to their own reconnaissance aircraft. In 1963 this was merged into a national program encompassing all peripheral reconnaissance aircraft, a JCS plan named WHITE WOLF.¹³⁸



The construction of the super-sites in the 1950s resulted in an intercept system that was increasingly effective in its ability [redacted].
[redacted] By 1960, USAFSS demonstrated a high level of competence to [redacted] during the U-2 shutdown. (See p. 148) But since [redacted]

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

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

communications in the 1950s

[Redacted]

The RB-47 Shootdown

As time went on, progressively fewer reconnaissance aircraft were shot down, but those that were took on a heightened diplomatic importance. Surely the most significant was the 1 May 1960 shootdown of the U-2 piloted by CIA's Francis Gary Powers. (This shootdown will be treated in detail in a separate section.) Second only to that, however, was the shootdown of an RB-47 ELINT mission over the Barents Sea on 1 July 1960. The aircraft took off from [Redacted] and proceeded on its charted course in the Barents, until it was intercepted by a covey of Soviet fighters. As the aircraft paralleled the Murmansk coast, two Kilp'Yavr fighters intercepted it, and at least one fired a burst, destroying two of the four engines. As the pilot fought to control the seriously damaged aircraft [Redacted]

[Redacted] After a twenty-minute struggle, the plane crashed in the icy waters of the Barents off the coast of Ostrov Kolguev. Two of the crew were picked out of the waters alive by a Soviet trawler, but the other four died.

Coming as it did only two months after the U-2 incident, it presented Soviet premier Nikita Khrushchev with another opportunity to heat up the Cold War. After waiting a few days to see what the Eisenhower administration would say, the Soviet leader went on the attack, revealing that they had shot down the plane and were holding the two survivors in Lubyanka Prison [Redacted]

[Redacted]

139

In the Oval Office, Eisenhower worried about the diplomatic and political implications of peripheral reconnaissance and asked his military advisors if it was worth it. General Nathan Twining of the Air Force delivered a ringing defense of the program, and he convinced Eisenhower to keep the airplanes flying. But the president directed that the Air Force find faster reconnaissance aircraft so that the Soviets would have a more difficult time shooting them down. The quest for a better aircraft eventually led to the SR-71 program.¹⁴⁰

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

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

During the Oval Office review of the peripheral reconnaissance program, the Air Force revealed the extent of the program in 1960. [redacted]

[redacted] SAC had two strategic reconnaissance wings flying worldwide missions, [redacted]

[redacted] In Europe the COMINT aircraft (mostly RC-130s) were operated by USAFE, which seemed to be getting all the newest and best aircraft and collection gear, in line with Eisenhower's expressed desire to [redacted]

[redacted]

(The promised nine RC-130s had evidently not yet arrived.) The Navy had a naval air squadron at [redacted] equipped with smaller naval patrol craft. [redacted] and the Marines operated an airborne collection unit from [redacted] A special naval unit operating from [redacted]⁴¹

As for the fate of the RB-47 flyers, Khrushchev kept them in Lubyanka until after the change of administration and then returned them as a cynical olive branch to the newly elected President Kennedy a few days after his inauguration. Kennedy met the released flyers at Andrews Air Force Base and, to flaunt his Cold War sympathies, had them to the White House for coffee.¹⁴² If Khrushchev hoped to use the reconnaissance program to curry favor, he failed. Kennedy was even more fervently anti-Communist than Eisenhower.

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

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

Notes

1. [redacted] "The History of SIGINT in the Central Intelligence Agency, 1947-1970," October 1971, CIA history office.
2. [redacted] Vol. II, 2.
3. CCH Series VI.D.1.1.
4. The best, and virtually the only, body of information on NSA's early organization is a manuscript by [redacted] [redacted] available in the Center for Cryptologic History.
5. George Howe working papers, History of the Directorate, in CCH Series VI.D.1.2.
6. Brownell Committee report.
7. "Report on Intelligence Activities in the Federal Government, Prepared for the Commission on Organization of the Executive Branch of the Government by the Task Force on Intelligence Activities, [the Hoover Commission Report]," App. 1, Part 1: The National Security Agency, May 1955, in CCH Series VI.C.1.8.
8. Classification Act of 1949, amended 24 Oct. 1951. See also file on manpower and personnel strengths in CCH Series VI.E.1.4.
9. Robertson Report, in CCH series VI.X.1.6.

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

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

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

~~TOP SECRET UMBRA~~

10. "NSA Review of the U.S. Cryptologic Effort, 1952-54," in CCH Series VI.EE.1.3.; interview, Louis W. Tordella, 28 June 1990, by Robert Farley, NSA OH 8-90; [redacted] "Glimpses of a Man: The Life of Ralph J. Canine," *Cryptologic Quarterly*, Vol. 6, No. 2, Summer 1987; Burns, *The Origins of the National Security Agency*, 61.
11. Interview with Abraham Sinkov by Arthur Zoebelin, [redacted] Dale Marston and Sam Snyder, May 1979, NSA OH 2-79 through 4-79.
12. [redacted] "Training in AFSA/NSA, 1949-1960," unpublished manuscript in CCH Series V.F.4.1.
13. "NSA Review of U.S. Cryptologic Effort. . . ."
14. Howe, "The Narrative History of AFSA/NSA" Part V.
15. NSA/CSS Archives, ACC 10460, CBRI51.
16. Howe, "Narrative History," Part V.
17. NSA oral history with Hugh Erskine, by Vince Wilson, 1972; oral history with Dr. Robert J. Hermann, 2 September 1994, by Charles Baker and Tom Johnson, NSA OH 45-94.
18. George F. Howe, "A History of U.S. Civilians in Field COMINT Operations, 1953-1960," *Cryptologic Quarterly*, Spring 1973, 5-9; and correspondence file in NSA/CSS Archives, ACC 26430, CBOM22.
19. NSA/CSS Archives, ACC 1664N, G14-0207-7.
20. File of sample COMINT Reports for 1948-1953, in CCH Series VI.M.2.1.
21. CCH Series VI.M.2.1.
22. Production memo 37/53, in "COMINT Reporting Responsibilities, Reports and Translations," in CCH Series VI.M.1.2.
23. NSA 901 Publications Procedures Memo #6, 6 October 1953, in CCH Series VI.M.1.7.
24. See "Reporting Policy" memoes in CCH Series VI.M.1.7.
25. Hoover Commission report.
26. The best, and practically the only, comprehensive discussion of AFSA and NSA training in the 1950s is in [redacted] "Training in AFSA/NSA, 1949-1960," unpublished 1961 manuscript in CCH Series V.F.4.1. Unless indicated otherwise, the material in this section derives from the Bauer work.
27. AFSA School Catalogue 1952, in CCH Series V.F.4.2.
28. [redacted] "Historical Study: The Security Program of AFSA and NSA, 1949-1962," unpublished manuscript in CCH Series X.H.7. See also Interview with Herbert L. Conley, 5 March 1984, by Robert Farley, NSA OH 1-84.
29. [redacted] "Historical Study: The Security Program. . . ." See also Interview, Cecil J. Phillips, 8 July, 1993, by Charles Baker and Tom Johnson, NSA OH 23-93, and written comments by David Boak, October 1994.
30. CCH Series VI.G.1.1.
31. [redacted] *History of SIGINT in CIA*, V. III, 158.
32. [redacted] "The Security Program. . . ."
33. Ibid.

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

- 34. Hoover Commission Report (VI.C.1.8.); "NSA Review of U.S. Cryptologic Effort. . ." (VI.EE.1.3.); Robert J. Watson, "Consumer Liaison Units, 1949-1957" April 1957, ACC 10684, CBRI 52; and "AFSS-NSA Relations, October 1952-September 1954," V. I, USAFSS Official History available at Hq AIA, Kelly AFB, San Antonio, Tx.
- 35. [redacted] "Early BOURBON - 1945: The First Year of Allied Collaborative COMINT Effort against the Soviet Union," *Cryptologic Quarterly*, Spring 1994, 1-40.
- 36. CCH Series VI.EE.1.3.; [redacted] "SIGINT Directives, 28 Sep 1992 NSA(P0443) paper; "Mechanization in Support of COMINT," collection of papers dated from 1954-1956, in CCH Series XII.Z.
- 37. "Mechanization in support of COMINT."
- 38. "Site Survey/Hearability Tests," in CCH Series VII.1.1.1.
- 39. George Howe, "Narrative History," Part V.
- 40. CCH Series V.A.28., and VI.M.1.5.
- 41. Letter, Canine to SCA chiefs, 14 June 1955, in CAHA, ACC 26418, CBOM 16.
- 42. CCH Series VI.M.1.5.
- 43. USAFSS History, "Historical Resumé: Development and Expansion of USAFSS Capability in the Pacific Area, 1949-1957," available at AIA hqs, Kelly AFB.
- 44. Memo fm MGen Samford (USAF) to Commander, ADC, 2 Mar 1954, in CCH Series VI.M.1.5; Robertson Report in CCH Series VI.X.1.7.



- 48. Holtwick memo 13 June 1955, in CCH Series VI.P.2.1.
- 49. CCH Series VI.NN.1.1. and VI.NN.1.3; see also VI.P.2.2.
- 50. CCH Series VI.P.1.3.
- 51. Richard R. Ferry, "A Special Historical Study of the Organizational Development of United States Air Force Security Service from 1948-1963," 1963, available at Hqs AIA, Kelly AFB, Texas.
- 52. Interview with John E. Morrison, 10 August 1993, by Charles Baker and Tom Johnson, NSA OH 24-93.
- 53. "A Brief History of AFEWC," May 1977, and "History of ACOM Tasking in the AFSCC, 1 July 1961-31 December 1964"; available at Hq AIA, Kelly AFB, Texas.
- 54. Interview with Lt Gen Gordon A. Blake, 19 April 1984, by Robert Farley, NSA OH 7-84.



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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

58. Howe, "Narrative History."; CCH Series VI.H.H.12.11; "AFSS-NSA Relations, October 1952-September 1954, V. I, available at Hq AIA, Kelly AFB, Texas.

59. NSACSS Archives ACC 37911, H03-0305-2; interview with Milton Zaslow, 14 May 1993, by Charles Baker and Tom Johnson, NSA OH 17- 93; interview with Louis Tordella, 28 June 1990, by Charles Baker and Tom Johnson, NSA OH 8-90.

60. See Ray S. Cline, *The CIA under Reagan, Bush and Casey* (Washington, D.C.: Acropolis Books, 1981), 78; Robert L. Benson, "A History of U.S. Communications Intelligence During World War II: Policy and Administration," CCH manuscript pending publication, Chapt II, 14.; [redacted], *Donovan and the CIA* (Washington, D.C.: CIA, 1981).

61. See Benson, "History"; interview with Oliver R. Kirby, 11 June 1993, by Charles Baker, Guy Vanderpool, and David Hatch, NSA OH 20-93.

62. [redacted] "A History of SIGINT in the Central Intelligence Agency, 1947-1970," Vol IV, App. M.; CIA history staff.

63. CIA's early role in COMINT is covered in [redacted] (throughout); in a second CIA history, by [redacted] April 1974; and in Cline, "The CIA ..."

64. Interview with Frank Rowlett, various dates, by Henry F. Schorreck and [redacted] NSA OH 14-81.

65. Interview with Louis W. Tordella, 28 June 1990, by Charles Baker and Tom Johnson, NSA OH 8-90.

66. Summary of CIA contributions to COMINT, 1975, in NSACSS Archives, ACC 27845Z, CBDC 53.

67. Undated memo in NSA/CSS Archives, ACC 19168, H20-0111-5.

[redacted]

71. [redacted] Vol II.

72. [redacted] Vol. II; NSACSS Archives, ACC 9136, G11-0602-1; ACC 3042, G15-0508-4; ACC 9136, CBIB 26; Capt George P. McGinnis, "The History of Applesauce," *Spectrum*, Winter 1973, 9-13.

73. See NARA, RG 457, SRH- 355.

74. [redacted]

76. [redacted] interview; Sinkov interview; Tordella interview.

77. [redacted]

[redacted]

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

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[Redacted]

81. David Kahn, *Hitler's Spies: German Military Intelligence in World War II* (New York: MacMillan, 1978), 429-42.

82. Mary Ellen Reese, *General Reinhard Gehlen: The CIA Connection* (Fairfax, Va.: George Mason University Press, 1990).

[Redacted]

[Redacted]

91. Eisenhower Library papers in CCH, Series XVI; ACC 17720, CBTE 18; ACC 4821, CBSB 57; ACC 2144, CBSB 11; ACC 20645, CBJG 14; ACC 16392N, CBRG 23; ACC 19631, CBTL 11; ACC 1910B, CBTI 33; ACC 5559N, CBDD 25; ACC 26424, CBOM 22.

92. [Redacted] *Operation [Redacted] The Berlin Tunnel*, U.S. Cryptologic History, Special Series, Number 4 (Ft. Meade: NSA, 1988); [Redacted] Vol. II, [Redacted] "Newspaper Items Relating to NSA," in CCH Series VI.II.1.2.; Kirby interview.

93. Thomas Powers, *The Man Who Kept the Secrets*, 83.

94. Interview with Richard Bissell, Jr., by Dr. Thomas Soapes, 19 Nov 1976, CIA history staff.

95. "CIA-NSA Relationships . . .," CCH Series VI U.1.2.; Tordella interview.

96. Robertson Report, in CCH Series VI.C.1.11; NSA/CSS Archives, ACC 29965, H01-0706-5

97. See Jones, *The Wizard War: British Scientific Intelligence, 1939-1945* (New York: Coward, McCann and Geoghegan, 1978).

98. Draft Robertson Committee report in CCH Series VI.X.1.7.

[Redacted]

100. "Background to the Robertson Report: Potentialities of COMINT for Strategic Warning," in CCH Series VI.X.1.7; Draft of Robertson Committee Report in CCH Series VI.X.17.; "ELINT History and Background

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

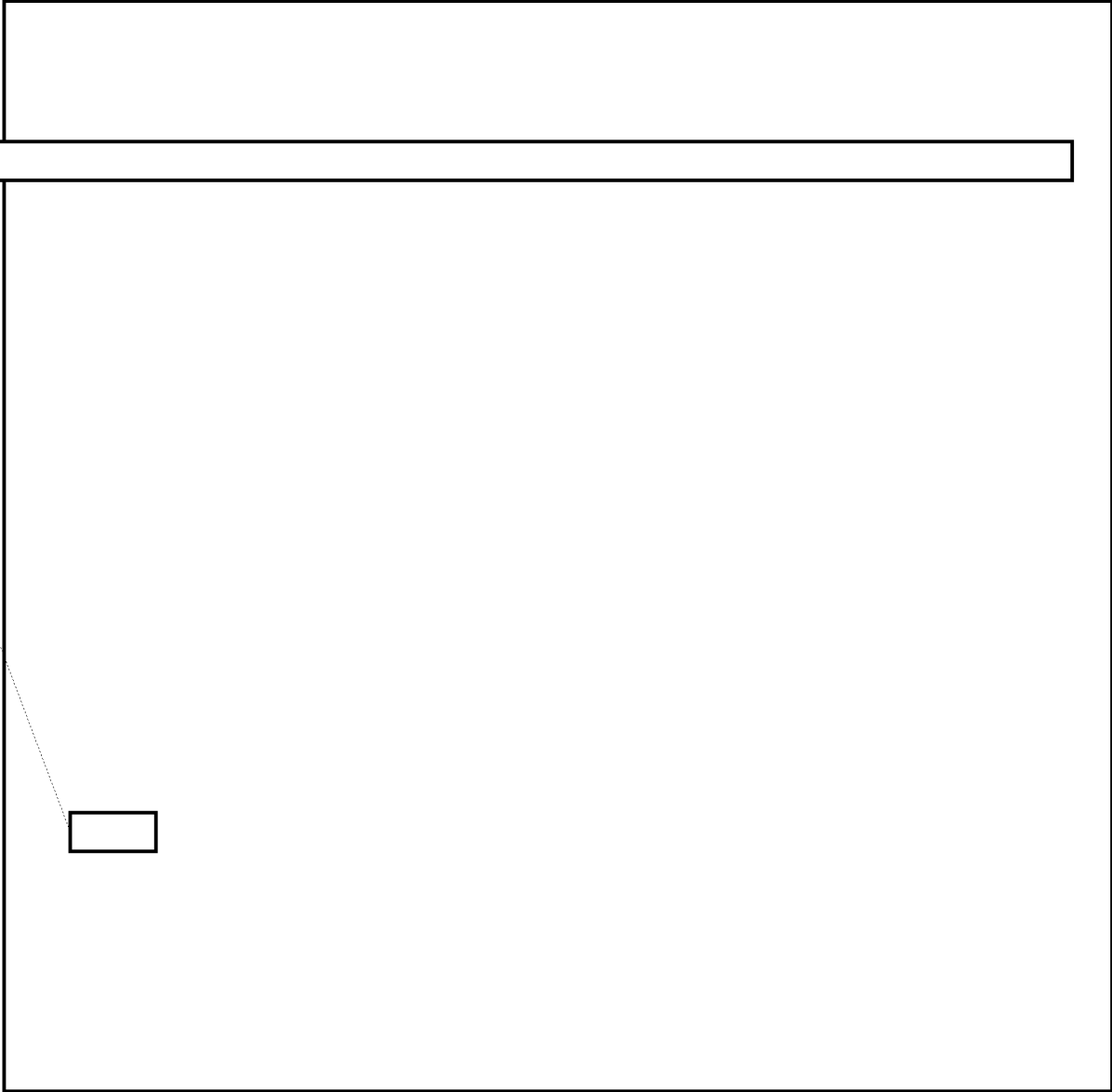
(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

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

~~TOP SECRET UMBRA~~

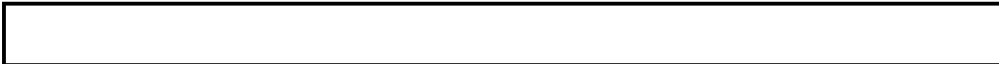
Papers," in CCH Series VI.O.1.1.; Hoover Commission Report in CCH Series VI.C.1.8.; "History of the Electronic Intelligence Coordinating Group, 1955-1958," in CCH Series VI.O.1.6.

101. NSA/CSS Archives, ACC 9092, CBIB 24; "Acquisition of COMINT Intercept Stations Overseas," in CCH Series V.F.6.1.



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

116. Howe, "Narrative History," Part V, Ch. XXVI-XXX; Ferry, "Special Historical Study..."; "Synthesis of ASA Programs, FY 53," in CCH Series VI.Q.1.14; NSACSS Archives, ACC 9092, CBIB 24; "History, Location and Photos of ELINT sites," in CCH Series VI.O.1.4.; "INSCOM: and its Heritage - a History," in CCH Series VI.Q.1.15; MSgt William R. Graham, "Misawa - Air Base and City," 1982.



(b) (1)
(b) (3)-10 USC 130
(b) (3)-50 USC 403
(b) (3)-18 USC 798

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

~~TOP SECRET UMBRA~~

[redacted]
119. "A Chronology of Significant Events in the History of Electronic Security Command, 1948-1988," 1990, available at AIA Hq, Kelly AFB, Texas; Interview with Gordon W. Sommers by Millard R. Ellerson and James E. Pierson, January 1990, available at AIA Hqs.

120. [redacted] article in NCVA *Cryptolog*, Fall 1989; "INSCOM and its Heritage - a History," in CCH Series VI.Q.1.15.

[redacted]
122. [redacted]
123. [redacted] "Radio Direction Finding in the U.S. Navy: The First Fifty Years," unpublished manuscript in the CCH Series VII.85.

124. Don East (Capt, USN(R)), "A history of U.S. Navy Fleet Air Reconnaissance, Part I: The Pacific and VQ-1," *The Hook*, Spring 1987, 16.; Oral interview with Samuel K. S. Hong, Dec. 9, 1986, by R. D. Farley, Honolulu, Hawaii, NSA OH 40-86.

125. East, 15-17.

126. [redacted] "Old BOURBON - 1947: The Third Year of Allied Collaborate COMINT Effort against the Soviet Union," *Cryptologic Quarterly*, Vol. 13 No. 3, Fall 1994.

127. William E. Burroughs, *Deep Black: Space Espionage and National Security* (New York: Random House, 1986), 58-9.; "A History of the USAFSS Airborne SIGINT Reconnaissance Program (ASRP), 1950-1977," in CCH Series X J.

128. "Analysis of AFSS Effort in the Korean Action," unpublished manuscript available in CCH Series V M.4.1.; "A History of the USAFSS Airborne SIGINT Reconnaissance Program (ASRP), 1950-1977," 20 Sep 1977, USAFSS history available in CCH Series X J.

129. See Buroughs *Deep Black*, 58-59, and Thomas Powers, *The Man Who Kept the Secrets*, 24.

130. The definitive study of reconnaissance incidents was done by NSA historian Donald Wigglesworth in an unpublished study entitled "A Summary of Peacetime Hostile Air and Sea Actions 1949-1985," March 1986, in CCH. In addition, [redacted] recently published an article in the *Cryptologic Quarterly* ("Maybe You Had to be There: The SIGINT on Thirteen Soviet Shootdowns of U.S. Reconnaissance Aircraft," Vol. 12 No. 2, Summer 1993, 1-44), which provides an excellent summary of the shootdown of reconnaissance aircraft.

131. "A History of the USAFSS Airborne Sigint Reconnaissance Program . . .," Mary Holub, Jo Ann Himes, Joyce Homs, and SSgt Kay B. Grice, "A Chronology of Significant Events in the History of Electronic Security Command, 1948-1988," in CCH Series X.J.6.

132. East, "VQ-1 . . .," and East, "The History of U.S. Naval Airborne Electronic Reconnaissance: Part Two, the European Theater and VQ-2," *The Hook*, Summer 1987, 32-35.

133. "Analysis of AFSS Effort in the Korean Action," USAFSS history available in CCH Series V.M.4.1.; CBTJ 44, NSA/CSS Archives, ACC 19220; USAFSS, "A Special History of the Advisory Warning Program, July 1961-December 1964," in CCH Series X.J.3.1.

134. USAFSS, "A History of USAFSS Airborne SIGINT Reconnaissance. . . ."

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

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

~~TOP SECRET UMBRA~~

Chapter 4

The Soviet Problem

THE EARLY DAYS

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

Winston Churchill, 6 March 1946

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

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

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

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

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

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

The Advent of BOURBON

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

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

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

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

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

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

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

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

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

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

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

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

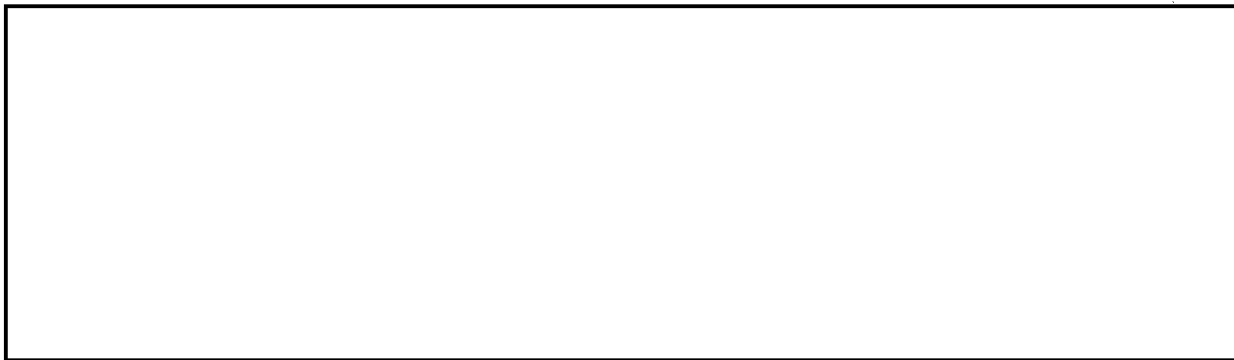
At the same time, ANCIB proposed to LSIB that their cooperation against Germany, Italy, and Japan now be extended to include the USSR. The Americans proposed that the cooperation be fully as close as it had been during the war. This included sharing all details, including the status and method of cryptanalytic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

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

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

~~TOP SECRET UMBRA~~

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



VENONA

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

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

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

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

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

~~TOP SECRET UMBRA~~

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

(b) (6)

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

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

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



Klaus Fuchs

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

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

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



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

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

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



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

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

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

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

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

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

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

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

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

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

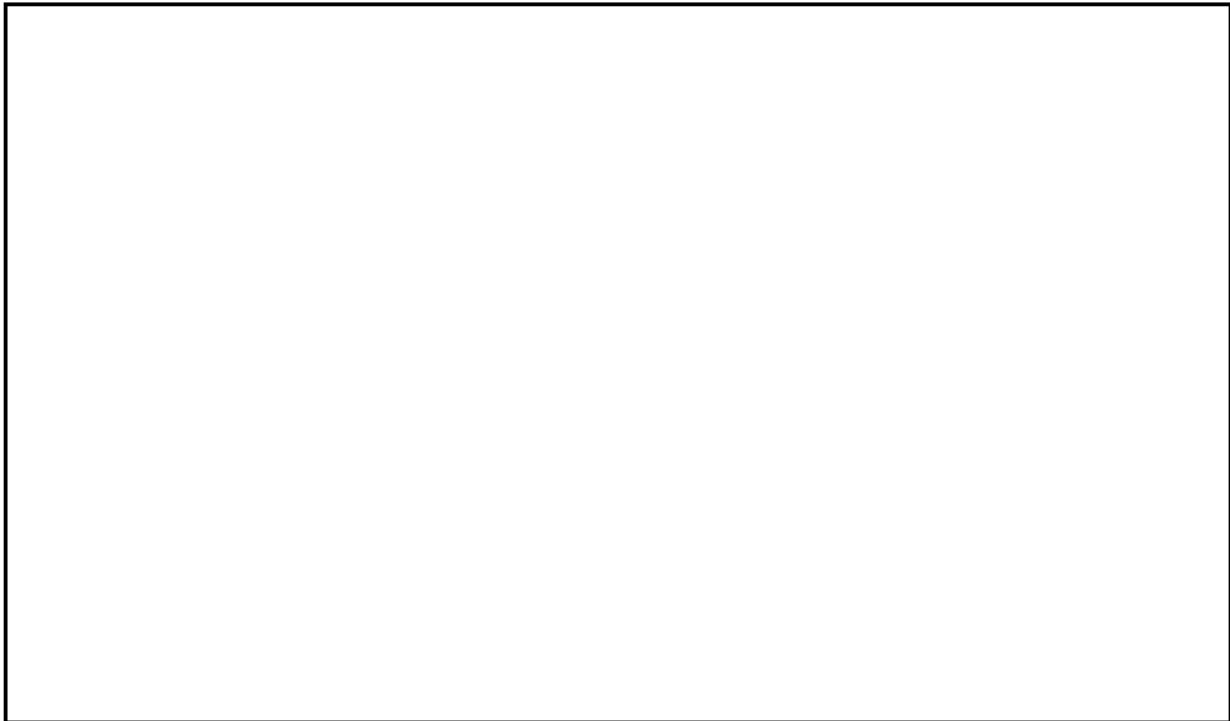
As for its long-term significance for cryptology, NSA learned several important lessons. First, the difficulty of an effort is not an automatic disqualifier. VENONA was one of the most intensely difficult projects that American cryptology has ever undertaken. The

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

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

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

"Black Friday"



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



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

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

~~TOP SECRET UMBRA~~

[Redacted]

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

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

ASA and AFSA Turn to Radioprinter

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

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

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

[Redacted]

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

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

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

~~TOP SECRET UMBRA~~

[Redacted]

Printer seemed to be the

wave of the future.

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

THE SOVIET STRATEGIC THREAT

[Redacted]

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

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

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

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

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

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

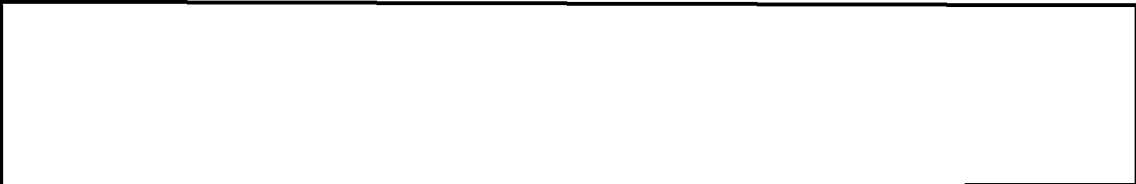
HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS

How It Began

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

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

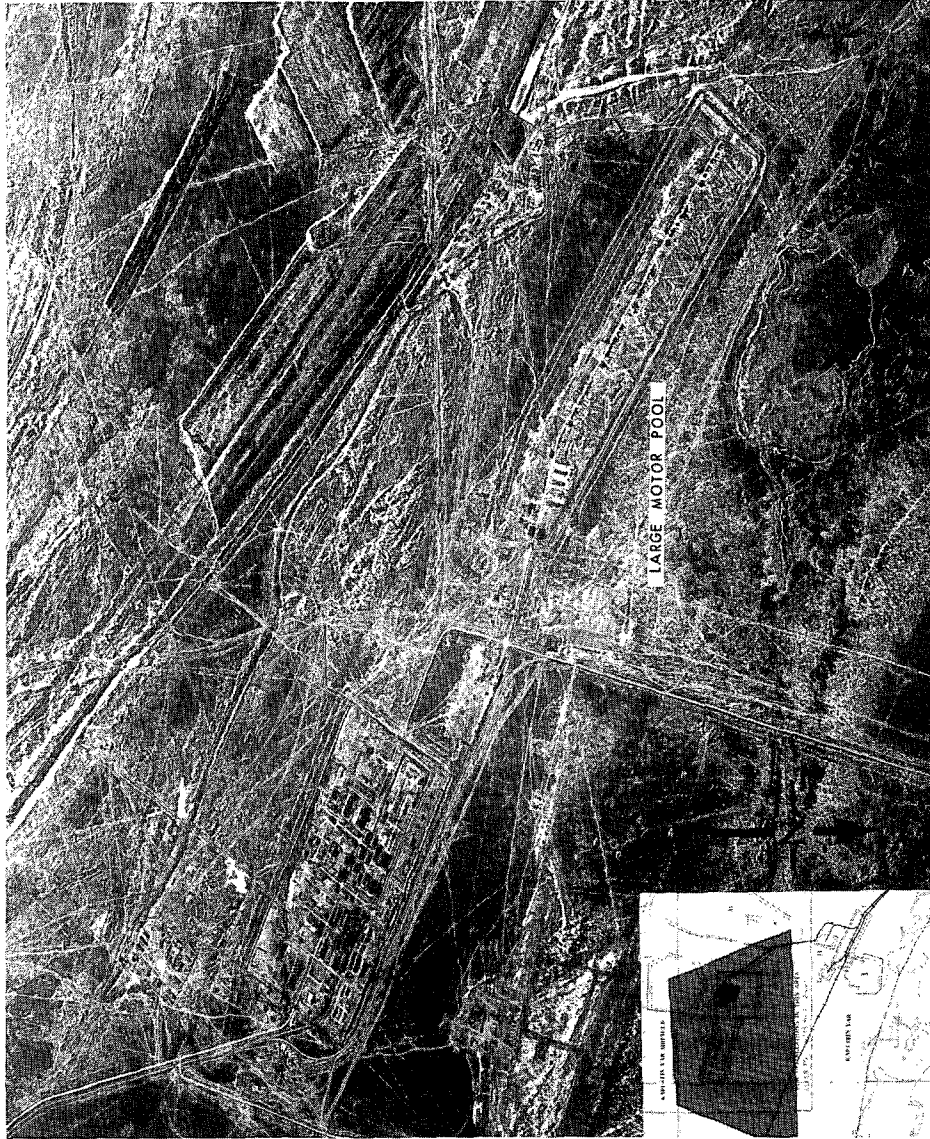
Reports of Soviet missile development reached the Oval Office, and the president demanded more information. But there were precious few assets to be had. In the latter days of Stalin's reign, the Iron Curtain completely closed off the Soviet Union from CIA HUMINT penetration - they had no secret agents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



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

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

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

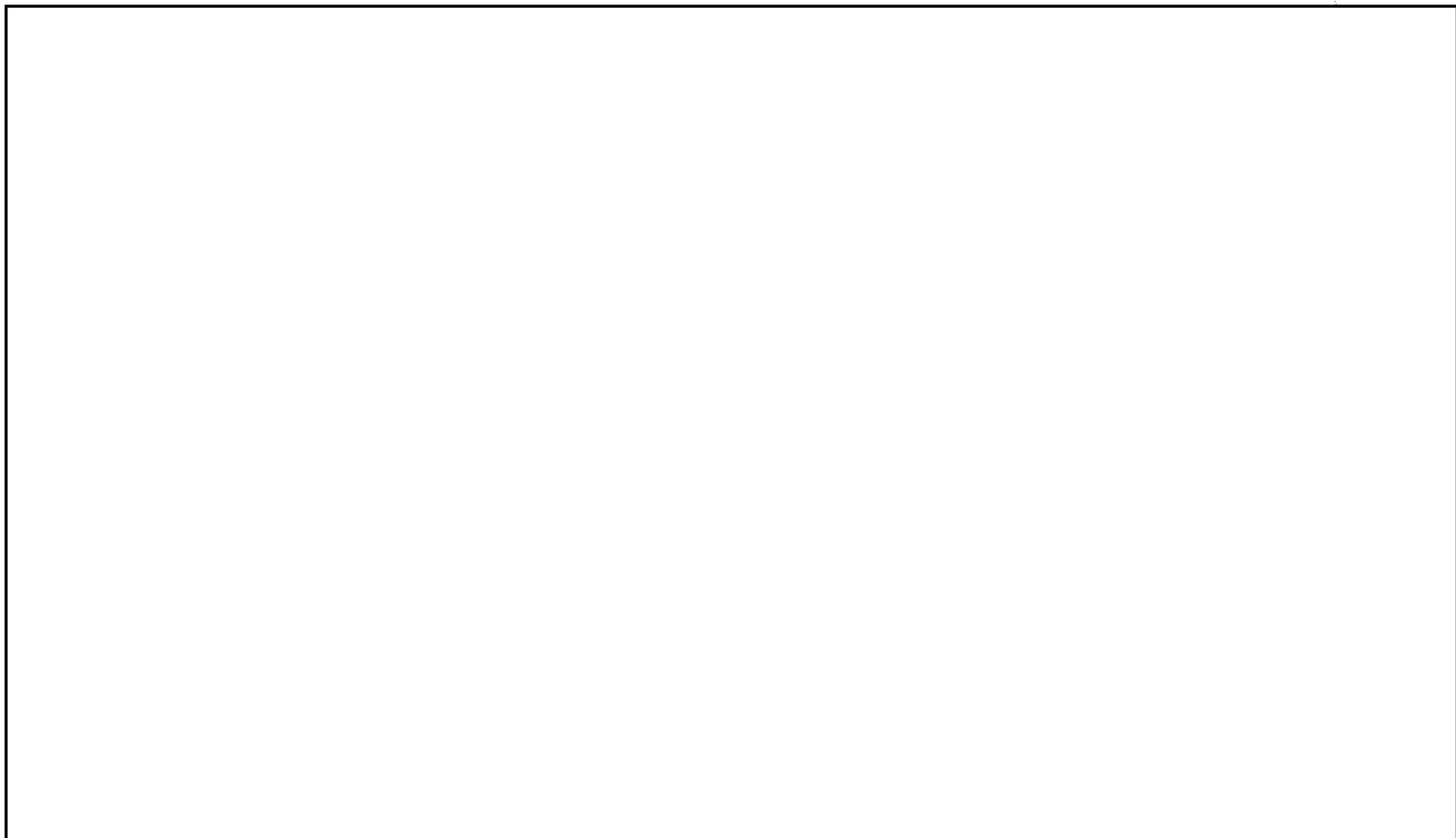


Missile fabrication and assembly area,
Kapustin Yar. This 1959 U-2 photograph provided excellent
detail on a range complex [REDACTED]

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

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

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

~~TOP SECRET UMBRA~~

The American Response

The main body of the document is a large rectangle containing approximately 15 smaller rectangular redaction boxes. These boxes are scattered throughout the page, covering what would be the text of the document. The boxes vary in size and orientation, with some being horizontal and others vertical. The redactions are complete, leaving no text visible within their boundaries.

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[REDACTED]

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

[REDACTED] confirmed this.²⁸
[REDACTED]

[REDACTED]

Moreover, [REDACTED] became more and more a cue card for U-2 missions. When U-2 pilot Francis Gary Powers was shot down in 1960, he was on a dangerous cross-Soviet mission searching for evidence of a new missile test site [REDACTED] [REDACTED] which had been recently identified [REDACTED] as being possibly missile associated.²⁹

[REDACTED]

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

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

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

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



Joseph Burke

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

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

The Soviet Atomic Bomb Project

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

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

~~TOP SECRET UMBRA~~

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

~~TOP SECRET UMBRA~~

was finally broken in 1955 with the explosion of an underwater device in the sea off Novaya Zemlya, a large Arctic island northeast of the Kola Peninsula. ³³

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

[Redacted]

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

[Redacted]

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

[Redacted]

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

[Redacted]

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

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

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

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

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

The Chinese Threat

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

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

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

In many ways, China resembled the USSR [REDACTED]

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

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

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

~~TOP SECRET UMBRA~~

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

[redacted]

The Early Days of Overhead

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

[redacted]

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

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

More determined were deliberate overflights of Soviet soil. SAC had a highly compartmented (and still obscure) overflight program, carrying a variety of sensors. This dangerous approach to intelligence collection was augmented by the RAF, which mounted occasional overflights. But their participation was limited and ended after one famous incident in 1953. At American behest, RAF aircraft overflew Kapustin Yar, [redacted] [redacted] They came back with their planes shot full of holes and allegedly told the Americans that if they wanted that sort of thing done, they could jolly well do it themselves. [redacted]

[redacted]

43

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

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

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

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

There was at the time no guarantee that the U-2 was the answer. In fact, the Eisenhower administration continued to play with the balloon option. Project [redacted] consisted of more than 500 balloons which were floated across the USSR from Europe to Asia in early 1956. [redacted] and some of them may have [redacted]. But [redacted] was no more successful than [redacted] and of the 500, only forty-four were ever recovered after their long ride from west to east.⁴⁵

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

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

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

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

[redacted]

[redacted]

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

[redacted]

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

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



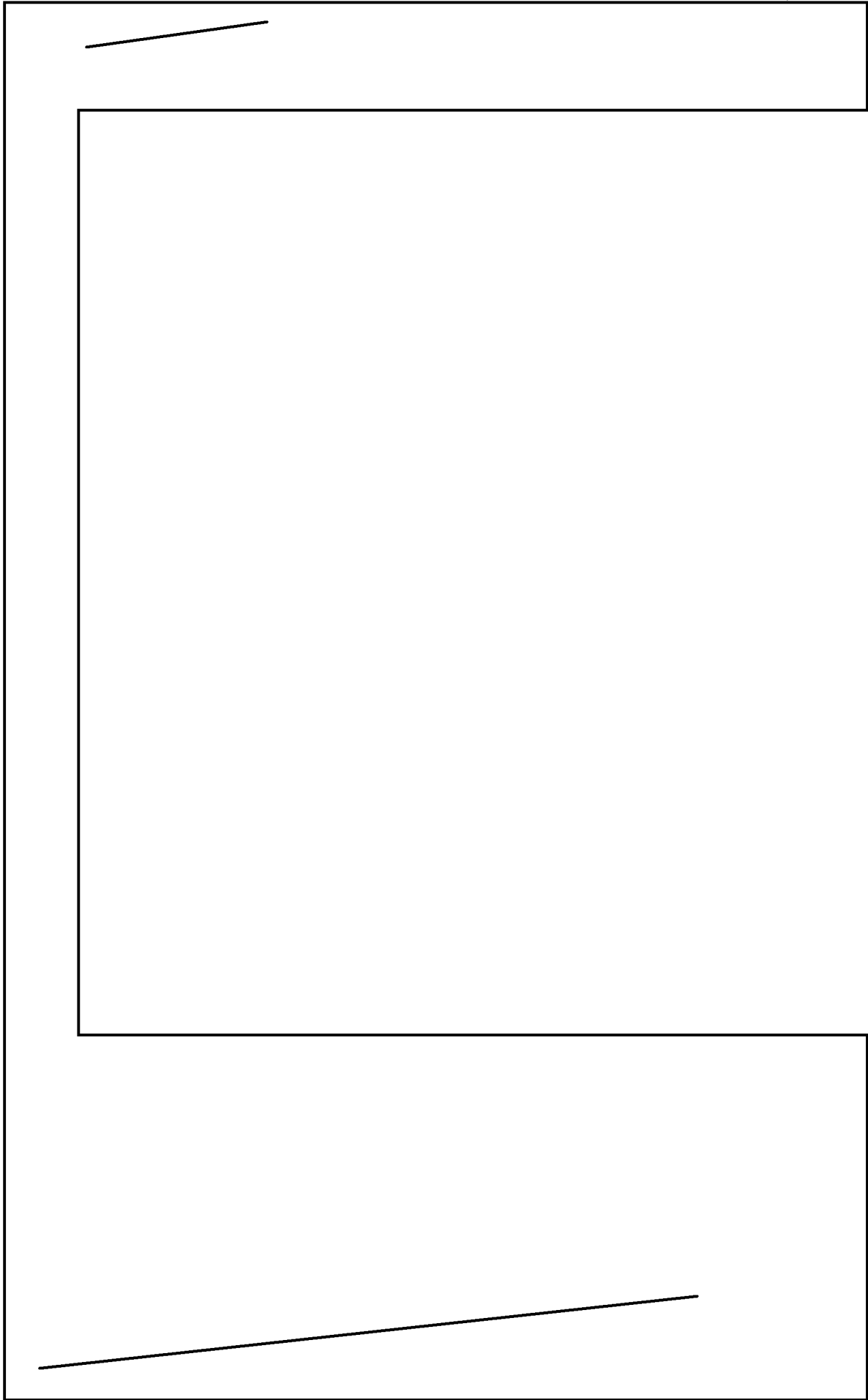
U-2

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

181

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



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

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

~~TOP SECRET UMBRA~~

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

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

[redacted]
[redacted]
[redacted]
[redacted]

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

[redacted]

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

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

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

[redacted]

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

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

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

~~TOP SECRET UMBRA~~

leaned so heavily on was suspect. [redacted]

[redacted]

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

[redacted]

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

THE ATTACK ON SOVIET CIPHER SYSTEMS

[redacted]

Baker Report, 1958

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

[redacted]

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

[redacted]

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

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

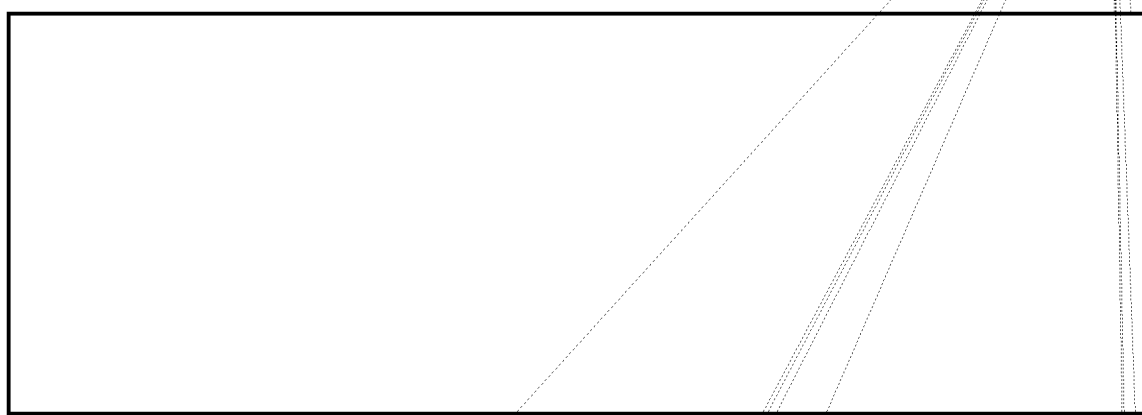
Project.⁵⁴ Then, two years later, AFSA's Scientific Communications Advisory Group (SCAG, a predecessor of NSASAB), chaired by Engstrom, [redacted] given sufficient resources and a strong research and development effort. The need for a skilled civilian work force or the employment of an outside research institute was essential. AFSA did not have a strong enough civilian work force, and the Brownell Committee made this point forcefully that same year.⁵⁵



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

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

~~TOP SECRET UMBRA~~



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

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

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

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



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

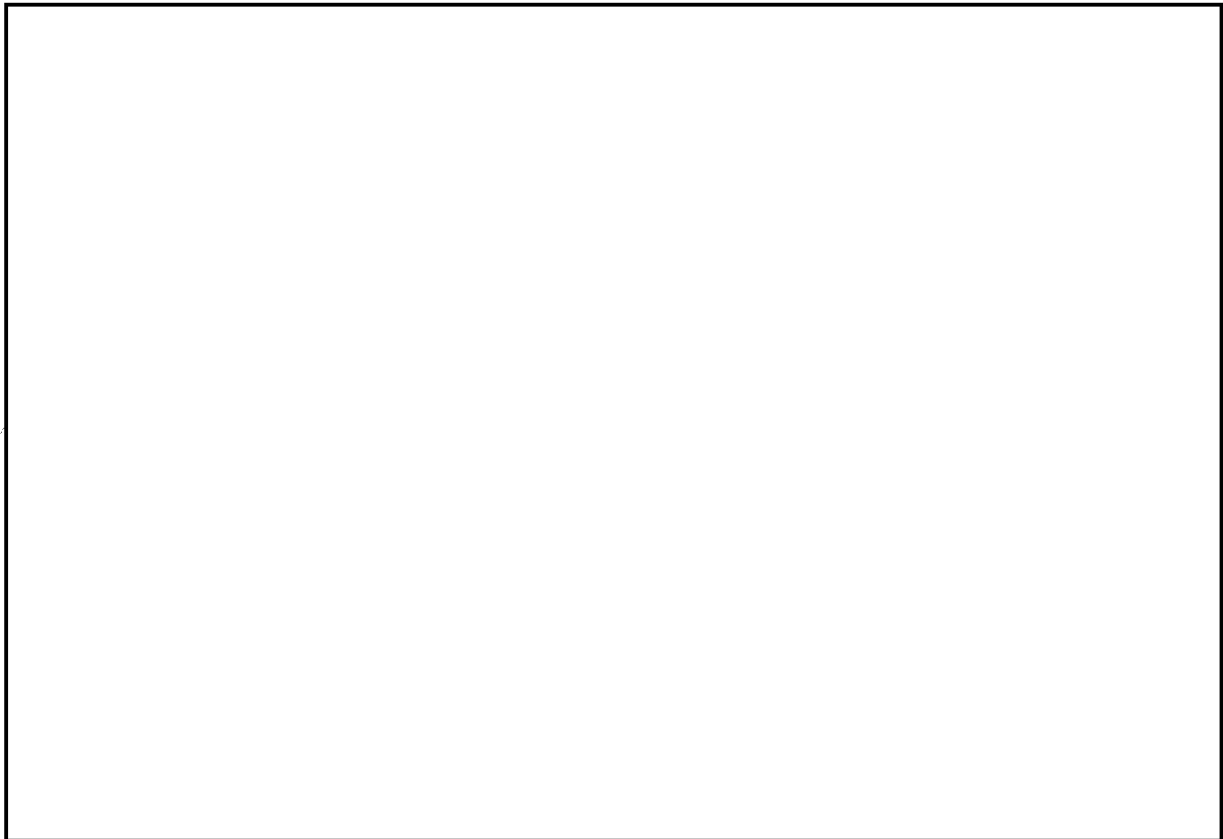
~~TOP SECRET UMBRA~~

TRACKING SUBMARINES - THE STORY OF BURST TRANSMISSIONS

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

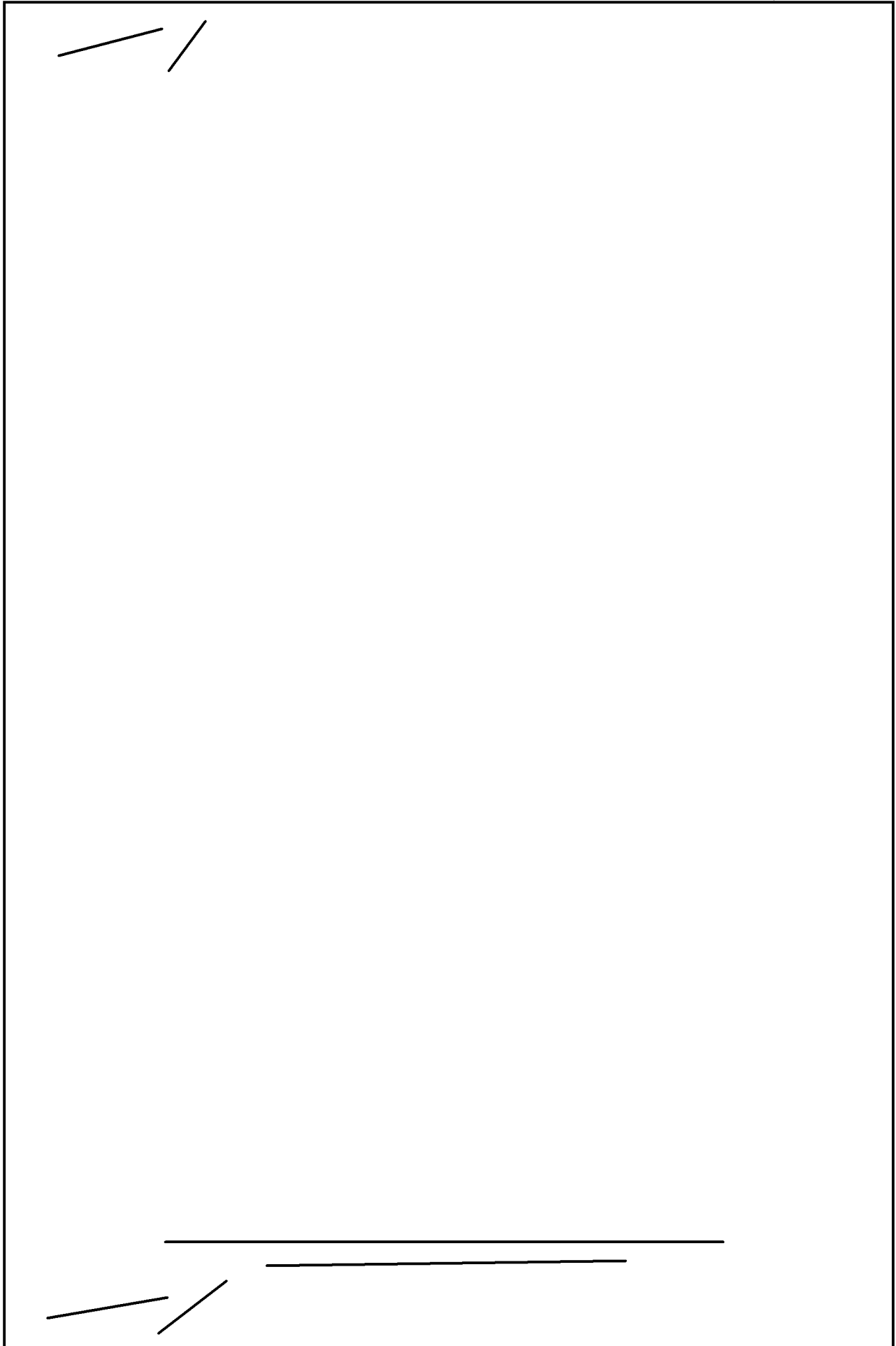
When the war ended, a German submarine surrendered in Argentina, the nearest landfall. Aboard the sub was a German scientist with extensive engineering notes and knowledge of the system, and he was willing to talk to the Americans about it. Even luckier, the British captured an actual KURIER system,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

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



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

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



(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 793
(b) (3)-P.L. 86-36

Notes

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

[redacted]

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

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

~~TOP SECRET UMBRA~~

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

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

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

[redacted]

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

[redacted]

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

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

31. Tevis interview.

32. Amato interview.

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

[redacted]

38. Kirby interview.

39. O'Neill, 279.

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

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

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

~~TOP SECRET UMBRA~~

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

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

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

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

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

46. Ambrose, *Eisenhower*, 265.



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

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

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



61. Baker Panel report.

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

63. Holtwick.



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

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

~~TOP SECRET UMBRA~~

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

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

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

68. [redacted]

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



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

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

~~TOP SECRET UMBRA~~

Chapter 5 Building the Internal Mechanism

CRYPTOLOGY IS AUTOMATED - THE STORY OF EARLY COMPUTERIZATION

The trouble with machines is people.

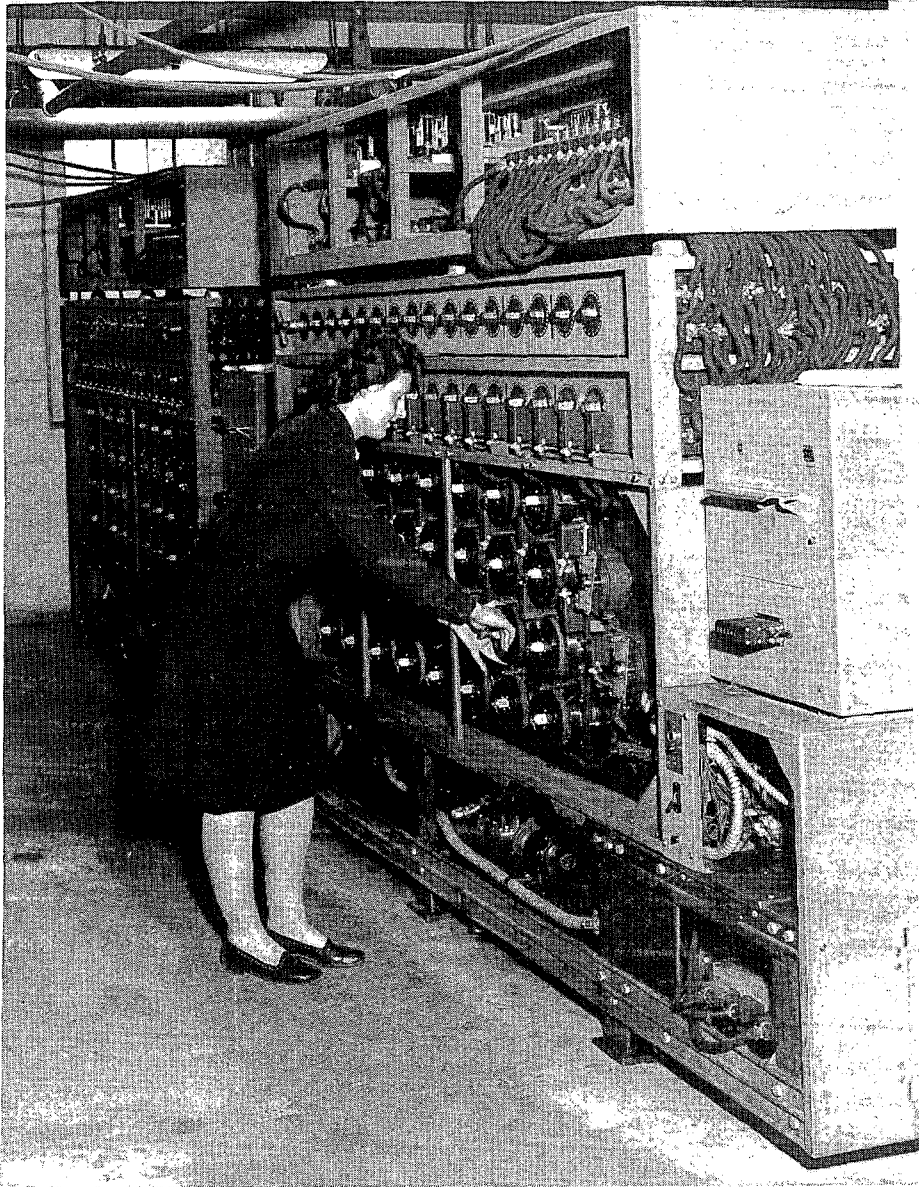
Edward R. Murrow, 1952

Antecedents

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

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

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



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

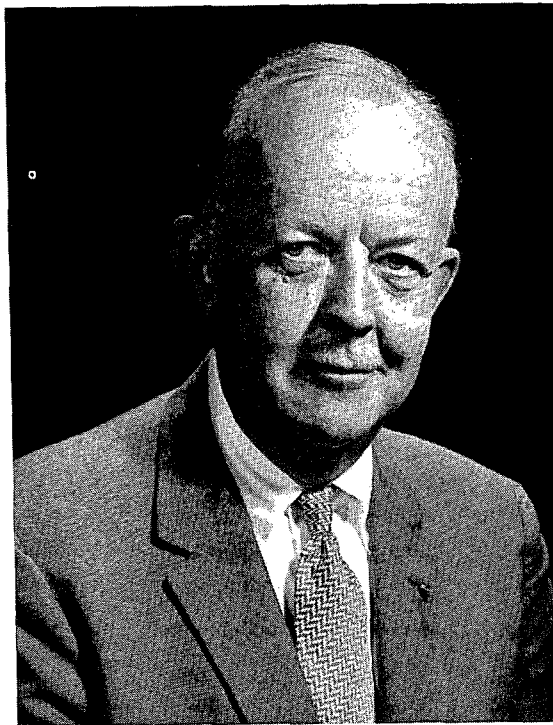
Although a very fast comparator, the bombe was not a true computer. It did not have a stored digital program which could be modified. But even as the Navy designed and built the bombes, the British were moving ahead into the era of true computers. To attack systems even more complex than ENIGMA, GCCS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

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

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

Postwar Developments

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



Howard Engstrom

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

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

~~TOP SECRET UMBRA~~

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

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

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

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

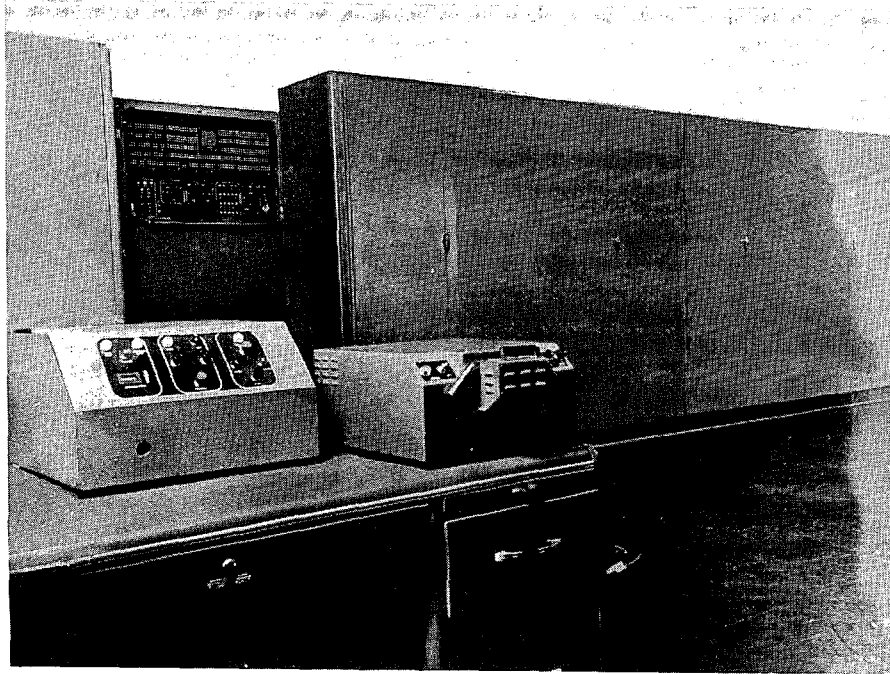
[redacted]¹⁰

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

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

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

~~TOP SECRET UMBRA~~



Atlas I

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

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

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

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

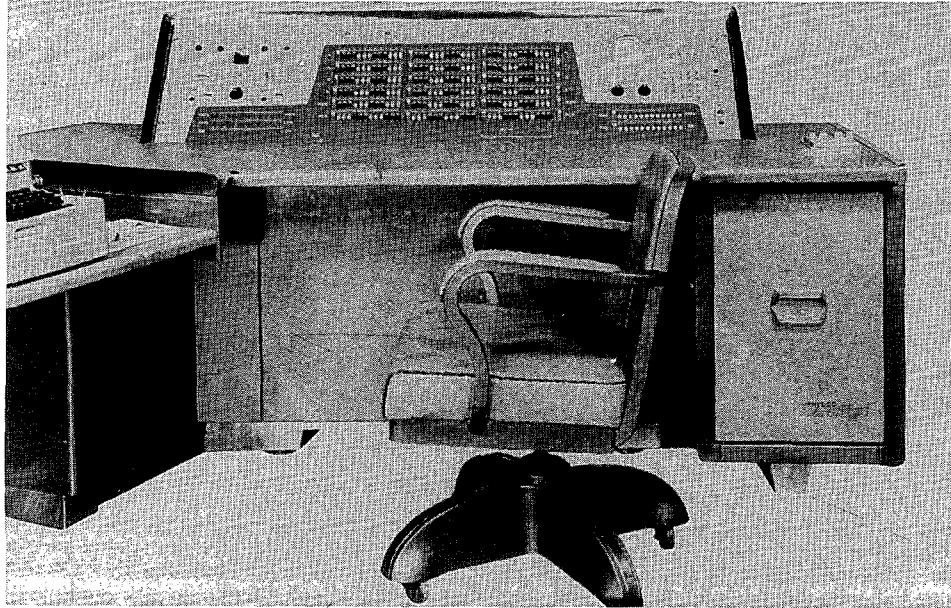
ASA decided to go ahead with development of a general-purpose analytic computer called ABNER. Working through NBS, ASA arranged for subcontracts on mercury delay memory and for magnetic tape drives from Technitrol and Raytheon, respectively. Snyder contended that ABNER I, which was released for use in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

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

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

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

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



SOLO

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

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

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

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

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

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

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

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

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

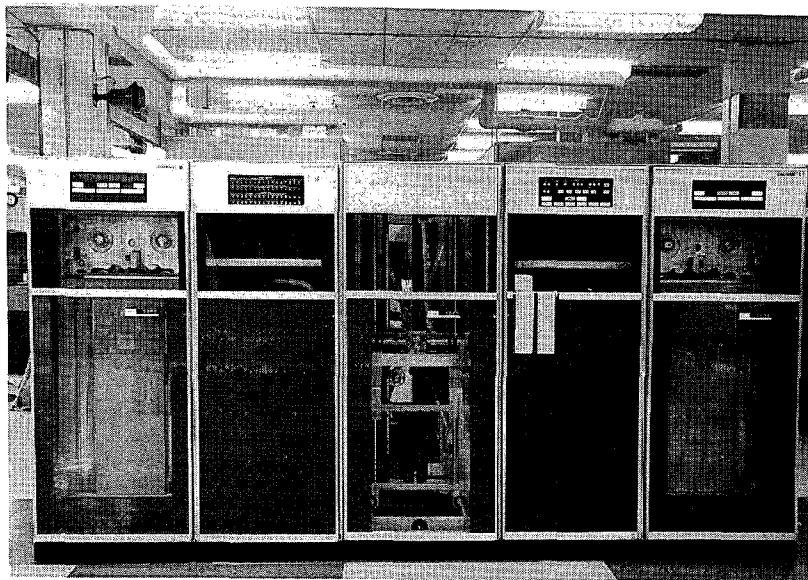
The most difficult part of the project turned out to be designing the magnetic tape drives. Under a project called TRACTOR, IBM developed new tape drives and a unique automatic cartridge loading system having 100 times the speed of the IBM Type 727 tape drives then in use. Each of the three TRACTOR units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

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

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



HARVEST



HARVEST tractor units

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

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

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

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

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

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

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

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



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

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

NSA COMMUNICATIONS IN THE PRE-CRITICOMM ERA

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

1955 study of the COMINT communications system

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

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

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

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

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



Arthur Enderlin

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

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

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

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

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

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

The COMINT Comnet

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

**Table 1
Total Mean Daily Average Group
Count at NSA³⁴**

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

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

~~TOP SECRET UMBRA~~

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

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

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

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

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

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

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

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

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

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

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

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



A bank of KW-26s installed in NSA's communications center

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

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

SECURING AMERICAN COMMUNICATIONS

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

Frank B. Rowlett

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

The Era of the Wired Rotor

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

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

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

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



SIGABA

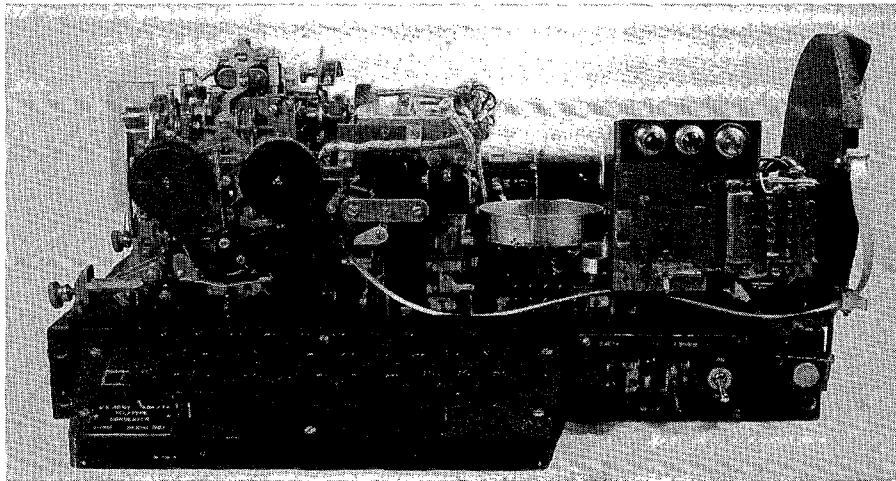
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

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

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

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

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



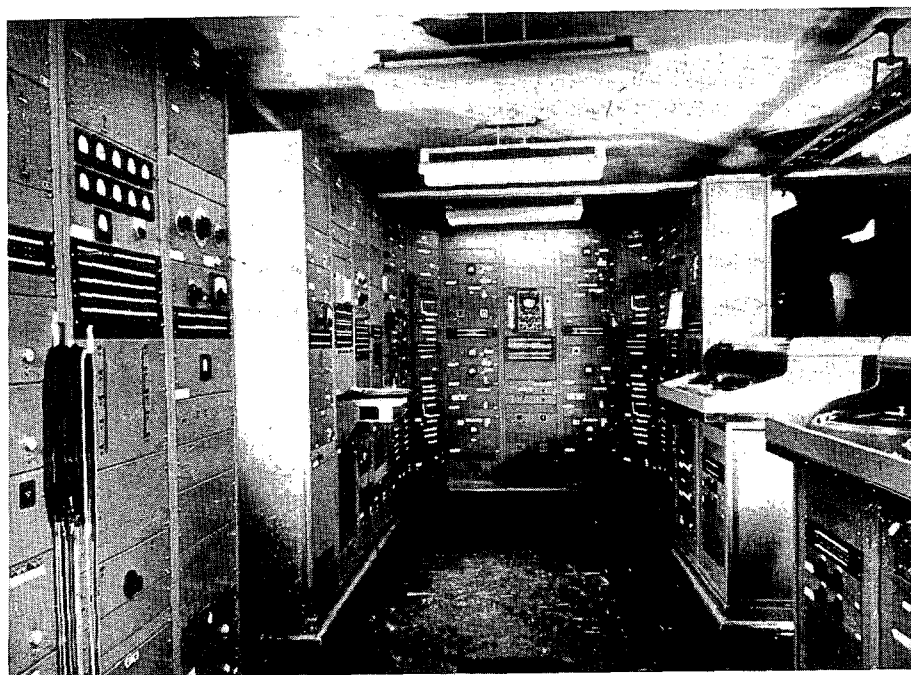
SIGTOT

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

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

The Early Years of Secure Speech

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



SIGSALY

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

Organizing for COMSEC in the Postwar World

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

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

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

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

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

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

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

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

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

Special Committee on Compromising Emanations (SCOCE) - TEMPEST. NSA acted as its secretariat and effectively did all the work.⁵⁶

Far more than just prescribing COMSEC policies, NSA became deeply involved in the design and production process. The Agency generated keying material using a wide variety of techniques. NSA also designed COMSEC machines and simply turned the production process over to a contractor after all the designs were completed. The contractor in those days was little more than an assembly organization. All the interesting work was done in-house.⁵⁷ This would change in the 1980s under Walter Deeley's "New Way of Doing Business."⁵⁸

AFSAM-7

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

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

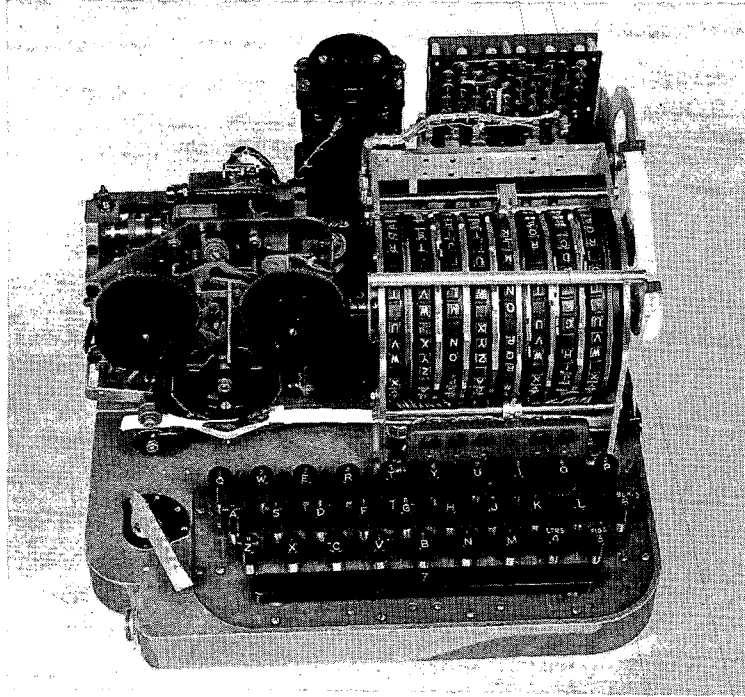
[redacted]

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

[redacted]

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

~~TOP SECRET UMBRA~~



AFSAM-7

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

59

The Push for On-line Encipherment

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

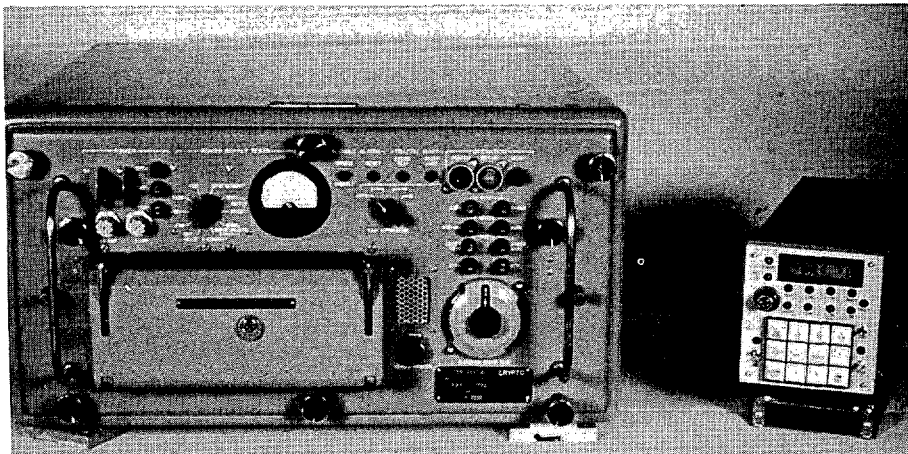
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

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

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

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

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



KW-37

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

~~TOP SECRET UMBRA~~

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

From SIGSALY to Modern Voice Encryption

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

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

TEMPEST

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

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

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

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

Notes

1. NSA/CSS Archives, ACC 6851, CBKI 61.
2. Colin B. Burke, "The Machine Age Begins at OP-20-G: Or, Don't Do It This Way Again," presentation at the 1992 Cryptologic History Symposium, 28 October 1992.
3. [redacted] "The Secret War," in CCH Series IV.V.7.18; Joel Shurkin, *Engines of the Mind: A History of the Computer* (New York: W. W. Norton, 1984).
4. SRH-267.
5. Ibid.
6. Samuel S. Snyder, "The Influence of U.S. Cryptologic Organizations on the Digital Computer Industry," SRH 003.
7. Ibid.

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

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

~~TOP SECRET UMBRA~~

62. Ibid.

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

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

65. Boak.

66. [redacted] "Evolution of Equipment..."; Boak.

67. [redacted] "Evolution of Equipment..."

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

68. Ibid.

69. Ibid.

70. Ibid.

71. Ibid.

72. Ibid.

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

Chapter 6 Cryptology at Mid-decade

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

THE EARLY ASSESSMENTS

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

The Killian Board, 1955

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

The Robertson Committee

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

Robertson reported during the dark days after "Black Friday," when Soviet [redacted] was still an unrevealed mystery. [redacted]
[redacted]
[redacted] The immediate result of this was the intercept, in 1954, [redacted]
[redacted] This opened up a new world [redacted]

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

~~TOP SECRET UMBRA~~

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

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

The Hoover Commission

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

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

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

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

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

The Killian Board

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

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

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



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

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

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

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

~~TOP SECRET UMBRA~~

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

Land believed that science made anything possible.

The Jackson Report

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

1956

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

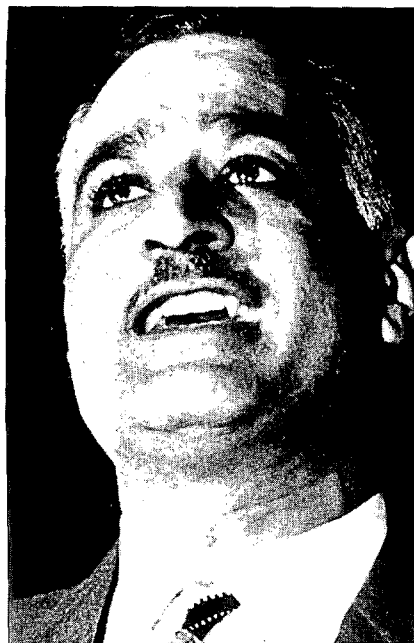


Certain years mark watersheds in cryptologic history. Nineteen fifty-six was such a year. Twin crises, Suez and Hungary, came virtually together in time to pressure a new NSA-managed COMINT system that had never been stressed in such a way. The conjunction of crises, rolled into a COMINT alert called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

Suez

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

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

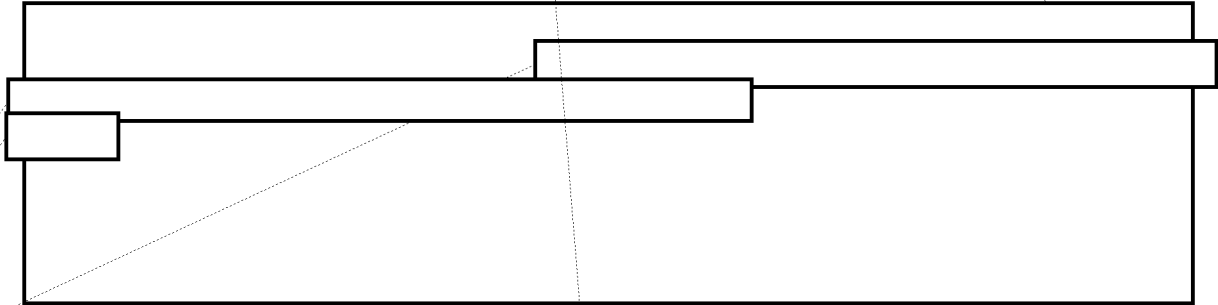


Gamal Abdel Nasser

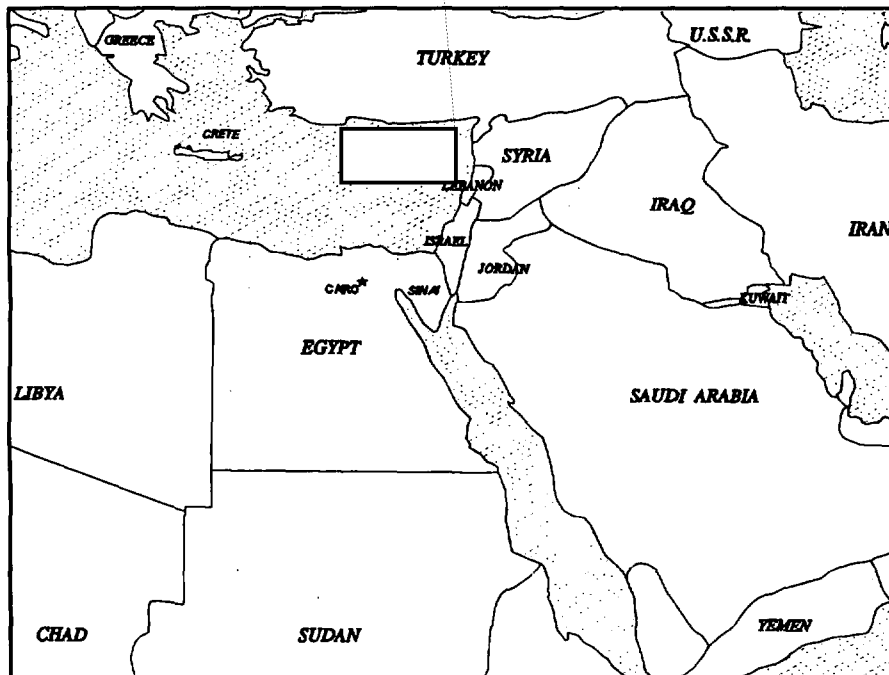
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY
NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

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



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

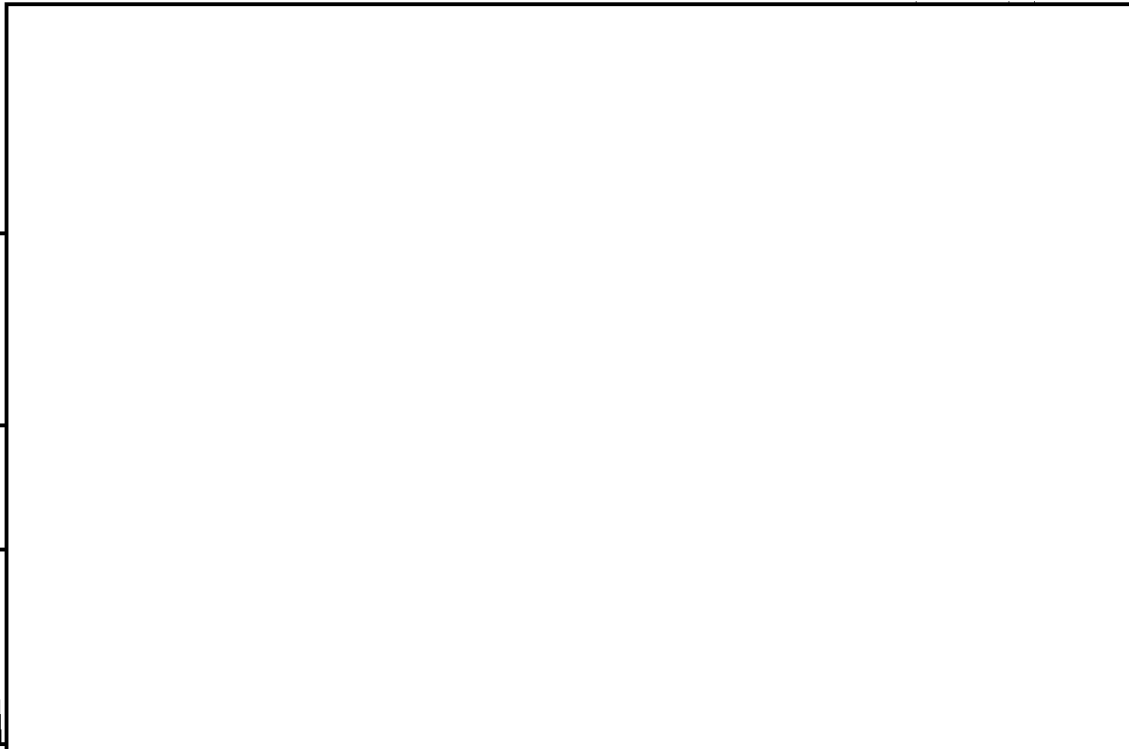


The Middle East in 1956

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



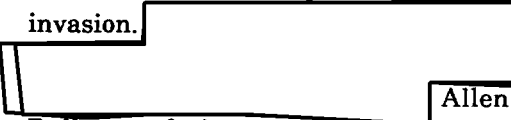
(b) (1)
(b) (3)
OGA

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



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

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



Allen

Dulles was furious.



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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

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

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

Hungary

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

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

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

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

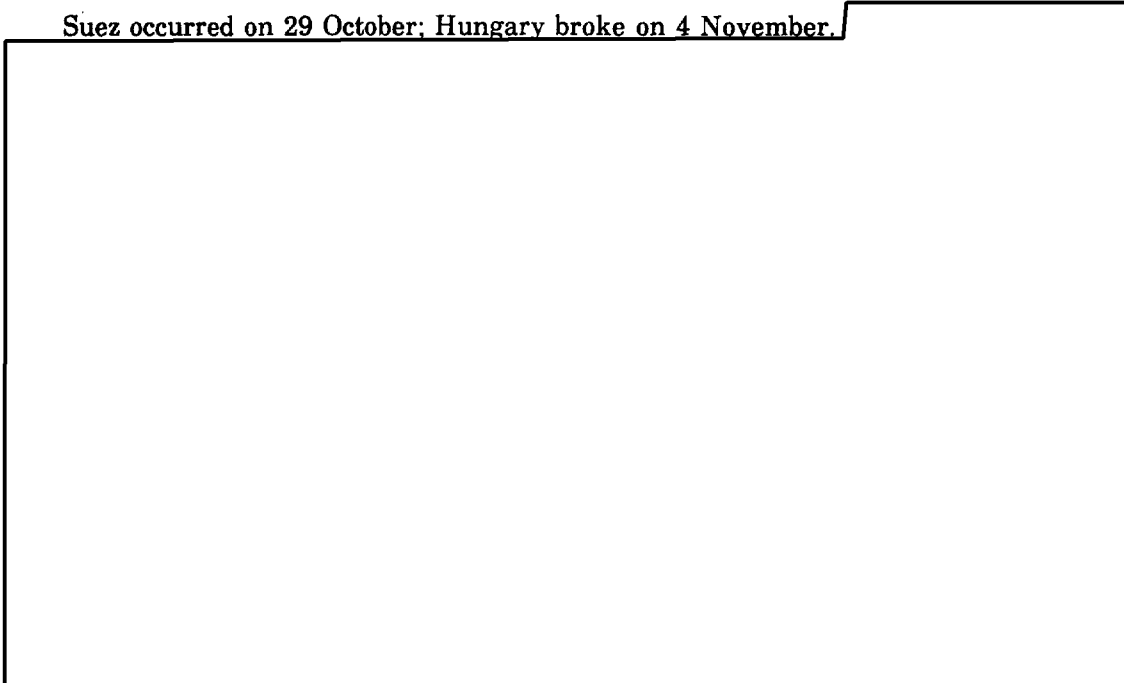
[redacted] It was an opportunity lost.

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

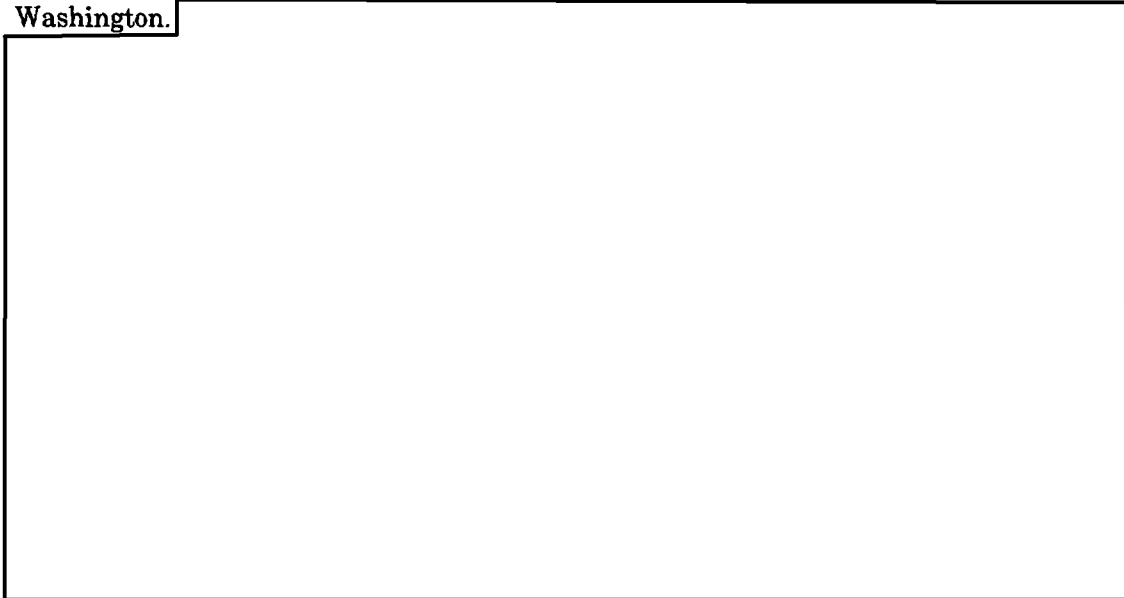
~~TOP SECRET UMBRA~~

The Yankee Alert

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



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



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

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

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

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

NSA technical support to the field was slow in coming.

Lebanon, 1958

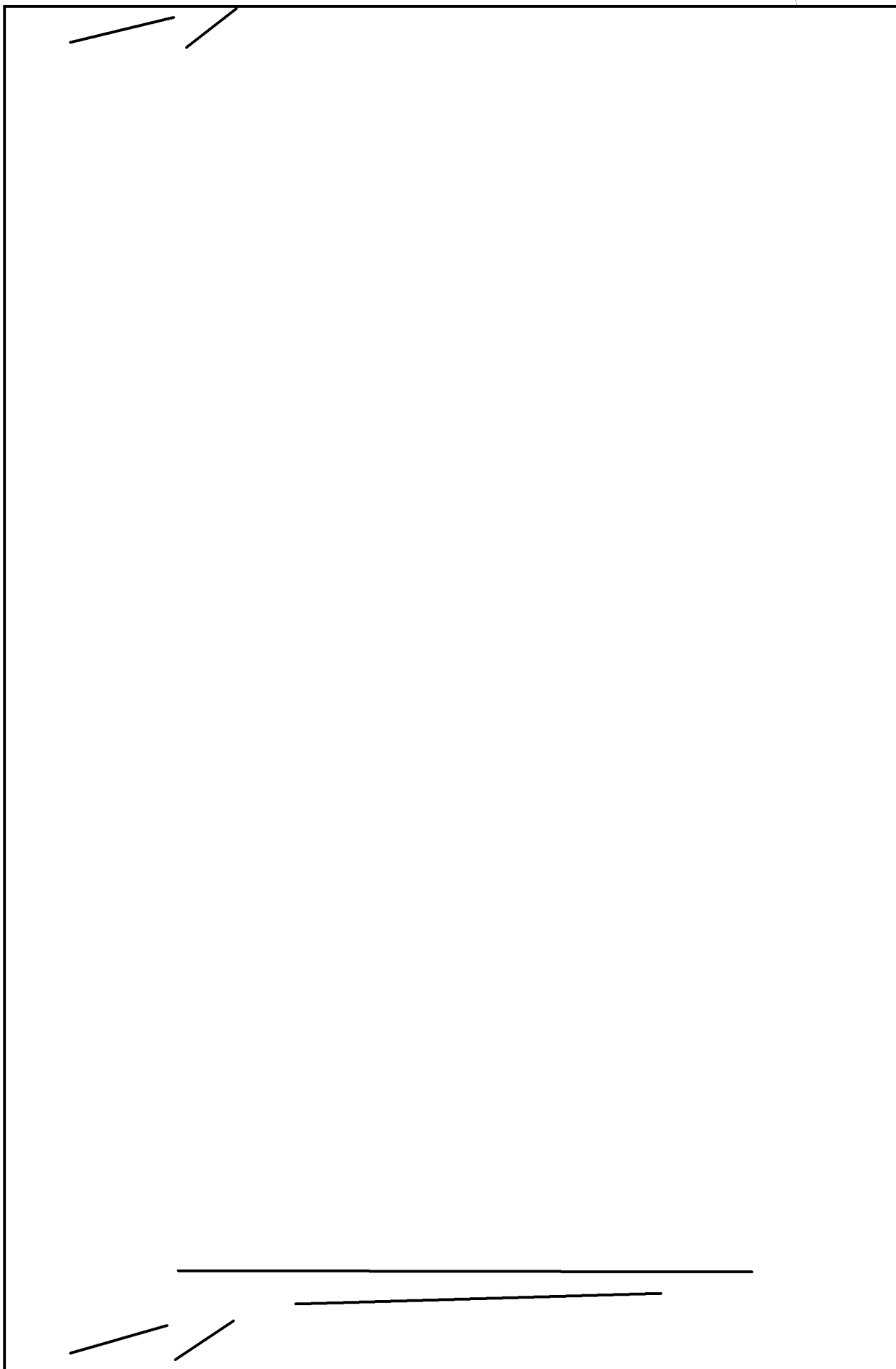
The Eisenhower administration was pulled into the Middle East quite by accident in 1956. But the president quickly yanked U.S. foreign policy into line with the new situation. In January 1957, in a State of the Union address focusing on the Middle East, he proclaimed what became known as the Eisenhower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

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

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

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

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

1956 in History

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

[REDACTED] By the time of the 1967 Arab-Israeli War, [REDACTED] The problem proved difficult to address because of the wild mood swings between somnolence and war in the Middle East. But the cryptologic community eventually had a core of expertise and resources [REDACTED]

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

Unfortunately, such sophisticated analysis, available in later decades, simply did not exist in 1956. [REDACTED] It was an art form that had to be learned.

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

The Reorganization

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

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

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

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

~~TOP SECRET UMBRA~~

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

GENS
ADVA
ACOM
ALLO



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

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



and even some logistics functions. It was a powerhouse organization.

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

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

GENS-2 [redacted] GENS-3 [redacted] GENS-4 [redacted] GENS-5 [redacted]
[redacted] and GENS-6 [redacted]

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

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

~~TOP SECRET UMBRA~~

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

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

THE MOVE

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

William C. Foster, Deputy Secretary of Defense, 1951

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

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

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

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

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

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

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



Thomas Dyer, chairman of the “Ad Hoc Site Board”

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

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

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

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

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

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

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

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

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

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

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

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

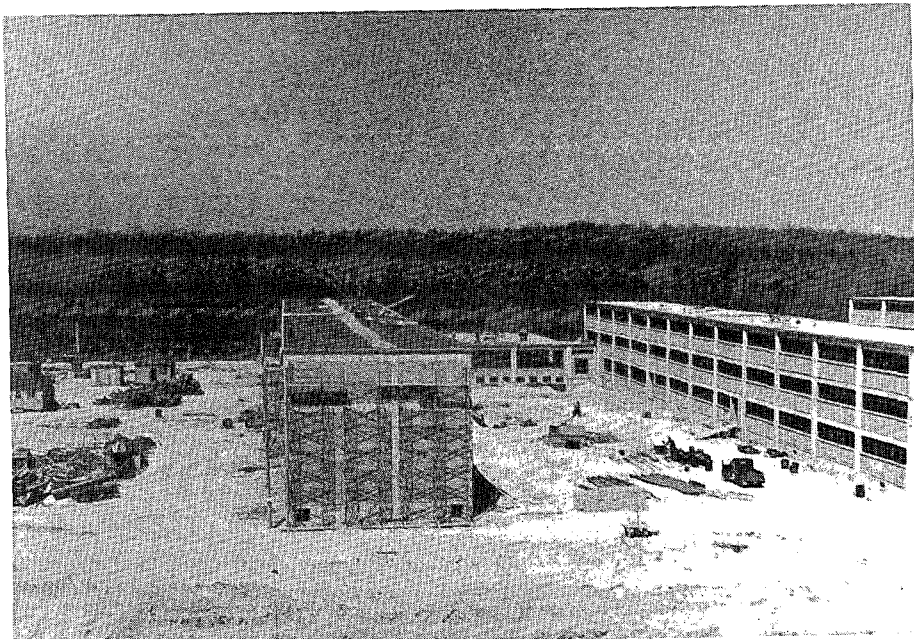
When Canine first looked at it, Fort Meade consisted of hundreds and hundreds of temporary wooden structures being used as barracks, offices and training facilities, with only a few permanent brick buildings. The corner of the post that NSA proposed to use

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

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

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

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

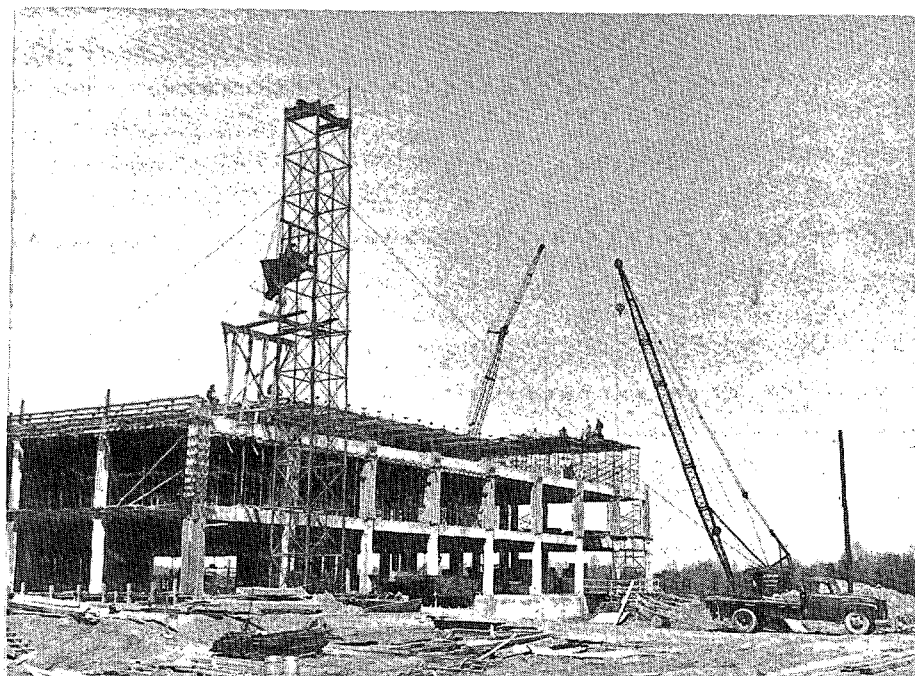


Barracks under construction, 1954

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

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

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

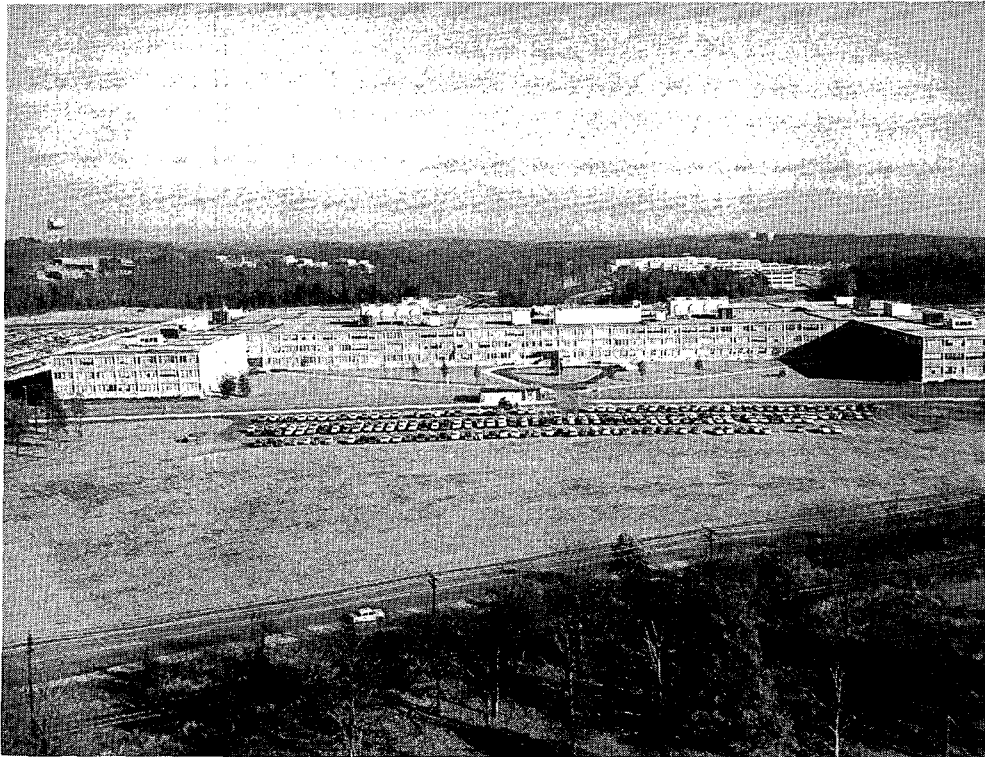


Headquarters construction, 1955, south wing

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

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

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



The NSA operations building in 1957

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

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

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

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

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

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

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

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

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



The Meademobile at Arlington Hall Station, 1954

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



The Saturday bus to Fort Meade, 20 April 1954

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

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

~~TOP SECRET UMBRA~~

Notes

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

[REDACTED]

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

[REDACTED]

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

[REDACTED]

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

~~TOP SECRET UMBRA~~

25. Ibid.



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

28. CCH Series V.F.5.1.

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

30. CCH Series VI.AA.1.5.

31. CCH Series V.F.5.1.

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

33. CCH Series VI.AA.1.5.

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

35. CCH Series V.F.5.2.

36. CCH Series V.F.5.1.

37. CCH Series V.F.5.1.

38. CCH Series VI.D.2.5.

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

40. CCH Series VI.AA.1.1.

41. *Washington Post*, 20 June 1957

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

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

44. CCH Series VI.AA.1.3.

45. CCH Series VI.AA.1.1.

46. CCH Series VI.AA.1.3.

47. CCH Series VI.AA.1.3.

48. CCH Series VI.E.1.4.

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

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

Chapter 7

The Eisenhower Reforms

THE POST-CRISIS CENTRALIZATION OF THE SIGINT SYSTEM

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

Criticomm

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

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

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

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

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

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

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



President Eisenhower

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

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

~~TOP SECRET UMBRA~~

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

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

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

The Baker Panel

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

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

[Redacted]

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



William O. Baker

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

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

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

[Redacted]

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

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



But this, said Baker, was not the whole story. Cryptology was a tremendously valuable asset to the nation, one which was producing most of the fast and reliable intelligence then available. It was doing it, [redacted] by putting together all the [redacted] disciplines, [redacted] The cryptologic system was capable of squeezing out of the ether a veritable cornucopia of information, if it were properly managed and funded. And this, said Baker, was the focus of his recommendations.

In order to properly employ the cryptologic system, NSA needed to focus on the important things. [redacted] had monopolized the talents of too many smart people. They should be spread throughout the organization, [redacted] This meant, in many cases, reallocating resources to ALLO and ACOM or to different divisions [redacted] What they had learned working [redacted] could now be employed against other [redacted] ¹³

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

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

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

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

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

~~TOP SECRET UMBRA~~

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

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

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

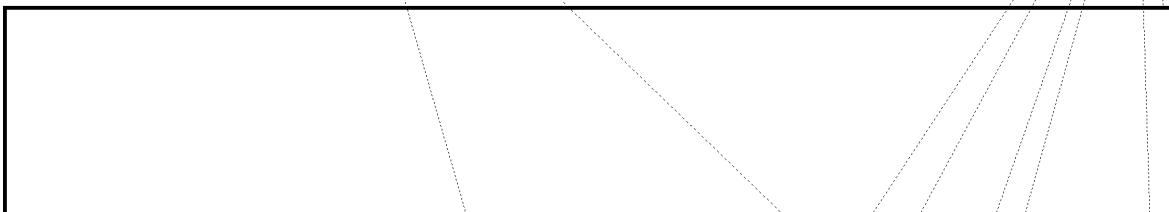
Baker's recommendation regarding a Los Alamos-style research institute met substantial skepticism. Some (like CIA) felt that it wasn't necessary. Edward Lansdale, deputy assistant to the secretary of defense for special operations, pointed out that success on high-level systems often stemmed from working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



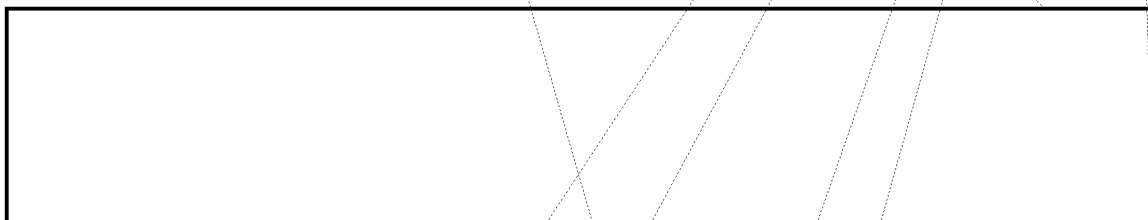
~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



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



The Reuben Robertson Report

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

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

What the committee came to understand, in the end, was that apparent duplication of targets and positions was usually not actual duplication. [redacted] Only [redacted] cases were being copied on more than 1 position, and in most cases there was sound rationale for the duplication. What had appeared so simple at Wilson's level did not look at all simple up close.²⁴

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

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

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

The Marriage of ELINT and NSA

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

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

~~TOP SECRET UMBRA~~

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

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

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

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

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

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

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

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

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

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

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

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

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

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

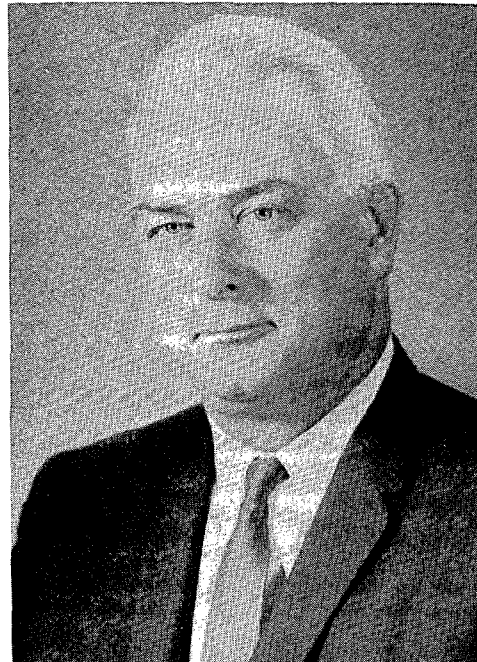
to the chaos, Louis Tordella, in the spring of 1960, created [redacted] [redacted] it became a clearinghouse for technical information, and it marked NSA's first big initiative in consolidating the effort.³⁷

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

The Kirkpatrick Committee

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

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



Lyman Kirkpatrick

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

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

~~TOP SECRET UMBRA~~

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

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

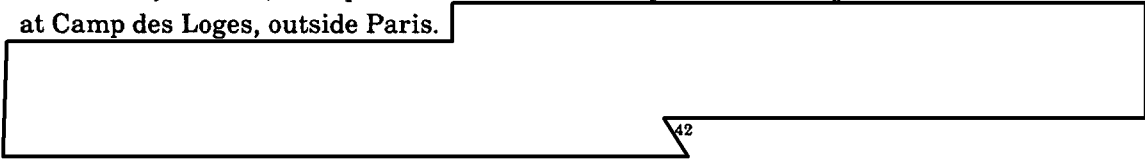
NSA Centralizes the Field System

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

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

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

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



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

~~TOP SECRET UMBRA~~

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

AFSS and the Development of Second-Echelon Reporting

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

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

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

[redacted] ⁴⁵

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

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

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

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

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



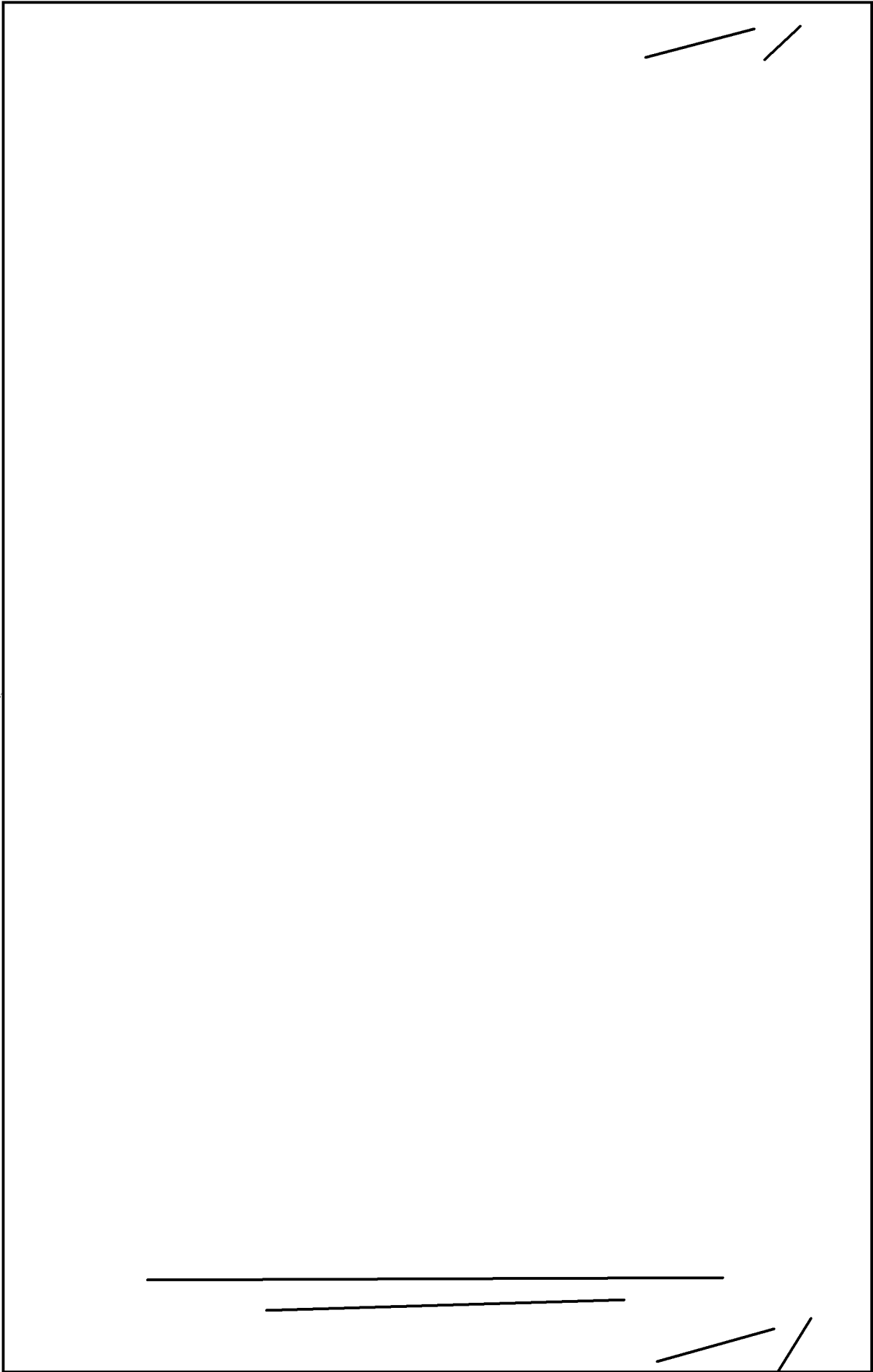
Benjamin Ardisana shown as a lieutenant, with his wife Betty, in the early 1950s

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

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

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

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



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

~~TOP SECRET UMBRA~~

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

51

The Struggle for Control in the Pacific

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

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



Samford Joins the Agency

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

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



John Samford, second director of NSA

His style was fluid - Samford was as smooth as silk. A CIA official described him as "more of a pedant than a pilot, more of a philosopher than a fighter, . . . a man who understood and loved the SIGINT business."⁵⁶ He set out to calm the waters between CIA and NSA, and when he left the job in 1960, the two organizations were back on speaking terms. His relations with USAFSS, contentious under Canine, settled back down. Samford had developed a close personal relationship with Gordon Blake, who became commander of USAFSS in 1957, based on old-school ties established when they had both

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

~~TOP SECRET UMBRA~~

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

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

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

Samford found, on being elevated to the directorship, that Robertson already had someone in mind. That someone was Joseph H. Ream, a top CBS executive. So, only some two months into office, Samford named Ream to the new job of deputy director, just to give the idea a whirl.

It soon whirled into oblivion. Ream had no SIGINT background, and the learning curve was too steep. He had serious family problems that required extended trips to Florida and that cut into his learning time. His lack of technical qualifications for the job simply could not overcome his well-documented managerial skills. Further, he found it hard to deal with an entrenched bureaucracy that viewed him as an outsider. Ream quit in frustration only six months into the job. It was the last time anyone successfully imposed a nongovernment outsider on NSA's top-level management structure.⁵⁸

In his place, Samford hired Howard Engstrom. Engstrom's impact on cryptology had already been considerable. He was brought into the Navy from the Yale math department during World War II. He quickly became influential in the development of computers for cryptologic work, and when the war ended, he left the Navy to form Electronic Research Associates (ERA), where he was the guiding genius in the effort to develop computers for NSG, AFSA, and later NSA. In the mid-50s he left Remington Rand (which had swallowed ERA), where he was a vice-president, to join NSA's R&D organization. When he arrived at NSA, Samford elevated Engstrom to the position of associate director, which gave him and his R&D organization special status and was designed to answer DoD-level

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

concerns that NSA was not doing enough in research and development. When Ream quit, Samford moved Engstrom to the post. But he remained only a year, and in August of 1958 NSA experienced yet another change in the revolving door position of deputy director.⁵⁹

The Tordella Era Begins

In late July of 1958, Samford summoned Louis Tordella, NSA's influential representative at Office of Special Operations (OSO), to his office to talk. Tordella remembers a short chat about inconsequential matters, following which Samford asked Tordella what a deputy director should be. Tordella told the director that the deputy should be his "alter ego." That sounded good to Samford, and he offered Tordella the job on the spot. It was the last time any director would have to do that for sixteen years. The revolving door shut with a bang behind the lanky form of Louis Tordella.⁶⁰



Louis Tordella changed the deputy directorship from an office to an institution.

Like Engstrom, Tordella had been plucked from a college math department for Navy service in World War II. Originally a Hoosier, he had gone to school in Illinois. OP-20-G's Laurance Safford found him on the campus of Chicago's Loyola University through his unique program of recruiting academics with an expressed interest in cryptology. And also like Engstrom, he was, in 1958, already a cryptologic legend. Tordella had pioneered in so many areas of Navy cryptology that he was close to being a universal man, like the Army's Frank Rowlett. He joined NSA when it opened its doors and served in numerous key positions which permitted him to push his favorite projects, especially the application of computers to cryptanalysis. Tordella had been NSA's representative on numerous high-level committees. This, and his tour in the Pentagon, had given him the opportunity to get acquainted with just about everyone who counted, and when Samford proposed his name to Deputy Secretary of Defense Donald Quarles (who had replaced Reuben Robertson) in 1958, he got no opposition.⁶¹

Tordella did indeed become the director's alter ego. Staying through the tenure of seven directors, he was the details man, the continuity. To many inside and outside the Agency, Louis Tordella was NSA.

Public Law 86-36

In 1959 Congress passed Public Law (PL) 86-36, which contained provisions permitting NSA to separate its personnel system from the regular Civil Service system, a permission which CIA had had since its inception. The problem that NSA had faced was that it had never been created by statute (only by executive order, the now-famous Truman Memorandum). There was thus no law which could keep NSA's personnel system apart from that of the rest of the federal government. Civil Service regulations straight-jacketed NSA procedures, and classification hampered NSA adherence to procedures which were intended for a completely open system. To eliminate the dilemma, PL 86-36 exempted NSA from the laws relating to the classification and grading of civilian positions from disclosing any information regarding the number of employees, the names, titles, or job descriptions. Public Law 86-36 was to have a major impact on NSA policies in both the personnel and security areas.⁶²

NSA AND THE AMERICAN PUBLIC - THE ISSUE OF LEGALITY

No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. . . .

Federal Communications Act of 1934

Cryptologic activities, which in the United States began during the early years of World War I, occupied an uncertain place in government. Early American cryptologists worked without the knowledge of the American public. They even worked without knowing if what they were doing was legal or not. It was an odd and unsettling position to be in.

Early statutes affecting cryptology were devised by Congress to protect radio, a new invention which required protection. Thus it was that a series of acts, beginning with one in 1912, was passed to protect information in radio messages from being passed to a third party to be used for commercial gain. This appeared to have a benign effect on cryptologic activities in the Army and Navy until 1927, when a revised statute stated that "no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purport, effect, or meaning of such intercepted message to any person. . . ." The aim of the legislation was the same as that of earlier statutes - to protect the information "unless legally required to do so by a court of competent jurisdiction or other

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

competent authority. . . .” Other competent authority could be the president or someone in the Army or Navy chain of command. But as the word “intercept” had crept into the statute, for the cryptologists who secretly plied their trade, this was unnerving news. It implied that what they were doing might be illegal. Further, it had the effect of shutting off liaison with the telegraph cable companies, who had in the early years supplied most of the material that the Army worked on. (But by the late 1920s the Army, like the Navy before it, was beginning to set up its own intercept stations.)⁶³

Meanwhile, the American public was blissfully unaware of any cryptologic activity at all – unaware, that is, until the publication of Yardley’s *The American Black Chamber* in 1931. Worse, Yardley was hard at work on a sequel, to be called “Japanese Diplomatic Secrets.” It was never published – it became, in fact, the first publication ever suppressed in the United States on the grounds of national security. To prevent any other revelations, Congress in 1933 hurried through a bill that prohibited all government employees from revealing their knowledge of American codes “or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States.” The penalty would be a \$10,000 fine or ten years imprisonment, considered to be a heavy enough hammer in those days. This appeared to be a backhanded way of authorizing other black chambers. If such activity were illegal, then why protect its activities from disclosure?⁶⁴

This step forward was followed immediately by disappointment. When the Federal Communications Act was passed the following year, it contained the same clause regarding “intercept.” There was a good deal of discussion about this within SIS and OP-20-G. Legal minds pointed out that the statute prohibited intercept “and divulging” of such communications. If it had said “or divulging,” it would clearly have singled out the process of intercept as illegal. But the intercept activity would not be illegal unless it were accompanied by “divulging,” which, once again, referred to use of the information for commercial gain. And the so-called Yardley Act the year before seemed to imply legality. But there was a lingering suspicion that they might someday be prosecuted for what they were doing on the basis of Section 605 of the Federal Communications Act of 1934. The penalties were exactly the same as they were under the Yardley Act.⁶⁵

Following the 1945 Pearl Harbor hearings, which amounted to the second public revelation of cryptologic activities, there were loud demands for legislation protecting this vital activity. Within the Army and Navy themselves, lawyers drafted protective statutes, and the Truman administration moved toward the introduction of legislation. Finally, in 1949 a draft was ready, and it was steered through the Senate by Lyndon Baines Johnson, a young senator from Texas. In 1950 the bill became law: Title 18, U.S.C. 798.⁶⁶

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

The United States already had legislation. But the Espionage Act of 1917 required proof that the person revealing the secret information intended to injure the United States. The courts had required a high standard of proof, including the direct involvement of agents of a wartime enemy, in order to secure a conviction. What if no enemy agents were involved? Or what if the agents were from a "friendly" country? Or what if the person simply gave the information to a reporter who published it?

Title 18 took care of all that. It made it a crime to divulge information relating to various aspects of cryptologic activities to an unauthorized person "or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government. . . ." It cast a very broad net, was almost totally inclusive, and was legally enforceable even in the absence of intent to injure. It could thus deter, or be used against, well-meaning but misguided idealists.⁶⁷

Just as important, it implicitly authorized COMINT activities by acknowledging that they were going on and by protecting their secrecy by law. Here was an implicit voiding of Section 605 of the Federal Communications Act of 1934 and earlier statutes as they related to cryptology.

This was followed two years later by the Truman Memorandum creating NSA and describing its responsibilities. Here was the "lawful authority," even though classified, so needed in the years prior to the war. As the years rolled on and Congress appropriated money for NSA's activities, the legal status of the business became less and less debatable. The 1959 anonymity statute (Public Law 86-36) for the first time named NSA in legislation. Finally, in 1968 the Omnibus Crime Control and Safe Streets Act specifically overruled Section 605 of the Federal Communications Act of 1934. Cryptology had made the journey from a secret black chamber to an officially authorized and avowed government activity.⁶⁸

PUBLIC REVELATIONS AND CRYPTOLOGIC SECRECY

[It is] of the essence of a secret service that it must be secret, and if you once began disclosure, it is perfectly obvious that there is no longer any secret service and that you must do without it.

Austen Chamberlain, British foreign secretary in the 1920s

Following Yardley, COMINT went underground. The Black Chamber had already been destroyed by Secretary of War Stimson in 1929 (through the device of pulling State Department funding). Its successor, Friedman's SIS, was so small (he started with a staff of six) as to be effectively invisible. The Navy had an effort of comparable size, and the entire enterprise proceeded reasonably secure from the eyes of the public.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

Beginning in 1939, a series of magazine and newspaper articles trumpeted the success of the federal government in breaking up German espionage rings. Some of the articles referenced German codes and discussed U.S. intercept activities. SIS and OP-20-G officials were livid – someone was calling attention to COMINT activities in such a way that the Germans could be alerted and might take countermeasures.

The “someone” turned out to be the Federal Communications Commission (FCC). FCC revelations to the press, designed to boost its stock with the public, were at least partly responsible for the War Department’s securing Roosevelt’s order in 1942 directing that such activities be discontinued in all but the Army, Navy, and FBI. Despite the order, the FCC continued its radio monitoring and codebreaking activities throughout the war and even accompanied this with leaks to the press boasting of its COMINT effectiveness.⁶⁹

Potentially more damaging was an article in the *Chicago Tribune* immediately after the Battle of Midway alleging that the U.S. had had advance knowledge of Japanese plans. The article was bylined by Stanley Johnston, a reporter who had been with the Pacific Fleet during the battle of Coral Sea. The next month columnist and broadcaster Walter Winchell stated that this knowledge had come from the breaking of Japanese naval codes. The Navy demanded that Johnson be indicted, and the case went to a federal grand jury in Chicago in August. No indictment resulted, a blessing for an over-eager Navy legal department that would have had to reveal far more damaging information in court to secure a conviction. The glare of national publicity was mercifully diverted, but in August, far ahead of schedule, the Japanese Navy changed all its codes. (There was never any direct evidence, however, that the Japanese read the *Tribune* or changed their codes in response.)⁷⁰

Classifying Cryptologic Information

Service cryptologists were almost instinctively aware of the extreme sensitivity of their work. They began in such small organizations, though, that the process itself was easy to protect. Once they developed information that needed to go to someone, they generally distributed it on a by-name basis to those few Army, Navy, and State Department people who had an absolute need to know. Information was often taken in locked containers, and a courier stood by while the official involved read and initialed the paper.

As for a formal classification, they had to use what was available. Existing service regulations at the beginning of World War II contained only two classifications: Secret and Confidential. Another quasi-classification, called Restricted (an earlier version of For

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

Official Use Only, or FOUO), was reserved primarily for information relating to military hardware.⁷¹

Their British allies had three classifications. Above Secret they added the term Most Secret. In 1944 the Army adopted the British three-tiered system, but called the highest category "Top" Secret. COMINT, being among the most sensitive items on the menu, was classified Top Secret.⁷²

When the Army obtained an agreement with GCCS in 1943, the Americans had to agree to attach a security caveat associated with COMINT. The most sensitive information (which at the time included ENIGMA and MAGIC decrypts) was now handled under a special codeword called ULTRA. Information derived from traffic analysis, DF, and plain text received codeword protection, but different codewords were used to denote lesser sensitivity - THUMB and PEARL were two which appeared during World War II. After the war the system devolved into two codeword categories: Top Secret Codeword, and everything else. That which related to COMINT but was not derived directly from communications intercepts began to receive the stamp Handle Via COMINT Channels Only (HVCCO).

Within cryptology, there were certain projects that received much more limited distributions. BOURBON, the early Soviet problem, was a good example, and VENONA got even more limited handling still. This system of ad hoc compartmentations continued into the early 1960s, when it was augmented by a more formal compartmentation system which was applied to SIGINT product reports. The most sensitive category was Gamma, A lesser category, called Delta, was often used to protect

Despite the strict secrecy applied to the trade, the number of people indoctrinated for COMINT rose steadily as its utility came to be recognized. By 1955 the number of COMINT clearances within the federal government (and to contractors) had grown to over 31,000, and the Hoover Commission expressed concern about the spread of highly sensitive information to such a large group. Of these This was a far cry from the six people that Friedman hired to carry on the Army's COMINT business in 1929 or the two people (Laurance Safford and Agnes Driscoll) who began Navy COMINT in the 1920s.⁷³

Pulling on the other end of the rope were the people who advocated an even broader dissemination of COMINT. In 1960 Lyman Kirkpatrick (who headed the Kirkpatrick Committee - see p. 263) took the Defense Department to task for over-strict rules regarding intelligence. (And by intelligence, he was clearly referring to COMINT.) Kirkpatrick wrote:

(b) (1)
(b) (3)-P.L. 86-36

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

Entirely apart from the well-known tendency throughout the intelligence community to over-classify, the special handling required for a very significant portion of intelligence information has at times deprived key personnel of information vital to the successful discharge of their responsibilities.⁷⁴

The tug of war between the advocates of secrecy and dissemination was never-ending. Nor could the conflict be resolved. As SIGINT became more successful, it became an inevitable victim of its own success. Utility meant dissemination, and dissemination meant risk.

BREACHES IN THE DIKE - THE SECURITY CASES

The first significant breaches of the security system came from within rather than from without. The first two were quiet, and while they both involved significant compromise, their very obscurity minimized the damage. Neither became a cause célèbre, although one of them became public. The third, however, did major damage primarily because it became a public case.

L' Affaire Weisband

The first case did the most real damage. But it was so successfully hushed that only a few insiders knew that it had occurred. It involved an AFSA analyst named William Weisband.

Weisband was an immigrant. Born in Alexandria, Egypt, in 1908, he had entered the United States in either 1925 or 1929. (The record on this point is obscure.) He became a citizen in 1938 and, while living in New York City, was inducted into the Army. Weisband went into the Signal Corps, and he first began working with ASA in 1943, where he became a favorite of Colonel Harold Hayes (who headed the Army's cryptologic activities in the Mediterranean). As an accomplished linguist, he was an ASA natural and received a transfer from North Africa to Arlington Hall in 1944. The end of the war found him still working there, and he hired on as a civilian. ASA needed all the help it could get in 1945, and getting a linguist like Weisband was a good day's work.⁷⁵

Unfortunately for ASA, Weisband was a Communist and suspected of being a spy. He had handled other agents passing defense information to the Soviets even before he entered the Army. He apparently gave up handling agents once he entered the service, but after he arrived at Arlington Hall he probably resumed his old avocation.

At the Hall he had a reputation as a stroller. He wandered around, chatting and picking up bits of gossip. He was also adept at getting himself on distribution for documents that did not directly concern the work of his section. Highly gregarious, Weisband had a wide circle of friends, and he entertained some of the top officers and civilians in ASA. His postwar wedding party was talked about as a who's who of Army cryptology.⁷⁶

Although Weisband had been on an FBI list of suspected Communists since 1948, he was first tagged as a possible spy through the VENONA project. In 1949 a Soviet agent identified in VENONA traffic led the FBI to another agent, who led them to another, who finally implicated Weisband as a "handler." The FBI began piecing together information on this new identity and was aghast to learn in 1950 that Weisband was employed at Arlington Hall, the very place whence the VENONA decrypts were coming. In April 1950 Wesley Reynolds of the FBI went to Carter Clarke, commanding general of ASA, to report the news. Clarke told Reynolds that Weisband had transferred to AFSA. They went to Admiral Stone.

At the time, Weisband was working as a section chief on the Soviet problem. Co-workers had already reported him as a possible security risk, and he had been removed from access to some of the more sensitive projects while security looked into it. He was immediately suspended and interrogated. He denied everything. But the walls were falling in on him even as he spoke. In August, as the subject of an unrelated investigation, he appeared before a federal grand jury in Los Angeles investigating West Coast Communism. Ordered to return for further testimony, he did not comply, was arrested and was convicted of contempt, for which he served a year in a federal prison.

He never returned to AFSA, and in 1951 he was mustered out of federal employment by a loyalty-security board in San Francisco, which, not surprisingly, found that removal from federal employment was in the best interest of national security.⁷⁷ He remained in the Washington area, working as a car dealer and apartment manager, and died in 1967 in Fairfax. He never admitted anything.

The FBI never found out what, if anything, Weisband passed to the Soviets. But his close involvement with the Soviet problem argued suggested some of the tightening up of Soviet communications was a result of Weisband's activities. Many AFSA employees believed, rightly or wrongly, that he was single-handedly responsible for "Black Friday." His case instilled a certain paranoia within the profession, and accounted to some degree for NSA's extremely close guarding of COMINT.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

The Petersen Case



Joseph Sydney Petersen, Jr.

The second security breach involved an NSA analyst named Joseph Sydney Petersen, Jr. Petersen had served with ASA in the South Pacific in World War II and had formed a close liaison with Dutch cryptologists with whom the United States was exchanging information. After the war this liaison came to an end, but Petersen decided on his own to become a one-man Third Party office to the Dutch intelligence service. He collected documents at his home and periodically passed them on to Dutch intelligence people from the embassy. This apparently went on for several years.

(b) (6)

Petersen's espionage might never have come to light had it not been for an unrelated naval security case involving an officer who had been separated from the service for [redacted]. He implicated Petersen as a [redacted] and an investigation was launched. But when NSA learned that Petersen had close friends at the Dutch embassy, the investigators forgot about the [redacted] charge and called in the FBI. In September 1953 the FBI began questioning Petersen, and he began revealing his story. A search of his apartment uncovered a large number of classified documents, and the FBI reckoned that it had enough to prosecute.⁷⁸

The joint NSA-FBI team consulted with Canine in his quarters. The options were to try to prosecute or to be satisfied with a simple resignation on his part. This would be the first prosecution under Title 18, and a hearing in open court might bring to light information that would be more damaging than just giving Petersen his walking papers. But Canine decided to go for prosecution, and he later overrode objections by USCIB that the resulting publicity would seriously damage NSA.

When Petersen's lawyer found out that the government had opted for prosecution, he began negotiating a plea bargain. On the day the trial was to begin, he told the judge that Petersen was pleading guilty to a violation of Title 18. Petersen fully cooperated with the FBI and in return was sentenced to seven years in prison. He was paroled after four years.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

The Petersen case was similar to that of a much more notorious case years later, the espionage of Jonathan Jay Pollard. He passed cryptologic documents to an ally who he felt had been left in the lurch. Along with technical information regarding the establishment of cryptanalysis courses, Petersen also informed the Dutch [redacted]

[redacted] When the FBI searched his house, they found cryptologic documents dealing with several COMINT targets, among them Korea and Communist China. The NSA damage assessment found that the number of documents passed to the Dutch was "very large."⁷⁹

When Petersen was indicted, the Associated Press ran a dispatch which was printed in many newspapers across the country. It was the first time the new agency had ever fallen under the klieglights. The dispatch described NSA as "essentially a radio monitoring service. It has a network of radio receiving stations and other equipment, some of which are based overseas. It listens in on the world's radio traffic, both conventional messages and coded material . . . secrecy even tighter than that shrouding the Central Intelligence Agency surrounds the National Security Agency. It is not listed by name either in the Washington directory or in the Pentagon phone directory."⁸⁰

A number of other details about NSA appeared to bring about a focus on the Agency's anonymity. NSA's obscurity had been so perfect that Richard Russell, the chairman of the Senate Armed Services Committee, once asked, "What does the NSA do?"⁸¹ The job description appearing in the *U.S. Government Organization Manual* was a marvel of obfuscation: "The National Security Agency performs highly specialized technical and coordinating functions related to the national security." The Petersen case was the first to pry open the lid of anonymity.

Martin and Mitchell

On 1 August 1960, a small story appeared in the local Washington newspapers. Two Department of Defense employees of the National Security Agency had failed to return from vacation and were still missing.

The story did not stay small very long. NSA's reputation for secrecy guaranteed that any news would be big news, and by the next day it was on the front page. On 5 August the Department of Defense issued a brief statement that it was now known that the two employees, Bernon F. Mitchell and William Martin, had flown to Mexico City and thence to Cuba. It was assumed that they were behind the Iron Curtain.⁸²

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~



Martin and Mitchell during their press conference in Moscow
(from the *New York Mirror*)

But the most shattering blow came on 7 September. Listeners to Radio Moscow tuned in on one of the most remarkable press conferences of the century. Now in Moscow, Martin and Mitchell were introduced by the Soviet announcer and proceeded to tell their story in exquisite detail. They related how they had become analysts at NSA, full of confidence in the integrity of their government. They described how the U.S. government was intercepting and breaking communications of its allies (Turkey was named specifically), about intentional violations of Soviet airspace to collect intelligence, about alleged American plans for a nuclear first strike, and how NSA was trying to exploit Soviet communications. They exposed NSA's organization (PROD does this and ADVA does that,

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

etc.). They described the arrangements between NSA, GCHQ, and Canada. They spent a good deal of time on the RC-130 shootdown in 1958. It was marvelous theater for Khrushchev, who had launched a diplomatic and press offensive against the United States in May following the U-2 shootdown.⁸³

Martin and Mitchell were young mathematicians. Both had gone into NSG and had been assigned together at [redacted] Mitchell, who was from California originally, was quite bright and had been something of a prodigy in high school. But he was extremely immature socially and had a great deal of difficulty adjusting. While he was at [redacted] Martin was his only close friend. Martin was from Columbus, Georgia. He, too, had been labeled as very bright and, compared with Mitchell, was more gregarious. Certain questions about their psychological health came up on the polygraph and background investigation but were not regarded as serious impediments to employment. Once out of the Navy, both pursued college degrees in mathematics, and upon graduation both were approached for employment by NSA. They entered on duty as GS-7s in 1957.⁸⁴

In 1959 Martin was sent to the University of Illinois for graduate study. While there he established Communist associations, and in his private conversations became more and more critical of the U.S. government. (He expressed special distaste for the U-2 overflights and other reconnaissance activities, and this was reflected in the statements of both men to the press in Moscow.)

At the time, Mitchell was having his own problems and finally sought psychiatric advice. The private psychiatrist concluded that Mitchell was in all probability a homosexual with serious personality disorders. But the psychiatrist felt that this sexual orientation was not the root of his problems. More serious was his poor relationship with his own family.⁸⁵

It has been alleged that in 1959, in violation of standing rules for government employees, Martin and Mitchell visited Cuba. Despite this, there was no evidence that they actually established an espionage relationship with any Communist country prior to the defection.

In June of 1960, just after Martin returned from Illinois, they both applied for annual leave. They stated that they were going to visit family on the West Coast. Instead, they departed for Mexico City and from there flew to Cuba. Apparently they proceeded from there via Soviet trawler to the Soviet Union.

Back at the office, no one thought to question their absence until they were a week overdue. When their supervisor failed to reach them either in their Laurel apartments or at their families' homes, the FBI was called in, and there began an intensive investigation. The security people concluded that the defections were impulsive and self-initiated.⁸⁶

There was no evidence that they carried off any documents, which argued for the theory that they made their decision after going on leave. Still, the route they took

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

required considerable planning, and they left a defection note in a safe deposit box in a Laurel bank, to which they referred during the Radio Moscow broadcast. So the whole idea had been evidently a long time abuilding.⁸⁷

The defection precipitated a storm of criticism of NSA. The secretary of defense initiated an investigation of NSA security practices. Not to be outdone, the House Un-American Activities Committee, chaired by Representative Francis E. Walter of Pennsylvania, launched its own investigation. Finally, President Eisenhower directed that the FBI initiate an investigation to determine if there were any more potential Martins and Mitchells in the ranks at NSA.⁸⁸

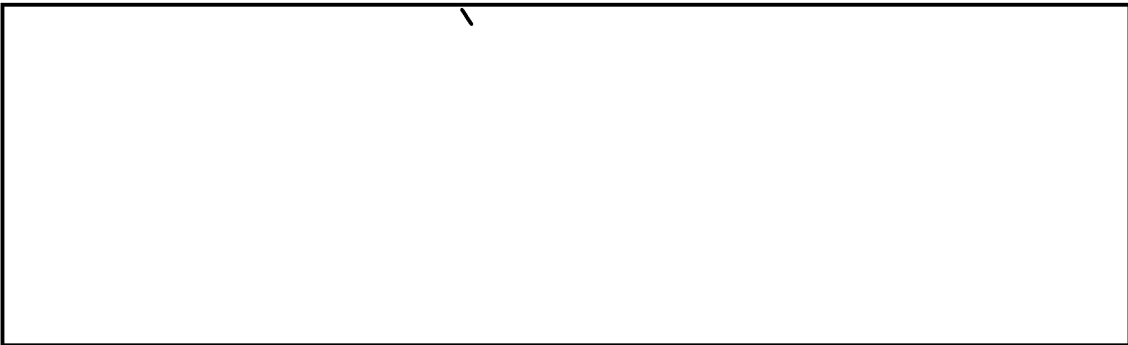
All three investigations lambasted the current practice at NSA of granting interim security clearances upon successful completion of the polygraph. Canine had authorized this procedure as an emergency measure during the Korean War, and it had come into routine use. After Martin and Mitchell the practice was terminated, and every employee had to have a complete background check in addition to the polygraph before performing any sort of classified work at NSA.⁸⁹

The Walter Committee investigation was exhaustive. It spanned thirteen months, took two thousand man-hours, covered fifteen states, and resulted in sixteen separate hearings. Thirty-four present or former NSA employees testified in closed session. NSA and the Department of Defense began by opposing committee access to NSA records, but eventually a compromise was worked out, and NSA and the committee finished on reasonably good terms. Still, the Agency could not keep the process from being sensationalized, and it was stung by a charge by Walter that NSA was a "nest of sexual deviates."⁹⁰

The legislative result of the Martin and Mitchell affair was a law which set up the legislative authority for NSA's security system. Among other things, it established that employment at NSA was appropriate only when it was "clearly consistent with the national security." It required a full field investigation prior to employment (i.e., no interim clearances) and gave the secretary of defense additional authority to fire NSA employees "when such action is deemed necessary in the interest of the United States..."⁹¹

In addition, the committee made certain recommendations concerning NSA's administrative practices - for instance, making professional psychological and psychiatric services available in assessing applicants and employees who revealed instability. But almost all the committee's recommendations had already been implemented, and in its final report the committee gave NSA credit for this. The most far-reaching of the changes related to the termination of the procedure of granting routine interim clearances, and the institution of the so-called three-hour rule, which required that employees three hours overdue for work would be reported to the security office. These and a long list of other changes became a permanent part of NSA's way of doing business.⁹²

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~



As the Walter Committee proceeded, the FBI investigation was winding down. An intensive screening of on-board employees had turned up a small number of people whose sexual conduct, in light of the sexual mores of the time, might be questioned, and of these some twenty-six had been terminated. The proceedings were not all that a civil libertarian might have wanted, but they calmed the waters long enough for NSA to begin functioning again.⁹⁴

The damage to NSA's public image was so severe that it overshadowed the cryptologic damage that had been done. Because it appeared that the two defectors had not carried away documents and that they had not had a previous relationship with the Soviets, just what the Soviets did know as a result was speculative. Martin and Mitchell had known about [redacted] the Soviet problem, but they were in a position to give away information [redacted] on certain Soviet cipher systems, especially a system called



[redacted] NSA employees blamed Martin and Mitchell. But no one ever had proof. And unlike Weisband, their defection was not coincident with any sort of "Black Friday." This, the most famous (or infamous) of NSA's security cases, was not the most damaging.

Notes

1. Max Davidson, "The Criticomm System," *Cryptologic Spectrum*, Spring 1975, 11-14.
2. "NSA's Telecommunications Problems, 1952-1968," CCH Series X.H.4.
3. "Report of the Secretary's Ad Hoc committee on COMINT/COMSEC" (the Robertson Report), June 1958, in CCH Series VI.C.1.11.
4. "NSA's Telecommunications Problems. . . ."
5. "NSA's Telecommunications Problems. . . ."; Tordella oral interview; Eisenhower Library papers in CCH Series XVI.
6. NSCID 7.
7. Tordella interview.

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 403
(b) (3)-18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

- 8. Davidson.
- 9. "NSA's Telecommunications problems..." [redacted] 108.
- 10. Eisenhower Library papers, "Report of the Joint Study Group on Foreign Intelligence Activities," 15 December 1960, in CCH Series VI.C.1.32.
- 11. "The Baker Panel Report and Associated Correspondence," in CCH Series VI.X.1.9.
- 12. Ibid.; Eisenhower Library papers.
- 13. Baker Panel Report, ACC 16667, CBRF 51.
- 14. Baker Panel; Eisenhower Library.
- 15. Baker Panel; Eisenhower Library.
- 16. Baker Panel.
- 17. NSA/CSS Archives, ACC 16667, CBRF 51.
- 18. Eisenhower Library papers.
- 19. Eisenhower Library papers; David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: MacMillan, 1967), 677; History of IDA/CRD by Richard Leibler, in CCH Series VI.A.1.6.2.
- 20. Baker Panel.
- 21. Howe, draft history of the Robertson report, in CCH Series VI.C.1.12.
- 22. Robertson report.
- 23. Ibid.
- 24. Ibid.
- 25. Ibid.
- 26. Ibid.
- 27. Memo for Mr. [redacted] Subject: Oversight of the National Security Agency by the Department of Defense, 9 Nov 1967, in CCH Series VI.C.1.27.
- 28. "History of the Electronic Intelligence Coordinating Group, 1955-1958," in CCH Series VI.O.1.6.; Collins, V. III, 12.; Tordella interview.
- 29. CCH Series VI.O.1.3.; VI.B.2.6.
- 30. CCH Series VI.O.1.3. [redacted] study, 16-17; interview with Dr. Robert Hermann, NSA OH 45-94, 2 Sept 1994, Charles Baker and Tom Johnson.
- 31. CCH Series VI.O.1.3.; VI.O.1.2.
- 32. NSA/CSS Archives, ACC 39471, H03-0311-4 [redacted] study, 16-26.
- 33. CCH Series VI.O.1.3.; NSA/CSS Archives, ACC 39471, H03-0311-4.
- 34. Melville J. Boucher, "Talomatry [sic] and How it Grew," Part I, *Spectrum*, Fall 1971, 13; CCH Series VI.O.1.3.; ACC 39471, H03-0311-4.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

- 35. NSA/CSS Archives, ACC 39741, H03-0311-4; [redacted] "The Soviet Land-based Ballistic Missile Program, 1945-1972: An Historical Overview," manuscript in CCH.
- 36. NSA/CSS Archives, ACC 39741, H03-0311-4.
- 37. CCH Series VI.O.1.13.
- 38. Eisenhower Library papers.
- 39. "Report of the Joint Study Group on Foreign Intelligence Activities," [The Kirkpatrick Report], 15 Dec. 1960, in CCH Series VI.C.1.32.
- 40. Ibid.
- 41. NSA/CSS Archives, ACC 26115, CBNE 48.
- 42. Informal correspondence between Gary Winch and Mel Boucher, 1977.
- 43. CCH Series VI.I.1.9.
- 44. Bob Rush, "AFSCC Tasking: The Development of the Three-Echelon Reporting Concept, 1949-1952," USAFSS history available at AIA, Kelly AFB, Texas.
- 45. "History of the USAF Security Service; Fiscal Year 1955," AIA, Kelly AFB, Texas.
- 46. Ibid.
- 47. Official USAF biography, Oct 1977.
- 48. Historical Data Report for the 6901st SCG, Semi-Annual, 1956-1964, available at AIA, Kelly AFB; Oral interview with [redacted] 25 March 1993, by Tom Johnson and Jim Pierson, NSA OH 15-93.
- [redacted]
- 50. Ibid.
- 51. Ellerson oral history; 6901 SCG Semi-Annual histories.
- 52. [redacted] "A Look at the Pacific Experimental Facility," *Spectrum*, Winter 1974, 18-21.
- 53. Howe, "Narrative History..." Part V, Ch. XXVI-XXX.
- 54. Howe, "Narrative History."
- 55. CCH Series VI.HH.12.10.
- 56. Collins, V. III, 40-41.
- 57. Transcript of videotapes of five former directors; [redacted] study, 16; CCH Series VI.NN.1.1.
- 58. Ibid.; Tordella interview.
- 59. CCH Series VI.D.1.1.; Stone interview; Kahn, *The Codebreakers*, 705.
- 60. Tordella interview.
- 61. Tordella biography in CCH Series VI.D.3.4; Tordella interview.
- 62. Summary of Statutes Which Relate Specifically to NSA and the Cryptologic Activities of the Government, available in CCH.
- 63. Ibid.

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

64. Ibid.
65. Ibid.
66. Ibid.
67. Ibid.
68. Church Committee Hearings, V. 5, 7-8, ACC 25958-25959, H0-02-0405.
69. John V. Connorton (LTJG) and Floyd W. Tompkins (LT), "The Need for New Legislation Against Unauthorized Disclosures of Communication Intelligence Activities," June 1944, SRH 016.
70. Ibid.
71. CCH Series V.C.2.8.
72. Ibid.
73. Hoover Commission report.
74. Kirkpatrick Committee report.
75. Benson and Phillips, V. I, 155.
76. Ibid., V I, 158.
77. Ibid., V. I.
78. Dr. Theodore W. Bauer, "Historical Study: The Security Program of AFSA and NSA, 1949-1962," unpublished manuscript available in CCH.
79. Bauer; Kahn, *The Codebreakers*, 690-92.
80. NSACSS Archives, ACC 2146, CBOI 37.
81. Quoted fm Thomas Powers, *The Man Who Kept the Secrets: Richard Helms and the CIA* (New York: Knopf, 1979), 276.
82. Wayne Barker, *The Anatomy of Two Traitors: The Defection of Bernon F. Mitchell and William H. Martin* (Laguna Hills, California: Aegean Park Press, 1981).
83. Press statement; copy available in ACC 27147, CBOI 37.
84. NSA/CSS Archives, ACC 24399, G11-0502.
85. Ibid.
86. Bauer.
87. Barker, CCH Series X.H.5.
88. Bauer; Eisenhower Library papers.
89. Bauer.
90. ACC 45399, G11-0502.
91. "Summary of Statutes . . ."; NSA/CSS Archives, ACC 24399, G11-0502.
92. Ibid.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~

93. Ibid.

94. Ibid.

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~
~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~TOP SECRET UMBRA~~