



**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 V*  
*The Early Postwar Period*  
*Volume 2*

**BOURBON to Black Friday (U)**  
*The Allied Collaborative COMINT Effort*  
*against the Soviet Union, 1945-1948 (~~S-CCO~~)*

Michael L. Peterson



CENTER FOR CRYPTOLOGIC HISTORY  
NATIONAL SECURITY AGENCY

1995



Table of Contents

	Page
Foreword .....	vii
Acknowledgments .....	ix
Introduction .....	1
 <b>Part One - Before BOURBON</b>	
Chapter 1: Cryptologic Origins .....	5
Chapter 2: Imperial Russian and Early Soviet Cryptology .....	7
Chapter 3: Early American Cryptanalytic Efforts .....	9
Chapter 4: Early British Cryptanalytic Efforts .....	17
Chapter 5: Early Allied Cryptologic Collaboration .....	21
Notes to Part One .....	24
 <b>Part Two - Early BOURBON, 1945</b>	
Chapter 6: Introduction to BOURBON .....	29
Chapter 7: U.S. Preparations for BOURBON .....	31
Chapter 8: The U.K. Dimension .....	37
Chapter 9: Collaborating While Negotiating .....	41
Chapter 10: The Effort Expands .....	47
Chapter 11: Progress, Problems and Promise .....	53
Notes to Part Two .....	58
 <b>Part Three - BOURBON Diary, 1946-1948</b>	
Chapter 12: Middle BOURBON, The Second Year - 1946 .....	65
Chapter 13: Old BOURBON, The Third Year - 1947 .....	79
Chapter 14: Beyond BOURBON, The Fourth Year - 1948 .....	85
Chapter 15: [Redacted] .....	95
Chapter 16: [Redacted] .....	99
Chapter 17: Personnel Resources, 1946-1948 .....	101
Chapter 18: Field Operations .....	105
Chapter 19: "Ferret" Plans and Early Operations .....	115
Notes to Part Three .....	118
 <b>Part Four - BOURBON Cryptanalysis</b>	
Chapter 20: Core Cryptologic Task .....	131
Chapter 21: [Redacted] .....	137
Chapter 22: [Redacted] .....	141
Chapter 23: [Redacted] .....	149

EO 1.4:(c)  
EO 1.4:(b)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

Chapter 24: [redacted]	155
Chapter 25: Other Soviet Service Systems	159
Chapter 26: IBM and RAM Contributions to Cryptanalysis	163
Chapter 27: GCHQ Proposal for Division of Cryptanalytic Effort	169
Chapter 28: Espionage or Normal Cryptographic Developments?	171
Notes to Part Four	173

**Part Five - BOURBON Traffic Analysis**

Chapter 29: From the Shadow of Cryptanalytic Support	185
Chapter 30: Into the Sunlight of Independent Contributions	191
Chapter 31: Reaching Analytic Mastery	197
Chapter 32: Project [redacted] "Removed from Normal SIGINT Procedure"	205
Notes to Part Five	213

**Part Six - BOURBON Language Processing**

Chapter 33: Language Support to Cryptanalysis	219
Chapter 34: U.S. Plain-Language Processing	223
Chapter 35: British Plain-Language Processing	231
Chapter 36: London Technical Conference of 1948	235
Notes to Part Six	238

**Part Seven - BOURBON COMINT Reporting**

Chapter 37: Early Reporting on Soviet Target	243
Chapter 38: GCHQ Leading the Way, Formally Speaking	247
Chapter 39: American Card Files and Other Media	251
Notes to Part Seven	258

**Part Eight - Afterword**

Chapter 40: One for the Road	261
------------------------------	-----

[redacted]	265
------------	-----

[redacted]	267
------------	-----

Appendix C: ASA Russian Plain-Language Unit Strength & Output	269
---	-----

Appendix D: Subject: Conduct of Russian Air Force and Army Problem	271
--	-----

[redacted]	EO 1.4.(c)
[redacted]	EO 1.4.273

PL 86-36/50 USC 3605

Bibliography	275
--------------	-----

Index	297
-------	-----

~~TOP SECRET UMBRA~~

## Illustrations

Page	Illustration
5	William F. Friedman
9	Herbert O. Yardley
10	Frank B. Rowlett (as Lt. Col. Signal Corps)
12	ASA Headquarters, Arlington Hall Station, Virginia
13	Dr. Louis W. Tordella, circa 1947
13	NCA Headquarters, Nebraska Avenue, Washington, D.C.
14	Joseph N. Wenger, Captain, U.S. Navy, Op-20-G
18	Brigadier John H. Tiltman
31	Admiral Ernest J. King, Chief of Naval Operations & Commander in Chief, U.S. Fleet
31	General George C. Marshall, Chief of Staff, U.S. Army
32	Winston Churchill, Prime Minister, Great Britain
32	Harry S. Truman, President, United States
36	Carter W. Clarke, General, U.S. Army, D/Chairman, ANCIB
37	Sir Edward W. Travis, Director, GC&CS
38	Bletchley Park, England, Headquarters, GC&CS
38	W. Preston Corderman, Colonel, U.S. Army, Commander, SSA
45	Baudot-Type Transmitter Keyboard and Undulator Tape Arrangement
45	Example of Baudot Intercept Transcribed with Cyrillic and Roman Equivalents
71	Grant C. Manson (1990 photograph at age 86)
73	Colonel Harold G. Hayes, U.S. Army, Chief, Army Security Agency
81	Mr. Stephen L. Wolf, during 1946 visit to GCHQ
82	Mr. Cecil J. Phillips, while assigned to GCHQ in 1946

~~TOP SECRET UMBRA~~

- 83 Mr. Francis A. Raven, circa 1947
- 105 Schematic Drawing of Baudot Sending and Receiving System
- 106 Schematic Drawing of Baudot Distributor System
- 111 Oliver R. Kirby, circa 1947
- 137 K-37 machine with cover removed
- 138 Example of [redacted] Message
- 141 Example of [redacted] Message
- 149 Example of [redacted] Message
- 155 Example of [redacted] Message
- 164 Mathew Machine
- 191 Chart 1: Soviet Baudot Two-Channel Net Diagram
- 192 Chart 2: Soviet Far Eastern Military Districts Morse Net Diagram
- 197 Chart 1: Soviet Main-Line Air Morse Links
- 198 Chart 2: Soviet PVO Administrative Net
- 198 Chart 3: Soviet LRA Morse Links
- 200 Chart 4: Soviet CINC Far East Morse Net
- 201 Chart 5: Soviet Far East Military Air Morse Links
- 243 ASA "V-Series" Intelligence Card (1945)
- 244 Op-20-G "G10-Z/Chronological Series" Intelligence Card (1945)
- 245 GC&CS Product Report Cover Sheet on a Soviet target (1945)
- 252 V-TAF-Air-I Item
- 254 Example of Russian Plain Language Analysis Item

~~TOP SECRET UMBRA~~

## Foreword

(U) The United States has had continuity in signals intelligence since the time of World War I, but the people and organizations involved have had to reconstruct many times at critical junctures in history. The first was in the 1920s, as the United States for the first time undertook peacetime signals intelligence. In the 1930s, as the U.S. Army and the U.S. Navy entered the cryptologic machine age, they also began building larger SIGINT organizations laid out along modern managerial and technical lines.

(U) As the United States prepared for and fought the Second World War, the military SIGINT organizations grappled with the problems of greatly increased size, greatly enhanced technical capabilities, the requirement to support forces engaged in global war, and the need to work closely with a foreign ally. America's military and civilian leadership emerged from the war with a strong appreciation for SIGINT and the determination to ensure its continued availability.

~~(S-CCO)~~ The end of World War II found the SIGINT professionals again confronting profound change. Victory over Germany and Japan had eliminated the primary targets of the SIGINT system. Diminishing budgets meant a need to combine resources, if not actually centralize operations across services. Intelligence and military leaders argued the value in continuing, even enhancing the relationship with the United Kingdom, which had been so valuable in wartime. Above all was the primary requirement: the need by all sectors of the national security community for reliable information on the Soviet Union.

~~(S-CCO)~~ The struggle to exploit Soviet communications in this complex milieu is the subject of Michael L. Peterson's *BOURBON to Black Friday*, which traces the origins of the Soviet problem through 1948. It is now clear that the decisions and actions taken by SIGINT authorities in the five-year period after World War II helped U.S. leaders make the decisions which shaped American policy for more than a generation; but it is also true, as Mr. Peterson shows, that these same decisions and actions reformed the shape of the SIGINT system for decades. Mr. Peterson has ably reconstructed the difficulties, triumphs, joys, and disappointments of the crucial postwar period. Based on extensive work in original documents, supplemented by numerous oral history interviews, *BOURBON to Black Friday* gives us also the beginnings of the post war SIGINT profession.

~~TOP SECRET UMBRA~~

(U) To learn about parallel themes, the reader is encouraged to delve into other books from the Center for Cryptologic History. In particular, Thomas L. Burns's *The Origins of the National Security Agency, 1940-1952* provides good background on the struggle within the intelligence community to create an efficient, centralized organization for signals intelligence.

David A. Hatch  
Director,  
Center for Cryptologic History

~~TOP SECRET UMBRA~~

## Acknowledgments

As is true with all publications of this size and scope, many people played a part in its production. From the Center for Cryptologic History, its director until March 1993, Henry F. Schorreck, suggested the topic and inspired, guided, and encouraged my early efforts. The Center's subsequent director, Dr. David A. Hatch, not only took up where Hank left off, but patiently and without audible complaint endured the seemingly endless readings and editings of each of my six BOURBON-related articles which were published in the CCH's *Cryptologic Quarterly*, as well as labored extensively over this manuscript. What I owe him is beyond measure and greatly appreciated. Also, Dr. Thomas Johnson of the Center reviewed, offered invaluable suggestions and helped correct the CQ articles and this manuscript. [redacted] made the administrative aspects of life easier for me around the Center - no small feat.

From the NSA/CSS Archives, particularly the Archival Services, I must thank in particular its chief, Ray C. Presley, an old colleague and friend from the 1960s who made me feel welcome, and especially Felix L. Plunkard, without whom I would have become trapped forever in the stacks (not unlike that fellow on the MTA) but still would not have found all the sources available. Also to be acknowledged is Jeanette Johnson, whose knowledge of the microfilm files put me and kept me on the right track.

PL 86-36/50 USC 3605

Also from the CCH, Guy Vanderpool, who while working on a history of the Chinese problem, kept an eye out for Soviet material, tipping me to a variety of otherwise unknown sources outside the Archives. Enormous thanks must go to [redacted] representing the best hope for the CCH's long-term future, whose youthful enthusiasm and archival and historical expertise kept me on my toes. For helping to keep life loose and the history office a congenial place to work, my friends and colleagues in the office, high fives go to Charlie Baker, Fred Bergman, Vera Filby, Jules Gallo, Bill Gross, Bob Hanyok, Brenda Jones, Renee Jones, [redacted] Sharon Maneki, Fred Parker, Ed Wiley, and Joe Yankowski.

A special word of appreciation must go to Dr. Colin (Brad) Burke, the CCH's Scholar in Residence during 1994. He shared in abundance his extensive knowledge of early computers, helping me understand that aspect of the Allied attack on Soviet communications; he also viewed my scribbles with a fresh, unbiased eye, helping me to discern the important trees in a cryptologic forest in which I had logged (and slogged) for over thirty years.

Of course, without the enormous publications support of Barry Carleen, who patiently allowed me to make many last-minute corrections, Jean Persinger, who taught me everything I know about the Xerox 6085, and [redacted] who endured numerous manuscript-related questions, this would still be an unpublished manuscript. This team of

~~TOP SECRET UMBRA~~

highly skilled publications professionals gave this manuscript the priority and attention it deserved.

Responsibility for thoroughness and completeness in the document search, for accuracy in the research, analysis, interpretation of the material, for the validity of my conclusions, and for any errors remaining in the manuscript, is mine alone.

MICHAEL L. PETERSON  
August 1995

~~TOP SECRET UMBRA~~

## Introduction

The world's defining international conflict for almost fifty years after World War II was the Cold War. It dominated American life like nothing else during that period, influencing its national politics, driving its defense policy, and dominating its intelligence budgets. In fact, the Cold War consumed most of the attention and a great deal of the resources of the Western nations, particularly the United States and Great Britain. It was West versus East, divided by an Iron Curtain. It was NATO versus the Warsaw Pact; capitalism versus communism. The threat of nuclear war hung like a deadly cloud over much of the civilized world for half a century.

The main focus of this threat to the West was, of course, the Soviet Union, which after World War II grew into an aggressive military superpower with perceived intentions of world domination. Atomic and hydrogen bombs, strategic bombers, nuclear submarines, and multiple-warhead intercontinental ballistic missiles formed the terrible weaponry of the Cold War, and the status of the Soviet Union's development, deployment and intentions to use these weapons by its military forces was the overarching question. Frightening images of a secretly developed doomsday weapon and Western fears of another Pearl Harbor drove intelligence requirements.

Intelligence requirements of course spawned signals intelligence requirements. The need for Allied SIGINT on the Soviet Union was such as to give it the highest priority. It received the most funding for cryptologic research and equipment, for the establishment of fixed field stations, and for mobile and overhead collection systems. It benefited from the steady application of brain power of the most and many of the best cryptologists, especially early on.

What is most interesting about Allied SIGINT on the Soviet Union is how quickly the United States and Great Britain shifted gears from breaking and reading the enciphered messages of Nazi Germany and Imperial Japan to exploiting the communications of the Soviet Union. In fact, as will become clear, the American effort began in 1943, in the middle of a world war; furthermore, almost 300 American cryptologists were hard at work on Soviet diplomatic and military message traffic as World War II ended in 1945.

Since the Soviet Union was a World War II ally, there was concern in some quarters about the propriety of reading their military and diplomatic mail. Consequently, the early organized cryptologic effort against the Soviet Union was compartmented.

BOURBON was the formally assigned covername for what was initially a joint American-British COMINT project to target the Soviet Union after World War II; but it quickly came to be used as a covername for the target country itself. Moreover, what started out as policy quickly became habit. Correspondence produced several years after the project title was formally cancelled continued to refer to the "BOURBON problem." It wasn't the Soviet Navy, it was the "BOURBON Navy." Those weren't Soviet or even Russian callsigns, those were "BOURBON callsigns," and so on.

By the 1980s, at the height of the Cold War, the Soviet problem had become the engine of an enormous SIGINT enterprise, with a several-billion-dollar budget, employing thousands of highly skilled people, many for their working lifetimes. They included civilian and military collectors, signals processors and analysts, linguists, traffic analysts, cryptanalysts, supported by engineers and computer analysts. They all operated sophisticated computer-controlled or computer-assisted intercept, processing and analysis equipment to extract the intelligence from a wide range of communications and electromagnetic emissions, signals that could be found across almost the entire radio spectrum.

During these years, the United States SIGINT System and its Second and Third Party collaborators used fixed stations, airborne platforms, ground-based communications satellite dishes, geosynchronous and orbiting satellites, and [redacted] facilities around the world. They poked every size and shape of antenna into the different electromagnetic environments, allowing the detection, recording and forwarding of a vast variety of Soviet military Morse networks, clear and scrambled teletype links, single-channel, multichannel, clear and enciphered voice communications, computer-to-computer emanations, and data transmissions, as well as radar and telemetry signals.

Now, in 1995, a noncommunist Russia [redacted] seems to be returning to its pre-World War II status as but one of many SIGINT targets. But where did the cycle begin?

This cryptologic history of the early Soviet COMINT problem, most of which has been previously published in six *Cryptologic Quarterly* articles\*, is now presented, considerably revised, in some cases corrected, with some new material added, in eight parts plus five appendices.

*Part One* ("Before BOURBON") tries to lay the groundwork and paint the background for the rest of the story. It relates American and British COMINT efforts against Imperial Russia and, after the "Great October Socialist Revolution" of 1917, the Soviet Union before 1945.

*Part Two* ("Early BOURBON, 1945") explains how both senior American and British officials reformed the cryptologic effort that helped win victories over Nazi Germany and Imperial Japan in World War II to postwar work, with particular focus on their erstwhile ally, Stalinist Russia, as the number one communications intelligence target.

---

\* "Before BOURBON: American and British COMINT Efforts against Russia and the Soviet Union before 1945" (TSC), *Cryptologic Quarterly*, Fall-Winter 1993, 1-20; "Early BOURBON - 1945; The First Year of Allied Collaborative COMINT Effort against the Soviet Union" (TSC), *Cryptologic Quarterly*, Spring 1994, 1-40; "Middle BOURBON - 1946; The Second Year . . ." (TSC), *Cryptologic Quarterly*, Summer 1994, 1-57; "Old BOURBON - 1947; The Third Year . . ." (TSC), *Cryptologic Quarterly*, Fall 1994, 1-57; "Project [redacted] 'Removed from Normal SIGINT Procedure'" (TSC), *Cryptologic Quarterly*, Winter 1994, 1-12; and "Beyond BOURBON - 1948; The Fourth Year . . ." (TSC), *Cryptologic Quarterly*, Spring 1995, 1-58.

*Part Three* ("BOURBON Diary, 1946-1948") provides a more-or-less chronological history of the important developments of the Allied cryptologic effort against the military and security forces of the Soviet Union through the watershed year of 1948, when all major readable Soviet cryptosystems were lost and [redacted]

[redacted] This part also addresses the [redacted]

[redacted] and discusses the enormous growth of resources, human and hardware, and development of field and liaison operations.

*Part Four* ("BOURBON Cryptanalysis") looks closely at the dominating and most [redacted] analytic effort during the BOURBON period, namely, cryptanalysis. This part [redacted]

[redacted] This part also contains a chapter on how tabulating machines and other electromechanical equipment were used to contribute to cryptanalysis during the last years of the precomputer generation.

*Part Five* ("BOURBON Traffic Analysis") traces the growing impact of traffic analysis on the Soviet problem, highlighting the unique contributions of this career field to COMINT production. This part also provides an object lesson (Project [redacted]) on how not to exploit a conventional traffic analytical problem.

*Part Six* ("BOURBON Language Processing") follows the Allied efforts to acquire sufficient Russian linguists, initially to provide translation support [redacted] [redacted] to attack what turned out to be an enormously rich bounty of plain language traffic.

*Part Seven* ("BOURBON Reporting") explores early COMINT reporting efforts by the United States and Britain, illustrating GCHQ's relatively advanced reporting program and showing in detail examples of the style, form, and content of relatively primitive, but presumably still effective, American product reporting practices. Also provided are some anecdotal examples of early postwar producer-customer relationships.

*Part Eight* ("Afterword") attempts to tie up loose ends, extract the essences of the previous parts, and produce a perspective on the BOURBON effort.

The *Appendices* provide detailed descriptions of [redacted] naming systems and verbatim presentations of especially colorful and pithy memoranda on selected BOURBON-related topics.



## Part One

### Before BOURBON:

## American and British COMINT Efforts against Russia and the Soviet Union before 1945

### Chapter 1

### Cryptologic Origins

Before BOURBON, there were several documented American and British cryptologic ventures against Imperial Russia and the Soviet Union. For starters, it should come as no surprise to anyone that the British, who were experts in this business for a couple of hundred years, had been reading Imperial Russian diplomatic correspondence since the eighteenth century. As might be expected also, America's cryptologic interest went back only to the World War I era, when Russia was but one on a long list of the United States' "potential" threats. But let's start at the beginning.

Unfortunately, searching for the beginning of a cryptologic event such as the origin of the Soviet problem is a bit like looking for the headwaters of a great river: There are many tributaries, all of which are sources of a sort. But which tributary is the "original" source, the fountainhead?

Organized cryptology itself, like both general history and rivers, seems to have no absolutely clear-cut beginnings. It is more like a continuum, its origins lost in the misty past, its turning points arbitrarily dated and ill-defined, its outline revealed mainly by example (from which generalizations are drawn at great risk), marked by high points, low points, and occasional no-points, all affected by the uneven application of usually insufficient resources, and often hindered more than helped by the sudden influx of new people and the inevitable reorganizations, restructurings, upgradings, and occasional downsizings. Nonetheless, there are several places we can begin to look.



William F. Friedman

If we define cryptologic history to include any form of secret communications, Mr. William F. Friedman, America's foremost cryptologist, will hark us back to the Spartan "scytale" (pronounced "sid-ah-lee") of 900 B.C. as the origin of military cryptography.<sup>1</sup> If we narrow the definition to comprise only secret electrical communications, he will cite the invention and development of Morse wire telegraphy in the 1830s and its fairly extensive use in the Civil War, with all the expected cryptographic and cryptanalytic consequences.<sup>2</sup>

If we want to get serious about the origins of U.S. cryptology in the era of wireless or radio communications, a practical starting point is World War I (1914-1918). And in a world where there is very little one can be certain about, it's a sure bet that in the United States there was no Russian problem before 1914. In fact, there was no significant U.S. government-sponsored COMINT effort until then, a situation that prevailed essentially from the end of the American Civil War.<sup>3</sup>

World War I is where one can begin to detect traces, vaguely drawn, of the origins of U.S. interest in what was to become the Soviet problem. It was at about this time, 1914-1916, that America began to include Imperial Russia in its focus.

When the Tsarist government was replaced in 1917 by the revolutionary Bolshevik regime, Russia became an increasingly important entry on both America's and Britain's "potential enemies" list, which included just about everybody who counted: each other as well as the larger, more advanced countries of the world like Austria, China, France, Germany, Italy, Japan, Spain, Sweden, and Turkey.

But before we proceed further, let's explore the origins of Russia's cryptologic efforts and the two Allies' early attacks. This is essentially the story of three countries - Russia, Great Britain, and the United States. First, let's look at what the fuss was all about in Britain and America. The target: Imperial Russia and the Soviet Union.

## Chapter 2

### Imperial Russian and Early Soviet Cryptology

Russian secret writing first appeared in twelfth- and thirteenth-century manuscripts as simple letter-for-letter substitutions. Serious political cryptography coincided with the reign of Peter the Great in the early eighteenth century; the best available evidence comes from English records showing the solution of a Russian cipher system in 1719. Ciphers remained primitive, however, until about 1754, when Russian cryptology blossomed under Peter's daughter, Elizabeth. The deciphering side of this cryptologic coin emerged early in the nineteenth century when Tsar Alexander I gave credit to Russian cryptanalysis for helping to defeat Napoleon in 1812. Black chambers (where diplomatic and terrorist-enciphered written correspondence was analyzed) were established in post offices across the land later in the nineteenth century under the Okhrana, the notorious secret police.<sup>1</sup>

According to Friedman, by 1915 Imperial Russian diplomatic cryptography was outstanding, "far ahead of anything anybody else had at that time."<sup>2</sup> Rather involved substitution and additive-based systems with very elaborately concealed indicators were employed.<sup>3</sup> These systems were also described as "frequently cumbersome in appearance, [but] adroit and cleverly devised."<sup>4</sup>

In contrast to his country's diplomatic cryptographic prowess, the last Tsar's military cryptography was so feeble as to be disastrous. This failing was aptly demonstrated by Russian fortunes in World War I during the Battle of Tannenberg. The Imperial Russian Army lost 100,000 men (or more) directly because German and Austrian commanders had detailed and absolutely reliable information on the disposition and movements of Russian troops and strategic plans from reading unenciphered or poorly enciphered Russian military communications.<sup>5</sup>

Following the overthrow of Imperial Russia in 1917, the Bolshevik successors, in an apparent eagerness to reject all vestiges of tsarism, initially abandoned the complex and relatively secure diplomatic systems. Government bureaus, military headquarters, secret police, and border guards compiled their own codes and ciphers and, until 1923, employed mostly primitive substitution and single transposition systems.<sup>6</sup> Involved, complex indicators seem to be the only phenomenon they retained.<sup>7</sup>

In general, Soviet cryptographers have heavily favored substitution systems over transposition systems. In the very early days after the revolution, however, they frequently employed transposition systems,

especially during the troubled years of 1920 and 1921, bearing with what might seem almost counter-revolutionary whimsy such names as the erudite SALAMBO, the political SPARTAK, the classical VULCAN, the grave SERIOZA, and folk names as TATIANA, MARTA, BAZIL. Other system names of this period are VIOLET, RAYON, KONGO, etc.<sup>8</sup>

Moreover, primarily the Latin alphabet and not Cyrillic script was used in these early systems.<sup>9</sup> In 1921, the Soviets began to make their cryptographic systems more complicated by combining transposition methods with substitution.<sup>10</sup>

After 1923, some Soviet diplomatic correspondents reverted to additive-based systems employing reusable key. In 1927, after the British Foreign Office published a white paper containing some deciphered Soviet telegrams, the functions of compiling and distributing cryptographic materials were again centralized, this time under a special department of the OGPU (a forerunner of the KGB). Shortly thereafter, systems and techniques originally developed in prerevolutionary times were revived and modernized to reflect current advances in cryptographic art, including the use of one-time pads. Also, extensive cryptographic training of carefully selected Communist party members was introduced.<sup>11</sup>

On the military side, the Red Army made little use of radio before 1937, as approximately 70 percent of all radiograms intercepted by the Germans were originated by various NKVD (formerly OGPU) organizations, chiefly the Border Troops. Before 1937, the Red Army and its subordinate air forces confined most radio communications to the Military District level, using simple systems in effect for only short periods of time. Radio was usually observed only when units were deployed for out-of-garrison activities or during maneuvers and communications practice sessions. Little is known of Soviet Navy communications practices in the 1930s. This is because there was relatively little interest by foreign COMINT organizations, except for the British, who themselves did not work on Soviet naval systems between 1935 and 1939 because collection sites were diverted to intercepting traffic related to the Italo-Abyssinian war.<sup>12</sup>

As might be expected, most of what we know about Soviet cryptography during this period comes from the British, who had varying levels of interest, and from German records acquired after World War II. Before we address the British interest, however, let's answer the timeless questions of what the United States knew and when it knew it.

### Chapter 3

## Early American Cryptanalytic Efforts against Russia and the Soviet Union

### LITTLE THAT WAS SOVIET IN YARDLEY'S BLACK CHAMBER



Herbert O. Yardley

In his book *The American Black Chamber*,<sup>1</sup> Herbert O. Yardley, America's first modern cryptanalyst, discussed the Russians mainly in a chapter on deciphering a coded letter (a transposition cipher in the German language), prepared in 1919 by a Soviet spy in Berlin, apparently intended for his superiors in Moscow and found in the wreckage of a plane that crashed in Latvia. Yardley's book put far greater emphasis on the U.S. attacking the ciphers of Germany and Japan. Moreover, French and Spanish and even British ciphers got equal time. In fact, he claimed his operation broke the diplomatic ciphers and codes of twenty countries, among which both Imperial Russia and the Soviet Union are listed, but not prominently.<sup>2</sup>

According to another source,<sup>3</sup> however, Yardley's Cipher Bureau, Department 8 of the Military Intelligence Division (MI-8), which was established at about the same time as the unfolding of the Bolshevik Revolution of 1917, received until April 1919 "a moderate quantity of Russian diplomatic intercepts," including cipher messages composed of five-digit groups and five-letter groups to ten-letter groups, of which apparently none was solved.

In May 1920, Yardley's Black Chamber in New York apparently planned to work on the traffic of five governments, among which was the Soviet Union, albeit last in importance.<sup>4</sup> By 1921, however, as an apparent consequence of changes in U.S. foreign policy, American interest in Soviet traffic became "considerable." Soviet messages were divided into thirteen different categories, including plaintext traffic in French or English, Moscow-Berlin messages, traffic bearing either discriminants or key words, and a variety of three-, four-, five-, six-, and ten-digit and letter traffic.<sup>5</sup>

None of these systems was solved by American cryptanalysts, however, despite work done on them and despite the availability of an interesting variety of collateral information such as the following:

- a. details of the COMINTERN "cipher code," surreptitiously acquired from Stockholm, Sweden, in 1923;
- b. similarly acquired explanation of a Soviet dinomic system in 1925;
- c.
- d. copy of a cipher system used by the Soviet Communist Party and its conduit for espionage, the AMTORG Trading Corporation in New York City, in 1928; and
- e. details of what was thought to be a Bolshevik code used in Java in 1928, acquired by the Office of Naval Intelligence from Dutch authorities.<sup>6</sup>

OGA  
EO 1.4.(c)

### AMTORG EFFORT MORE A FALSE START THAN A TRUE BEGINNING

When Yardley's Black Chamber was closed in 1929, the Soviet traffic was turned over to the Army's Signal Intelligence Section (SIS) (a forerunner of the Army Security Agency), staffed at the time with only five cryptanalysts (Friedman and his four assistants, Messrs. Rowlett and Hurt, and Doctors Kullback and Sinkov). A brief attempt was made to solve this and subsequently acquired Soviet traffic but with no success.<sup>7</sup>



**Frank B. Rowlett**  
(as Lt. Colonel, Signal Corps)

The AMTORG Trading Company was the focus of cryptanalytic attention again in 1931 when Representative Hamilton Fish of New York conducted an investigation into Communist propaganda in the United States. A congressional committee subpoenaed about 3,000 code messages from the cable companies and submitted them to the Navy's Code and Signal Section, itself composed at the time of only two cryptanalysts (Commander Safford and Lieutenant Wenger). When the analysis was unsuccessful, the messages were turned over to the army, with its five experts. All efforts proved fruitless, despite a great deal of work being done.

Mr. Friedman even conveyed Representative Fish's offer to Mr. Yardley of payment of \$100 per week for a few weeks to work on them. Friedman clearly anticipated Yardley's lack of interest ("I told them that your peg was higher up . . ."). Yardley was then at work on his articles on *The American Black Chamber*, which were about to be published in *The Saturday Evening Post* before appearing in book form.<sup>8</sup>

If one is looking for another "origin," Frank Rowlett, one of those army civilians who emerged as a major leader in the postwar cryptologic undertaking against the Soviet Union, recalled that the AMTORG operation was the first formal U.S. effort to solve a Soviet cryptosystem.<sup>9</sup>

Consequently, in Rowlett's view, in the 1930s three nations stood out from all others in the list of priorities, and the Soviet Union was not one of them. Exposing America's Pacific focus, Japan was by far the highest ranked, followed by Germany and Italy.<sup>10</sup>

The USSR was not totally ignored, however, as Rowlett remembered:

Several times between 1935 and the outbreak of World War II we [SIS] examined the Russian materials available to us; however, this examination was cursory and no serious effort was started in this period.<sup>11</sup>

During the period 1939-1941, the Soviet Union was truly an enigma, neither friend nor outright foe. Americans had no love for the USSR, but their closest allies, Great Britain and France, were courting Stalin. From April to August 1939, with Austria, the Sudetenland and Czechoslovakia having fallen into German hands, Britain and France tried to negotiate a peace treaty with the Soviet Union in hopes of blocking further German aggression. But Stalin had other ideas. He was flirting with Nazi Germany during the summer of 1939, with an eye on acquiring a little land for himself - namely, the Baltic states, Finland, and parts of Poland. The Soviets would have to fight for the West. They would have to stay neutral only for Hitler. On 23 August 1939, the Soviet-German Nonaggression Pact was signed, and the Soviet Union took on the more formal trappings of a foe.

Those garments were ripped off rather dramatically on 22 June 1941, however, when Nazi Germany invaded the Soviet Union. Suddenly, Soviet Russia, if not a beloved friend, was turned into a beleaguered ally of two English-speaking democracies. President Roosevelt, squirming out of the neutrality legislation and bucking the American public's isolationist sentiments, quickly made promises of aid, as did the British.

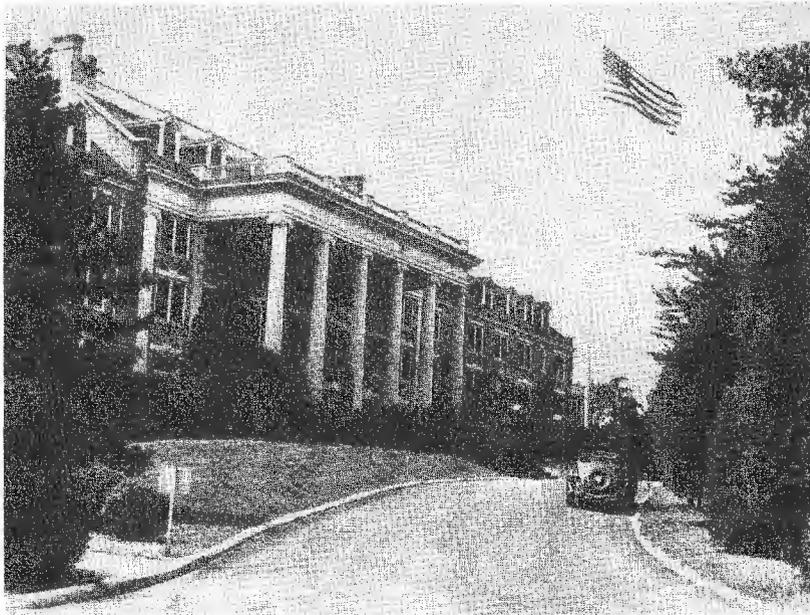
British COMINT relations with the Soviet Union also changed dramatically (as we'll see below). But America, not yet at war, continued to concentrate cryptanalytically on Japan.

After Pearl Harbor and America's entry into the war, apparently there was considerable discussion in American COMINT circles as to whether cryptanalytic resources should be diverted to the Soviet problem, among others. It was decided that some effort should be put on the diplomatic systems of the USSR, Spain, Vichy France, and others, because discussion of peace terms and the status of Germany's progress in the war might be found in such traffic.<sup>12</sup>

## **ORIGIN OF U.S. ARMY CRYPTOLOGIC EFFORT AGAINST THE SOVIET UNION**

Despite the AMTORG effort in 1931, little was done against the Soviet target until, as Rowlett recalled, "late 1942." Actually, it was more likely in February 1943 when a small

section, the General Cryptanalytic Branch, in the Signal Security Agency (SSA), the predecessor to the Army Security Agency (ASA) at Arlington Hall Station in Virginia, was formally established to organize the intercepted and otherwise acquired Soviet diplomatic traffic and to attempt a diagnosis of the Soviet cryptosystems under the strictest compartmentation.<sup>13</sup> A group made up initially of two, soon of five, analysts in early 1943 was gradually expanded to twenty-five persons by 1 January 1944. A portion of this group eventually evolved into the dedicated VENONA party, which spent the next thirty-seven years deciphering a small portion of Soviet diplomatic messages used by the KGB, the GRU, and their predecessors that were running espionage operations against the United States, particularly against the Manhattan Project (the secret American atomic bomb building effort) in 1944 and 1945.<sup>14</sup>



ASA Headquarters Arlington Hall Station, Virginia

After V-E Day (May 1945), ASA intensified the buildup of its Soviet effort. Skilled technicians, freed up from the German effort, were assigned to the Soviet section. The growing importance of the Soviet problem was indicated by the fact that these technicians were being carefully selected from the best of the population that had worked on the German effort.<sup>15</sup> By V-J Day (August 1945), ASA had from between "about seventy-five"<sup>16</sup> and "ninety-nine"<sup>17</sup> cryptanalysts dedicated to the Soviet problem.

During this period, there were three major sources of Soviet traffic. The most important, in Rowlett's view, was the Washington-to-Ladd Field, Alaska, landline, which the Soviet government had been allowed to use and to which ASA had surreptitious access.<sup>18</sup>

Another important source were the American telegraph companies. Until the end of World War II, wartime censorship laws allowed military intelligence access to copies of most telegrams leaving the United States.<sup>19</sup>

Rowlett recalled that the third source was diplomatic traffic on foreign-controlled radio circuits copied by surplus communications operators of the cable companies, under contract. He remembered that there was also low priority coverage by army and navy intercept operators.<sup>20</sup>

### **ORIGIN OF U.S. NAVY CRYPTOLOGIC EFFORT AGAINST THE SOVIET UNION**

The U.S. Navy also entered the Soviet sweepstakes in the middle of World War II. Dr. Louis W. Tordella, who from 1958 to 1974 was NSA's deputy director, recalled that "fairly early on" in 1943, as acting officer-in-charge of the U.S. Navy's intercept site at Bainbridge Island in Puget Sound, Washington State, he received an "eyes only" message from Washington, D.C., directing him to establish one or two intercept positions to collect Soviet signals. He was also instructed to keep the purpose of these positions concealed from those not actually involved.<sup>21</sup>



**Dr. Louis W. Tordella, circa 1947**

A later history of the Navy effort against Soviet communications confirmed Dr. Tordella's account, dating the initial intercepts as 14 July 1943 and placing the initial study of Soviet cryptographic systems at Op-20-G, the Navy's cryptanalytic section located at the Naval Communications Annex on Nebraska Avenue in Washington, D.C., (NCAW), about a week earlier, 6 July.



**NCA Headquarters, Nebraska Avenue, Washington, D.C.**

It was probably Navy captain Joseph N. Wenger, who was renowned for his work on the Japanese naval codes during World War II and who was now head of Op-20-G, the Navy's cryptologic section, who remembered that the U.S. Navy began processing Soviet traffic in August 1943.<sup>22</sup> Five Navy cryptanalysts were working "exclusively on the Russian project," making their first break into Soviet cryptographic systems in October.<sup>23</sup>



**Joseph N. Wenger**  
Captain, U.S. Navy  
Op-20-G

By January 1944, the Navy's Soviet cryptanalytic section had grown to twenty people, who were working on approximately 2,200 messages a month, intercepted by both Army and Navy sources. Working-level collaboration between Op-20-G and ASA was established at this time:

A regular program of cooperation between the Russian section at Arlington Hall and [the Navy Soviet cryptanalytic] section was inaugurated. Weekly meetings, held alternatively at Arlington Hall and at NCA[W], commenced.<sup>24</sup>

A new four-man intercept unit was established at Winter Harbor, Maine, in June, bringing to twelve the number of intercept operators at three sites copying Soviet communications. Twenty-six analysts were working the traffic at NCAW. Traffic receipts averaged 1,000 a month from the Army and 1,375 a month from the Navy, including about 100 plaintext messages. By September, twenty-one Soviet cryptographic systems had been identified, and five had been solved. However, according to the Navy, "recovery of the code of two systems was handicapped by the shortage of trained language personnel."

This problem was soon addressed, as ten new Russian-language-trained officers joined the section in October, followed a month later by ten more. All had completed a six-to-seven-month course at the Naval School of Oriental Languages, University of Colorado at Boulder. The Navy's first intelligence summary containing Soviet COMINT was published in November. Most interestingly, at NCAW, in an effort to disguise the rapidly growing "number of persons working the Russian project," the section's designation was changed from GV to G-10.<sup>25</sup>

In January 1945, the Navy added a traffic analysis section in Washington, D.C., with sixty-one people assigned to the Soviet target generally. Further expansion in February brought the number to seventy-three. By March, twenty-five operators were copying Soviet targets, still at three sites; meanwhile, Op-20-G-10 received 3,100 messages, translating 143 of them. In May, following the Allied victory over Germany, Admiral King ordered increased emphasis on the Soviet target. Specifics seemed to include more intercept of Soviet weather traffic and consideration of collaboration with the British. Meanwhile, another twenty "new language officers" reported to the section after seven months training at Boulder. The size of the Navy effort, not counting collectors, rose to 106, and the BOURBON project had not yet been implemented.<sup>26</sup>

Admiral King's order affected collection as well. Lieutenant Tordella, who had been transferred to Skaggs Island near San Francisco in late 1944, had become the officer in command early in 1945. He recalls that it was in the May time frame that he received a message from Op-20-G requesting that the site try to find and intercept a "2 channel Russian printer signal, frequency unknown, with a sync[hronization] pulse of 180 to 210 times per minute." Tordella remembers that they found it a week later and began copy on undulator tape.<sup>27</sup>

### **WHY 1943, RIGHT IN THE MIDDLE OF A WORLD WAR?**

As has been detailed above, U.S. Army cryptologists at Arlington Hall Station established a Soviet cryptanalytic section focused on diplomatic communications in February 1943, and Op-20-G shortly thereafter tasked Navy field sites to intercept Soviet military communications, itself undertaking cryptanalytic processing in July. Something happened during the winter of 1942-1943 that triggered the American decision to target an ally's communications, despite an ongoing world war against the Axis powers. No explicit reason has yet been found in the cryptologic archival record. However, the decision to target Soviet communications followed shortly in time and therefore seems to have flowed implicitly from some combination of three related historical events in January and February 1943.

First, the Casablanca Conference of 14-24 January 1943, among other things, led to a joint American-British decision to invade Sicily and put off a cross-channel invasion of northern Europe until 1944. In preparation for the conference, American military planners studied the relative fighting strengths of the Axis and Allied nations by "investigating political, economic, and psychological factors, intelligence, manpower, and

the status of ground, naval, and air forces."<sup>28</sup> These studies would have required detailed information on the Soviet Union. Interestingly, strategic military options included actions necessary "in the event Russia collapsed,"<sup>29</sup> which illustrates the level of American military understanding of the Soviet Union at the time.

Second, Soviet military successes in early 1943 got the West's attention. After taking terrible losses and appearing greatly inferior to the Nazi military following Germany's invasion of the Soviet Union in June 1941, Soviet forces proved resilient as early as December 1941 during their counteroffensive at Moscow. And despite having survived for almost five months the siege of Leningrad, clearly Soviet military successes at the Battle of Stalingrad in February 1943 must have made American leaders take notice and begin to fully appreciate that Soviet military power was substantial. "Substantial" needed to be quantified by information gained from intelligence.

Third was Stalin's attitude toward British and American failure to open a second front against the Germans in northwest Europe (as confirmed at Casablanca) and Anglo-American fear that Stalin might make a separate peace with Germany. The Soviet premier was proud of his forces' successes in the Stalingrad campaign, but he cautioned that "our troops are tired, they are in need of rest and they will hardly be able to carry on the offensive" beyond the middle of February.<sup>30</sup> Two weeks later, Stalin urged the Western Allies to move up their plan to open a second front in France, claiming that Anglo-American inaction in December 1942 had allowed Hitler to move twenty-seven divisions from France to the Eastern front.<sup>31</sup> Churchill responded with effusive congratulations for Red Army victories and offered a detailed list of Anglo-American military advances in North Africa and in Southern Europe, plus an outline of reasons why an earlier offensive against Hitler's armies in France was not yet possible,<sup>32</sup> trying (successfully as it turned out) to forestall "serious Soviet efforts for a separate peace with Nazi Germany in 1943, when months passed without a second front in northwestern Europe."<sup>33</sup>

Either condition, Soviet military success against Nazi Germany, demonstrating a military force for the world to reckon with, or Stalin's complaints leading to U.S. fears of a Soviet withdrawal from the war, would be reason enough for American intelligence officials to ask the Army and Navy to carve out some cryptologic resources from the war effort to mount at least a minimal attack on Soviet communications. It looked like time to begin to get a better intelligence handle not only on the USSR's diplomatic intentions but on the heretofore enigmatic Red Army and Soviet Navy. A recent cryptologic analysis cites Army SIGINT doctrine of the time which held "in spite of the need to give maximum intelligence support to the war against Japan and Germany, SIGINT collection against other actual or potentially important targets must continue."<sup>34</sup>

Meantime, the third main player in this cryptologic triangle, Great Britain, had a long history of reading Russia's communications.

## Chapter 4

### Early British Cryptanalytic Efforts against Russia and the Soviet Union

As mentioned earlier, Great Britain had been reading Russian secret diplomatic messages since at least 1719. And because the German government, whose communications had been Britain's focus during World War I, had reverted after the war to impregnable one-time pads, the absence of any useful German signals to intercept allowed the newly created Government Code and Cipher School (GC&CS) to begin concentrating its efforts on Soviet military traffic in about 1920. The British Army monitored the Soviets, while the Royal Navy handled Japanese signals.<sup>1</sup>

GC&CS (the forerunner of today's GCHQ) had a leg up on most SIGINT organizations targeting the Soviet Union: a Russian refugee named Ernst Fetterlein. Nigel West, in his *The Sigint Secrets*, describes Fetterlein as "the eccentric Russian emigré who . . . before the October Revolution . . . had been employed by General Jilinski's Russian cipher service."<sup>2</sup>

Brigadier John Tiltman (about whom more later) was more specific. "Fetterlein," he wrote, "had been Chief Cryptanalyst of the Russian Tsarist Government and held the ranks of both admiral and general" prior to the revolution. He had come to work for GC&CS and easily mastered early Soviet codes.<sup>3</sup>

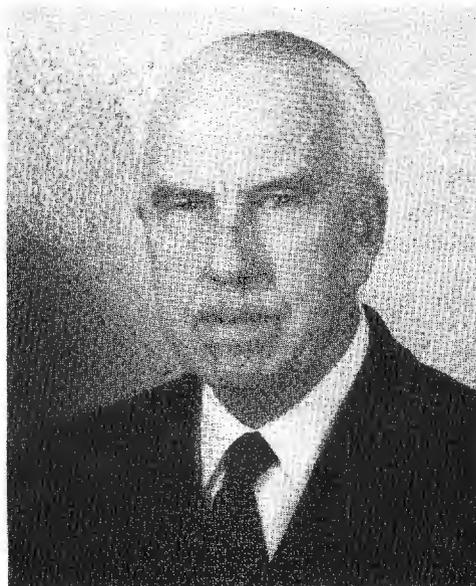
Decrypts of Soviet diplomatic cables provided the British with "invaluable insights into Soviet foreign policy," particularly evidence of Soviet attempts to subvert India and provide financial support to socialist extremists in England. In fact, in August 1920 the intelligence was so revealing of Soviet skullduggery that Prime Minister Lloyd George allowed some of the more incriminating decrypts to be published in the press in hopes of embarrassing the Soviet government into more acceptable behavior. Some cabinet members and Alistair G. Denniston, director of GC&CS, were appalled. As might be expected in circumstances where sources (if not methods) were revealed, in December 1920 all Soviet radio traffic disappeared. It was replaced by a system of couriers. Soviet transmitters resumed operations in March 1921 in a more secure cipher. GC&CS broke the new codes within a matter of weeks, however, and the decrypts (forwarded to the cabinet with a cautionary note: "If intelligence is used for publicity it will be lost to us") showed that the Soviet government had no intention of honoring certain clauses of a new treaty in which Britain had formally recognized the Soviet Union.<sup>4</sup>

In 1923, the British government again deliberately compromised the decrypts in a note of protest to the Soviet foreign minister. Additional changes in Soviet coding practices followed, culminating in the introduction of one-time pads later in the year.<sup>5</sup> Fetterlein reportedly broke the new Soviet codes at the end of 1925, allowing GC&CS to provide important decrypts to the British government until his retirement in April 1938.<sup>6</sup>

In 1930, military service sections were introduced into what had been primarily a civilian-based GC&CS. Here the name of Brigadier John H. Tiltman first appears.

Tiltman, who was in 1930 a retired major from the King's Own Scottish Borderers, was placed in charge of the Army Section at GC&CS.<sup>7</sup> After Fetterlein, Tiltman became the best-known British cryptanalyst of Russian systems (he was ultimately promoted to brigadier after being recalled to military service in World War II).

Tiltman had studied the Russian language as a young military officer. Upon graduation in 1920, he was placed on temporary attachment for two weeks to GC&CS to attack a growing backlog of untranslated Soviet diplomatic messages. Those two weeks grew into a year, and he never did return to his regiment. Initially, he worked for Fetterlein, learning cryptanalysis through on-the-job training. The British interest in Soviet cryptosystems is not better demonstrated than by the fact that in 1921 Tiltman was posted to the intelligence branch of the British General Staff in Simla, India, where he then worked on Soviet diplomatic cipher systems for the next eight and one-half years.<sup>8</sup>



Brigadier John H. Tiltman

Until 1936, GC&CS's chief concern was illicit communications emanating from the Soviet Union.<sup>9</sup> Tiltman wrote that from 1931 through 1934, his primary preoccupation was with the study of COMINTERN cipher systems. Although the systems were complicated, the messages were virtually all read.<sup>10</sup>

He explained:

Starting about 1929, the Communist International set up a world-wide clandestine radio network to carry the intercommunications of the various national Communist parties with Berlin (not Moscow) as control. During 1930, our intercept consisted almost exclusively of telegrams between:

- a. Kompartei, Berlin and Komintern [sic], Moscow and
- b. Kompartei, Berlin and Comparty, London, known by us as 'Komintern' and 'Comparty' respectively.

Both classes of intercepts were sent in 5-figure groups and were shown to have concealed indicators.<sup>11</sup>

Meanwhile, also in 1929, the British Army was keeping watch on foreign air traffic for the Royal Air Force, intercepting in particular Italian and Soviet traffic from Sarafand in Palestine and from India. By 1932, the Waddington field station had accumulated a considerable amount of Soviet air material.<sup>12</sup>

In 1936, Soviet air traffic was still one of four requirements levied by GC&CS, the others being Spanish Revolution, Italian air, and German air.<sup>13</sup> And in 1940, although discussions took place on how to acquire Soviet air traffic from the Transcaucasus to support British Middle East intelligence needs, apparently no traffic was collected.<sup>14</sup>

Turning to the Soviet naval target, by 1937 the naval Y station (i.e., field intercept site) at Scarborough was taking Soviet, along with German, traffic.<sup>15</sup> But there was a definite lack of purpose in the cryptanalytic work done on Soviet naval codes and ciphers until 1935, at which time all study was abandoned entirely until the outbreak of World War II. Limited traffic analysis was then resumed, supplemented in 1940 by the work done by a party of Polish analysts. Information was exchanged with the Finns; incidentally, the British cooperated with both the Finns and the Poles in SIGINT exploitation of Soviet traffic until 1941.<sup>16</sup> Several minor naval systems were broken into and the decrypts were circulated, but they were too fragmentary to be of much interest. In September 1941, the Soviet Naval Section was disbanded.<sup>17</sup>

Despite the lack of analysis at GC&CS, Soviet naval traffic was being included, along with German, Italian and Spanish, in the intercept of a fixed British Y station with the interesting nautical name of HMS Flowerdown from September 1939 until at least April 1940.<sup>18</sup>

Also in 1940, the British were reading five Soviet weather codes.<sup>19</sup> It was the effort on these codes which brought about an interesting development following the German invasion of the Soviet Union in June 1941. In the minds of some, as we have seen, the Soviet Union had, by virtue of having been invaded, become an ally. Therefore, she was no longer a SIGINT target but now a potential collaborator in SIGINT matters.<sup>20</sup> Consequently, in early July 1941 the head of the air section at GC&CS wrote to the air ministry in connection with the meteorological problem. "It seems a pity," he penned, "that we should have to spend time breaking the cypher of a friendly power. Given an approach through the right channels, the Russians could surely be persuaded to hand over their cypher."<sup>21</sup> Inquiries were made, but with no success. After meeting with the Soviets on the subject in September 1941, a British Army officer reported, "The greatest difficulty I experienced was the fact that no Russian officer can answer a question when it is put to him. Everything must be referred to the Kremlin for a decision." Negotiations continued into 1942,<sup>22</sup> but when the Soviets requested information about British success with the ENIGMA material, the British backed away;<sup>23</sup> and, like Lenin's view of the future of Soviet state power, British Army COMINT liaison with the Soviets "was to wither away."<sup>24</sup>

In contrast to the army experience, British and Soviet collaboration in the area of naval SIGINT briefly showed promise. In July 1941, the Soviets consented to the establishment of a small British naval Y unit at Polyarnoe near Murmansk. The station produced valuable intercept - 60 percent unique by one account - on the communications of German U-boats operating out of northern Norwegian fjords. But there were reporting timeliness problems and concerns over sharing the material with the Soviets. In the first instance, the station had great difficulty transmitting the intercept results back to the United Kingdom because of unpredictable ionospheric conditions in the northern latitudes

interfering with radio communications. In addition, the British knew that the Germans were reading Soviet ciphers and feared that their collaboration with the Soviets would be discovered by the Germans. The station was closed in 1944.<sup>25</sup>

As World War II wound down, the Soviet target quickly reemerged. By April 1945, Flowerdown's collection tasks included Soviet along with Italian, French, Spanish, Portuguese, Swedish, and German, including merchant shipping frequencies.<sup>26</sup>

Also by 1945, all British liaison with the Soviets had effectively collapsed, and Soviet material was again being analyzed, with plans for an expansion of coverage. On 23 May 1945, the military services were instructed to make 643 radio sets available for Soviet interception, and Y station commanders were to be informed that the new effort was to be treated as an "exotic" task, a label placed on any target except Germany and Japan.<sup>27</sup>

After the German surrender, intercept positions became available at all British Army stations for "exotic" tasks hitherto slighted. Foreshadowing the future: "Reports show how the operations were extended; shortly afterwards, directions were received to take up Russian problems on a larger scale."<sup>28</sup>

Related so far have been the individual efforts of the United States and Britain against Russia and the Soviet Union. Before BOURBON, however, there was also a history of Allied collaboration against the Germans in World War I and against both Nazi Germany and the Empire of Japan in World War II, cooperation that eventually segued into BOURBON.

## Chapter 5

### Early Allied Cryptologic Collaboration

Over the years British COMINT authorities actively collaborated with a variety of counterparts in other countries. GC&CS liaised with the French during World War I, with the Poles and the Finns before World War II, and even in a limited fashion with the Russians during World War I and, as we have just seen, in World War II.

Initial collaboration between Britain and its allies during World War I began in 1914, with the sharing of German naval code books; the Russian Imperial Navy offered the British Admiralty such a book recovered from a German cruiser run aground on Russian territory, and the Australians provided the British with a package of photographed German documents, among which was another naval code book.<sup>1</sup> Subsequently, French military cryptanalysts began sharing German SIGINT information with the British Directorate of Military Intelligence (MI1).<sup>2</sup> In 1916, French direction-finding stations were apparently sharing with the British tracking information on German Zeppelin reconnaissance flights.<sup>3</sup>

In the fall of 1917, the Americans provided the British with a code book retrieved from a downed Zeppelin. In a note of thanks from Admiral Hall to Pershing's staff, the British promised that "any information therein which will be of value to the United States forces will be at once communicated to them."<sup>4</sup>

The British, of course, had already made good in spades on that promise in the diplomatic arena. In February 1917, the British Foreign Office shared a translation of the famous Zimmermann telegram (which, incidentally, they had intercepted from a State Department landline) with the American ambassador to England. British motives for sharing this information were not altogether altruistic: they wanted the United States to enter the war, and they were successful.<sup>5</sup>

The British also urged the American government to improve its methods of encoding War Department cablegrams, to protect them from German intercept and decipherment. Collaboration between Yardley and British cryptographers took place during his official visit to London in August 1918. This trip was in conjunction with Yardley's attendance at the Paris Peace Conference and his assignment to liaise with the French and the British in an attempt to learn all he could about the cryptologic methods of the Allies.<sup>6</sup> It was during this trip, by the way, that Yardley became aware that the British were probably reading American diplomatic and military correspondence,<sup>7</sup> a favor the Americans returned to a limited extent over the next decade.<sup>8</sup>

Eventually, Yardley was allowed to study all the methods of the British Military Cipher Bureau,<sup>9</sup> and he was invited to visit the Cipher Bureau at British General Headquarters in France.<sup>10</sup> Yardley was also given extensive access to French cryptologic practices except their work on diplomatic ciphers in *La Chambre Noire*.<sup>11</sup>

In addition, at least by 1918 the American and British fleets kept a close liaison, which included maintaining radio communications between their units and, consequently, sharing of cryptographic systems between their navies.<sup>12</sup>

Formal discussions on COMINT collaboration between the U.S. Army and the British began in the summer of 1940. Early in 1941, a mission made up of two Army and two Navy officers went to London, taking with them two PURPLE machines (analogs of cipher equipment that permitted the timely American decryption of certain high-level Japanese diplomatic communications) and associated materials. In exchange, the British provided much valuable information not only on German and Italian systems, but also on Soviet systems, specifically including detailed reports on Red Army and Soviet meteorological codes, and Russo-German liaison. Also obtained was a synopsis of callsigns and communications methods in the "Russian Military, Air and Internal Affairs organizations."<sup>13</sup>

Active collaboration against the wartime enemies began soon thereafter and reached the point where in 1944 the Army was communicating continuously by radio with GC&CS. The U.S. Navy was in similar, but separate, communications with GC&CS. In separate agreements between GC&CS and the Army, and between GC&CS and the Navy, a division of effort was arranged whereby America would have primary responsibility for COMINT activities in the Pacific, and the U.K. would have similar responsibility in the Atlantic and in Europe, with intelligence and technical data exchanged freely.<sup>14</sup>

This arrangement would provide the basis for U.S. and British collaboration against the Soviet target in 1945. But in the early days (circa 1943) little or no Soviet intercept or technical results of its long-established effort against the Soviets were provided by the British to cryptanalysts at ASA. The American military intelligence offices (the Army's G2 and the Navy's Office of Naval Intelligence) received on a limited distribution basis certain information developed by GC&CS, but the ASA technical effort was denied the advantage of British technical results until about the end of the war.<sup>15</sup>

Finally, American collaboration with the British against the Soviet Union in BOURBON involved extensive cooperation between the United States Army and the United States Navy. Before BOURBON, that was not the case.

To be concise about it, William Friedman wrote:

Except for a brief collaborative effort to solve a large batch of AMTORG messages submitted by a member of Congress to the Navy in 1930 (both Services were unsuccessful, however), there was no collaboration in COMINT activities in the years 1920-1935, but only a more or less friendly rivalry in the solution of test messages.<sup>16</sup>

Summing up, the Soviet Union before World War II was neither a military superpower nor a significant COMINT target. She was nonetheless cryptanalytically challenging. Before BOURBON, the USSR's diplomatic ciphers were relatively difficult to break; her military ciphers were relatively easy to read. That pattern would continue well into the BOURBON period.

Allied collaboration was limited before BOURBON, but precedents were set and seeds were sown that took root and blossomed during BOURBON. Clearly, British cryptanalysis was more advanced than America's, at least against the Soviet Union. The British seemed to be reading almost everything, the Americans virtually nothing. Moreover, British collection of Soviet communications in Europe far surpassed anything America could manage at the time. So, collaboration, given British cryptanalytic expertise, initially benefited the United States, which eventually paid its bill many times over in terms of resources applied to the target and information shared.

From the beginning, and well into the BOURBON period, collection was a sometime thing. Telegrams, acquired by hook and by crook mostly from the cable companies, comprised the bulk of raw traffic.

Moreover, the cryptanalyst was king. COMINT exploitation meant cryptanalytic exploitation; the skills of traffic analysis and plain language processing played important but supporting roles. This relationship would change after 1948, when the analysis of communications externals and plain text began to provide greater value for money. Still to be heard from were the signals analysts and processing specialists, and ELINT,  and telemetry analysts, as well as the computer programmers and analysts, who in the 1940s were not even yet waiting in the wings, not required to join the cast and bring their act on stage until the 1950s and after.

But the extraordinary American performances by Friedman and his team of Army cryptanalysts and by the Navy's Op-20-G cryptanalysts led by such stalwarts as Safford and Wenger, against Imperial Japan, and the equally outstanding work done by Britain's GC&CS against Nazi Germany, set the standard for the next fifty years of collaborative COMINT effort against the Soviet Union. It was the skilled and dedicated people, trained and tested in the cryptologic battles of World War II, who became the leaders of the BOURBON project against the Soviet Union. With that kind of support, could BOURBON be anything but successful?

EO 1.4.(c)  
PL 86-36/50 USC 3605

## Notes

### Chapter 1: *Cryptologic Origins*

1. (U) *The Friedman Legacy: A Tribute to William and Elizebeth Friedman* (U), NSA/CSS, United States Cryptologic History, Sources in Cryptologic History Number 3, 1992, 29.
2. *Ibid.*, 75-119.
3. *Ibid.*, 121.

### Chapter 2: *Imperial Russian and Early Soviet Cryptology*

1. David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: The Macmillan Co., 1973), 614-618. Chapter 18, "Russkaya Kriptologia," 614-671, is one of the most comprehensive and interesting accounts of early Russian and unclassified Soviet cryptology available.
2. ~~(S, CCO)~~ Quoted in *Data on Soviet Cryptographic Systems 1917-1933*, Serial TRQ-77 (Washington, D.C.: Army Signal Security Agency, 1945) ~~(TSC)~~, 2; NSA/CSS Archives, Accession No. 6600, box CBMN61. Hereafter, TRQ-77.
3. ~~(S, CCO)~~ Tony Naples, *Soviet Manual Systems* (Unpublished Manuscript, drafted circa 1974, edited 1987), Part II, ~~(TSC)~~, 1. NSA/CSS Archives, accession No. 27859, location H03-0108-3.
4. ~~(S, CCO)~~ Burton Phillips and Suzanne Snook, "A Brief History of Russian Cryptographic Systems," circa 1946 ~~(TS)~~; NSA/CSS Archives, Accession No. 42572, location G03-0205-1.
5. *Friedman Legacy*, 164: Mr. Friedman says Russia "lost 100,000 men in the three-day battle. . . ." Kahn, 627, writes that 100,000 men were taken prisoner, with an estimated 30,000 dead or missing.
6. Naples, 1.
7. Phillips.
8. *Ibid.*
9. *Ibid.*
10. *Ibid.*
11. Naples, 2.
12. *Ibid.*, 7.

### Chapter 3: *Early American Cryptanalytic Efforts against Russia and the Soviet Union*

1. Herbert O. Yardley, *The American Black Chamber* (Indianapolis: Bobbs-Merrill Co., 1931), 239-249.
2. *Ibid.*, 332.
3. TRQ-77, 3.
4. *Ibid.*, 6.
5. *Ibid.*, 7.
6. *Ibid.*, 9-13.
7. *Ibid.*, 8.
8. *Ibid.*, 14-17.
9. ~~(S)~~ Frank Rowlett, "Recollections of Work on Russian," 11 February 1965 ~~(TSC)~~, CCH Collection, Series VII.83, 1.

10. Ibid., 2.
11. Ibid.
12. Ibid.
13. Ibid., 2-4. ~~(TS)~~ Also, Robert L. Benson, during research for his VENONA study, found several sources which placed the start of ASA's Soviet effort as 1 February 1943.
14. (U) ASA Memorandum for Col. Solomon, U.S. Army, at Pentagon, subject: History of BOURBON Problem, 12 March 1946 ~~(TS)~~; NSA/CSS Archives, Accession No. 5333, box CBNI21. Also, *The History of VENONA*, by Robert Louis Benson and Cecil James Phillips, National Security Agency, 1995 ~~(TSC)~~.
15. Rowlett, 5.
16. ASA History of BOURBON Problem.
17. (U) ANCICC Liaison Officers, Special Project (BOURBON) Memorandum to ANCICC, subject: Semi-Monthly Project Report, 15 August 1945 ~~(TS)~~; NSA/CSS Archives; Accession No. 4835, box CBQM36.
18. Rowlett, 4.
19. Ibid.
20. Ibid.
21. ~~(S/CO)~~ Louis W. Tordella, handwritten paper entitled "Collection of Russian Transmissions by the Navy; My Recollections," 5 May 1978 ~~(TSC)~~; CCH Collection, Series XI.H, box 12.
22. (U) Joseph Wenger, Cdr, USN, informal paper on history of BOURBON, February 1946 ~~(TSC)~~; CCH Collection, Series IV.AA.6.1.
23. (U) Naval Communication Activity informal history entitled Russian Language Section (July 1943 - January 1948); undated ~~(TSC)~~; NSA/CSS Archives; Accession No. 45021, location H06-0308-2. Hereafter, NCA informal history.
24. Ibid.
25. Ibid.
26. Ibid.
27. Tordella.
28. Grace Person Hayes, *The History of the Joint Chiefs of Staff in World War II: The War against Japan* (Annapolis, Maryland: Naval Institute Press, 1982), 254.
29. Ibid.
30. "Personal and Secret Message from Premier Stalin to the Prime Minister, Mr. Churchill, and the President, Mr. Roosevelt," sent on 30 January 1943, *Stalin's Correspondence with Churchill, Attlee, Roosevelt and Truman, 1941-1945, Volume Two* (Moscow: Foreign Languages Publishing House, 1957), 52-53.
31. "Personal and Secret Message from Premier Stalin to the President, Mr. Roosevelt," 17 February 1943, *Stalin's Correspondence with Churchill, Attlee, Roosevelt and Truman, 1941-1945, Volume Two* (Moscow: Foreign Languages Publishing House, 1957), 55-56.
32. "Personal and Most Secret Message from the Prime Minister, Mr. Winston Churchill to Marshal Stalin," 11 March 1943, *Stalin's Correspondence with Churchill, Attlee, Roosevelt and Truman, 1941-1945, Volume One* (Moscow: Foreign Languages Publishing House, 1957), 99-102.
33. *Encyclopedia Americana*. Volume 29 (Danbury, Connecticut: Grolier Incorporated, 1987), 515.
34. Benson and Phillips, *History of VENONA*, ~~(TSC)~~, 12.

**Chapter 4: Early British Cryptanalytic Efforts against Russia and the Soviet Union**

1. Nigel West, *The Sigint Secrets: The Signals Intelligence War, 1900 to Today* (New York: William Morrow and Company, Inc, 1988), 100.
2. Ibid., 101.
3. (U) John H. Tiltman, "Experiences 1920-1933," ~~(TSC)~~ *NSA Technical Journal*, Summer 1972, 1.
4. West, 101-103.
5. Ibid., 104.
6. Ibid., 117.
7. Ibid.
8. Tiltman, "Experiences," 1-9.
9. West, 118.
10. (U) John H. Tiltman, "Some Principles of Cryptographic Security," ~~(TSC)~~ *NSA Technical Journal*, Summer 1974, 17.
11. (U) John H. Tiltman, "The Development of the Additive," ~~(TSC)~~ *NSA Technical Journal*, Fall 1963, 2.
12. ~~(S)~~ GC&CS history: Army & Air Force SIGINT, Vol. IV - The Organisation and Evolution of British Air Force SIGINT - I (~~TSC~~), 27. CCH General Collection.
13. Ibid., 35.
14. Ibid., 84-85.
15. ~~(S)~~ GC&CS history: Naval SIGINT, Vol I - The Organisation and Evolution of British Naval SIGINT, Part 1 - The Making of SIGINT (~~TSC~~), 17. CCH General Collection.
16. GC&CS history: Army & Air Force SIGINT, Vol. IV (~~TSC~~), 201.
17. GC&CS history: Naval SIGINT, Vol. I (~~TSC~~), 222.
18. ~~(S)~~ GC&CS history: Naval SIGINT, Vol. II, The Organisation and Evolution of British Naval SIGINT, Part 1 (Continued) - The Making of SIGINT (~~TSC~~), 32. CCH General Collection.
19. GC&CS history, Army & Air Force SIGINT, Vol. IV (~~TSC~~), 137.
20. Ibid., 50, 75.
21. Ibid., 99.
22. Ibid., 100-104.
23. Ibid., 162.
24. Ibid., 135.
25. GC&CS history, Naval SIGINT, Vol. II (~~TSC~~), 40-45.
26. Ibid., 36.
27. ~~(S)~~ GC&CS history: Army & Air Force SIGINT, Vol. II - The Organisation and Evolution of British Army SIGINT - II (~~TSC~~), 348. CCH General Collection.
28. Ibid., 362.

**Chapter 5: Early Allied Cryptologic Collaboration**

1. West, 62.
2. Ibid., 57.
3. Ibid., 70.
4. Ibid., 83.
5. Ibid., 88-92.
6. Yardley, 203-209.
7. Ibid., 212.
8. ~~(S)~~ *Remarks on British Cryptographic Systems (1917-1932)*. (Washington, D.C., Signals Security Agency, 2 May 1945), ~~(S)~~; NSA/CSS Archives, Accession No. 3985, box CBNI16.
9. Yardley, 217.
10. Ibid., 219-220.
11. Ibid., 221-230.
12. Ibid., 201.
13. (U) War Department, Office of Chief Signal Officer Memorandum (from Sinkov and Rosen) to Asst. Chief of Staff, G-2, subject: Report of Technical Mission to England ~~(S)~~, 11 April 1941. CCH Collection, Series IV.V.10.6.
14. ~~(S)~~ Friedman memorandum for Mr. Grant Hanson, subject: Brief History of U.S. COMINT Activities, 20 February 1952, ~~(TS)~~, 10; CCH General Collection. Also ~~(S)~~ ~~(TS)~~ "Review of Current U.S.-British Collaboration in the Communications Intelligence Field," August 1947, 1-12, ~~(TS)~~; NSA/CSS Archives, Accession No. 1377, box CBPB57.
15. Rowlett, 7.
16. Friedman memorandum, 7.



## Part Two

### Early BOURBON - 1945

#### The First Year of Allied Collaborative COMINT Effort against the Soviet Union

##### Chapter 6

##### Introduction to BOURBON

###### WHAT DID YOU DO AFTER THE WAR?

The extraordinary American cryptanalytic achievements against Imperial Japan in World War II and the equally outstanding British code breaking work done against Nazi Germany set high standards of performance that would be difficult to duplicate in subsequent years. Nevertheless, with enormous confidence founded in success and buttressed by a battery of skilled and dedicated people who had been trained and tested in the cryptologic battlefields of a great war, both countries' cryptologic communities prepared for new challenges in 1945.

It's not too surprising that two nations' cryptologic organizations would quickly seek out new tasks. They assumed that their unique capabilities were still needed in a world of "potential adversaries." How better to be prepared for future threats - no more Pearl Harbors. How better to maintain their human resources and funding in a postwar budget atmosphere involving a search of what's now called a "peace dividend."

It's not too surprising either that American and British cryptologists planned to tackle the next tasks together. The two allies had explored new waters of collaborative code breaking during a hot war. Consequently, despite some wartime ups and downs, they found the experience generally to their liking. They found that indeed a special relationship had developed, wherein much of their countries' most secret intelligence sources, techniques and information were exchanged for the benefit of each. Carefully they negotiated formal agreements of cooperation, established formal channels for exchange of technical materials, and assigned top personnel as liaison officers in each other's camps. Then they plunged in up to their necks in Cold War cryptanalysis.<sup>1</sup>

What might also be surprising at first glance was the initial postwar focus of the partners' collaborative effort. Theoretically, the joint target could be any nation or group of nations. Potential threats abounded. Why turn on a wartime ally? Because, like the mythical phoenix rising from its own ashes, this ally emerged from the rubble of World War II, reincarnated as a big, nasty Siberian bear, symbol of a communist state commonly called then "Stalinist Russia." She turned out to be unappreciative and suspicious of

wartime friends, secretive about her military capabilities, domineering of her neighbors, and disrespectful of international treaties and agreements.

Despite being a valued partner against Nazi Germany, the Soviet Union was no friend of the West. The Soviet-German Nonaggression Pact of 1939 had allowed Hitler to launch a war in the first place. Stalin's aggression in Finland in 1939 and 1940 gained no Western sympathy. Later, as the war drew to a close in 1945, Soviet demands for retention of all territories acquired while collaborating with Hitler, her insistence on installing a subservient government for Poland, her aggression in the Balkans generally, and her contrary behavior over the creation of the United Nations gave Churchill and Truman nothing but headaches.

In fact, it was apparently American recognition in 1943 of the reality of growing Soviet military power (Stalin's armies had emerged victorious at Stalingrad in January 1943, and had stopped and begun to roll back Hitler's forces along the eastern front during the first half of 1943), and possible apprehension as to future Soviet intentions in a postwar world, that sparked the prescient decision by American cryptologic officials to begin to target Soviet communications in 1943. And after the war ended, it was for all these reasons that American and British cryptologists turned a major portion of their COMINT collection, processing, and analysis focus toward the Soviet Union.

They gave their joint effort the title BOURBON, which was used formally for almost a year as the project covername. For several years thereafter, however, it continued to be used synonymously with the Soviet Union. Interestingly, the actual country name was avoided like bad breath in formal correspondence for several years. The reason appears to be that in the summer of 1945, when the project was implemented, with the Soviet Union technically still a partner in the war against the Axis powers, there was some question as to the propriety of listening in on one's allies. It therefore had to be compartmented.

The BOURBON project not only required that the United States and Great Britain work closely together but made it necessary for the U.S. Army and U.S. Navy to begin to get serious about cooperating with each other. The first part was relatively easy. That last bit took some doing.

What follows now is an account of pertinent events, beginning in March 1945 and running through December. This chronicle relates the final stages of the internal U.S. Army-U.S. Navy and external U.S.-British negotiations, agreements, work, progress, problems, successes, and failures of what was to become a model of Allied cooperation, Project BOURBON.

## Chapter 7

### U.S. Preparations for BOURBON

#### SPRING PLOWING FOR ARMY-NAVY COOPERATION

On 10 March 1945 precisely, after almost a year of discussions and negotiations on improving the coordination of their COMINT efforts, Admiral Ernest J. King, Chief of Naval Operations (CNO) and Commander in Chief, U.S. Fleet, and General George C. Marshall, Chief of Staff, U.S. Army, the two senior military officials who would later bless the BOURBON project, agreed to the establishment of what they called the Army-Navy Communication Intelligence Board (ANCIB). It formally became the sole U.S. spokesman for the conduct of policy negotiations with all foreign countries on COMINT matters. BOURBON would be the foremost and probably the first project under ANCIB. An official working committee of the board, called the Army-Navy Communication Intelligence Coordinating Committee (ANCICC), would coordinate the day-to-day activities of BOURBON.<sup>1</sup>



Admiral Ernest J. King  
Chief of Naval Operations &  
Commander in Chief, U.S. Fleet



General George C. Marshall  
Chief of Staff, U.S. Army

#### NEW PRESIDENT INTRODUCED TO THE SOVIET THREAT

Meanwhile, events in Europe moved rapidly, bringing the war to a close, making it possible to transfer cryptologic resources from the German problem to such projects as BOURBON. On 25 April, the Soviet Red Army encircled Berlin. Five days later, Hitler committed suicide. Eight more days later, Germany surrendered, and V-E Day was at hand. Only four days after that, on 12 May 1945, British prime minister Winston Churchill offered his first "iron curtain" metaphor for the Soviet threat in a telegram to President Harry S. Truman (Churchill would not give his "iron curtain" speech in Fulton,

~~TOP SECRET UMBRA~~

Missouri, at which time the phrase became a public byword, until almost a year later, on 5 March 1946).



**Winston Churchill**  
Prime Minister, Great Britain



**Harry S. Truman**  
President, United States

While the Truman Doctrine, which enunciated America's policy to contain the expansion of Soviet communism, was not fully developed until March 1947, the Soviet problem was laid on Truman's plate his first day in office on 13 April 1945. On that date the secretary of state, Edward Stettinius, sent Truman a special report which, among other things, related Britain's "increasing apprehension of Russia and her intentions" and U.S. concerns over a "puppet regime of Russia's own making" in Poland, and of Soviet "unilateral political interference in [the Balkans]."<sup>2</sup> In fact, the first three months of Truman's presidency, which included the United Nations Conference at San Francisco (25 April - 26 June 1945), were taken up heavily with problems caused by the Soviet Union's intransigence over Europe and the UN Charter.<sup>3</sup> Within eight months, Truman saw the possibilities of war with the Soviet Union:

There isn't a doubt in my mind that Russia intends an invasion of Turkey and the seizure of the Black Sea Straits to the Mediterranean. Unless Russia is faced with an iron fist and strong language, another war is in the making.<sup>4</sup>

### **ABYSMAL ABSENCE OF INTELLIGENCE ON USSR**

While the Soviet military threat was made real by its presence throughout Eastern Europe, Allied knowledge of Soviet military capabilities was made significant by its relative absence, particularly if one can believe an April 1945 memorandum from a United States Army lieutenant to a wing commander at the British Air Ministry. The American officer raved about the windfall of information on the Soviet Air Force acquired from captured German documents. He was excited because the Germans had reconstructed "a substantially complete Order of Battle of the Soviet Air Force *on the Soviet-German front* [emphasis added]," which in fact would have represented only a fraction of a complete

Soviet military order of battle (OB). Discussion of aircraft strength reports showed that the Allies did not know if the Germans were presenting "first line" figures or "maximum capability" numbers, allowing the inference that the Allies probably had no independently derived numbers in which they had much confidence.<sup>5</sup>

This also showed what little the Allies knew about Soviet military capabilities in the Far East. Earlier intelligence reports alleged that Japanese "couriers traveling through Siberia reported having seen 500-600 aircraft being shipped to the East," which was presumably corroborated by a report from an American pilot who had several months earlier traveled through Siberia, observing that the Soviets were moving a substantial number of aircraft eastward on the Trans-Siberian railroad.<sup>6</sup> This was not much with which to construct a force-wide OB of national scope.

So, by mid-1945 all the organizational elements had come together. The approaching end of the war would free up the resources to make BOURBON *possible*. Meantime, the newly identified Soviet threat was emerging, and a serious intelligence gap relative to the Soviet Union was recognized. These two circumstances made BOURBON *necessary*.

#### MID-YEAR SCORE: NAVY 1, ARMY 0

The earliest covername for the Soviet problem was RATTAN, adopted by Op-20-G and probably ASA (then called SSA) in February 1945;<sup>7</sup> it gave way five months later to the BOURBON moniker.

But before concentrated and coordinated U.S. cryptologic efforts could begin against the Soviet target, the American military components had to sort out their differences. The Army and the Navy accepted the fact that they had to work better together cryptanalytically. But they still held different views on how. On 13 June, the Navy submitted an extensive and elaborately detailed proposal for coordinated "joint" but still "independent" Army and Navy efforts against the Soviet Union:

- The Army and Navy will maintain *coordinated and independent* [emphasis added] D/F [direction finding] activities, intercept activities, communications systems, processing centers, research centers, and coordinated and semi-independent dissemination.
- A Joint RATTAN Allocation Control and Joint RATTAN Security Control shall be formed whose function is to: (a) allocate unsolved systems. . . ; [and] (b) control dissemination and security of Communications Intelligence from RATTAN sources.
- A Joint RATTAN Intercept Sub-committee shall: (a) exchange frequencies and calls; (b) standardize circuit designations; (c) allocate coverage, [and] (d) standardize intercept message forms, filings systems, and nomenclature.
- [A] Joint RATTAN Cryptographic Intelligence Center and Joint RATTAN Raw Traffic Exchange Center shall be formed, whose function is to: (a) collect, evaluate, and exchange fully all cryptographic intelligence, and disseminate rapidly to processing centers; (b) standardize system designations. . . ; (c) assign unsolved systems . . . (d)

handle and sort raw traffic on non-workable systems . . . ; [and] (e) maintain [the] master file of all intercepts, regardless of source.

- A Joint RATTAN Collateral Information Center, and Joint RATTAN Communications Intelligence Center shall be established to: (a) collect, process, and disseminate collateral information to processing centers; [and] (b) maintain central file of all RATTAN Communications Intelligence, regardless of source.
- Each service shall have access to all intercepted traffic, code and cipher recoveries, and cryptanalytical techniques in the possession of the other.<sup>8</sup>

Five days later, Signal Corps lieutenant colonel Frank Rowlett (renowned as a member of the small Friedman team which broke the Japanese Purple diplomatic cipher and for his work designing American cryptographic equipment), who was now chief of SSA's General Cryptanalytic Branch, critiqued the Navy's proposal. First, Rowlett pointed out, with qualifications, some advantages of the proposal:

Duplication in certain aspects of the problem would be avoided, and . . . both services would share equally in receiving credit for successes in RATTAN solution. A tangible basis of operations is provided through joint policy committees and joint operational control committees. The proposal for a Joint RATTAN Collateral Information Center . . . is a real advantage, but its fullest usefulness could be realized only if the two operating centers are geographically adjacent to it.<sup>9</sup>

Rowlett then strongly criticized the Navy's proposal, giving a long list of disadvantages:

- (1) The proposal if adopted will make permanent a bifurcated effort on a homogeneous mass of material.
- (2) The proposed Raw Traffic Exchange Center is not feasible . . . due to the geographical separation of the two operating centers.
- (3) Duplication of effort will result . . .
- (4) The plan as proposed makes the assignment of unsolved systems a matter of policy . . . contrary to sound practice since only operations personnel are in a position to assess possibilities of solution . . . .
- (5) The proposal [to handle and sort raw traffic on non-workable systems] is not understandable since it does not define 'non-workable' systems.
- (6) The proposed master file of all intercepts . . . is impractical because the advantages accruing therefrom would not justify the additional space, personnel, and filing facilities required . . . .<sup>10</sup>

He squeezed his own counterproposal for attacking Soviet communications in between another barrage of criticism:

The cryptanalysis of RATTAN then should be assigned as the responsibility of one of the two services but not both. The service which is not responsible will allocate cryptanalytic and other personnel to the operation sections maintained by the other service. . . .<sup>11</sup>

Rowlett thought the Navy should have addressed the need for maintaining adequate translation facilities close to the cryptanalysts. He wrote, "Experience shows that translation and cryptanalysis to be effective must be closely connected in physical facilities."<sup>12</sup>

Moreover, he felt that the State Department, whose interest in Soviet diplomatic intelligence was "paramount," should provide support personnel and collateral services to the effort.<sup>13</sup>

Rowlett also found fault with the Navy for leaving the British out of the proposal:

No plan for the future is complete which leaves the British out of consideration. This is because of:

- (a) The expressed desire of the British to collaborate with the Army;
- (b) The known success of the British in the prewar era with RATTAN systems; and
- (c) The traffic resources of the British

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

Rowlett's support of British participation was unqualified:

An important point in this connection is that the British will be able to provide cable and long-wave intercepts which will not otherwise be available. Work on RATTAN with the British will be far simpler if it involves just one American unit . . . thus the British will have no opportunity of playing the Army off against the Navy, and vice versa.<sup>15</sup>

## COLLABORATION GETS THE GO-AHEAD

Viewed fifty years later, it appears that Rowlett was a bit unfair concerning the lack of any reference to the British in the Navy's proposal. Surely, the Navy would say that it was beyond the scope of the specific Army-Navy plan, that there was no intention of leaving out the British. This view is supported by the fact that, while some elements of the Army and Navy cryptologic centers were squabbling among themselves, negotiations were under way between other American authorities and the British specifically addressing a joint attack on the Soviet problem.

For example, two days before Rowlett's criticism went to SSA management, Admiral Hewlett Thebaud (U.S. Navy, chairman of the ANCIB) and the newly promoted General Carter W. Clarke (U.S. Army, deputy chairman, ANCIB) were informed of an exchange of messages between Thebaud - through a British liaison officer, Colonel O'Conner - and Sir Edward W. Travis, director of the Government Code and Cipher School (GC&CS), predecessor to the present Government Communications Headquarters (GCHQ). The message Colonel O'Conner sent to Travis, ironically in a formal, written dispatch conveys the sensitivity of the subject:

~~TOP SECRET UMBRA~~

ANCIB have (*sic*) agreed verbally to complete cooperation at earliest practical date. Am mailing you personally exact copy of full verbal statement made to me by Admiral Thebaud today. Nothing has been put in writing.<sup>16</sup>

And Travis's positive written response was also delicately phrased, particularly in terms of dancing around the name of the target country:

Statement by Thebaud has not reached me but please convey to him, for ANCIB, that arrangement referred to in your paragraph 1 is most welcome and that I am most grateful for their cooperation. On receipt of full statement I will communicate further with you with a view to earliest possible implementation of our understanding on this matter.<sup>17</sup>



**Carter W. Clarke**  
General, U.S. Army  
Deputy Chairman, ANCIB

Meanwhile, in July 1945, Admiral King authorized 743 billets for the Navy's cryptologic effort against the Soviet target; specifically, this allocation was broken down as: "exploitation 418, IBM [processing] 125, intercept coverage 200." At the time, in Op-20-G, 76 officers, 114 enlisted and one civilian (a total of 191) were assigned. Incidentally, total messages received in July were, 6,600, with 308 decrypted and/or translated.<sup>18</sup>

## Chapter 8

### The U.K. Dimension

#### U.S.-U.K LIAISON IN JULY

Given the absence of a decision to give cryptanalytic responsibility on the Soviet problem to one service only (Rowlett's, and presumably the Army's, preference), the inference is that the Navy's coordinated-but-independent proposal won the battle for how the U.S. would proceed. Typically, as the fruit of victory (or the price, depending on one's view of staff work), the Navy was given the task to work out details of the arrangement with the British, again presumably in coordination with the Army. About a month after the Rowlett critique, Captain Joseph N. Wenger reported that Op-20-G and SSA had worked out a plan for handling RATTAN liaison with the British. All liaison with GC&CS would be through U.S. Army or Navy liaison officers representing ANCICC, not their individual service. Wenger added: "It is believed that this is a workable and equitable arrangement from the Navy's point of view and [echoing Rowlett's concern] will minimize the danger of having GC&CS play one service off against the other."<sup>1</sup>



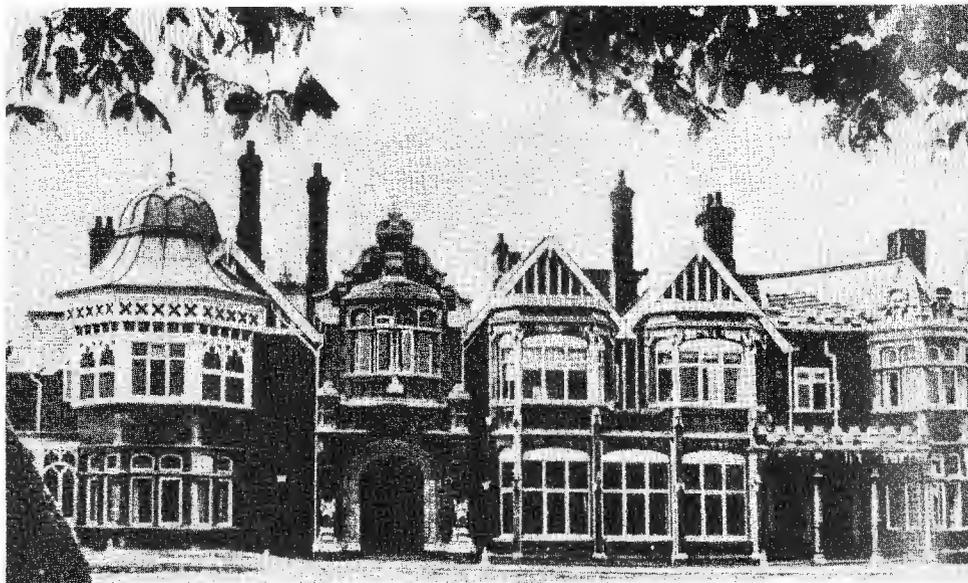
**Sir Edward W. Travis**  
**Director,**  
**Government Code & Cipher School**

Meanwhile, the U.S. Army's liaison officer to Travis' Bletchley Park operation, Major John N. Seaman, was informing SSA that the British were planning to transfer some "good men" to the "exotics," a euphemism for any target but German and Japanese but meaning the Soviet Union in this case. GC&CS was also well along on traffic analysis work against the Soviet Union, a project which had been called "BLUE" but was being relabeled "TAPER." He elaborated:

My tour of BLUE T/A confirms highly able staff about 50 with well planned embryonic organization. Plenty of military traffic which we do not get at all. Card file of 20,000 call signs.<sup>2</sup>

Seaman then warned of the possible consequences of delay in the negotiations and added the status of the British cryptanalytic effort against Soviet cryptosystems: "Doubt I

will be allowed to see [the] cryptanalytic section unless liaison is cleared up," he cabled, adding: "About 30 systems under study."<sup>3</sup>



**Bletchley Park, England  
Headquarters, GC&CS**

Two days later, on 24 July, Colonel W. Preston Corderman, commander of SSA, assured Seaman that planning was under way for complete liaison with GC&CS on the Soviet problem, and announced an important assignment for Seaman:

Plan calls for you to represent U.S. Army and Navy at GCCS and Commander [R.J.] Fabian of U.S. Navy will be principal liaison officer in Washington. Assisting Commander Fabian here will be Colonel Rowlett . . . while Lieutenant Commander [Grant C.] Manson [USNR] will act as assistant to you. Expect entire program will be completed very shortly and details to you will follow.<sup>4</sup>



**W. Preston Corderman  
Colonel, U.S. Army  
Commander, SSA**

While the negotiations were going on, American and British cryptologists were studying "TICOM documents." Contemporary readers of these reports knew what TICOM meant, of course. For those readers new to this historical period, this author among them, it is interesting to discover that TICOM collateral played a big role in BOURBON right from the start. TICOM, acronym for Target Intelligence Committee, was a joint U.S.-U.K. effort after the war to investigate all phases of German and Japanese cryptologic organizations. After the war, TICOM teams composed of U.S. and British officers scoured the German and Japanese countryside, locating their former enemies' COMINT centers and intercept stations and appropriated any COMINT materials that could be found, including hardware, working aids, traffic, etc. They also interrogated as many German and Japanese cryptologic personnel as they could identify and locate.<sup>5</sup>

Although final agreement was still a month off, by late July the main outlines of the Anglo-American cooperation were emerging. By 26 July, the ANCIB had accepted the British proposal to collaborate on RATTAN, agreeing that there should be a full exchange with the British on intercept material and information, on collateral, cryptographic information, and resulting intelligence, and that the collaboration should commence "at the earliest practicable date."<sup>6</sup>

Also on 26 July, the Navy informed its representatives in London of the liaison arrangements and named the liaison officers.<sup>7</sup>

Two days later, the ANCICC authorized Seaman in London to begin formal negotiations and to recommend that GC&CS adopt the code word BOURBON for the project.<sup>8</sup>

On 31 July, in a flurry of messages, the Navy, apparently in the spirit of the technical exchange agreement not yet final, began to report on the status of American work on assorted categories of Soviet cryptosystems, adding at the end a cautionary note about the sensitivity of the collaboration:

Nondiplomatic traffic on hand since February 1944 in following categories: Weather, Plain text, and Miscellaneous, all predominantly Siberian, about 9,000 sheets. Naval traffic mostly Pacific bases, but some Moscow and all mainly in 3 and 5 numeral and 5 character [groups], about 20,000 sheets. . . . For your personal information and guidance, ANCICC has not and will likely not enter into any written agreements on this collaboration; suggest you handle all arrangements orally.<sup>9</sup>



## Chapter 9

### Collaborating While Negotiating

#### THE BOURBON OF AUGUST

August was a very big month for BOURBON; both the covername and the project became official. But many things happened on the way to reaching those milestones.

TICOM interrogations were ongoing. On 1 August, Fabian forwarded to Seaman in London some Navy questions to be asked of German prisoners with cryptologic expertise on the Soviet target:

Were only western Russian systems worked, or was some work done on Siberian systems? . . .  
Dr. Paschke spoke of a Russian Diplomatic one-time pad which was read up to [the German defeat at] Stalingrad; could some of these recoveries be located and forwarded?<sup>1</sup>

Also on 1 August, Seaman met with the director, GC&CS, who had expressed full agreement with and "pleasure at" the decision to work together. Seaman confirmed that technical material, [redacted] was already being exchanged.<sup>2</sup>

If there was any doubt about a technical exchange taking place, a CNO message sent a few days later to Seaman to pass to the GC&CS cryptanalysts would settle the matter.<sup>3</sup>

In answer to GCCS 09647 . . .

[redacted]

Meanwhile, Seaman escorted three American visitors on a tour of the GC&CS's Soviet analysis sections at Bletchley Park. The visitors were Mr. William Friedman, SSA; Mr. Frank Lewis, U.S. integree at GC&CS; and Lieutenant Commander Grant Manson, USNR, who was scheduled to replace Seaman as the Senior U.S. Liaison Officer in London in December.<sup>4</sup>

A later cryptologic history on the origin of NSA summarized succinctly the BOURBON negotiations:

Five years after the initial U.S.-U.K. collaboration in COMINT, the two nations began a new chapter in their cooperation in COMINT matters. Following several months of technical discussions, both in London and Washington, representatives of the London Signals Intelligence Board (LSIB) [the British counterpart to the U.S. ANCIB] and the Army-Navy Communications Intelligence Board on 15 August 1945 informally approved the concept of establishing U.S.-U.K. cooperation on the Soviet problem. . . . This unwritten agreement was predicated on an understanding arrived at by Group Captain Eric Jones, RAF, and Rear Admiral Hewlett Thebaud, [U.S. Navy,] Chairman of ANCIB.<sup>5</sup>

Details of that 15 August approval (which, incidentally, occurred about a week after the atomic bombs were dropped on Nagasaki and Hiroshima and perhaps not-so-

incidentally one day after the Japanese surrender) were reflected in an ANCIB memorandum which documented the British reply to the U.S. proposals regarding BOURBON. The essence of the reply was that the British agreed to drop the coverword RATTAN in favor of BOURBON and that the director, GC&CS, had confirmed "cooperation on BOURBON is to be complete, though informal." British liaison officers were named, and assurances were given that an exchange of technical materials would begin soon.<sup>6</sup>

On 18 August, Admiral King and General Marshall met and approved nine proposals on subjects ranging widely from [redacted] recommendations that the Office of Strategic Services (OSS), Treasury, and the Federal Communications Commission (FCC) be excluded entirely from cryptanalytic activities. Two recommendations are of particular interest in the BOURBON context:

EO 1.4.(c)  
 EO 1.4.(b)  
 PL 86-36/50 USC 3605

- That collaboration with the British be continued and extended as determined by proper authority to be in best U.S. interests; that Signal Intelligence agreements and commitments with the British must be determined finally on a governmental level;
- That when BOURBON reaches stage for dissemination, it be disseminated as joint Army-Navy product...<sup>7</sup>

Early in the month, Seaman had complained to Corderman that he could handle the BOURBON liaison adequately only at the expense of letting slip his "TICOM, diplo[matic] and normal duties."<sup>8</sup> In response, on 25 August Rowlett asked Seaman to nominate Commander E.W. Knepper, USNR, to the director, GC&CS, for receiving clearance to work in their Soviet section while on three months' temporary duty from the United States.<sup>9</sup> This noncontroversial request apparently came at an touchy time for the British. It had interesting ramifications. (Meanwhile, also on 25 August, the first pouch of Soviet traffic copied by the British arrived in Washington.)<sup>10</sup>

Three days later, on 28 August, the British liaison officer, in his response on Knepper, revealed one of the sources of sensitivity and desire for compartmentation on this project:

Travis must refer Knepper clearance to chief because at this time with prospect dissolution Combined Chiefs of Staff whole question post war collaboration will be under review. He is most anxious to continue it but may not be able to do so quite as openly because of possible necessity to conceal it from Foreign Office elements.<sup>11</sup>

Not to worry. These dark clouds over the British Isles quickly dissipated: "BOURBON collaboration soon resulted in a broad exchange of operational materials between the COMINT centers of both nations..."<sup>12</sup>

Indeed! But there was a bit more to it than that. From the beginning, it was clear to all that many people had already been working on many Soviet systems for a considerable length of time. The August publications of GC&CS product (see p. 43) showed much British work on Soviet systems. Now, a 31 August 1945 memorandum from the U.S. side presented impressive statistics on the status of the American effort already directed against the Soviet problem:

- a. Navy: 192 (61 officers, 131 enlisted);
- b. Army: 99 (5 officers, 94 civilians); and
- c. Systems: 35, of which:
  - (1) 6 were diplomatic, 2 in process of solution; and
  - (2) 29 were "non-diplomatic" of which 4 were being read (2 enciphered codes and 2 substitution systems);
- d. Intercepts: 12,500 messages, of which 6,000 were diplomatic; and
- e. Collateral: 10,000 separate items, "on 60,000 cards."<sup>13</sup>

There it was in black and white; almost 300 Americans were already at work on the Soviet problem, and thirty-five cryptosystems were already identified. For the past year each service had been training language personnel, and the numbers of working linguists were currently adequate. But because of expected losses through impending demobilization, "further attention will have to be given to this matter."<sup>14</sup>

### PROJECT DOCUMENTATION

Despite being compartmented (or because of it), the BOURBON project was well documented, with status reports exchanged between the principals every two weeks. Addressed in each U.S. report was a list of liaison activities, an accounting of what was received from and sent to the British, highlights of cryptanalytic progress, and contributions made by collateral materials, particularly TICOM materials.<sup>15</sup>

The TICOM section of the semimonthly reports provided details of the contents of recovered German documents acquired from the teams. The 31 August report noted, for example, receipt of photographs of an unspecified type of "cryptomachine," about which details would be provided after study.<sup>16</sup> Subsequent analysis of these photographs showed that the equipment was a Soviet version of the Hagelin B-211 cipher machine.<sup>17</sup>

The Exchange section of these reports listed all technical materials sent to London and received in Washington. The initial report was fairly representative of what was exchanged for the next three and one-half years:



EO 14.(c)  
EO 14.(b)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

All BOURBON material, at the preference of the British, presumably for security reasons as well as volume, went not electrically but by pouch across the Atlantic.<sup>19</sup>

### ALLIED GIVE-AND-TAKE

A good working relationship did not mean there were not disagreements between the British and Americans. In one case, Army's Military Intelligence Service (MIS; also called G-2), which controlled the intercept sites in 1945, refused a British request to provide

[REDACTED] It is not clear why the Army refused. Since this issue was addressed in a status report on BOURBON, it is assumed that the British request was for Soviet collection. But the [REDACTED] apparently did not have a Soviet mission in August 1945, because General Corderman, chief SSA, the next month made his case to MIS that one be established:

[REDACTED]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

It is possible, too, that the British request was for non-Soviet intercept, which of course would have fallen outside the BOURBON charter and would explain why the Army refused.

Illegible, usually hand-copy, intercept dogged the British for years. An early example of an American attempt at improvement in this area was seen in August 1945 when the British were urged to "adopt typewriter copying in order that both Op-20-G and SSA would receive legible copies of intercept."<sup>22</sup>

Intercept problems went beyond illegible copy. There were also complaints that the

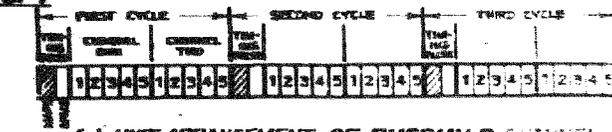
[REDACTED] "Baudot" was the term used in the 1940s to describe Soviet teleprinter. The term originated with a Frenchman named Baudot who had invented a five-unit printer code which the Soviets adapted to conform with the peculiar characteristics of the Cyrillic alphabet. Each letter or character was of equal length, being made up of five positive or negative currents (represented by marks or spaces).<sup>23</sup> The intercept copy consisted of a continuous "squiggly" line on half-inch-wide paper (undulator) tape. The up-and-down squiggles represented letters, numbers, and punctuation marks, but someone had to hand write the Cyrillic letters, Roman numbers, etc., on the tape, a time-consuming and tedious task, before cryptanalysis could begin.<sup>24</sup>

**FIG. 3**

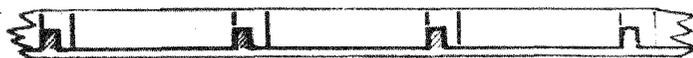


*BAUDOT TYPE TRANSMITTER KEYBOARD*

**FIG. 4**



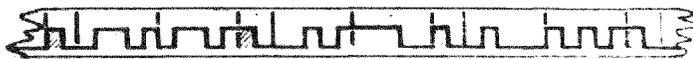
*(a) UNIT ARRANGEMENT OF RUSSIAN 2 CHANNEL*



*(b) SENDING ONLY THE TIMING PULSE*



*(c) CHANNEL ONE SENDING*



*(d) BOTH CHANNELS SENDING*

**Baudot-type transmitter keyboard and undulator tape arrangement**



**Example of Baudot intercept transcribed with Cyrillic and Roman equivalents**

EO 1.4.(b)

EO 1.4.(c)

PL 86-36/50 USC 3605

**THE SPIRIT OF DOE**

The division of effort between the two Allies was straightforward, although there was (as there still is) a certain amount of duplication of effort on systems perceived by each partner as particularly critical to its own nation's interests. By reviewing the status reports of the two sides' cryptanalytic attacks on the Soviet systems, it is clear immediately that the British were working primarily on Soviet traffic intercepted from European sites, while the U.S. emphasized Soviet Far Eastern intercept. One of the main



**UNLIKELY BETROTHAL OF U.S. PARTNERS**

In addition to getting the BOURBON project to fly in August 1945, ANCIB authorities were still in a centralization mood. They toyed with the possibility of launching a real marriage of the Army and Navy cryptologic activities. The ANCICC even established a Subcommittee on Merger Planning whose major task was to recommend the site for unified operations.<sup>26</sup> Of course, that was a flight of fancy. It never did get off the ground until the creation of the Armed Forces Security Agency (AFSA) in 1949, and even that early creature, like Howard Hughes' wooden airplane, the "Spruce Goose," did not fly far before finally being replaced by NSA in 1952.<sup>27</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

## Chapter 10 The Effort Expands

### SEPTEMBER SUCCESS

The all-too-brief engagement for a wedded Army-Navy cryptologic operation was broken off in September 1945 when "higher naval authorities" concluded that a complete physical merger was "inadmissible," offering as an alternative an agreement to take steps to improve coordination of the two cryptanalytic activities. As a consequence, American participation in BOURBON remained a "joint effort under joint direction."<sup>1</sup>

Meanwhile, Allied COMINT generally (of which BOURBON was a specific example) quickly received the highest level of U.S. government support; on 12 September, President Truman added his august approval to the alliance by authorizing "the Army and Navy to continue collaboration in the field of communication intelligence with the British."<sup>2</sup>

### PROBLEMS WITH INTERCEPT QUALITY AND FORMAT

Meanwhile, relations between the Allied cryptologists remained spirited. The

[REDACTED]

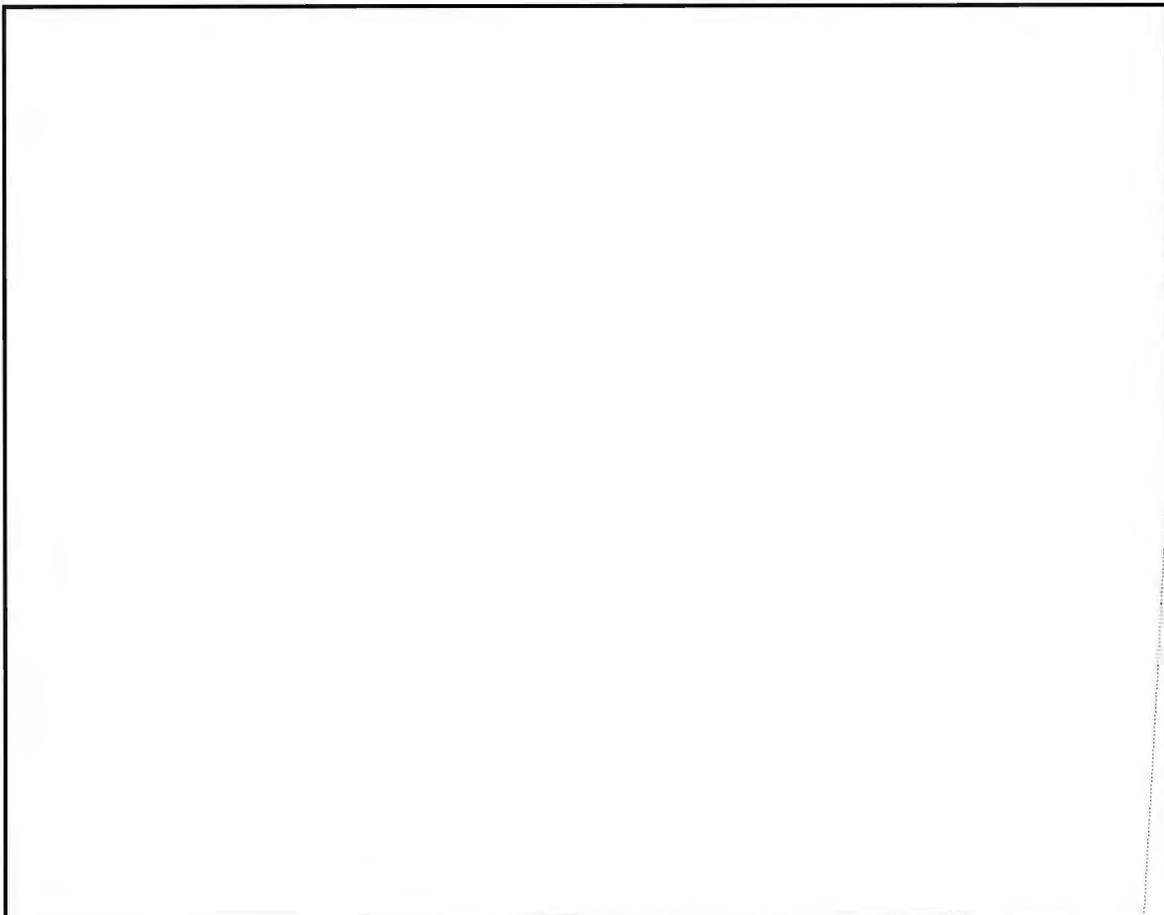
The term IBM processing referred, not to computer processing per se but to the keypunching, card indexing, and printouts of various sorts by IBM statistical machines of the major elements of cryptograms, including significant externals (callsigns, frequencies, etc.) and what were believed to be the important cipher and message text groups such as the initial (A1, A2, A3) textual groups, the final (Z2, Z1, Z0) groups, circuit serial numbers, indicator groups, etc. Programmable computers were not yet in general use for aid to cryptanalysis.<sup>3</sup>

[REDACTED] Rowlett admitted to some variance:

[U.S.] Navy intercept operators copy BOURBON transmissions on Russian-character typewriters. Army uses all-capitals Latin letters typewriter (MC-88) and copies international Morse equivalents of Russian characters . . . Minor variations exist in order of appearance of material on traffic copied by Army and Navy. On Navy traffic, for example, intercept date and time commonly occur at the end of the message, while Army includes this information in the heading placed on messages. . . .<sup>4</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

[REDACTED]



**EARLY CRYPTANALYSIS**

Back in 1945, however, after only one month of existence for the BOURBON project, Frank Lewis, the ASA integree (SSA was renamed the Army Security Agency on 15 September 1945) at GC&CS, reported that he saw the first phase of the Soviet problem complete; he also commented on the status of a couple of cryptosystems, which makes it necessary to introduce the reader to the extraordinary and various naming systems for Soviet cryptosystems that emerged during the BOURBON collaboration:

The BOURBON problem seems to have passed its first phase here where they were feeling their way through preliminary identifications, tentative cryptanalytic attacks, etc., and the next phase of settling down to well-defined solution activities is near. There are several four-figure systems which are developing into fairly large-scale enterprises, and with the several three-figure systems, the [mixed figure and letter cipher] [redacted] [redacted] and the [5-figure cipher] [redacted] which the Brigadier [presumably John Tiltman] is studying, a rather clear-cut program seems to be forthcoming.<sup>7</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

An enterprising cryptanalyst-writer could make a career out of explaining the naming systems used for Soviet cryptographic systems in the 1940s. At least seven different

naming systems were in use at one time or another. Early on, Op-20-G (and probably GC&CS) used a one-up system prefaced by the letter [redacted] which was changed to the letter [redacted] and used briefly by the U.S. Navy and the British. Then the British introduced such terms as [redacted] to describe individual cryptosystems, before settling on the [redacted] naming system (e.g., [redacted] for five-letter systems, [redacted] for four-figure military and air systems, [redacted] for mixed figure-letter systems, etc.). (See Appendix A for a listing of [redacted] and their equivalent cryptosystems types.) ASA, working mostly Soviet [redacted] systems at the time, preferred to use a three-letter system, [redacted]

[redacted] and a third letter, added presumably one-up alphabetically, which gave the titles this look: [redacted] etc. In fact, the [redacted] system mentioned above was classified initially as [redacted] Another, generally universal system was finally introduced in 1946 (see Part Three and Appendix B).

As Frank Lewis indicated, solutions were indeed near. In September, a Soviet [redacted]

[redacted] While the decrypts provided nothing of intelligence value, they contributed significantly in traffic analysis work.<sup>9</sup> Two months later, the TICOM effort acquired a German SIGINT report that contained 4,000 code recoveries [redacted] 2,000 of which were identical with local recoveries, 500 of which were new, and the remainder of which were values which had not yet appeared in "Siberian" traffic.<sup>10</sup> (The term "Siberian" was usually used in the 1940s to refer to the Eastern part of the Soviet Union, from the Urals to the Soviet Far East.)

**THE GOUZENKO AFFAIR**

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

September also provided Allied cryptanalysts with some interesting collateral information on Soviet cryptography, but more importantly it gave the Allies significant insight into Soviet espionage activities. Igor Gouzenko, a code clerk assigned to the Soviet military attaché in Ottawa, working out of the Soviet embassy there, defected to Canadian authorities on the night of 5 September. Rowlett interviewed Gouzenko (code name CORBY) in Canada between 25 and 29 September (GC&CS officials also had access to him).<sup>11</sup>

Allied cryptanalysts learned more about *why* they were unable to read most Soviet diplomatic messages. For normal communications, the messages were protected by [redacted]

[redacted] It was based on one- and two-digit equivalents for the Cyrillic alphabet, enciphered by a one-time key [redacted]

Perhaps the most important cryptologic information learned by the Allies was that the NKVD was responsible for preparation, control, and use of the cipher systems and for the

training of the code clerks. Soviet communications security was considered by Rowlett to be "extremely high." Incidentally, while readability may have been nearly impossible, access was not; once the telegram was enciphered, it was simply filed with the local commercial telegraph office for transmission to Moscow.<sup>13</sup>

Gouzenko's defection became public knowledge in 1946 when journalist Drew Pearson, in his 3 February ABC radio network broadcast, reported that Canadian prime minister Mackenzie King had informed President Truman about a Soviet agent who had surrendered to Canadian authorities. Gouzenko reportedly had exposed the existence of a Soviet spy network in the United States and Canada which had, among other things, surveyed North American rivers and waterways and had acquired maps of those parts of Canada which were next to Siberia.<sup>14</sup>

Looking back fifty years, the practice of using the term BOURBON in the place of the country name, Soviet Union, would seem to have fooled no one. Rowlett wrote a detailed analysis of the Gouzenko defection and never once used the names Russia or the Soviet Union. He titled the paper "Special Report on BOURBON Cryptography," with chapter headings entitled "Report on Interrogation of Corby" and "BOURBON Cryptography," but openly in that text he provided the code clerk's Russian name and wrote right up front that the clerk was "assigned to the Soviet Military Attaché, in Ottawa, Canada." Rowlett went on to mention "authorities in Moscow" and to describe how personnel of the "Soviet Embassy" broke into Gouzenko's apartment shortly after he defected, etc. The entire twenty-one-page report was strewn with Russian terms, letters of the cyrillic alphabet, and references to the NKVD.<sup>15</sup> No one privy to the report would have the slightest doubt what target nation was involved. What kind of compartmentation was this? Reference *could* be made to the titles of the documents, of course, without giving away the actual name of the target country. Although it is puzzling, it probably all made sense at the time; Rowlett and his cryptologic colleagues on both sides of the Atlantic were serious people, and they took security very seriously.

## **MORE COLLECTION, COLLECTORS, AND LINGUISTS**

Concurrent with the Gouzenko affair, the U.S. Navy kept developing new collection positions targeting Soviet communications. On 7 September, they sent sixteen officers and enlisted collectors to Port Lyautey, French Morocco, to open a "BOURBON intercept station at the Naval Air Station at that place" and twenty collectors to Wahiawa, Territory of Hawaii, for the same reason. Also, twenty-two more officers completed Russian language training at Boulder, Colorado. It was transfers like these that swelled the Op-20-G Soviet work force to 243 by the end of the month.<sup>16</sup>

The first Soviet traffic copied at Wahiawa arrived at NCAW in October. Also, GC&CS's Brigadier Tiltman visited the Navy section on 15 October, and Travis himself toured the offices on 5 November. Despite fourteen more naval officers having just graduated from Russian language school at Boulder, arriving for duty at NCAW,

apparently substantial demobilizations had cut the Soviet work force to 149 by December, down ninety-four people in three months.<sup>17</sup>

While this history attempts to survey *all* the known main elements of the Allied cryptologic effort against the Soviet Union, there is one area which has been for the most part left to others; that's the story of a select portion of Soviet clandestine or "agent" communications, reflected in diplomatic channels and generally covered under the rubric "the VENONA intercepts." This material was acquired during the early 1940s but not exploited until late in the decade. It was used primarily for counterintelligence purposes in conjunction with Federal Bureau of Investigation (FBI) investigations and surveillance, contributing important leads in exposing the Soviet atomic spy ring in the early 1950s, among others.<sup>18</sup>

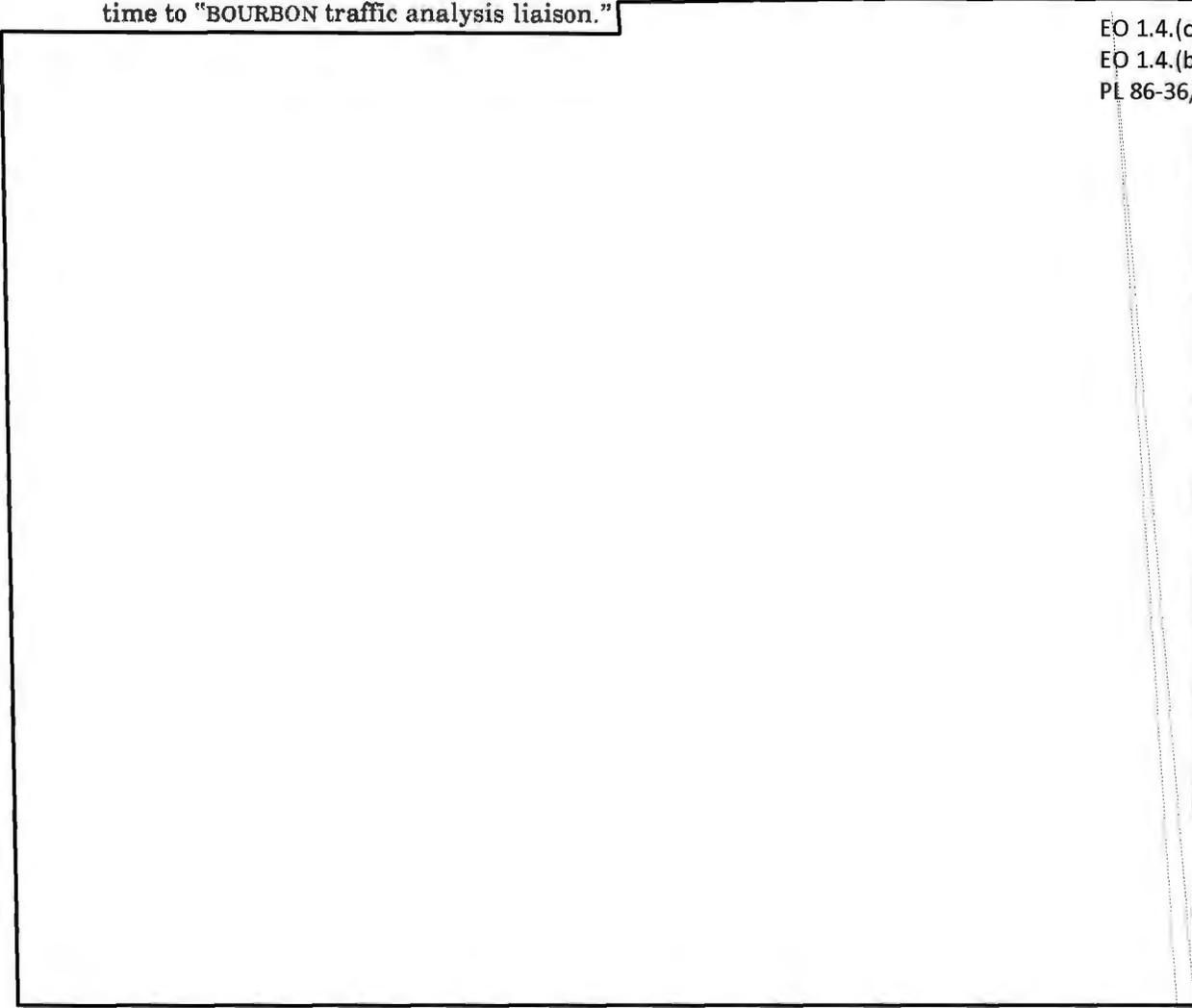


Chapter 11  
Progress, Problems and Promise

THE EFFORTS OF OCTOBER

Early BOURBON was primarily the cryptanalysts' show. But traffic analysis soon began playing a more visible supporting role. In October, for example, a Major John Manson, British Army, was relieved of his other liaison duties in the United States to devote full time to "BOURBON traffic analysis liaison."

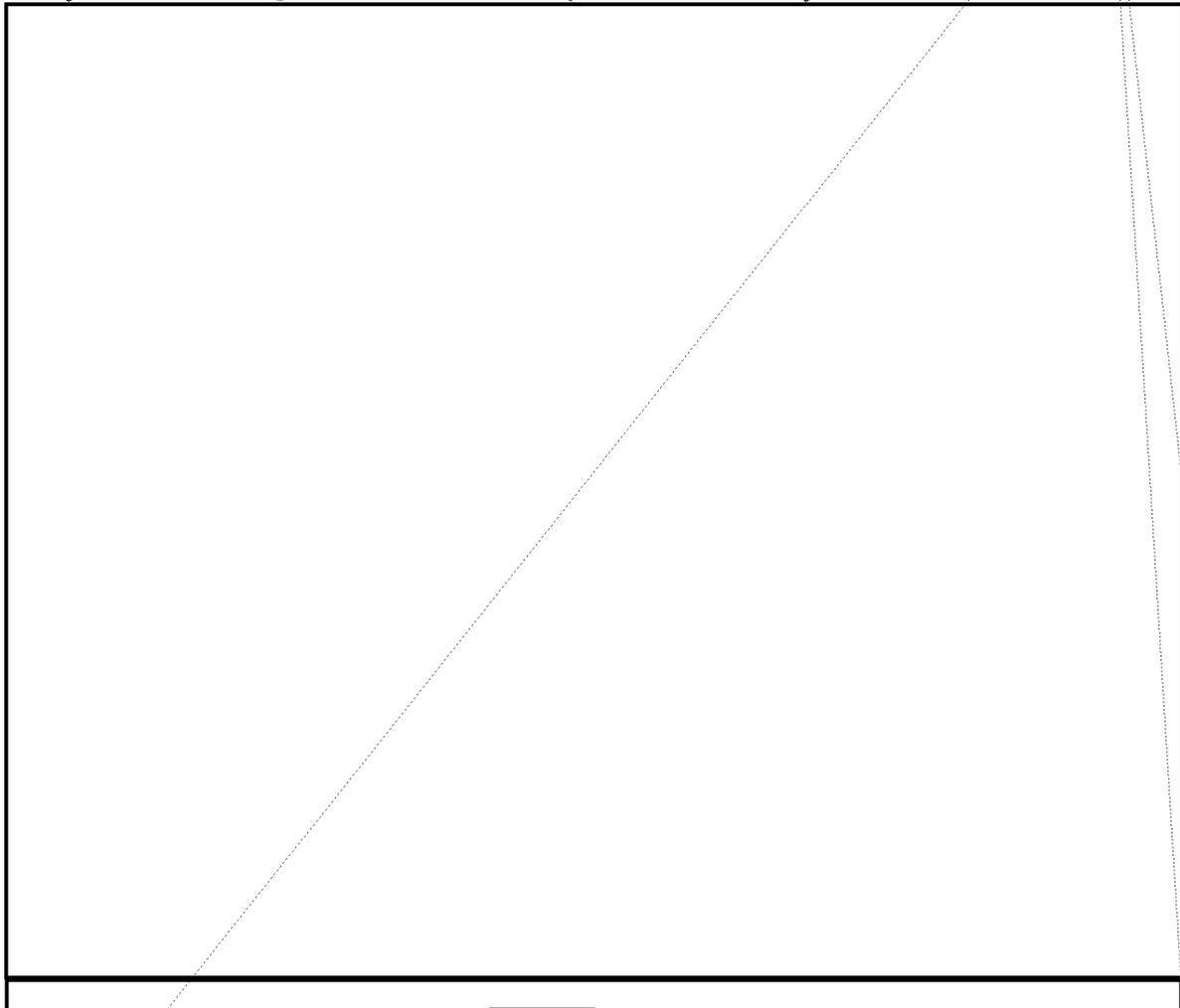
EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



The term Monster referred to any ocean-going vessel capable of twenty-plus knots, which allowed it to proceed independently, without convoy, during wartime. Two well-known "Monsters" used during this period were the HMS *Queen Elizabeth* and HMS *Queen Mary*, which at this time were in wartime livery

and which could cross the Atlantic in four to five days. The other seaborne shipping method was by packet ship, which took up to twelve

days between Liverpool and New York City. When the two Queens were demobilized in



[redacted] About a month later, the [redacted] system was found to be using [redacted]

Meanwhile, the TICOM people in the Pacific had acquired a Japanese document revealing "tentative identification of all BOURBON submarines, destroyers, two heavy cruisers, and one light cruiser." In addition, they had interviewed a Japanese lieutenant commander who allegedly had extensive knowledge of Soviet military and cipher systems:

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Principal codes used by Soviet Navy are 5-numeral [5-digit] systems; a 5-letter code was also used but volume . . . was low. NKVD and Navy also used 4-numeral systems; one of the two used by NKVD was a one-time pad. Russian Air Force used a 3-numeral code, a simple substitution system easy to read when sufficient traffic was intercepted; changed frequently. Russian submarines used a 3-numeral code which was not broken; messages were always very short; thought to be an abbreviated procedure system.<sup>10</sup>

There was a bit of a misunderstanding between the partners in connection with the B-211 Hagelin cipher machine, which the TICOM people had acquired and photographed,

but which had come ultimately into the physical possession of the British. A report to ANCICC gives the reader the flavor of the problem:

By reason of an erroneous assumption made by the British in connection with the study on the B-211 Hagelin machine, considerable confusion has resulted and progress has been slow. It has been, further, necessary [redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

[redacted]

Calmer heads prevailed, as it may have just been a misunderstanding.<sup>12</sup> Regardless, on 1 November [redacted]

Later in October, Brigadier Tiltman, visiting Washington, candidly hung out some British dirty linen by explaining that the U.S. could expect a notable drop in the volume of [redacted] "by reason of personnel losses and lack of interest by personnel expecting to leave the service."<sup>15</sup>

On 15 October, a meeting was held in Washington between the ANCIB members and a GC&CS party led by its director, Sir Edward Travis (Tiltman was part of this party). Discussions centered on the postwar scope of Allied collaboration, with the BOURBON project presented as the *model* for extended cooperation in "all branches of communications intelligence and on all tasks." Agreements reached at this meeting eventually evolved into the BRUSA Agreement, signed in March of the following year.<sup>17</sup>

### THE PROMISE OF NOVEMBER

In November 1945, automatically enciphered Soviet mixed letter-figure teletype traffic (identified in November as [redacted] was seen for the first time by Army intercept sources. It was considered noteworthy at the time that much of the intercept did not duplicate British sources.<sup>18</sup> [redacted]

[redacted]

Small but significant cryptanalytic successes followed one upon another. A [redacted] proved to have a pad indicator system "somewhat like other diplomatic systems." And the Far Eastern Army Net 4-letter traffic appeared in bulk for the first time; some analysts believed that "this may be the long awaited machine traffic."<sup>20</sup>

Two weeks later, further cryptanalytic progress was reported. A new [redacted] [redacted] was isolated and in the process of solution. The basis of the [redacted] [redacted] was recovered. In the diplomatic cipher arena:

Messages in one code, [redacted] [redacted] This work is now being pushed.<sup>21</sup>

Progress in the exploitation of Soviet systems required an expansion of the exchange agreement. In December, the U.S. directed the immediate exchange with the British of [redacted] probably as oversight in the initial agreement.<sup>22</sup>

Also in December, the indicator system for the [redacted] was solved. [redacted] was the GC&CS [redacted] name for a high-echelon Soviet naval system transmitted in five-digit groups. A [redacted] the underlying code, and attempts were being made to isolate [redacted] This solution, however, was a long way from the reading of clear text.

Additional benefits of a cryptanalytic nature accrued from the study of TICOM-acquired Japanese material on Soviet systems:

A study of stereotypes of recovered message [redacted] shows that probably valuable data can be gained from them. Such study of routines is now in its infancy in the BOURBON problem and is an example of the adaptation of techniques taken from Japanese work.<sup>24</sup>

In the plaintext area, a somewhat gloomy tone clouded the generally sunny picture of general progress being made in BOURBON:

A project of scanning all [Russian] plain text traffic from Army intercept sources shows that, as had been believed, a very small percentage of messages have general intelligence value.<sup>25</sup>

Within a year these clouds, too, would dissipate as the intelligence value of plain text would increase dramatically.

GC&CS, which had undoubtedly been embarrassed by its recent collection problems brought on by demobilization of its collectors, rebounded dramatically in December 1945, [redacted]

Plans for expansion of Soviet collection were under way in December 1945. U.S. Naval Station ABLE on Guam<sup>27</sup> would soon take on a new Soviet mission. The message to the station also displayed a great deal about the BOURBON project, especially its sensitivity and need for compartmentation, and accurately predicted plans for its decompartmentation in the future:

It is contemplated that, in the near future (probably shortly after 1 March 1946), a certain amount of Russian intercept will be undertaken at ABLE. Initially ABLE's share of this work will be the intercept of certain high speed morse and non-morse circuits, for which suitable equipment will be provided. Thereafter, ABLE will participate increasingly in Russian

intercept and will eventually be required to maintain a number of manual morse intercept positions. Trained personnel for all phases of the work will be provided in due course. . . . Communication intelligence effort against Russian targets is designated by the code word "BOURBON". *For obvious reasons* [emphasis added] BOURBON activity is, for the present, accorded greater security than any other communication intelligence activity. Knowledge of the existence of BOURBON and the meaning of the word must be limited to the minimum practicable number of persons, and BOURBON operations must be segregated from other operations. It is contemplated that this restricted circulation of information and segregation of activities will continue until all reserve personnel have either left the organization or transferred to the regular Navy. When the COMINTORG has settled into its post-war status, manned entirely by permanent personnel, BOURBON will share the security status of all other communication intelligence activities and will, probably, in fact, become the organization's principal task.<sup>28</sup>

#### FOUR MONTHS DOWN THE ROAD

Thus ended the first four months of the BOURBON project, a period more about starting than achieving, more about process than results, more about early and esoteric cryptanalytic solutions than readable, intelligence-producing, decrypts.

When 1945 began, Britain and America were still at war, still five months from a victory few could see and desperately turning back the German offensive in the Battle of the Bulge. Fighting was still heavy in Italy. In the Pacific, while it was apparent that Japan had lost the war, she would not admit defeat and continued to fight on for another eight months. The Philippines were still under Japanese control, and Iwo Jima and Okinawa had not yet been recaptured.

By the end of 1945, however, it was a different world. The war had been over for almost four months, and the threat of the Soviet Union loomed foremost on Allied military minds. In the secret world of cryptology, British and American officials had hammered out a new "informal" relationship in regard to the Soviet target.

Sure, there were problems. The Americans complained about British illegible hand-copy and garbled printer intercept. The British would have nothing to do with fanfold paper. Both nations struggled with timely and affordable methods of shipping traffic across the Atlantic. Standardization of intercept media plagued both partners. Each had its own, differing views about how cryptosystems should be named. But despite the expected problems of two proud nations "separated by a single language" working together on a politically sensitive, highly secret project, they nonetheless were freely exchanging liaison officers, enormous volumes of intercepted traffic, cryptanalytic and traffic analytic techniques, technical analyses, and cryptographic descriptions and hardware. They were sharing successes. Finally, they were preparing to do much more of the same, together.

Notes

**Chapter 6: Introduction to BOURBON**

1. (U) Thomas L. Burns, *The Origins of the National Security Agency, 1940-1952* (Ft. Meade, MD: Center for Cryptologic History (CCH), NSA, 1990) (~~TS/CCO~~), 1-20, provides an excellent primer on both the British-American negotiations and the U.S. Army-U.S. Navy coordination efforts. Bradley F. Smith, *The ULTRA-MAGIC Deals: And the Most Secret Special Relationship, 1940-1946* (Novato, CA: Presidio Press, 1993), provides an outsider's view of the British-American cryptanalytic partnership. Based exclusively on unclassified sources, it may be worth the while of a reader interested in the origins and early struggles of this most unusual "special relationship."

**Chapter 7: U.S. Preparations for BOURBON**

1. Burns, 24.
2. Harry S. Truman, *Memoirs, Volume One: Year of Decisions* (New York: Doubleday & Co., 1955), 14-16.
3. Ibid, 9-296.
4. Ibid, 552.
5. (U) Memorandum for Wing Commander A.D. McDonald: A.I.3, [British] Air Ministry from Gordon D. Stott, 1st Lt., U.S. Army, subject: Soviet Air Force, 27 April 1945 (~~TSC~~); CCH Collection, Series XI.B.2.14.
6. Ibid.
7. NCA informal history.
8. (U) Op-20-3-G memorandum, unaddressed and unsigned, subject: Proposed plan for the coordination of U.S. Army-Navy Communication Intelligence effort on the RATTAN project, 13 June 1945 (~~TS~~); NSA/CSS Archives, Accession No. 4832, location G05-0302-3.
9. (U) SPSIB-3 memorandum from Lt. Col Rowlett for Colonel Hayes, subject: Comments on Navy proposal for RATTAN, 18 June 1945 (~~TS~~); NSA/CSS Archives, Accession No. 4832, location G05-0302-3.
10. Ibid.
11. Ibid.
12. Ibid.
13. Ibid.
14. Ibid.
15. Ibid.
16. (U) U.S. Fleet, Hq of the CIC, Navy Department memorandum from Capt. Smedberg (ANCICC staff officer) for Admiral Thebaud and General Clarke, subject: RATTAN, 16 June 1945 (~~TSC~~); CCH Collection, Series IV.AA.6.1.

17. Ibid.

18. NCA informal history.

### Chapter 8: *The U.K. Dimension*

1. (U) Op-20-G (Wenger) memorandum for Op-20, subject: RATTAN Liaison, 16 July 1945 (~~TS~~), CCH Collection, Series IV.AA.6.1.

2. (~~S~~) GCCS message from Seaman to SSA (SPSIS-9), 22 July 1945 (~~TSC~~), NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

3. Ibid.

4. (U) SSA (SPSIS-1) message from Corderman to Seaman, 24 July 1945 (~~TSC~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

5. (~~S~~) Oliver R. Kirby, "The Origins of the Soviet Problem: A Personal View," (~~TSC~~), *Cryptologic Quarterly*, Winter 1992, 51-58.

6. (U) SSA (SPSIS-1) memorandum from Robert T. Walker, Major, Signal Corps, Executive Officer, to Chief, Military Intelligence Division, subject: RATTAN Liaison, 26 July 1945 (~~TSC~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

7. (U) CNO message for COMNAVEU, 26 July 1945 (~~S~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

8. (U) Op-20-G message for Seaman (~~S~~), 28 July 1945; NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

9. (U) CNO messages (AO 56243, 56244, 56245 and 56246) to COMNAVEU for Seaman, 31 July 1945 (~~S~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

### Chapter 9: *Collaborating While Negotiating*

1. (U) OIC, Op-20-3, memorandum from Fabian to Seaman, subject: Questions on Ticom Documents, 1 August 1945 (~~TS~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

2. (U) Op-20-G memorandum for Secretariat of ANCICC, subject: Progress Report on Special Project, (~~TS~~), 8 August 1945; CCH Collection, Series IV.AA.6.1.

3. (U) CNO message (AO 58642) for COMNAVEU (for Seaman to pass to Manson), 8 August 1945 (~~TS~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

4. (U) Seaman memorandum, subject: BOURBON, 8 August 1945 (~~TSC~~); NSA/CSS Archives, Accession No. 10336N, location G09-0707.

5. Burns, 25.

6. (U) Admiral Hewlett Thebaud, Chairman, ANCIB memorandum for General Bissell, Admiral Redman and General Corderman, subject: British Reply to US Proposals regarding RATTAN (BOURBON), 15 August 1945 (~~TS~~); CCH Collection, Series IV.AA.6.1.

7. (U) ANCIB draft memorandum for General Marshall and Admiral King, subject: Signal Intelligence, 21 August 1945, (~~TS~~); CCH Collection, Series IV.AA.6.1; and 22 August signed memorandum, (~~TS~~); CCH Collection, Series V.F.1.10.

8. (~~S~~) GCCS message from Seaman to Corderman, 7 August 1945 (~~S~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

9. (U) Informal Rowlett message to Seaman, 25 August 1945 (~~TS~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

10. (U) Naval Communication Activity informal history entitled RUSSIAN Language Section (July 1943 – January 1948), undated (~~TSC~~); NSA/CSS Archives, Accession No. 45021, location H06-0308-2.

11. (U) Op-20-3-G-10 memorandum for ANCICC, "Post War Collaboration with the British," 28 August 1945 (~~TS~~); CCH Collection, Series IV.AA.6.1. The Combined Chiefs of Staff (CCS) was formed in December 1941, residing in Washington, D.C., throughout the war. The Joint Chiefs of Staff were the U.S. members, and representatives of the British Chiefs of Staff acted for the U.K. Most major military policies and strategic plans went to the CCS before being presented to the prime minister and president for decision.

12. Burns, 25.

13. (U) ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Project Report, 31 August 1945 (~~S~~); CCH Collection, Series IV.AA.6.1.

14. Ibid.

15. (U) ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 15 August 1945 (~~TS~~); CCH Collection, Series IV.AA.6.1.

16. Semi-Monthly Report on BOURBON, 31 August 1945, (~~TS~~).

17. (U) ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON," 14 October 1945 (~~TS~~); CCH Collection, Series IV.AA.6.1. (~~S~~) Photographs of this machine, which the Germans believed was called the "K-37" by the Soviets, are presented in two technical reports: CNO's Communications Intelligence Technical Paper TS-35, entitled "The B-211 Machine;" 14 February 1946 (~~TS~~), and AFSA publication: *History of* [redacted] 3 May 1951 (~~TSC~~), both available in the CCH's <sup>EO 1.4.(c)</sup> <sub>EO 1.4.(b)</sub> Collection, box CC041. PL 86-36/50 USC 3605

18. Ibid.

19. (U) Dr. George F. Howe and Dr. Robert J. Watson, *Historical Study of COMINT Under the Joint Operating Plan, 1946-1949*, April 1970 (~~TSC~~), 32; CCH Collection, Series V.E.1.1. Hereafter, Howe, JOP study.

20. Semi-Monthly Report on BOURBON, 31 August 1945.

21. (U) SSA (SPSIS-9) memorandum from W. Preston Corderman, Brigadier General, USA, Commanding for Deputy Chief, MIS, subject: BOURBON [redacted] 14 September 1945 (TSC); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

22. Semi-Monthly Report on BOURBON, 31 August 1945. ~~(S-CCO)~~ [redacted]

23. (U) Op-20 Handbook on BOURBON Non-Morse Communications Procedures, 1 February 1946 (TS); CCH Collection, Series V.B.2.2.

24. Ibid.

25. Semi-Monthly Report on BOURBON, 31 August 1945.

26. Howe, JOP study, 15-16.

27. Burns, 59-80.

PL 86-36/50 USC 3605

### Chapter 10: *The Effort Expands*

1. Howe, JOP study, 16.

2. Ibid., 34.

3. (U) ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Project Report, 14 September 1945 (TS); CCH Collection, Series IV.AA.6.1. (U) Also discussion with Cecil Phillips, 31 December 1992.

4. (U) Rowlett memorandum for [redacted] 6 September 1945 (TSC); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

5. (U) Report on the [redacted] 20 September 1945 (TSC); NSA/CSS Archives, Accession No. 10336N, location G09-0707.

6. (U) [redacted] title: [Soviet] Telecommunications as of May 1948, 26 July 1948 (TSC); CCH General Collection.

7. (U) U.S. Liaison Officer memorandum for Cdr Fabian, subject: BOURBON, 27 September 1945 (TSC); NSA/CSS Archives, Accession No. 10336N, location G09-0707.

8. Semi-Monthly Report on BOURBON, 14 September 1945.

9. (U) ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 16 November 1945 (TS); CCH Collection, Series IV.AA.6.1.

10. Ibid.

11. (U) ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 14 October 1945 (TS); CCH Collection, Series IV.AA.6.1. (U) The Soviet People's Commissariat for Internal Affairs (NKVD) had paramilitary forces, including armored units, and also ran the prison camps; it was replaced by the Ministry of Internal Affairs (MVD) in 1946.

- 12. (U) Rowlett paper, subject: Special Report on Bourbon Cryptography, 15 October 1945 (~~TSC~~); NSA/CSS Archives, Accession No. 4834, box CBQM36. Hereafter, Rowlett, Bourbon Cryptography.
- 13. Ibid.
- 14. (U) ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 16 February 1946 (~~TS~~); CCH Collection, Series IV.AA.6.1.
- 15. Rowlett, BOURBON Cryptography.
- 16. NCA informal history.
- 17. Ibid.
- 18. (U) Robert Louis Benson and Cecil James Phillips, *History of VENONA*, Three Volumes (Ft. Meade, MD: National Security Agency, 1995 (~~TSC~~)). Also, Robert J. Lamphere and Tom Shachtman, *The FBI-KGB War: A Special Agent's Story* (New York: Random House, 1986). This personal narrative contains many interesting insights, but, as the authors themselves admit, they did not have access to the full documentation; thus it should be used with care. The Benson/Phillips publication should be considered the definitive study of VENONA.

**Chapter 11: Progress, Problems and Promise**

- 1. (U) ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 2 October 1945 (~~TS~~); CCH Collection, Series IV.AA.6.1.
- 2. Ibid.
- 3. (U) Cecil Phillips discussion, 31 December 1992.
- 4. (U) NEGAT message to GCCS (from Fabian for Knepper), 3 October 1945 (~~TS~~ BOURBON); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.
- 5. (U) COMNAVEU message to Op-20-G (from Seaman for Fabian), 5 October 1945 (~~TS~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

PL 86-36/50 USC 3605

- 6. (~~S~~) Fabian memorandum to [redacted] subject: Minutes of the Meeting Regarding [redacted] [redacted] 10 October 1945 (~~TS~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

Fanfold paper, incidentally, according to *Webster's Third New New International Dictionary* (Unabridged), 1966, is "a collection of sheets . . . interleaved [*sic*] with carbon paper so as to permit a multiple record . . . to be made with a single written or typed impression."

- 7. (U) ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 7 November 1945 (~~TS~~); CCH Collection, Series IV.AA.6.1.
- 8. (~~S~~) GCCS message to NEGAT (from Knepper to Fabian), 10 October 1945 (~~TS~~); NSA/CSS Archives, Accession No. 30886, location G05-0302-3.
- 9. (U) ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 1 December 1945 (~~TS~~); CCH Collection, Series IV.AA.6.1.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

10. ~~(S)~~ [redacted] memorandum to Director, GC&CS, subject: Japanese Work on BOURBON, 23 October 1945 (TS); NSA/CSS Archives, Accession No. 7497, box CBQM 36.

EO 1.4.(c)  
EO 1.4.(b)

11. Semi-Monthly Report on BOURBON, 2 October 1945.

PL 86-36/50 USC 3605

12. ~~(S)~~ COMNAVEU message to Op-20-G (from Seaman for Fabian), 5 October 1945 ~~(TS)~~. Seaman cabled:

[redacted]  
[redacted] NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

13. (U) COMNAVEU message to Op-20-G (from Seaman for Fabian), 2 November 1945 ~~(TS)~~; NSA/CSS Archives, Accession No. 30886, location G05-0302-3.

14. Semi-Monthly Report on BOURBON, 1 December 1945.

15. Ibid.

16. Semi-Monthly Report on BOURBON, 7 November 1945.

17. Howe, JOP study, 34-35.

18. Semi-Monthly Report on BOURBON, 7 November 1945.

19. Semi-Monthly Report on BOURBON, 16 November 1945.

20. Ibid.

21. (U) ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 16 December 1945 ~~(TS)~~; CCH Collection, Series IV.AA.6.1.

22. ~~(S)~~ Op-20-G memorandum for Brig. General Carter W. Clarke, subject: [redacted] with British, 4 December 1945 ~~(TS)~~, and a Secretariat, ANCICC memorandum to Colonel Rowlett, ASA, subject: [redacted] 19 December 1945 ~~(TS)~~; CCH Collection, Series IV.AA.6.1.

23. (U) ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 1 January 1946 ~~(TS)~~; CCH Collection, Series IV.AA.6.1.

24. Semi-Monthly Report on BOURBON, 16 December 1945.

25. Ibid.

26. Semi-Monthly Report on BOURBON, 1 December 1945.

27. (U) Undated Chart I-1, between pages 28 and 29 of U.S. Navy Communication Intelligence Organization, Liaison and Collaboration, 1941-1945 (U), SRH-197, identified Station ABLE as Guam.

28. (U) Op-20-G memorandum for OIC, Station A, subject: BOURBON, 26 December 1945 ~~(S)~~; CCH Collection, Series IV.AA.6.1.



### Part Three

## BOURBON Diary, 1946-1948

### Chapter 12

#### Middle BOURBON, The Second Year - 1946

As the war became more recollection than reality for many Americans in 1946, domestic victories dominated the daily news. Joe Louis knocked out Billy Conn to retain the world heavyweight boxing title. The St. Louis Cardinals defeated the Boston Red Sox in the World Series. At the movies, *The Best Years of Our Lives* won seven Oscars for telling the story of three servicemen returning with varying degrees of success to civilian life.

Postwar victories were not as common in the Allies' foreign affairs. In 1946, the American and British governments worked for a permanent world peace through the newly established United Nations. But this effort was made difficult by the increasingly hostile conduct there and elsewhere by a wartime ally.

The Soviet Union cast nine vetoes in the Security Council in 1946, dragged its feet in evacuating Red Army troops from Iran, and interfered with the internal politics of its European neighbors. Winston Churchill was among the first to speak out publicly against the behavior of the Russian Bear, denouncing the "iron curtain" that Stalin had thrown across the face of Eastern Europe, calling for Anglo-American cooperation to prevent further expansion of Communist totalitarianism.

As if anticipating the appearance in 1946 of the obscure outlines of future confrontation, American and British cryptologists were already hard at work exploiting the communications of the nation that would become their Cold War archenemy.

#### THE CRYPTOLOGIC SETTING

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Throughout the decade of the 1940s, Soviet communications of cryptanalytic interest were essentially limited to those [redacted]

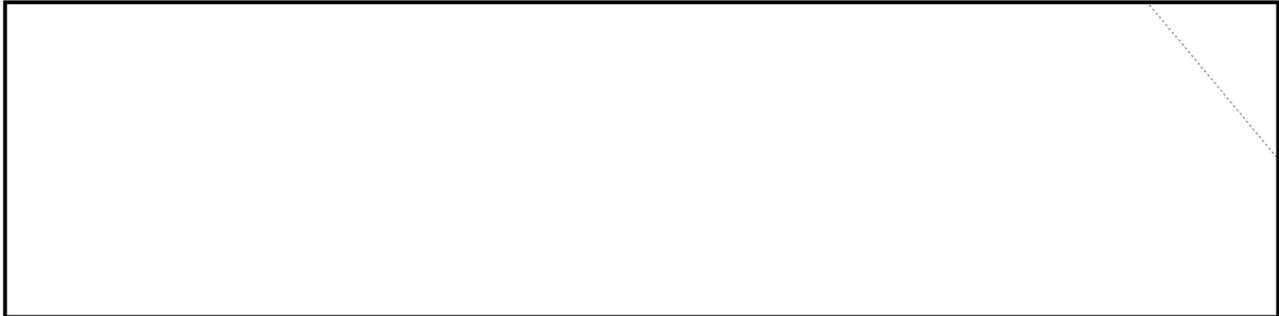
[redacted] There were few operational modes outside manual Morse and radioprinter; [redacted]

[redacted] And virtually all substantive military communications were in the form of a telegram - prepackaged, usually short, messages, [redacted]

[redacted] and were moving quickly to the top of the target list.

A significantly more important exception to the general picture was the existence of a special form of nonmilitary telegram. Appearing in ever-increasing volume were [redacted]

~~TOP SECRET UMBRA~~



At this time, electronic intelligence (ELINT), mostly emissions from early generation radars, was being dealt with apart from COMINT by the noncryptologic elements of the military services. Also, the USAF ferret airborne reconnaissance program, which initially focused heavily on ELINT but increasingly targeted otherwise inaccessible Soviet communications, began to display an ever-increasing degree of collaboration with the other two services' fixed and mobile station operations.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

**SOVIET CRYPTOSYSTEMS BEGIN TO FALL TO CRYPTANALYSIS**

Cryptanalysis was the core effort in 1946. It was the source of success.



a four-letter Soviet off-line enciphered machine

system,



Also in 1946, important cryptanalytic breakthroughs were made in several Soviet diplomatic code systems, successes that would lead over the next ten years to the identification of major Soviet spy rings operating in the United States.<sup>1</sup>

**COMINT REQUIREMENTS**

A formal COMINT requirements process was in place in the intelligence community at least as early as December 1945.<sup>2</sup> It was a rudimentary procedure which involved simply prioritizing each target country or area as either a "primary target" or an "ancillary target" and listing two categories of requirement for each country - military and non-military.

For example, in April 1946 the Office of Naval Intelligence (ONI) submitted an update to its December 1945 requirement.<sup>3</sup> Five countries/areas made the "primary target list." Number one was the Soviet Union, followed by China/Manchuria, France and her colonies, Argentina, and the Near and Middle East. All other countries were classified as "ancillary targets." By October, only the top three of those five made the "primary" target list, and the only country to get a military category of "1" was the Soviet Union. Both China and

France received a number "1" in the nonmilitary category but only a number "2" in the military column.

The COMINT requirements system was well developed by June 1947. For example, for the U.S. Army, the Military Intelligence Division (MID) had by then developed five tables or charts that expressed and prioritized its intelligence requirements: Table I - Military; Table II - Scientific; Table III - Political; Table IV - Economic; and Table V - Sociological. The countries of the world were listed across the top of each table, individually and grouped by political leanings or geography; e.g., Soviet Union, Soviet Satellites (Yugoslavia, Poland, Czechoslovakia, Albania, Romania, Bulgaria, and Hungary), and Countries Adjacent to or Near the USSR contained twenty-seven countries in four groupings (Far East, Near/Middle East, [redacted] Dozens of specific requirements were listed down the left side of each table. The prioritized degree of importance, expressed in the numbers from 0 (very little interest) to 3 (vital interest) filled the boxes created by the intersecting vertical and horizontal lines; e.g., on the chart (Table III), for the USSR, the political requirements were (1) National Policy and Activities, (2) Intelligence, Counterintelligence, Espionage, and Subversive Organizations and Activities, (3) National Stability and Efficiency, and (4) Important Personalities, all elaborated on and amplified by specific examples. These tables also conveyed the relative importance of the Soviet target; all the Soviet requirements boxes were filled with 3s. [redacted] and the two Chinese forces (Nationalists and Communists), the next highest priority targets, generally rated only 2s.<sup>4</sup>

In addition to these tables, ASA was provided intelligence guidance in the form of two lists that were updated monthly, presumably by MID. The first of these, List A, included those subjects considered to be of the "greatest immediate priority value." The number one requirement on the 2 June 1947 list was the "Greek situation, particularly: . . . b. Yugoslav, Albanian, Bulgarian and Soviet assistance to the anti-government movement in Northern Greece, . . ." List B contained subjects "of particular interest for the period following publication of the list," implying lesser importance than subjects on the first list. One entry on list B, for example, contained the following: "Europe - Hungarian situation, particularly: Soviet intervention and activities."<sup>5</sup>

From these tables and lists, representatives from the Soviet cryptanalysis, traffic analysis, translation, and intelligence sections of ASA's Cryptanalytic Branch developed intercept requirements and priorities. Next, a similarly composed committee at division level adjusted and approved the intercept priorities.<sup>6</sup>

## **ESTABLISHING COMINT NORMS AND BUILDING AN ORDER OF BATTLE DATABASE**

Given that in 1946 the Soviet Union was the number one COMINT target in the eyes of U.S. and British intelligence officials, it was clear also that in 1946 the Allied cryptologic agencies were fairly free, within the given resource constraints, to target whatever mode

of Soviet communications they could and produce whatever COMINT on the Soviet Union they chose.

Hence, it was a period more important for establishing a COMINT technical base for understanding how the Soviets communicated than for actually producing timely intelligence on specific Soviet targets. Before publishable COMINT information could be produced, the Soviets' communications capabilities, practices, and procedures had to be learned. It was this knowledge that would eventually allow COMINT analysts to infer with confidence intelligence information from the raw traffic.

The basic "norms" had to be developed. More importantly, the order of battle had to be built. COMINT needed to identify *who* the players were before it could report on *what* games (however serious) they were playing. Consequently most COMINT produced on the Soviet service problem in 1946 dealt with the identities of Soviet military and police units, and their locations and subordinations. Other than the detection of occasional unit relocations, it wasn't until late in the year that British COMINT could report, for example, on the conduct of tactical naval exercise activity off the German coast by Soviet Baltic Fleet forces.

### EARLY EVALUATIONS OF THE SOVIET PROBLEM

Despite Project BOURBON being less than a year old, the Soviet problem per se was going on for three years in America. The Army and Navy saw 1946, however, as a time for looking back, for reassessing the effort. Sometime in February, someone in the Navy knowledgeable on the BOURBON program (probably Captain Wenger, chief of Op-20-G) drafted an informal summary report on the status of the program. It was short and to the point:

The Navy began its attack on BOURBON traffic in August 1943. During demobilization the BOURBON section dwindled somewhat, but an early policy caused only persons who could be relied upon to stay with it for an appreciable time to be assigned to it. On 7 February 1946, 32 intercept positions covered RU naval circuits and at the Army's request, five intercept positions on military circuits.

There was a full exchange of raw traffic with the Army [redacted]

Out of 100 or more [Soviet cryptographic] systems, 50 were isolated. The navy studied [redacted]

[redacted]. The texts were of low intelligence value but considerable long range value.

The Navy concentrated on naval, police, and weather traffic, and helped Army with diplomatic. Certain low-level naval and police systems were brought to a point which enabled

[redacted] The value of the resulting intelligence was necessarily problematic.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

The Army Security Agency (ASA) followed suit in March, summarizing the history of its cryptanalytic attack on the Soviet problem and spelling out a major benefit of collaborating with the British:

For reasons not known to personnel now at ASA, the BOURBON problem was first begun late in 1942 (employing two persons), was for some reason abandoned soon after, and was again started early in the spring of 1943. The unit grew to number twenty-five persons by 1 January 1944, an increase necessitated by the tremendous volume of traffic passed by the country in question. The first solution entry was gained late in 1943 in diplomatic traffic, and the exploitation of this break-in, combined with the increase in traffic, brought the number of personnel employed in the project to about seventy-five by V-J Day. Solution of two military systems (now obsolete) had been accomplished in the winter 1944-45, but otherwise little had been done with operational traffic before 15 August 1945. This was true also of (radio teletype) traffic, which began to come in only in the spring [of] 1945. After victory over Japan when personnel became available and positions in the monitoring stations became idle, it was possible at last to study military-operational traffic and to develop the teletype activity; the availability of personnel also affected favorably the diplomatic studies, in which a large amount of hand work is essential because of the nature of the systems. Finally, collaboration with the British, becoming effective on the technical level in August 1945, gave a much extended picture of the BOURBON traffic of every sort, since their intercept covers an area hitherto unattained by U.S. sources.<sup>8</sup>

### GETTING AMERICA'S CRYPTOLOGIC ACT TOGETHER

Cryptologists on both sides of the Atlantic struggled even to intercept Soviet Morse and teleprinter signals from an essentially predictable but often unstable HF environment. Getting the traffic to the cryptologic processing centers was no small feat in the early postwar period of low volume telecommunications and demobilization of air and sea transportation. Then, the cryptanalysts devoted enormous energy and skill to diagnose the traffic which was protected by an assortment of Soviet military and diplomatic cryptosystems. The traffic analysts scrutinized the message externals, building net diagrams and reconstructing call sign and frequency rotas, eventually inferring such facts as military district tables of organization. The Russian linguists translated the decrypted and plaintext contents of those signals.

Meantime, their bosses (who in the 1940s in America and Great Britain were mostly senior military officers) endeavored mightily to establish formal and informal working relationships conducive to the effective and efficient exploitation of all targets worldwide. As the new year 1946 began, American officials were negotiating both among themselves and with the British. By spring, formal arrangements had been worked out in both areas. Both agreements affected Allied cryptologic efforts focused on the Soviet Union.

## USCIB'S JOINT OPERATING PLAN

First, in April, several months after the U.S. Army and the U.S. Navy renewed efforts to find an effective working arrangement between their two cryptologic organizations (i.e., ASA and Op-20-G), they published a Joint Operating Plan (JOP) which claimed to effect the "quasi-merger of the services."<sup>9</sup> The JOP created a Coordinator for Joint Operations (CJO) under the umbrella of the United States Communication Intelligence Board (USCIB), whose membership, of course, comprised the most senior of America's intelligence officials responsible for making COMINT policy and generally monitoring U.S. COMINT operations. USCIB tasked the CJO to execute its policies, foremost of which was the "coordination" of the joint efforts of ASA and Op-20-G. The CJO, who became the closest thing to a single director of U.S. COMINT operations as was to exist until 1949, was supported by three subordinate groups: the Joint Intercept Control Group (JICG), the Joint Liaison Group (JLG), and the Joint Processing Allocation Group (JPAG). It was the JPAG that sorted out which Soviet targets were to be worked by which agencies.

The JPAG was responsible not only for allocating COMINT targets but also for documenting cryptanalytic progress and, later, traffic analytic and intelligence developments.<sup>10</sup> JPAG made ASA responsible for Soviet Ground Forces, joint service, diplomatic, and air systems, with Op-20-G covering the Soviet Navy, NKVD police, and weather systems. JPAG also named a special deputy coordinator for the Soviet problem to ensure a cooperative, nonduplicative ASA and Op-20-G efforts against Soviet cryptosystems. Commander E. W. Knepper, USN, served as the first BOURBON coordinator from May 1946.<sup>11</sup>

## BRUSA AGREEMENT

The second accord of significance to the Soviet problem was between America and Great Britain, reached on 5 March 1946. It was signed by representatives of USCIB and its British counterpart, the London Signal Intelligence Board (LSIB) and was called the British-United States of America (BRUSA) Agreement. It formally confirmed a postwar cryptologic collaboration between the two nations, especially on the Soviet Union. The agreement also instituted standardized naming systems for target cryptosystems, established technical exchange procedures and parameters, and created a formal liaison arrangement, all which affected the Allied exploitation of the Soviet target.

The BRUSA Agreement explicitly absorbed Project BOURBON as part of its plans for a wider collaboration. Additionally, a technical conference was held in London to develop appendices to the agreement which would govern such areas as security, collection, liaison, etc.<sup>12</sup> One appendix, for example, created country digraphs (e.g., RU for the Soviet Union), and replaced Britain's [redacted] designation system (see Appendix A) with a BRUSA-wide system (see Appendix B), and introduced intercept case notations.<sup>13</sup>

EO 1.4.(b)  
EO 1.4.(c)  
PL 86-36/50 USC 3605

## GOOD-BYE BLETCHLEY PARK, HELLO EASTCOTE

Meanwhile, on the eastern side of the Atlantic Ocean, Britain's Government Code and Cipher School (GC&CS) was moving and changing its name. In the spring of 1946, GC&CS packed up its code books and transferred its cryptologic operations from Bletchley Park, the now-famous Buckinghamshire estate located almost fifty miles northwest of London (where World War II military cryptanalysis had been conducted) to Eastcote, at the time a drab London suburb.

## GOOD-BYE GC&CS, HELLO GCHQ (OR IS IT LSIC?)

At the same time, GC&CS changed its name. In what to some viewers looking back half a century was a very confusing procedure, the British cryptologic organization took the new title Government Communications Headquarters (GCHQ). This was a fine name, but British instructions were not to use it in secret correspondence. Everyone involved in cryptologic operations was to use only its secret title, London Signals Intelligence Centre, abbreviated LSIC.<sup>14</sup> Hence, for the next two years, GCHQ was actually called LSIC.

The coexistence of these two names must have been a bit of a problem back then, too. In October 1946, five months after the change, the JLG sent to the two American cryptologic centers a reminder, which did not do all that well in clearing things up:

LSIC is Secret, and the title Government Code and Cipher School (GC&CS) has been dropped, with title LSIC to be substituted in all cases. In all documents classified Confidential and below, LSIC should be referred to as Government Communications Headquarters (GCHQ).<sup>15</sup>

## BRUSA LIAISON AND TECHNICAL EXCHANGE

In order to facilitate the exchange of Soviet collection, technical analyses and intelligence between Britain and the United States, liaison offices were established in both capitals. In May 1946, Colonel Patrick Marr-Johnson, Royal Air Force (RAF), who had been a liaison officer for the British War Office in America for several years, was formally assigned to represent the British COMINT establishment in Washington, D.C., and Commander Grant C. Manson, U.S. Naval Reserve, also a former liaison officer on the Soviet problem, became the first formal Senior U.S. Liaison Officer (SUSLO), representing USCIB and the CJO in London.



Grant C. Manson  
(1990 photograph at age 86)

Within three months, no less than sixteen Americans, including three civilians, were accredited to GCHQ in London and at Eastcote. Moreover, nine British citizens, seven civilians and two military, were assigned either to ASA, Arlington Hall Station in Virginia, or to Op-20-G at the Communications Supplementary Activity, Washington, D.C. (CSAW), on Nebraska Avenue.<sup>18</sup>

But even before these officials were assigned, the Soviet technical exchange was ongoing. During the first two weeks of February,

[REDACTED]

The technical exchange became more extensive in May. The SUSLO London office sent ASA

[REDACTED]

The problems of exchanging traffic with GCHQ were put in perspective in November by the deputy coordinator for liaison, U.S. Navy commander Rufus Taylor. He pointed out to the Soviet coordinator that there were limits to what GCHQ could provide, especially when it came to

A request was received through USLO [London] from [Washington] . . . for [REDACTED]  
The matter was discussed with USLO who sent a reply. You will note that traffic received from [REDACTED] will be forwarded at follows: (a) [REDACTED]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

[REDACTED] Either as perforated tape or photograph. The traffic which is not being forwarded is the plain text being received on single channel teleprinter and multichannel Baudot. *There is a high volume of this traffic approaching 100,000 messages per week, which is received on printed tapes (one copy only) which is then stuck onto sheets [emphasis added].* We cannot consider the large increase of staff necessary to duplicate this traffic or even to take the traffic on reperforators and forward the tape to the USA. I feel sure that the U.S. authorities will understand this and probably do not want it as they would require a staff of 50-60 to digest the material. A full service of the Intelligence produced from this material is being sent.<sup>20</sup>

Personal liaison between the top COMINT chiefs took place in 1946 as well. Colonel Harold G. Hayes, U.S. Army, wearing two hats as chief, ASA, and CJO, spent a week in London in August,<sup>21</sup> and Captain Wenger, chief Op-20-2 (successor to Op-20-G), visited London in November.<sup>22</sup> Commander Travis, director, GCHQ, departed England in December 1946, touring British Far Eastern facilities and visiting Australia before calling on Washington on the way home in the middle of January 1947.<sup>23</sup>



**Colonel Harold G. Hayes, U.S. Army  
Chief, Army Security Agency**

### **A U.S. LIAISON OFFICER'S VIEW OF THE GCHQ PERSONNEL SITUATION**

Liaison officers also learned more about their partners' operations. U.S. Army captain C.P. Collins, who had been stationed in England for several years and was Manson's deputy until late June, returned to the States and shared his views on GCHQ. Because of their relevance to the British attack on the Soviet problem, herewith are some of Collins' more cogent comments on the personnel situation at GCHQ (i.e., LSIC) in 1946:

Every effort is being made by administration to eliminate all processing except the most essential and to obtain the utmost in efficiency. The amalgamation of Berkeley Street [where diplomatic traffic was worked] and Bletchley Park under the same roof at Eastcote has already increased efficiency over 50 percent.

LSIC is making a great effort to obtain more personnel and the outcome of a general staff investigation held at the end of June will determine whether or not LSIC will obtain a larger allotment of funds.

In a comparison of personnel between U.S. agencies and LSIC, U.S. would have . . . a four-to-one advantage in over-all personnel strength. However, LSIC, even with its fewer personnel, has been in the past, and undoubtedly will be in the future, on a par with U.S. agencies in cryptanalytic breaks.<sup>24</sup>

Then, Collins waxed specific about the Soviet problem, particularly GCHQ's progress on Soviet cryptosystems:

LSIC is not working on BOURBON [redacted] systems but is doing excellent work on [BOURBON] NKVD and service systems. Most of the crypto brains at LSIC have been thrown into the BOURBON section and they are doing promising and profitable work.<sup>25</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Collins also praised GCHQ's outstanding traffic analysis capabilities, particularly on the Soviet target:

The TA section at LSIC is superb on European military nets. Their BOURBON TA section is unexcelled. In these TA aspects, LSIC is far superior to Washington agencies because of their vast experience in this field during the War. . . . It is felt that a TA liaison officer would gain experience from a tour of duty at LSIC which would be invaluable to him on his return to this Agency [i.e., ASA].<sup>26</sup>

### BRITISH ATTEMPT TO SCOTCH THE BOURBON COVERNAME

Commonality of Allied cryptologic purpose never meant uniformity of policy. In fact, if differing views on the details, and the frank exchange of those opinions, made for a healthy relationship; the partnership was indeed to be a robust one. For example, even before the formal BRUSA Agreement was signed in March, senior British intelligence officials were trying to persuade the U.S. to drop the BOURBON moniker. First they tried to demonstrate its irrelevance (while, by the way, forecasting [redacted]). On 27 February, Marr-Johnson informed Washington that

I am instructed by the Chairman of the London SIGINT Board to inform you, in accordance with paragraph 6(B) of the Communications Intelligence Agreement, that it has been found impossible to treat BOURBON differently from any other subject during the Commonwealth Conference. It is, therefore, being openly discussed in general and such detailed arrangements concerning it as appear advisable will be made. You will realise that all the Dominion representatives are definitely interested in BOURBON and that to omit any reference or avoid answering questions would be unwise and would create suspicion which we wish to avoid.<sup>27</sup>

By May, the U.S. side appeared to go along with a policy of decompartmenting the Soviet problem ("removing the special walls around the subject of BOURBON," according to Commander Manson, SUSLO London),<sup>28</sup> but there was obviously a reluctance to do away with the term.

Apparently being pressed by the British, Manson again queried Washington in June:

In passing, I wonder what the attitude would be in Washington COMINT Center [a fiction attempting to convey the impression that there indeed existed a single U.S. cryptologic organization] for the proposition that the cover name BOURBON be now dropped? It is thoroughly dropped at LSIC, and I believe you will find record in the minutes of the executive committee meetings of the London conference that USCIB had undertaken to follow suit on the basis that everything was safe within the confines of LSIC and Washington COMINT Center.<sup>29</sup>

Washington responded in August, insisting on keeping the BOURBON name.<sup>30</sup> But GCHQ did not give up. Two months later, Manson mentioned GCHQ's continuing desire to drop the BOURBON label:

Cmdr. Loehnis [Director, GCHQ's, special assistant] has asked me once again to raise with USCIB the question of abandonment of the covername "BOURBON." You will remember that your opinion expressed last July . . . was valid only until Fall, and I thus feel that I can oblige LSIC by calling upon you for another canvass of views in the Washington COMINT Center. LSIC desires to abandon the covername only so far as its use within COMINT compounds and in LSIC-USCIB correspondence is concerned.<sup>31</sup>

The U.S. was unmoved. But the British were undaunted. They tried again in February 1947, and failed again. Op-20-2, when asked its views, replied that it had no objection to the official dropping of nationality cover names such as BOURBON but would "not undertake, however, to cease using them. Although not strictly necessary, they are convenient and well established, and OP-20-2 reports and communications will probably continue to contain instances of them for some time to come."<sup>32</sup>

Indeed, JPAG continued to use the BOURBON covername in its monthly reporting for another entire year. It was December 1947 before JPAG finally retitled that portion of its monthly report covering the Soviet Union: "The Russian Section."<sup>33</sup>

### THE SECRET OF COLLATERAL SOURCE 267

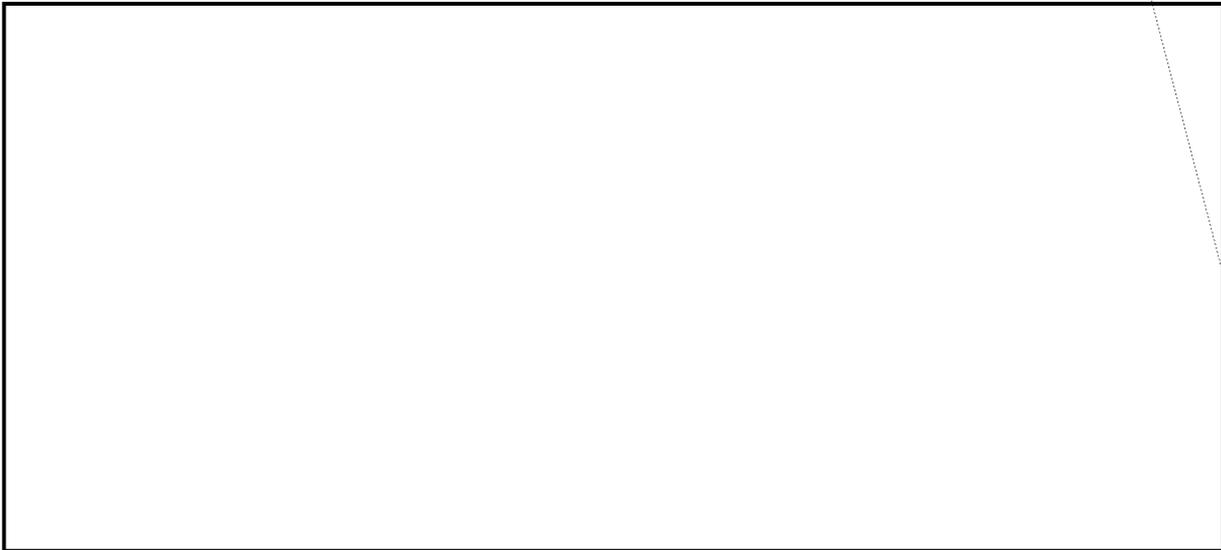
Brigadier John H. Tiltman, now head of GCHQ's Soviet cryptanalytic section, called for a special meeting in January 1946. After assembling British and integrated American cryptanalysts and U.S. liaison officers, Tiltman announced that GCHQ had recently received a "big haul" of Soviet cryptographic documents dating up to November 1944. He said that the origin of the material, which he called "Source 267," would remain secret. Tiltman said that from a cursory glance of the material, he saw nothing of immediate practical value but thought it could be of use in substantiating some of the TICOM-acquired German material on Soviet cryptosystems.<sup>34</sup>



Nothing more surfaced about this material until early in August. Apparently out of the blue, Commander Manson, SUSLO, London, was made privy to the secret of Source 267, revealed from none other than the director, GCHQ, himself:

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

These documents, a cryptographic pinch, came from [redacted]  
[redacted] is not  
clear; but how the British got it [redacted] is - they bought it!<sup>37</sup>



**U.S. COMMUNICATIONS BECOME A COMSEC CONCERN**

Captain Wenger, chief, Op-20-G (which had been redesignated Op-20-2), responded to a concern expressed by Admiral Nimitz (Chief of Naval Operations) about Soviet interest in "U.S. communications" in September 1946. Characterizing his reply as incomplete, since a full report would "require considerable research" and "would be submitted after further investigation," Wenger said flatly in the interim that "there has been no evidence whatsoever that any of our high level cipher machines have been or are being read."<sup>40</sup> American low-level traffic was, however, vulnerable:

It would appear that the Russians are probably able to read certain [American] Hagelin traffic, uninterrupted-strip-cipher traffic, and a large part of code-book traffic. . . . These conclusions are based on the premise that: (a) the Russians are at least as good as the Germans [who apparently were reading such American communications], and (b) that the Russians in their invasion of Germany obtained much the same information about the enemy's communication intelligence efforts that we secured when we invaded Germany.<sup>41</sup>

**EARLY U.S. COMSEC SUPPORT TO THEATER COMMANDS**

While visiting ASA Europe (ASAE) at Frankfurt, Germany, in 1946, Arlington Hall's top traffic analyst, Stephen Wolf, was permitted to observe for two days in October the organization's participation in a Command Post Exercise (CPX) conducted by U.S. Forces European Theater (USFET). The war game scenario assumed that enemy forces (unidentified but, for all practical purposes, Soviet) had suddenly attacked the major headquarters of the theater, forcing the command posts into the field. The exercise task for the theater command posts was to set up communications and pass a certain quantity of

traffic. ASAE's assignment was to intercept these command post communications and reconstruct the net. An unknown number of collection operators and six traffic analysts were dedicated to the effort, and by the end of the exercise, the USFET command post net had been reconstructed and the stations located.<sup>42</sup>



## Chapter 13

### Old BOURBON, The Third Year - 1947

#### QUOTATION MARKS FOR A COLD WAR

The BOURBON covername felt as comfortable to American cryptologists as an old shoe by 1947. It also leaked, no longer providing the protection for what had become an open secret within the Allied cryptologic community; GCHQ had used it seldom since it was coined.

After the post-World War II celebrations of 1946, American life became in 1947 more of a struggle - with a variety of opponents. In baseball, the New York Yankees battled their crosstown rivals, the Brooklyn Dodgers, through a full seven games before winning the World Series. In boxing, Joe Louis slugged it out with his adversary, Jersey Joe Walcott, for fifteen rounds merely to eke out a split-decision victory. In virtually every other struggle in America, it seemed that the competitor was communism, with small successes on both sides and the ultimate victor in doubt.

American labor unions and the Hollywood movie industry discovered communists in their midst in 1947. Union members and celebrities who wanted to keep working were asked to sign noncommunist affidavits. The State Department set up regulations to identify and expel security risks.

The conflict spread into the fields of science and economics. Atomic energy was the chief topic of American scientific interest in 1947, and it became embroiled in communist controversy; the United Nations' effort to apply international controls to nuclear power was foiled by Soviet intransigence. Inflation in America, which in 1947 added 10 percent on top of 1946's 18 percent cost of living rise, could be traced in part to the U.S. providing financial support for Western Europe, helping the war-ravaged nations there to successfully fight off Soviet-backed communist takeovers.

Eastern Europe was not so fortunate in 1947. The Soviets engineered the establishment of communist governments in Hungary and Romania and helped purge anticommunist forces in Poland, Yugoslavia, and Bulgaria.

Consequently, 1947 became a watershed year for America. A year earlier, most Americans felt there was still hope for the West to work things out with the Soviets. Now these dreams were dashed. Fault lines of a permanent split between the Capitalist West and Communist East became visible. The appellation "Cold War" came into regular use, albeit still in quotation marks.

The call to Cold War arms came on 12 March 1947, when the "Truman Doctrine" was enunciated. It marked the beginning of an official, focused, Allied effort to contain communist expansion. (The concept of "containment" of Soviet communism had been articulated and developed within the Truman administration by George Kennan, a senior State Department official.) The "Marshall Plan" was proposed on 5 June to provide U.S.

economic and technical assistance to Europe. It helped the Western European nations suffering from the effects of World War II to restore their productive capacity, thereby reducing the appeal of Soviet communism.

The Truman administration made modifications to the U.S. intelligence community structure as well. Congress passed and President Truman signed into law the National Security Act of 1947 on 26 July. Also called the Unification Bill, the Act abolished the existing National Intelligence Authority (NIA), putting in its place the National Security Council to serve in an advisory capacity to the president.

Moreover, the NIA's operating component, the Central Intelligence Group (CIG) was replaced by the Central Intelligence Agency (CIA), to be headed by a Director of Central Intelligence (DCI), who also reported directly to the president.

Finally, the act established as an independent entity the United States Air Force (USAF). Both the CIA and the USAF would affect the structure and operations of the U.S. intelligence establishment and, more specifically, its communications intelligence community.

#### **USCIB INTEREST IN SOVIET TARGET**

Although USCIB was responsible for policy direction of COMINT targets worldwide, its main focus since 1945 clearly had been the Soviet Union. However, while USCIB probably had an appreciation for the value of the Soviet plaintext traffic that contained information on the Soviet atomic energy program, the oversight organization apparently did not speak to the issue. As late as October 1947, USCIB's stated major Soviet joint interest projects were limited to the study of code and cipher systems, non-Morse intercept processing, and abbreviations.<sup>1</sup>

USCIB stopped using the BOURBON coverword in its correspondence in December 1947, taking what remained of the compartmented wraps off the "Russian Problem."<sup>2</sup> The BOURBON covername was finally dead; long would live, however, the problem it had been designed to protect.

#### **EXTENSIVE BRITISH-U.S. LIAISON**

Much liaison in 1947 took the form of personal visits and exchange tours, many by Americans to Britain. The year began with a visit by Commander Sir Edward Travis, director ("Head" in British parlance) of GCHQ (still referred to as the London Signals Intelligence Centre - LSIC - in virtually all correspondence) and a party of senior GCHQ officials to Washington, D.C., in January. The Travis party had departed London in December 1946 and had traveled first to Australia, with Washington on the return itinerary.<sup>3</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Also in January, two special cryptochannels were established between London and Washington "for exchange of administrative dispatches between the three principals [presumably Travis of GCHQ, Hayes of ASA/CJO, and Wenger of CSAW]," with procedures set up for especially sensitive "eyes only" exchanges between the chiefs.<sup>4</sup>

Dr. Louis W. Tordella, who was now a civilian employee working for CSAW, visited GCHQ in January and February.<sup>5</sup> He had been put in charge of developing for the U.S. Navy equipment to intercept the various Soviet two-, six- and nine-channel Baudot printer signals, and he went to Britain to "see and learn what GCHQ was doing" in the teleprinter collection field against the Soviets. At the time, U.K. intercept systems, which included captured German equipment, were more advanced than what was available to the Americans.<sup>6</sup>



Mr. Stephen L. Wolf during 1946  
visit to GCHQ

Mr. Stephen L. Wolf, ASA traffic analysis specialist, who had spent almost four months in Britain and in Germany in late 1946, reported extensively on GCHQ's Soviet traffic analysis and collection operations in February. He was particularly impressed with GCHQ's "elaborate but effective system of setting intercept priorities." He described in detail the British direction finding (DF) operations.

U.S. Army major E. Dale Marston, who had spent seven months (June-December 1946) at GCHQ in a liaison capacity, returned to ASA in February 1947 and wrote of his experiences, commenting on the personnel, facilities, organization, and operations of GCHQ at Eastcote, the suburban London headquarters which he unkindly characterized as a "drab looking place resembling an average chicken farm." Marston was more complimentary about GCHQ's work: "The strength of the combined [redacted]

[redacted] I must say that they turn out a very large amount of work." Also, on the subject of [redacted]

[redacted] he wrote: "I would like to point out that the whole section there was extremely cooperative. The only limiting factor was their lack of personnel. They are willing to do anything to help as long as they have someone to do it."<sup>7</sup>

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

Frank Rowlett, chief of ASA's Operations Division, forwarded Wolf's trip report to chief, ASA, pointing out three areas where ASA could profit from replicating GCHQ's procedures: (1) setting intercept priorities; (2) organization of a separate search and development unit; and (3) specific traffic analysis techniques "which has resulted in outstanding progress in the reconstruction of [redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Mr. Cecil J. Phillips, who began his career in 1943 as an ASA cryptanalyst on the Japanese weather problem and rose to senior executive positions at NSA, including chief, [redacted] in the 1970s (he remains active as a historian at the Center for Cryptologic History, fifty-two years later), had spent six months at GCHQ in 1946 as a liaison officer, reported in February 1947 on his assignment, summarizing his activities at Eastcote and applauding the cooperative relationship between British and American cryptanalysts but recommending more informal exchanges:



Mr. Cecil J. Phillips while assigned to GCHQ in 1946

EO 1.4.(c)  
PL 86-36/50 USC 3605

In conclusion, mention should be made of the spirit of cooperation of the British. Within the limits of available man-power, every effort was made to supply any information requested by USCIB. They were most anxious to exchange ideas on difficult research problems, although they were somewhat discouraged by the number of copies necessary. Informal correspondence between the principals of sections at USCIB and LSIC would do a great deal in furthering cooperation.<sup>9</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

U.S. liaison officers/analysts and British analysts met at GCHQ in March in an effort to coordinate their respective attacks on [redacted]

[Large redacted block]

Also in May, a liaison visit by a U.S. Navy officer to Great Britain designed to improve Anglo-American cryptologic coordination resulted in a lack of coordination between the Navy and USCIB. U.S. Navy commander Francis A. Raven, who in the 1960s and early 1970s rose to senior executive ranks at NSA (he was chief of G Group, 1966-1974), was in 1947 head of Op-20-N-2's [redacted] team, visited GCHQ to discuss "theories, methods, resources of manpower and future planning of work on all types and aspects of [redacted] . . ."12 Raven apparently neglected to inform USCIB of his discussions, and when the JPAG found out later in the year, a nasty exchange of correspondence resulted between the Navy and JPAG.13



Mr. Francis A. Raven, circa 1947

Mr. Herbert Conley, ASA traffic analyst and future NSA senior official (he was NSA's assistant director for personnel management, 1965-1967), arrived in Great Britain on 30 June to replace P.J. Patton as the SUSLO staff officer assigned to Eastcote.14

### U.S. REVIEW OF THE COLLABORATION

Frank Rowlett, again wearing his hat as deputy coordinator for processing allocation, JPAG, wrote on 5 August to Captain Wenger, who had replaced Colonel Hayes as the CJO in April, providing a review of the status of U.S.-British cryptologic collaboration generally. Rowlett characterized the principal British contribution, [redacted]

[redacted] . . . ASA and CSAW, on the other hand, were better organized for the *production of COMINT on a current basis* [emphasis added], though they lacked enough first-rate technicians to cope with the high-level Russian problems."15

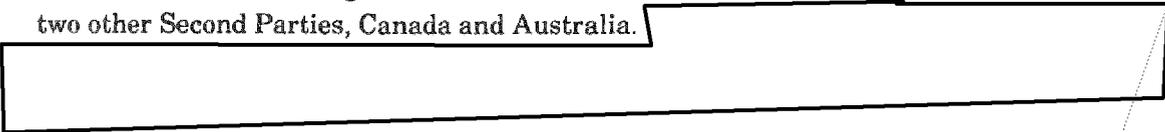
Although Rowlett's report addressed all targets, the effort against the Soviet Union was included in a fine piece of understatement justifying the ongoing "completely interwoven" Allied duplication of effort which would come to characterize the entire scope of joint cryptologic work achieved throughout the last half of the twentieth century:

Due to the unique intelligence requirements of each country it is desirable that both sides work on most of the systems of most countries. Although this leads to a certain extent to duplication of effort in the mutual working of problems, the exchange of technical information is so complete and so rapid that this duplication is limited to production and can thus be held to a minimum. In all cases where both centers are solving the same problems the exchange of results aids each in the final solution,

supplementing the work of each, rather than duplicating it. So integrated has the work become, that it is the exception, rather than the rule, that one center attains a success without a substantial contribution from the other.<sup>18</sup>

That the Soviet target dominated GCHQ's cryptologic effort there was little doubt. Rowlett first reminded his readers that GCHQ employed a group of highly skilled and experienced technicians "integrated into a powerful research and diagnostic organization, with eminently qualified specialists in every branch of cryptanalysis and traffic analysis." Then he added that the British effort was "swinging toward the production of Russian intelligence to the near exclusion of other fields. . . . [GCHQ] contemplates maintaining only a token force on other problems."<sup>17</sup> Needless to say, the collaboration continued.

Most American dialogue with Britain of a liaison nature thereafter in 1947 dealt with two other Second Parties, Canada and Australia.



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

## Chapter 14

### Beyond BOURBON, The Fourth Year - 1948

BOURBON had been essentially a compartmented project in 1945, and the covername was used extensively throughout 1946 before being replaced by the descriptive "Russian problem" in late 1947. Therefore, 1948, [REDACTED]

[REDACTED] but the year that still represents an essential continuity of the effort begun in 1945, went beyond BOURBON.

In America generally, prices and inflation rose at record rates in 1948; by July a buck was worth 45¢ in prewar dollars. Employment, production and corporate profits also climbed to record levels. Wages rose 39 percent. But by December, employment was down again, and retail stores reported lagging sales. The year 1948 ended with most businesses in decline, and the economy as a whole being characterized with words like "unstable" and "uncertain."

In other words, 1948 had its ups and downs, usually with unhappy endings, much like the prince in Shakespeare's play *Hamlet*, the movie of which won the Oscar for Best Picture of 1948. Other unhappy endings included India's Mahatma Gandhi, who was assassinated, and Babe Ruth, who died of cancer.

An ominous nonevent ended the year - the Nobel Committee decided to award no peace prize for 1948, which perhaps explains why quotation marks fell off the Cold War idiom. The two sides of that conflict which had vaguely formed in 1947 became more clearly drawn a year later: Soviet Union versus United States; East versus West; communism versus capitalism; totalitarianism versus democracy.

Specifically, the Soviets began to turn that part of Germany they controlled into a separate nation. First, they decreed a new economic administration for their German zone, then declared a separate currency. Finally, the Soviets blockaded Berlin, which the United States and Britain countered with an airlift of food, fuel, and other supplies. Meanwhile, Czechoslovakia fell to the communists, but Tito's Yugoslavia escaped Soviet control.

The Marshall Plan was working in Western Europe, but in Asia large losses were being taken. North Korean Communists decreed a "People's Republic," and Mao Tse-tung's Communist army swept through Manchuria, taking control of the northern half of China.

Back in America in 1948, Harry S. Truman won reelection to the presidency after asking Congress to restart the draft in case it was needed to meet "Soviet threats," asserting that world peace depended solely on Russia.

Finally, with implications for the intelligence community, 1948 was an early year of the Soviet spy; Elizabeth Bentley, Vassar graduate and long-time courier for a Soviet

espionage ring, blew the whistle on dozens of top "U.S. Reds." Another defector from communism, Whittaker Chambers, named Alger Hiss and others. The spies' mission, largely successful, had included stealing America's atomic secrets.

### DIRECT CIA ACCESS TO "RAW TRANSLATIONS"

Protecting *American* atomic secrets was a counterintelligence concern, mostly of the FBI. Uncovering *Soviet* atomic secrets, of course, should have been the main objective of America's intelligence community. USCIB, the COMINT member of that community, seemed more occupied, however, working community-wide COMINT policy and organizational issues. This effort included making intrusions into the COMINT processing business. In April, for example, USCIB gave CIA (and other consumers) greater access to COMINT activities, authorizing them to receive raw translations and other unfinished products considered by them "necessary for the fulfillment of their mission of producing finished intelligence."<sup>1</sup> Furthermore, COMINT consumer organizations were also allowed to place indoctrinated representatives within COMINT producing sections.<sup>2</sup>

R.H. Hillenkoetter, Rear Admiral, U.S. Navy, and director of Central Intelligence (DCI) approached ASA early in 1948 requesting additional COMINT, particularly "raw translations" [redacted] Unrestricted access to the COMINT "activities," i.e., agencies, was required, according to Hillenkoetter, because it was of "fundamental importance" for CIA to "not only have working access both to the material and activities to determine the existence of *positive* intelligence, but also that [CIA] be aware of gaps in COMINT coverage to shift greater emphasis to other sources when required."<sup>3</sup>

Hillenkoetter had worked out acceptable arrangements with both ASA and CSAW, but the Army wanted USCIB to "take official notice of the solution." Consequently, the issue was on the agenda for a USCIB meeting held in April. A discussion of terminology started off the issue, with Colonel Hayes preferring the term "raw translations" over CIA's choice: [redacted]

According to the minutes of the meeting, Lieutenant General S.J. Chamberlin, director of Intelligence, General Staff, U.S. Army, supported Colonel Hayes' position:

The term [redacted] means to Colonel Hayes a large volume of material much of which is ultimately screened out and hence never reaches the stage of being translated and written up as COMINT information. He outlined illustrative steps in the processing at ASA and commented that he had been informed that sometimes as little as 20% of the original volume of intercepted material is finally processed. He said he would have no objections to supplying the CIA with any specific messages in raw form, for use in verifying particular translations, but that the wholesale delivery of a great mass of crude COMINT material to the CIA by ASA would be mutually inefficient and merely a disorganized approach to a problem that could be handled much more satisfactorily by the Army's furnishing translations to the CIA. He said he believes the CIA really wanted raw translations and that [redacted] was a misnomer.<sup>4</sup>

OGA  
EO 1.4.(c)

EO 1.4.(c)  
PL 86-36/50 USC 3605

Although all members agreed with the change of terminology, it was clear from the minutes that Chamberlin was still not happy with CIA's increased access to ASA's material; he launched into a detailed lecture on the importance of protecting the security of COMINT, expressing his concern that "too many people are receiving such information." Hillenkoetter replied that he agreed, but that "a companion problem dealt with the imperative necessary for the CIA to get all available intelligence from all sources, in order to discharge its statutory responsibilities." Chamberlin said he would "personally assume the responsibility to insure that CIA received from the ID [Intelligence Division] all products of the Army CI [communications intelligence] system which would be valuable to the CIA in performance of its mission." Hillenkoetter continued the sparring by observing "that no one could ask for a firmer guarantee than the one given by General Chamberlin." At this point Thomas B. Inglis, Rear Admiral, U.S. Navy and commander, Office of Naval Intelligence (ONI), took up the cudgel, commenting that "even so, the existence of such a guarantee would not in practice act to protect the person guaranteed, because such a guarantee would not be accepted by superiors as a valid excuse for failure to discharge one's responsibilities." At this point, the State Department representative, Mr. Park Armstrong, said he assumed that these procedures applied as well to State. All members agreed.<sup>5</sup> While this policy applied to all COMINT, it was clearly directed at and had its largest impact on Soviet COMINT.

#### **EARLY U.S. CENTRALIZATION EFFORTS**

Surprisingly, Soviet cryptographic practices played a role in influencing the U.S. government's early efforts to centralize the processing of COMINT. In October 1948, a new Service Cryptologic Agency (SCA), the United States Air Force Security Service (USAFSS), was established, joining the existing "dynamic duo" of ASA and CSAW. From a Department of Defense perspective, a new agency meant not only three SCA's to deal with, but added costs. Perhaps it would be less expensive, the thinking went, to create a unified or joint agency. Centrally controlled and directed Soviet cryptography was looked at as a possible model to emulate. Some U.S. policymakers recognized that a centralized cryptanalytic attack on centrally controlled Soviet cryptosystems might make more sense than the "coordinated but separate" attacks being mounted at the time by the Army and Navy, with the Air Force in the cryptologic wings.<sup>6</sup>

This kind of thinking was behind the establishment of the so-called Stone Board (named after Admiral Earl E. Stone, its chairman), which met as directed by the secretary of defense, James V. Forrestal, initially in August 1948, publishing its report in December 1948. This led ultimately to the creation in 1949 of the Armed Forces Security Agency (AFSA), the immediate predecessor to the National Security Agency.<sup>7</sup>

#### **ADVANCES IN COLLECTION, ANALYSIS AND REPORTING . . .**

Mr. Herbert Conley, who had been on the SUSLO staff in London in 1947 and was by late 1948 an ASA supervisor involved in analysis and reporting of Soviet targets, assessed

the strides made in collection and forwarding. First, he reported on recent intercept improvements:

Continued attempts to build up intercept strength [redacted] had made it possible by the summer of 1948 to begin intercept of Russian operational or low-level Military and Military Air circuits in this area. The intercept and analysis of such links has been increased during the past few months, with emphasis being accelerated as the Russians have reduced transmission [redacted] Operational air links employing radio-telephone transmissions have not been intercepted regularly, but cover of Morse links is extensive.<sup>8</sup>

Then Conley pointed out how forwarding to ASA of selected intercept had been made more timely by December 1948:

At the present date, Army Security Agency, Washington, is receiving daily by teletype all air defense and operational air traffic intercepted at U.S. Stations [redacted]

[redacted] Information on flights of Russian planes in Europe is available in Washington within a few hours after the flight has been scheduled.<sup>9</sup>

... EXCEPT FOR SOVIET [redacted]

Speculation as to the reasons ranged from normal development in Soviet cryptographic security (the early thinking) to later leanings strongly toward espionage (see Part Four for details).

All of these [redacted] had been providing [redacted] but Conley, in his December 1948 ASA-based assessment, picked out [redacted]

[redacted] But by year's end, with only backlogs to clean up, U.S. cryptanalytic resources dropped 5 percent.

Traffic analysis of Soviet communications reached maturity. Again, Conley, speaking only for ASA, said it well:

Military and Military Air links were successfully intercepted [redacted]

EO 1.4.(c)  
PL 86-36/50 USC 3605

[Redacted]

Traffic analysis against the Soviet target was so well developed that when [Redacted]

[Redacted]

Soviet plain language processing in 1948 rose like a phoenix out of the ashes [Redacted]

[Redacted]

The major 1947 problem of a shortfall in Russian linguists was on the road to being rectified in 1948. The Russian language work force in ASA and CSAW increased 131 percent, overtaking the number of traffic analysts, and falling only twenty-one people short of the cryptanalytic work force. Two million plain language messages were reviewed during the year, and ASA alone published 748 reports (more than three every working day) based on plain language material. Limited statistics were available for CSAW, but its linguists in March 1948 scanned over 107,000 plain language messages and translated 8,000 of them.<sup>13</sup>

GCHQ also quickly recognized the potential significance of Soviet plain language material, pointing out in its April proposal for an expanded BRUSA exchange that the British were [Redacted]

[Redacted]

Allied cryptologists published thousands of COMINT reports in 1948, making little distinction between technical and product, probably limiting some technical reports to producer agencies only on the basis of presumed customer lack of interest; the consumer seemed to be able to get all the technical details he wanted. More important contemporary distinctions were made between the processing sources, i.e., cryptanalysis, traffic analysis, or plain language (see Part Seven).

Conley, in his December memorandum, also addressed how timely ASA reporting was becoming.

EO 1.4.(c)  
PL 86-36/50 USC 3605

Material from [Redacted] plain text messages is integrated both at ASA Europe and at ASA Washington so that composite information on aircraft movement is available to intelligence consumers within a minimum of time. ASA Europe is presently issuing to USAFE, through SSO channels, current information on plane concentrations and plane movements in Europe.<sup>14</sup>

**CONTINUED U.S.-BRITISH LIAISON**

SUSLO, London, had long wrestled with the problem of shipping copies of British-intercepted Soviet traffic back to Washington, having had to depend for the most part on British transportation assets since BOURBON had been implemented. Therefore, it was with great pride, declared a major USCIB accomplishment, when in January 1948 there was finally established a U.S.-controlled air courier service for the transportation of raw traffic from London to Washington. On 20 January 1948, the first batch of raw traffic for

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

shipment to the United States was delivered at the American embassy, London, by SUSLO.<sup>15</sup>

There was no doubt that cryptologic liaison between America and the British in 1948 was required. Captain Wenger, the CJO, confirmed in February in a statement of collection requirements that the collaboration with GCHQ remained highly desirable. He then cited as justification for the continued collaboration the fact that the British [redacted]

[redacted] considerably augmenting America's manned counterpart numbers, [redacted]

Liaison channels were used, for example, for the expression of American concerns over British intercept tasking. Washington informed GCHQ through liaison channels in May 1948 that British diversion of intercept emphasis toward the Soviet target should [redacted]

[redacted]

The centerpiece for American and British cryptologic liaison in 1948 was the second BRUSA Technical Conference, held from 15-26 July. The first conference had been convened in the spring of 1946, shortly after the BRUSA Agreement was signed. GCHQ called for the second conference to review and make changes to the appendices produced during the first conference. ASA was eager for a conference to plan for "emergency relocation of its stations in Europe." CSAW, on the other hand, "yielded reluctantly to the urgings of the CJO," Colonel H.G. Hayes, chief ASA, who had replaced Captain Wenger in April 1948.<sup>18</sup> The conference agenda was to be restricted to five general topics: security and processing; intercept; communications; traffic analysis; and standardization.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

One topic, however, got very specific as applied to the Soviet problem. Plain language loomed large for ASA managers responsible for the Soviet target. Consequently, Appendix B of the BRUSA Agreement was revised so that the security and dissemination regulations applied to Soviet radiotelephone [redacted] intelligence, and the grading of plaintext messages. Furthermore, a new Appendix K was formulated to embody the results of a complete survey of the Soviet plaintext and radiotelephone targets.<sup>19</sup> There was considerable correspondence between GCHQ and America concerning the exchange of Soviet plain language traffic in 1948 (about which more later in Part Six).

During preparations for the London Conference, Lieutenant Fred Bright offered his view on what it took to prepare for a liaison officer assignment at GCHQ. There were three things he believed his replacement should do:

- One is to become completely conversant with the communications end, especially Porter's Rockex and communications unit. . . . A second is to become as familiar as possible with all the IBM and RAM techniques used by the crypt sections. A third is to learn about the Russian P/T [plain text] units in detail.<sup>20</sup>

Although American cryptanalysts had worked together with British cryptanalysts in GCHQ spaces since 1945, in December 1948 the first formally integrated "working party"

was formed at GCHQ, when three Americans arrived in London to join the [redacted]

[redacted] It integrated U.S. and British experts in cryptanalysis, traffic analysis and reporting as an element in one of GCHQ's departments, controlled by the director, GCHQ.

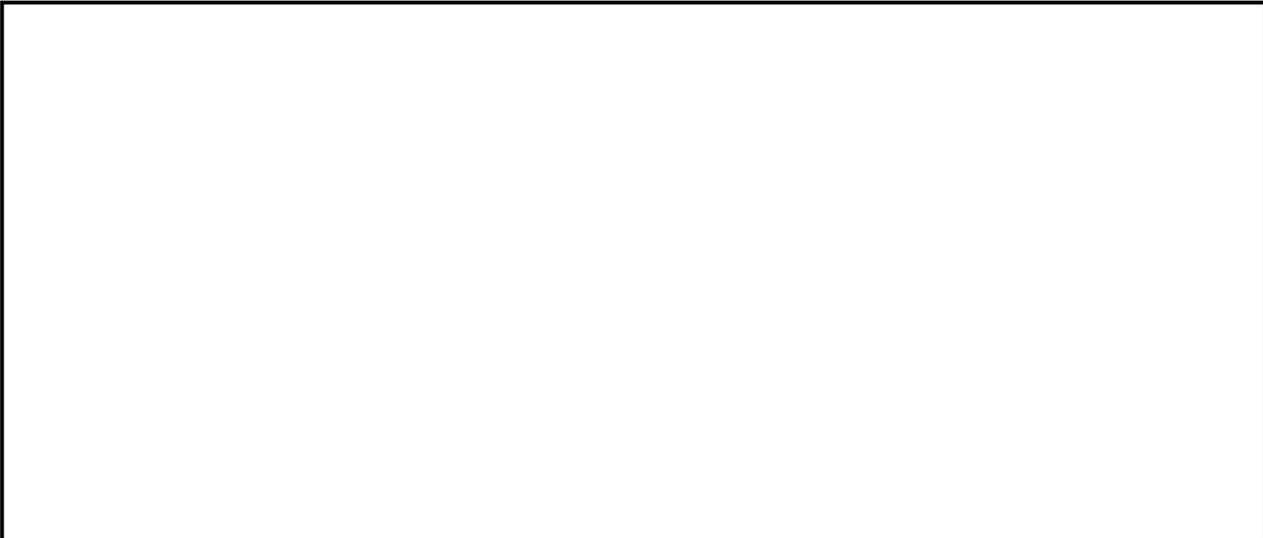
The MET Party, as it was called, minimized duplication of effort and increased the

identification of [redacted] "the understanding of what they were

transmitting, and [redacted] Combined parties dealing with

traffic analysis, cryptomachines, and intelligence followed.<sup>21</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



**AN ALL-TOO-BRIEF U.S. AFFAIR WITH ELINT**

In early 1948, British intelligence authorities proposed collaboration with the United States in the field of electronic intelligence (ELINT) or, as it was then called, electronic reconnaissance. In the U.K., ELINT was "supervised" by the COMINT Board of the LSIB. In America, however, the military services controlled ELINT, with USCIB playing no part. Nevertheless, Captain Wenger, in his last month as the USCIB's CJO, was the recipient of the British request for collaboration. Wenger called a meeting of all service representatives to address the issue. Ultimately, the director of intelligence, USAF, proposed that the commanding general, USAF Europe, and the U.S. commander in chief, Mediterranean Fleet, be allowed a "limited and controlled exchange of raw information (not analysis) with the British. . . ." Also recommended was that the overall joint supervision of the exchange "be vested in the Joint Chiefs of Staff."<sup>26</sup> Presumably, these recommendations were agreed to, and for the time being, USCIB apparently played no further part in U.S. ELINT.

**WELCOME GCHQ; GOOD RIDDANCE LSIC**

The good news for future writers and readers of cryptologic history was found in a JLG announcement of 15 October that the secret title LSIC would be abolished on 1 November 1948, with instructions that only GCHQ should be used for all purposes.<sup>27</sup>

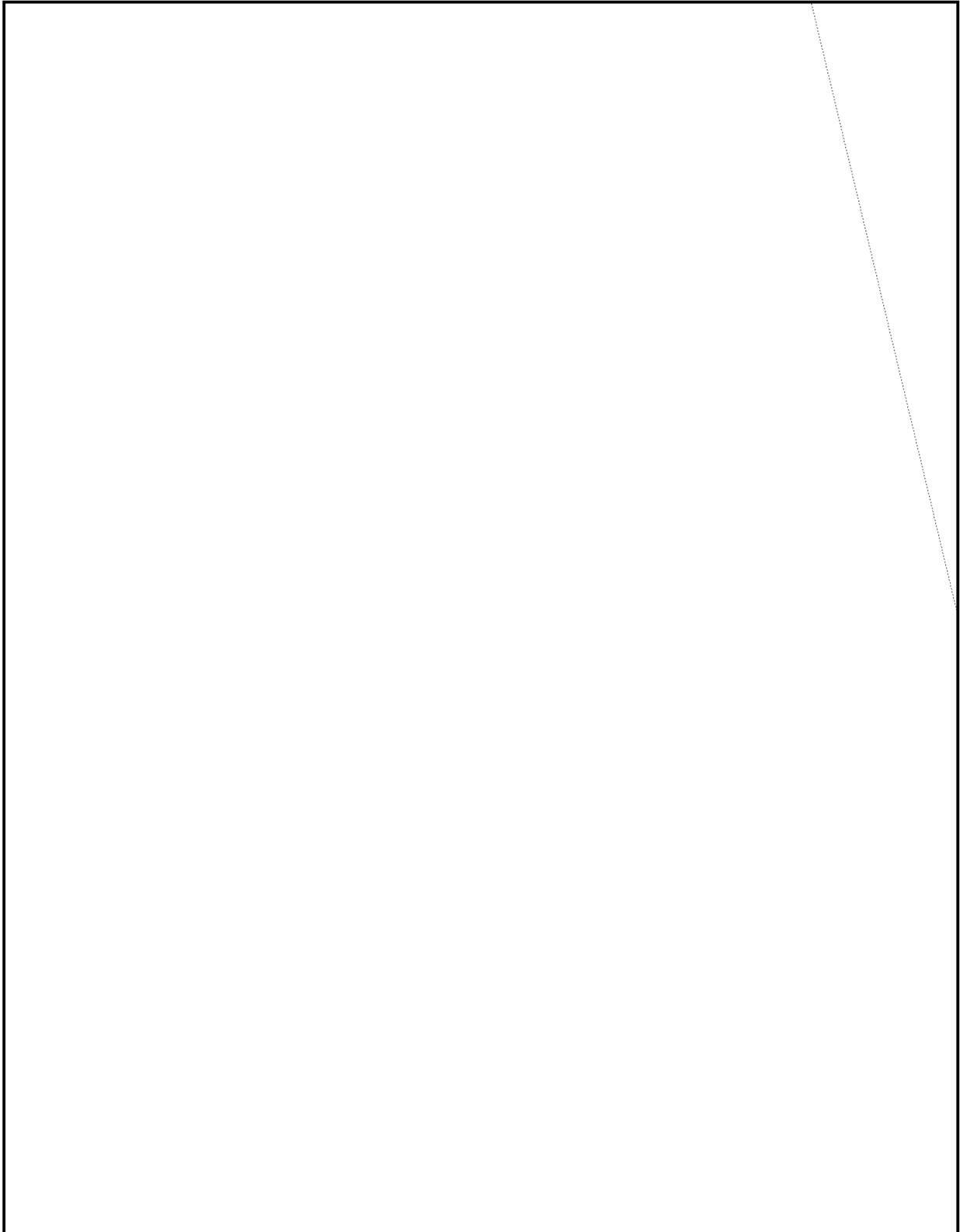


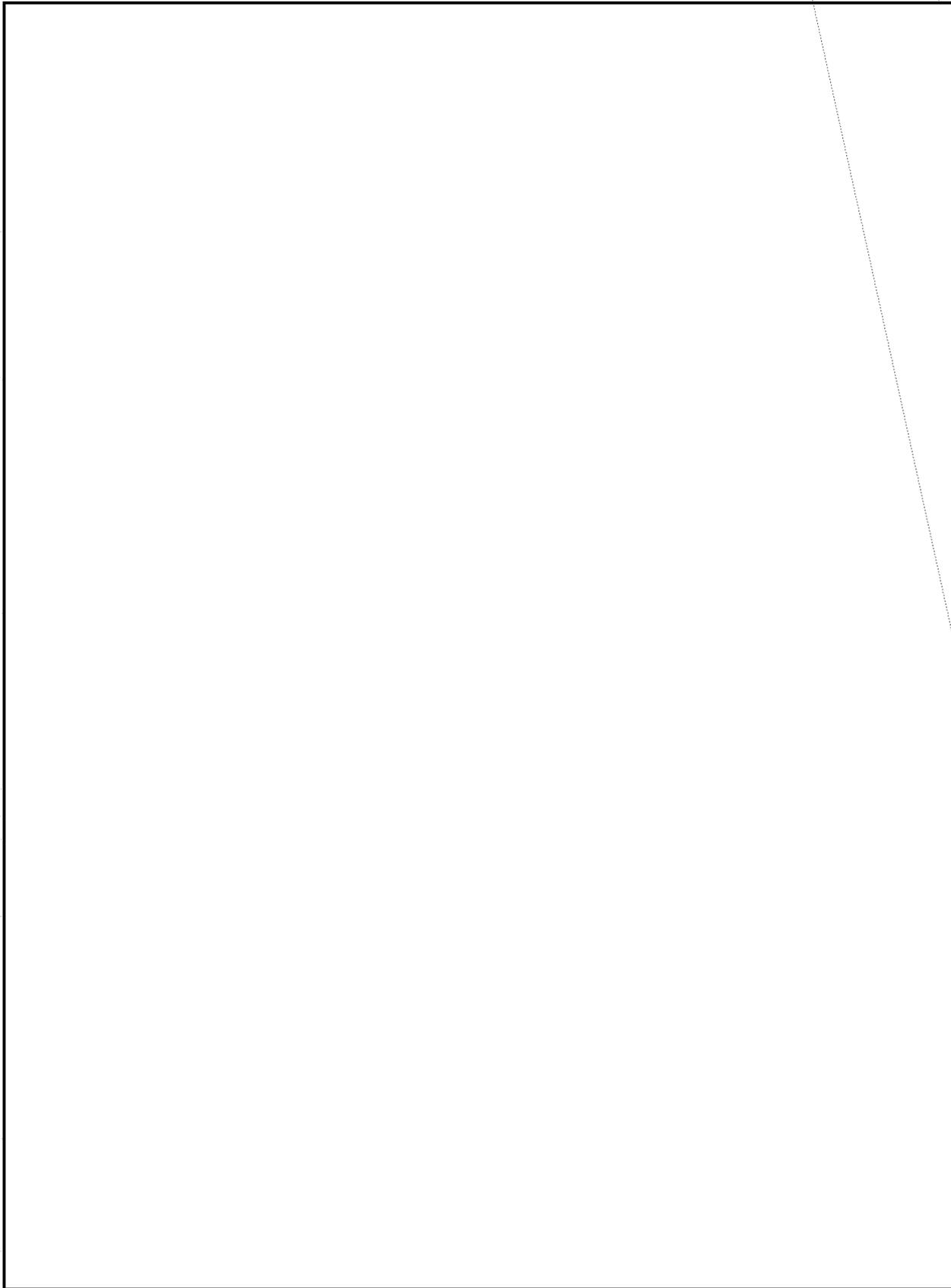


EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



## Chapter 15





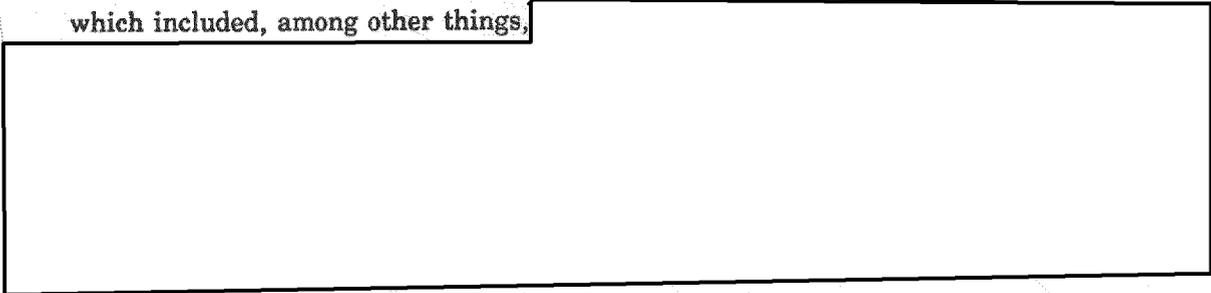


sinister reflections, they could not fail to observe that the partnership resembled the equality of the beef-and-rabbit stew - one steer to one rabbit.<sup>15</sup>

USCIB was also concerned with the increased risks to COMINT security that went along with widening the knowledge base about COMINT activities generally, and it "was disturbed by implications of the [redacted] that there was a weakness somewhere in the existing chain of COMINT security."<sup>16</sup> No agreement was reached, but negotiations would continue. Formal letters [redacted] [redacted] were exchanged throughout the fall and winter of 1948, slowly narrowing the differences between the two parties.

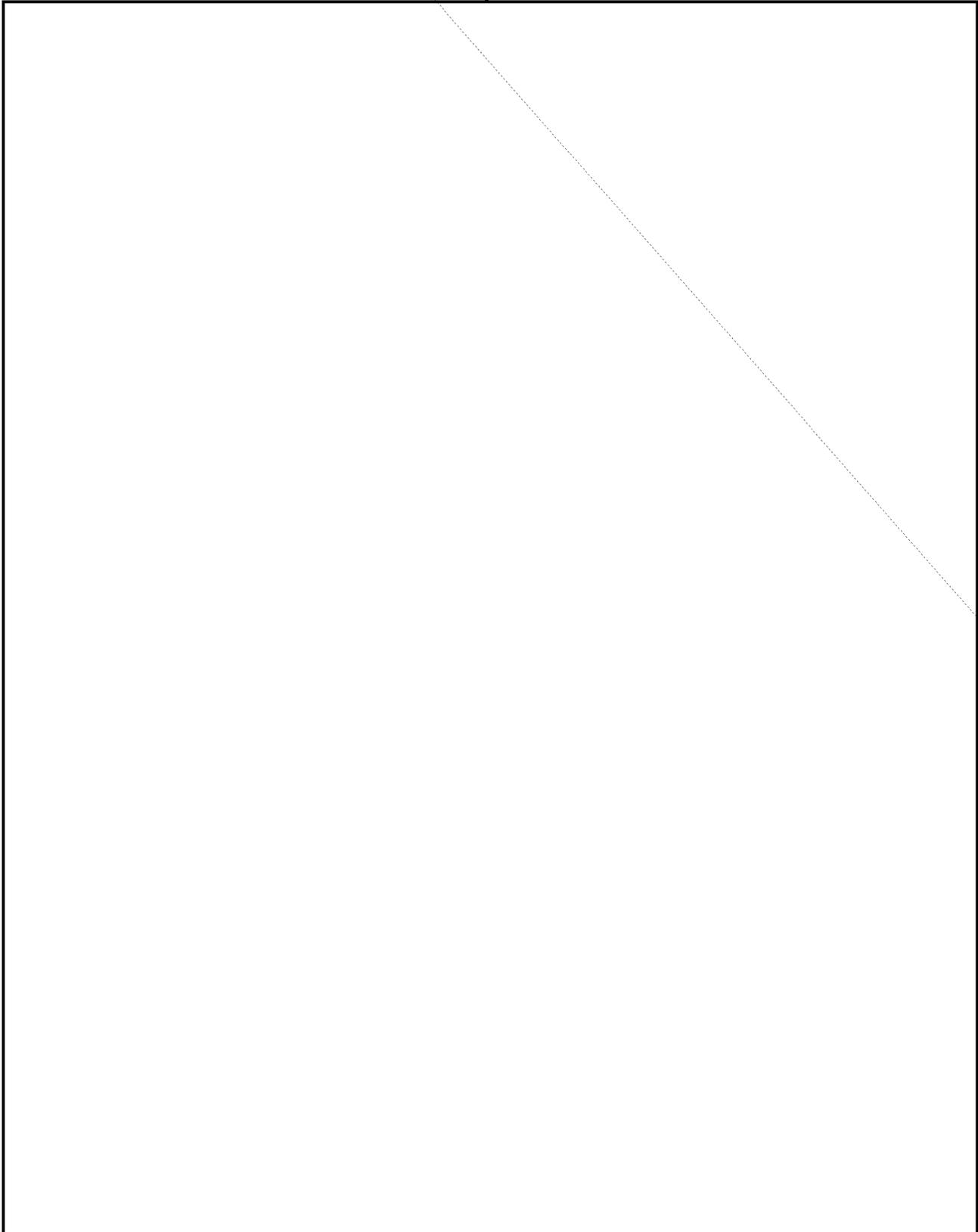
Meanwhile, working-level liaison continued. By 1948, USN lieutenant Max Gunn of CSAW was [redacted] a special representative to coordinate technical matters [redacted] [redacted] pertaining to the establishment and construction of radio intercept stations [redacted]

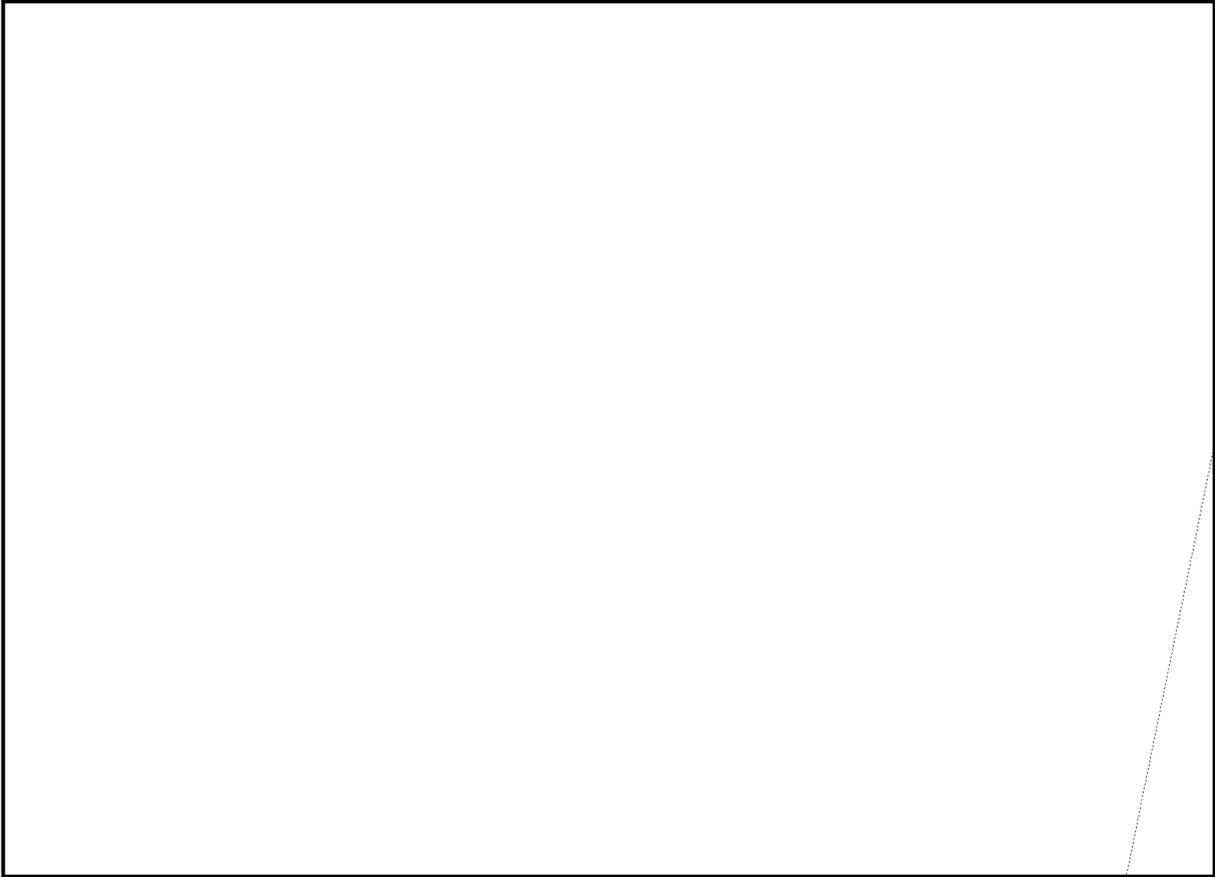
USCIB kept GCHQ informed as to the nature of materials being sent [redacted] For example, USCIB provided GCHQ with a list of materials sent [redacted] on 28 January which included, among other things, [redacted]



DOCID: 4314365

**Chapter 16**





EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

### Chapter 17 Personnel Resources, 1946-1948

#### AMERICAN MANPOWER ON PROJECT BOURBON

For readers interested in the bottom line, the following numbers tell the tale. They show the high rate of growth in the number of Americans dedicated to the Soviet effort from the start of the project in 1945 until December 1948, almost a fourfold increase in about three and one-half years:

	Total	Percentage Increase
September 1945		-
January 1946		20
December 1946		39
December 1947		39
December 1948		59

PL 86-36/50 USC 3605  
EO 1.4.(c)

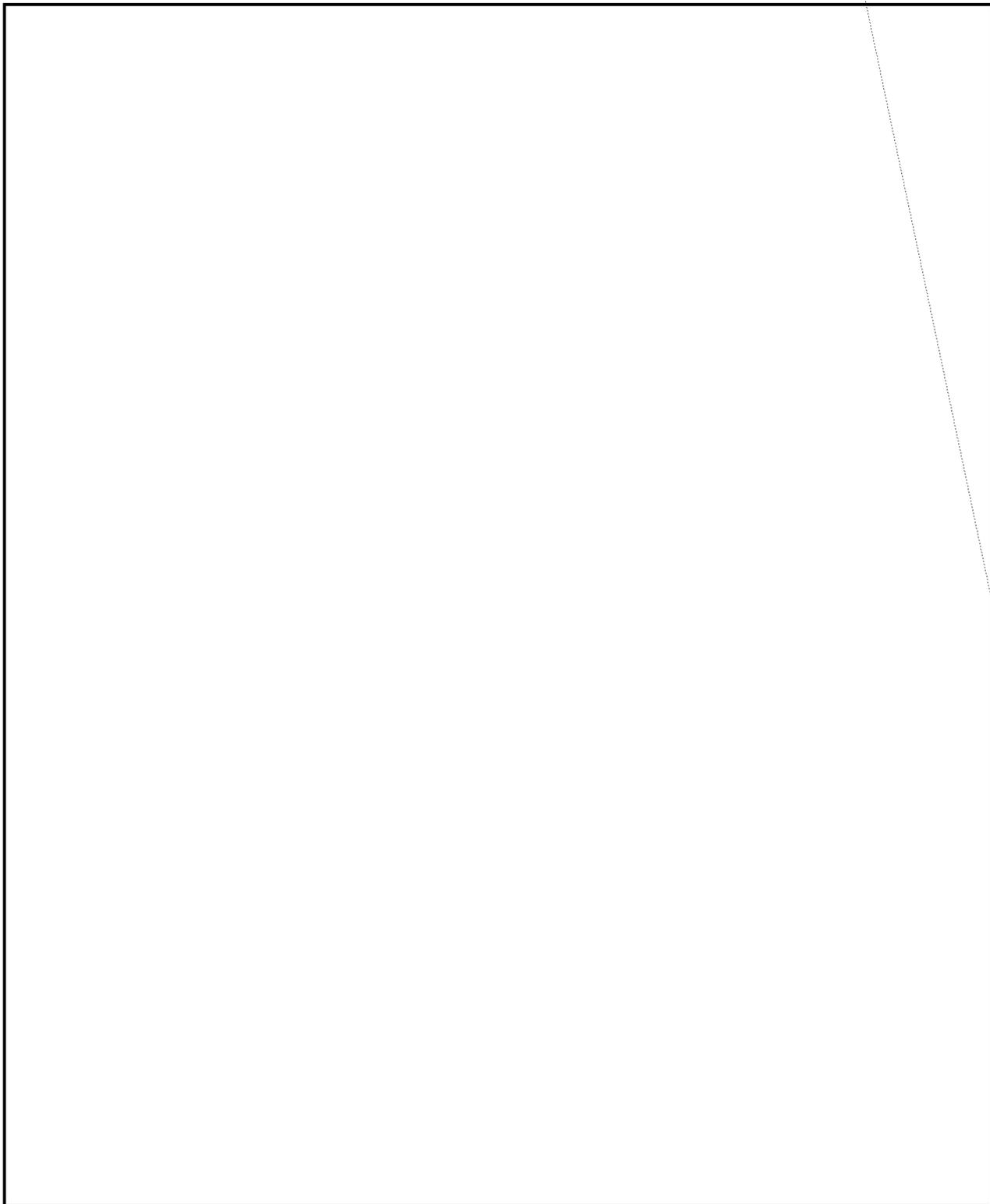
The above statistics represent only processing personnel in Washington, D.C., and do not take into account the intercept operators and other field personnel. Limited statistics show that ASA collectors dedicated to the Soviet target numbered thirty-six in April 1946, growing threefold to [redacted] by August of that year.<sup>2</sup>

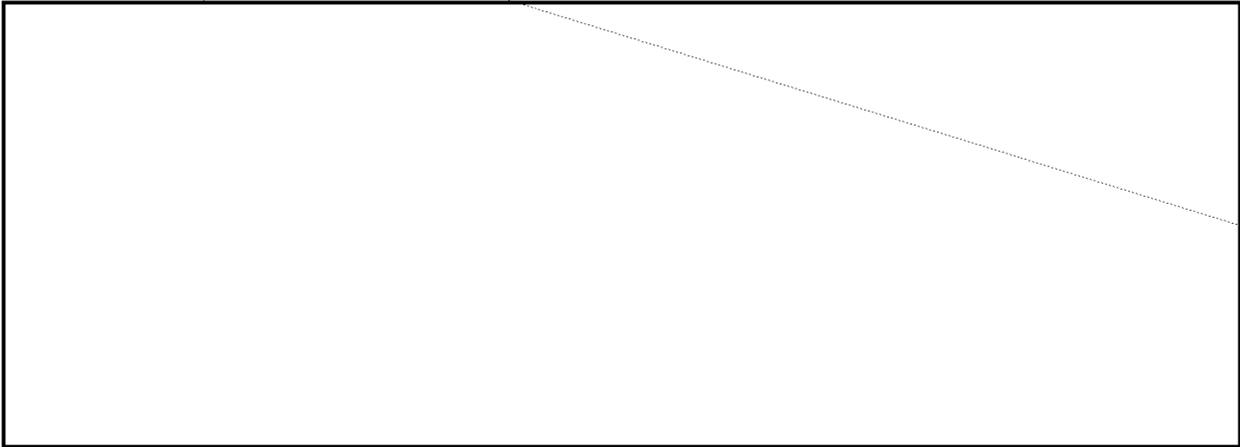
Available statistics, by U.S. cryptologic agency, of personnel (i.e., including personnel working non-Soviet targets) show that people dedicated to the Soviet problem accounted for 27 percent in 1947 and 34 percent in 1948 of the total population at the two Washington COMINT centers. The following chart also indicates that two-thirds of all the new hires in 1948 were apparently assigned to the Soviet problem:

	ASA	CSAW	Total Soviet	Total ASA/CSAW
December 1946				
December 1947				
December 1948				

ASA cryptologic processing people power dedicated to the Soviet target grew by 44 percent in 1947, and counterpart Navy personnel increased by 31 percent. In 1948, the percentage increases were 48 percent for ASA and a whopping 78 percent for CSAW.

Also, a careful review of available statistics will show that, while there were [redacted] Americans assigned to the Soviet problem in December 1948, only [redacted] were cryptanalysts, traffic analysts or language analysts. It turns out that the other [redacted] people were in support functions such as administration, traffic preprocessing, maintenance, and clerical. Another [redacted] (or 40 percent) were in the training pipeline, a tail that did not appear identifiable in the monthly statistics until February 1948.<sup>4</sup>





	U.S.	U.K.	Total
December 1946			
December 1947			
December 1948			

A breakdown of these statistics into the number of cryptanalysts, traffic analysts, and linguists will be presented when the contributions by these individual skills are addressed in Parts Four, Five, and Six.

PL 86-36/50 USC 3605  
EO 1.4.(c)



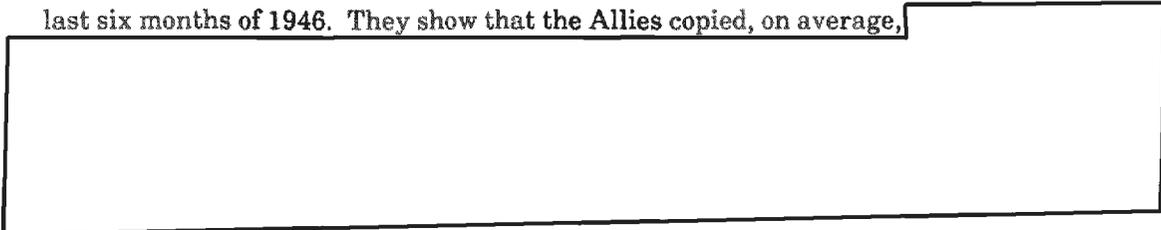
### Chapter 18 Field Operations

#### FIELD OPERATIONS DIARY - 1946

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

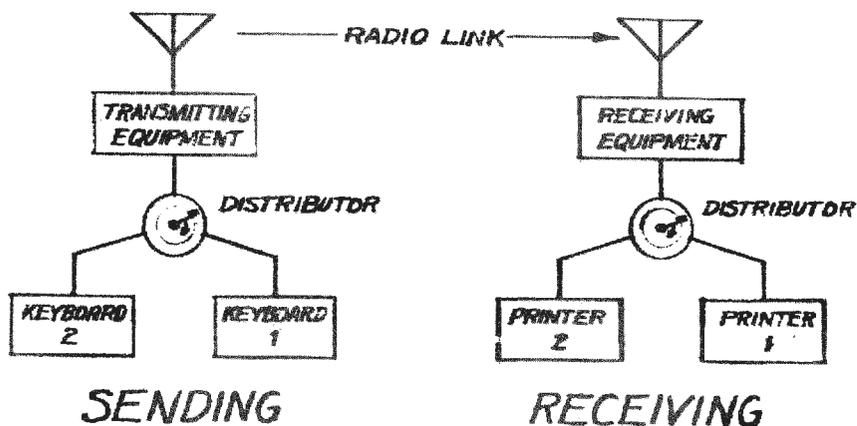
#### *Intercept Facilities and Volumes*

By February 1946, thirty-seven Navy intercept positions were dedicated to Soviet communications,<sup>1</sup> but no data are available for Army sites or the number of tasked positions in either the Army or Navy. Intercept volumes are available, however, for the last six months of 1946. They show that the Allies copied, on average,



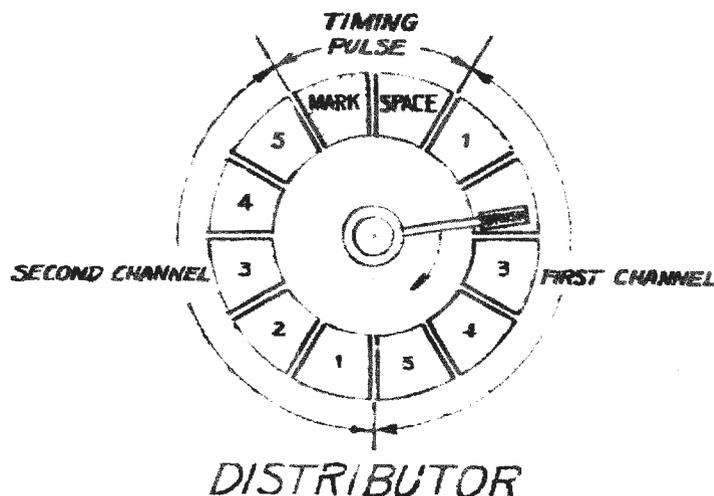
While the bulk of the historical record on the early Soviet problem dealt with the cryptanalysis of the various cryptosystems, records do exist to show glimpses of the kind of support being provided to collection operations. In January 1946, for example, Op-20-G published a "BOURBON Non-Morse Glossary," designed to assist field collection personnel and analysts with no Russian language training to understand whatever clear text appeared in the traffic externals.<sup>3</sup>

FIG. 1 RUSSIAN 2 CHANNEL SYSTEM



Schematic drawing of Baudot sending and receiving system

Op-20-G followed this up by publishing in February a working aid entitled "BOURBON Non-Morse Communications Procedures," which contained the information "presently available" on the Soviet non-Morse circuits. Designed primarily for intercept personnel, it contained examples of messages, "scrambled" printer traffic, service messages, operators procedure, and circuit practices. Among the tips included was the fact that major Soviet stations used four different covernames but only one at any given time, a period normally of ten days. The appendix contained a functional description of a Baudot Two-Channel Teleprinter System, including drawings of the sending and receiving system and of the distributor system.<sup>4</sup>



Schematic drawing of the distributor system

Meanwhile, the U.S. struggled with finding the collection resources for increased intercept of Soviet traffic. The first JPAG monthly status report, published in May, complained:

Effort on all Soviet systems is being hindered by inadequate traffic interception resulting from rapid demobilization and inadequate replacement of intercept personnel.<sup>5</sup>

In the Soviet non-Morse collection arena, the need for more collection equipment and planned solutions were quantified in a midyear study by ASA:

There are some 22 known [Soviet] two-channel links, 4 six-channel links, and 3 nine-channel links now in operation. For the time being most of the coverage of six- and nine-channel links comes from British intercept, but considerable emphasis is being placed here on two-channel intercept. Within the next six months it is hoped that the Army and Navy working together can put 15 BOURBON two-channel intercept sets into the field. Assuming little or no

duplication of intercept, with full coverage on the known links, the two-channel intercept time expressed in hours per month is expected to be approximately 12,000 hours per month.<sup>6</sup>

But by August the influx of intercept operators to U.S. Army intercept sites in the Pacific began to contribute to the expansion of Soviet collection coverage.<sup>7</sup>

U.S. cryptologic management's recognition that informed intercept operators could produce better collection as well as provide more sophisticated assistance to both cryptanalysis and traffic analysis brought about a plan in September to publish "purely technical information" on the Soviet problem at the secret level for distribution to field stations.<sup>8</sup>

### ***Intercept Forwarding***

A small snapshot of the state of intercept and forwarding timeliness in April 1946 can be found in a Navy study of the difference between time of intercept and time of receipt of Soviet signals copied at Adak, Alaska, and transmitted to Washington, D.C. Cited were about 200 intercepts and the relatively short delay in (presumably electrical) forwarding, which ranged from eleven to twenty-five hours.<sup>9</sup>

### ***British Red Forms and the Case of the Mysterious Disappearance of the Fan-Fold Paper***

British Morse intercept operators hand-copied all collection onto "Red Forms," whose often unreadable carbons caused no end of problems for the U.S. side, as summarized by one liaison officer:

Most of the LSIC military intercept is taken by hand on Red Forms. The problem of producing an extra copy of this intercept may cause some delay in its delivery to Washington.

The conversion from hand copied Red Forms to taking intercept on typewriters will probably require a couple of years. The problem of (1) obtaining typewriters and (2) training operators to use them will require at least this long to solve.<sup>10</sup>

The U.S. had broached the issue, suggesting a solution on 5 March 1946 and explaining to the director, GCHQ, that the U.S. Navy had "recently acquired several Russian-language typewriters made by Remington Rand under Lend-Lease for ships under construction for the "BOURBON [i.e., Soviet] Navy," trying to interest the director in accepting one to look over.<sup>11</sup>

The Navy provided not only typewriters but also a substantial supply of (believed to be five-ply) fan-fold paper to use in the typewriters. Apparently, while GCHQ officials supported the conversion, British collectors and GCHQ analysts were not so enthusiastic.

Consequently, in July what was described as "tons" of U.S. Navy-provided fan-fold paper was reported by Commander Manson, SUSLO London, to have disappeared. A British search turned up no trace of the shipment of paper, which had last been seen in March sitting on a Boston pier.<sup>12</sup> Manson expressed some urgency on the subject, adding "I hope you can stumble on to the trail."<sup>13</sup>

The saga of the Red Forms continued into November, as Manson related:

Washington's great desire for cleaner Red Form carbons, now emphasized by your advertising campaign, has been stressed. . . . Of course, the technical personnel at Eastcote have always jumped to the defense of Red Forms for the reason that they claim handwritten intercepts are more reliable than typed ones, being more flexible and much more readily corrected and modified as the messages are being taken; but this argument has little value where the carbons are concerned, as I realize. I continue to point out to . . . the Director that this issue is one which will rise rather embarrassingly at Washington in January unless it can be shown that some concrete improvements are either underway or contemplated. [A party of GCHQ officials, led by the director, was scheduled to visit Washington in January 1947.]<sup>14</sup>

As 1946 ended, neither a solution to the mysterious disappearance of the fan-fold paper nor a resolution of the Red Forms problem had been found.

**FIELD OPERATIONS DIARY - 1947**

**Intercept Facilities, Tasking and Intercept Statistics for 1947**

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

By May 1947, the U.S. was operating some nineteen intercept facilities, eleven in the states and its possessions and eight overseas.<sup>15</sup> At the same time, Britain managed [redacted] intercept stations, [redacted] on the British Isles and [redacted] worldwide. In terms of twenty-four-hour-a-day, fully manned terminals, the U.S. stations operated 196 terminals, Great Britain some [redacted]

How many of the American sites were tasked with intercepting Soviet communications is unknown. However, on the British side, Soviet communications were tasked at [redacted] stations, [redacted] at home and [redacted] overseas in May 1947.<sup>17</sup>

Tasking in terms of the number of U.S. and British collection terminals directed against Soviet communications is available, however, as well as the consequent collection take:

Target Country	Intercept Terminals		Traffic Intercepted (Messages per Month)	
	British	U.S.	British	U.S.
Soviet Union	[redacted]	104	[redacted]	[redacted]
All Other (21 targets)	[redacted]	35	[redacted]	[redacted]
International circuits	[redacted]	57	[redacted]	[redacted]
Total:	[redacted]	196 <sup>18</sup>	[redacted]	[redacted]

PL 86-36/50 USC 3605  
EO 1.4.(c)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

The above statistics are quite revealing, particularly concerning the dominance both of the Soviet target compared to other problems and of British collection vis-a-vis U.S. intercept. First, in 1947 the statistics show that 53 percent of American intercept positions were tasked against Soviet communications, as well as almost one-third of British intercept terminals. Second, the take of Soviet traffic swamped the available

monthly intercept on other targets, with 92 percent of British take and 75 percent of U.S. intercept being Soviet traffic. Perhaps most significantly, the British, with only twenty-eight more dedicated terminals than the U.S. but with better geographical access to the Soviet Union, accounted for 87 percent of all Soviet collection over the period under review.<sup>13</sup>

Another way of looking at the relative contribution each of the three partners (ASA, CSAW, and GCHQ) made in terms of intercept of the five categories of Soviet traffic shows clearly Britain's major contribution in 1947:

	ASA	CSAW	GCHQ	
	48%	2%	50%	EO 1.4. (c)
	15	5	80	EO 1.4. (b)
	10	30	60	PL 86-36/50 USC 3605
	38	28	34	
	2	15	83	

America's contribution to Soviet intercept in 1947 began with the Navy complaining that a lack of collection in February made it difficult to reconstruct both the Soviet naval and MVD police networks in the Far East. Attempts were being made to solve the problem by assigning additional collectors and "search" positions for these targets.<sup>21</sup> Later in the year, CSAW installed new Baudot teleprinter intercept equipment (presumably developed by Dr. Tordella's team) at many of its field stations and informed the secretary of the navy in October that "the kinks are being ironed out . . . and traffic from this source is on the increase."<sup>22</sup>



**British Intercept Developments**

On the European side of the Atlantic, GCHQ had a very busy year making procedural changes and detecting new Soviet signals. GCHQ made a serious attempt to reduce the copy of unidentified Soviet transmissions,<sup>25</sup> developed the capability to produce pageprint of Soviet nine-channel Baudot, and, after almost two years of foot-dragging in converting from hand-copy to typewriter copy,<sup>26</sup> reported that "the station at [redacted] is making some comparative tests on the various methods of copying Russian Morse circuits . . . with a view toward determining the best ways to utilize typewriters in the recording of Morse

transmissions."<sup>27</sup> The British were more successful intercepting newly detected Soviet signals. GCHQ copied Soviet air-ground HF Morse, on one occasion being used by Soviet [redacted] Naval Air Force elements in [redacted] found a Soviet unit subordinate to Headquarters Group of Soviet Occupation Forces Germany [redacted] transmitting two-channel Baudot printer traffic on [redacted] [redacted] and discovered a Morse group on the Moscow [redacted] naval link referring to what GCHQ believed was the "first known instance of the use of Baudot by the Russian Navy."<sup>29</sup>

### **HF Direction Finding (HFDF) Developments**

As touched on earlier, the British ran an elaborate HF Direction Finding (DF) network, divided into two main groups. The home net had its control at the Royal Navy station in [redacted] with six outstations stretching from the north of Scotland to [redacted] the southwestern tip of England. The overseas nets were composed of [redacted] with no single control, but they were subject to the direction of their theater commands. There were [redacted] [redacted] and [redacted] along a line running loosely from [redacted] in the west [redacted] in the east.<sup>30</sup>

DF requests came from three sources: the DF section itself in anticipation of other requirements; GCHQ's target country sections which needed bearings for net reconstructions; and the intercept sites, usually to identify new signals found in general search. GCHQ also had a system of four priorities based on importance of the signal, with emergency (SOS) or distress signals ranked at the top.<sup>31</sup>

Britain's home DF net had a tip-off arrangement which permitted bearings to be taken on the desired signal simultaneously, with results available "within a few minutes."<sup>32</sup>

ASA had no comparable system early in 1947, and one unidentified senior ASA official (possibly Frank Rowlett) annotated Wolf's February trip report with the charge: "More emphasis should be placed on [U.S.] DF, at least to the point of perfecting procedures in the hope that better equipment will be available in the future."<sup>33</sup>

By September, the Army apparently had developed a DF capability at one of its stations in Germany, and a proposal was put forward to work with one neighboring British station to do

some D/F work and it would certainly be an advantage now if they were able to do something on the Russian [redacted] LSIC has trouble on some of these because [U.K. intercept station at] [redacted] can take only line bearings. If these lines could be compared with others . . . , much more could be done in determining where these [redacted] are located.<sup>34</sup>

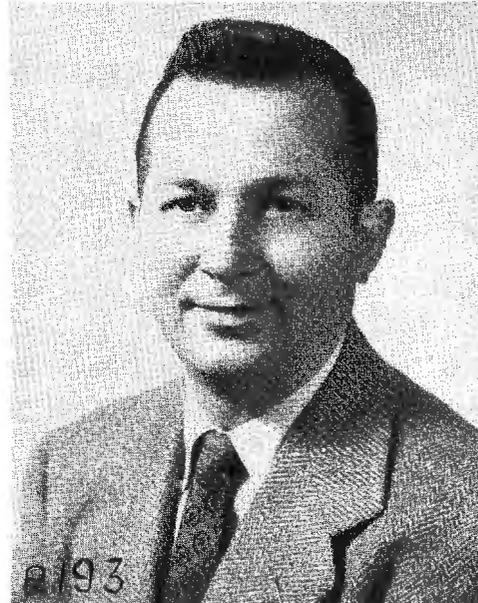
The U.S. Navy had had a substantial DF net during the war. In response to a September query from Herbert Conley, SUSLO London staff officer, apparently on behalf of GCHQ, the Chief of Naval Operations (CNO) office responsible for Navy DF activities reported that the Navy's DF net had been "curtailed" after the war, but "the nucleus is still there, and it could be expanded, or placed in full time operation, on short notice." Navy

agreed to do a study of bearings both in the Atlantic and Pacific Oceans; in the case of the latter: "it is probable that noon positions reports of BOURBON [i.e, Soviet] ships will be used as a basis for this study. This type of study is an invaluable aid in determining the errors of the various stations. . . ."<sup>35</sup>

### ***Development of Soviet Teleprinter Collection & Processing Equipment***

Both CSAW and ASA saw the need for new intercept and processing equipment, particularly for Soviet printer collection. As stated earlier, CSAW's Dr. Tordella visited GCHQ in January 1947 to learn about the printer processing equipment being used by the British. He then worked closely with ASA's counterpart to develop the required systems.

Like Tordella, ASA's equipment developer would rise to senior executive positions in NSA. He was Oliver R. Kirby, who had been a member of the TICOM<sup>36</sup> teams in 1945, and who was in 1947 a U.S. Army captain stationed at Arlington Hall. (Kirby would become in 1966 NSA's first civilian assistant director of production - equivalent of today's DDO.)



Oliver R. Kirby, circa 1947

In March 1947, Kirby proposed a project be established "for the development and/or procurement of suitable equipment for the operational processing of non-morse intercept," [which was later specified as "Russian Baudot tapes"] to replace the so-called IBM regeneration units "presently used to process non-Morse intercept tapes." Kirby explained that twelve units were presently processing tapes, with eight more units on order. Original estimates had indicated that the twenty units, working fifteen hours per day, seven days a week, could process approximately 12,000 intercept hours per month. Experience, however, showed the estimate to be greatly in error, with output very low because of the inability of the units to interpret Chadless tape and extensive maintenance necessary to keep the units in operation.

Because of these problems, in February 1947 each unit had averaged only 4.5 hours per day in operation. Consequently, a backlog of tapes was building up.<sup>37</sup> Before the project would be allowed to begin, however, a study was to be made as to the most feasible solution to the problem, with rough time and cost estimates included.<sup>38</sup>

**Minor Flap: Soviet Use of American - and British - Radio Equipment**

It seems that in January 1947 the British intercepted a Soviet operator's discussion about an "SCR" transmitter. Believing the transmitter to be American made and wanting more details from his correspondent (SCR is believed to expand to Signal Corps Radio). Mr. Phillip ("PJ") Patton, SUSLO London staff officer, asked the JICG to look into how the Soviets got hold of the equipment and find out what type and quantity were turned over. Patton explained that as there was "much dismay felt at [British intercept station] Knockholt over [the] fact that [the] Russians are using some American tone-type radioteletype equipment, believed to have been given to them by the U.S. Army."<sup>39</sup>

In February, Patton added that the Soviets were testing the American "two-tone" equipment daily [redacted] at "1200 [hours] GMT. . . [redacted] kcs is used ordinarily."<sup>40</sup> In March, Patton informed JICG that the American-made teletype equipment was being used at "both ends" of the [redacted]

It turned out, after much ado, that during World War II not only had the U.S. Army provided the Soviets with radios, but so, too, had the British. In June, Patton, hiding whatever American dismay that may have existed, forwarded a list of electronic equipment supplied to Soviet authorities during the war by the British. Dozens to thousands of radios, radars, jammers, telephones and testing equipment had been delivered under the "first to the fourth protocols," probably of the Lend-Lease Act, between 1941 and 1945.<sup>42</sup>

EO 1.4.(c)  
PL 86-36/50 USC 3605

**FIELD OPERATIONS DIARY - 1948****Intercept Facilities, Tasking and Collection**

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

By April 1948, the United States had thirty-six Army and Navy field stations, located both stateside and overseas. Britain operated [redacted] Less than a year later, in January 1949, as a result of various closings and openings of stations, the U.S. number was thirty-five (including one USAF site: [redacted])

[redacted] By then, the number of [redacted] sites had dropped by one [redacted]

A glimpse of U.S. intercept tasking for 1-15 October 1948 shows that of 824 U.S. collection positions, 548 (or 67 percent) were tasked against Soviet Morse and radioprinter targets. The same picture revealed that [redacted] intercept positions were so tasked.<sup>45</sup>

To show once again how statistics can be misleading, however, apparently not all of those tasked positions were manned. More elaborate statistics for January 1949 indicated that of 874 U.S. intercept terminals installed, only 372 were manned. Accepting the manned figure as a more accurate reflection of reality, extrapolation would suggest that of the 548 terminals *tasked* against the Soviet Union, only about 233 were *manned*.<sup>46</sup> This number (233) compares favorably with the 196 manned terminals tasked against the Soviet Union in 1947.<sup>47</sup> As in 1947, probably about one-third of the more widespread

British intercept terminals, which numbered [ ] in 1947, were tasked against Soviet targets in 1948.<sup>48</sup>

Soviet collection statistics vary widely in 1948, depending on the source. Rowlett reported an average of almost 67,000 messages per month being intercepted by U.S. stations during 1947.<sup>49</sup> Another study reported an October 1949 total of 733,000 Soviet messages.<sup>50</sup> Therefore, by extrapolating those 1947 and 1949 figures, U.S. collection apparently averaged between 150,000 and 450,000 messages a month, including plaintext traffic in 1948. This range of numbers appears consistent with the given statistics for the number of plain language messages scanned per month in 1948 of between 163,000 and 277,000 (see Part Six below for details).

Captain Wenger, in his last month as CJO in February 1948, forwarded to USCIB a statement of intercept terminal requirements which presented an excellent picture of the state of development of collection, including against the Soviet target. For example, it had been determined that an average of six persons was required to staff each terminal, including intercept, maintenance and communications support. Additional radioprinter intercept terminals were deemed "essential." Moreover, all Morse intercept terminals needed to be retrofitted with frequency shift converters to allow for radioprinter collection as well as Morse intercept. The statement added that, currently, thirty Soviet two-, six- and nine-channel and simplex radioprinter intercept terminals were manned at U.S. facilities, but that 116 were required to provide adequate coverage, assuming continued British collaboration.<sup>51</sup>

Washington informed London in March that a newly opened intercept station on [ ] would include Soviet military communications in its tasking.<sup>52</sup> One of ASA's analytic branches urged its superiors in April to downgrade the classification of Soviet [ ] from Top Secret Codeword to Secret Codeword, arguing that "it is essential that the [ ] be available to the intercept station, in order that accurate [ ] identification can be made by the station."<sup>53</sup>

The U.S. had depended primarily on the British for intercept cover of Soviet targets in the European area. In fact, the new CJO, Colonel Hayes, estimated in 1948 that 65-70 percent of all Soviet raw traffic still came from British sources.<sup>54</sup> By July, however, ASA was acquiring its own collection capabilities, with four stations open in Germany, three at Herzo Air Base and one at Scheyern. All sites were undermanned, but operators were being trained as rapidly as possible. The four installations were authorized a total of 1,049 positions, but had only 497 installed and only 116 operators trained. Soviet Morse and printer links were prominent among the tasked targets.<sup>55</sup> By September, one of the ASA stations was concentrating on intercept of "Soviet low-level activity."<sup>56</sup>

Soviet [ ] Morse signals were intercepted by the British emanating from the Black Sea in July. GCHQ believed the signals were part of a Soviet naval exercise involving five major mobile surface units, a group of up to nine submarines,

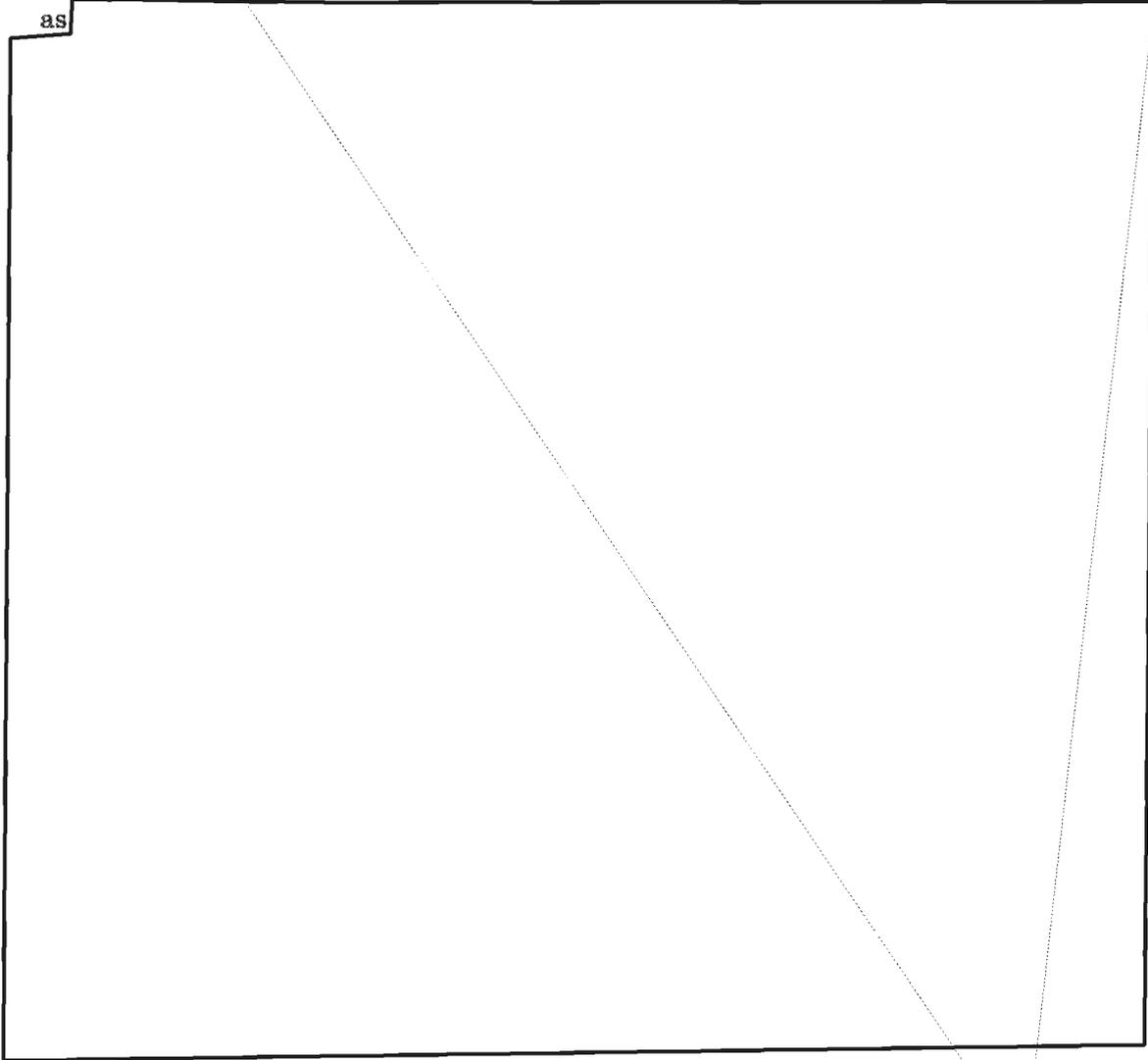
and five air units, under the direction of Black Sea Fleet Naval Air headquarters and the commander in chief, Black Sea Fleet.<sup>57</sup>



*Transmissions*

In October 1948, CSAW reported that a "peculiar type of Russian transmission has been noted for several months and a fair amount of unsuccessful effort [has been] expended in attempting to identify the purpose of those emissions." The transmission was described

as



EO 1.4.(c)  
PL 86-36/50 USC 3605

## Chapter 19

**"Ferret" Airborne Reconnaissance Plans  
and Early Operations**

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

**EARLY BRITISH CAPABILITY****EARLY AMERICAN CAPABILITY AND OPERATIONS*****U.S. Army Air Forces' Capability***

In July, USCIB apparently got its first detailed explanation of the U.S. Army Air Force's "Ferret" program as it would be applied to the Soviet target. U.S. Navy lieutenant C.T.R. Adams, acting assistant secretary, USCIB Secretariat (but effectively on Wenger's staff), had hand-carried a CJO-originated letter to General McDonald's office for coordination. During the visit, McDonald, who was the chief of staff for U.S. Army Air Force (USAAF) Intelligence (A-2), asked Adams if he was familiar with "ferret" operations. When Adams said he was not, McDonald and a Brigadier General Harbold, who was also present, put Adams in the picture in a very large way. Immediately after the session, Adams drafted a memorandum, recalling in great detail General McDonald's disclosure of the "ferret" capability and his appeal for USCIB collection guidance.

First, the general explained that the term ferret described the activities of "specially equipped airplanes which contained the latest (including classified) intercept and DF and radar equipment. Among other things, they are capable of intercepting very high frequency transmissions." General Harbold then interrupted McDonald to point out that at present the ferret aircraft were "employed in projects of primary interest to A-2, such as DF and radar locations and weather data." Harbold added that when a mission was planned, A-2 had normally notified ASA so that a COMINT person could be assigned to the project if such were the desire of ASA. Said Adams: "General Harbold gave me the distinct impression that ASA's interest to date has been cursory."

General McDonald said that thus far the COMINT aspect of ferret activities had had very little direction from responsible COMINT authorities, "with the result that much material of value is being wasted." Harbold's point was that USCIB-USCICC would seem to be the mechanism through which proper collection guidance could be acquired.

Laying out an "equidistant" world map, General McDonald explained that the intent of A-2 was to "completely encircle the USSR with adequate intercept facilities," with these ferret activities appearing to be well adapted for integration in this program. The general proposed that in order to do this, "some overall world-wide intercept program should be devised . . . to take the most advantage of the ferret plan." "I agree," said Adams, adding that the USCICC could request the Subcommittees on Intercept and DF and on Intelligence and Security to undertake a joint study and make recommendations concerning proper security measures for "ferret" as well as concerning the most effective mapping of routes to be flown by such planes. General McDonald was pleased with Adams' suggestion, expressing "the hope that this will be done."

Despite having already unloaded a great deal of information on Lieutenant Adams, General McDonald was not through. Adding, almost as an afterthought, that he already had three "ferret" aircraft operating in the Arctic, the general launched into a spirited argument in support of U.S. "self sufficiency" in COMINT. He recalled that during a recent USCIB meeting, Colonel Hayes, chief, ASA, had reported that "60-70 percent of our European intercept comes from the British." General McDonald also remembered Hayes' further comment that "this figure would probably grow as the U.S. forces are withdrawn from the various Theaters." McDonald condemned the "defeatist" attitude implicit in such statements. "The U.S. should begin immediately to take positive steps towards becoming self-sufficient. . . . Ferret activities would seem to have great possibilities in this respect." Not surprisingly, given the general's forceful presentation, Adams said later, "I agreed."

Finally, the USAAF A-2 returned to the issue of creating a mechanism for introducing USCIB collection guidance into "ferret" operations. Adams reported that "General McDonald ordered me to convey the substance of the above remarks to Captain Wenger and to express the general's hope that positive steps would be taken through USCIB-USCICC to correlate and guide ferret activities as well as to take the larger steps indicated." Again, said Adams, "I agreed to do this." The Navy lieutenant reported immediately back to Captain Wenger, who replied that he had known something about ferret activities, but that "General McDonald's remarks had added considerably to that knowledge." Adams believed that the CJO would "take some action in the matter."<sup>2</sup>

In August, additional information became available to the COMINT community on USAAF "ferret" airborne reconnaissance plans and operations against the Soviet Union:

1. The subject operations are divided into two projects, PASSIONATE and BIOGRAPH, both of which are classified Top Secret.
2. PASSIONATE consists of one especially fitted B-29 electronic search airplane. It is operating in the Alaska, Kurile, Siberian coastal areas and has been over the North Pole. Its primary mission is a

search for enemy radar and loran data, covering a search range of from [redacted] MCS. The crew includes six countermeasures specialists and one man from ASA.

3. This mission is considered a most hazardous one both from the natural peril and capture standpoints. All flight personnel are volunteers and are fully apprised of possible consequences should the plane be forced to land in foreign territory. The crew is warned that in the event of detention in foreign territory repatriation will be attempted but will probably be unsuccessful. For purposes of cover the project is described as a weather mission. Equipment for complete demolition of the plane and its contents has been provided. Foreign coasts are approached to within 15 or 20 miles.

4. As a supporting project, three other planes (not B-29's) are in the Alaskan area but electronic search in this instance is considered secondary to regular operations.

5. Mission BIOGRAPH operates in the European area primarily in search of guided missile activity. Operations are conducted in the Baltic and other suspected areas using two B-17 planes.

6. These two projects will be rapidly expanded and by July 1948 it is expected that 10 B-29's, especially fitted as in PASSIONATE, will be available for special electronic search projects under cognizance of the Strategic Air Command.<sup>3</sup>

### ***Early USAF "Ferret" Operations***

A month later, the U.S. Air Force was born, and by the end of the year USAF "ferret" flights had become public knowledge. For example, on 23 and 25 December 1947, U.S. reconnaissance aircraft flew missions over the Bering Strait against Soviet Far East targets along the Chukotsk Peninsula, and the Soviets publicly protested both missions.<sup>4</sup>

On 5 August 1948, a "stripped down" USAF B-29 "ferret" overflew Soviet "Siberia" on an almost twenty-hour-long reconnaissance mission from Alaska to Japan; on 8 August, the same aircraft reversed the flight path, returning to Alaska. These two missions were repeated on 1 and 6 September.<sup>5</sup>

## Notes

### Chapter 12: Middle BOURBON, The Second Year – 1946

1. (U) Robert Louis Benson and Cecil James Phillips, *History of VENONA*, National Security Agency, 1995 (~~TSC~~), CCH General Collection.
2. (U) ONI memorandum of 18 December 1945 to Chief of Naval Communications relative to priorities of interest to ONI for communications intelligence, cited in Op-23-Y memorandum to STANCICC, subject: Communications Intelligence, Priorities of Countries as to Interest to ONI, 24 April 1946 (~~TS~~); CCH Collection, Series XII, H. box 47.
3. (U) Op-23-Y memorandum to STANCICC, subject: Communications Intelligence, Priorities of Countries as to Interest to ONI, 24 April 1946 (~~TS~~), which was itself updated in October 1946. Assistant Chief of Naval Intelligence (Op-32-Y) memorandum for the Chairman, USCICC, subject: Communications Intelligence Targets - Priority List of, 18 October 1946 (~~TS~~); both memoranda in CCH Collection, Series XII, H. box 47.
4. (U) WDGAS-90 (Rowlett) memorandum to Chief, WDGAS-93, et al., subject: Mechanism for Determination of Intercept Priorities, 25 June 1947, and inclusions (~~TS~~); NSA/CSS Archives, Accession No.1494, location G16-0407-3.
5. Ibid.
6. Ibid.
7. (U) Handwritten note stating: "From a desc[ription] of cryptanalytic situation in Feb. 1946 in Wenger files;" CCH Collection, Series IV.AA.6.1.
8. ASA History of BOURBON Problem.
9. Burns, 35-37.
10. Howe, JOP study, 28.
11. Ibid, 107.
12. Burns, 37.
13. Ibid, 64.
14. (U) STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 1 May 1946 (~~TS~~); CCH Collection, Series IV.AA.6.1.
15. (U) JLG memorandum from Rufus L. Taylor, Cdr, USN, D/Coordinator for Liaison, for Chief, ASA and Op-20-2, subject: Short Title LSIC, Security Classification and use of in Correspondence. 28 October 1946 (~~S~~); NSA/CSS Archives, Accession No. 1374, location G16-0406-3.
16. (U) Enclosure A [to unspecified correspondence] entitled "Personnel on Duty with United States Communications Intelligence Liaison Center in Great Britain" and Enclosure B similarly entitled ". . . in Washington," 16 August 1946 (not marked, but treated as Secret); NSA/CSS Archives, Accession No. 1421, location G16-0406-6.

17. (U) STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 16 February 1946 (~~TS~~); CCH Collection, Series IV.AA.6.1.
18. Semi-Monthly Report on BOURBON, 1 May 1946.
19. (U) LSIC/USLO cover memoranda from Christopher (for Manson) to Col. Rowlett, subject: BOURBON Reports B-89 to B-99, dated from 1 to 31 May 1946 (~~TSC~~); NSA/CSS Archives, Accession No. 30886, location G-05-0302-3.
20. (U) Deputy Coordinator for Liaison memorandum for BOURBON Coordinator, subject:  5 November 1946 (~~TS~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.
21. (U) Senior USLO, LSIC, memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB Newsletter No. 13-46, 25 August 1946 (~~TS~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.
22. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB Newsletter No. 24-46, 22 November 1946 (~~TS~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.
23. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB Newsletter No. 22-46, 12 November 1946 (~~TS~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.
24. (U) Collins memorandum, subject: Report on Liaison between United States Communications Intelligence Agencies and the London Signal Intelligence Centre, 25 July 1946 (~~TSC~~); CCH Collection, Series V.J.2.9.
25. Ibid. Italics added.
26. Ibid.
27. (~~C~~) British Joint Staff Mission memorandum for STANCIB-STANCICC, subject: Treatment of BOURBON during Commonwealth Conference, 27 February 1946 (~~TSC~~); NSA/CSS Archives, Accession No. 4835, location G05-0302-3.
28. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: STANCIB Newsletter No 2-46, 27 May 1946 (~~TS~~), NSA/CSS Archives, Accession No. 759, location G16-0407-3.
29. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USCIB Newsletter No 6-46, 25 June 1946 (~~TS~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.
30. (U) Senior USLO, LSIC, memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB "Special" Newsletter No. 11-46, 1 August 1946 (~~TS~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.
31. (U) Senior USLO, LSIC, memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB Newsletter No. 20-46, 27 October 1946 (~~TS~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.
32. (U) JLG memorandum for CJO, subject: Cover Names, 24 February 1947 (~~S~~); NSA/CSS Archives, Accession No.1489; location G16-0407-1.
33. (U) JPAG Monthly Status Report, December 1947, (~~TSC~~); NSA/CSS Archives, Accession No. 42466, location H10-0106-3.
34. (~~S~~) Minutes of Brigadier Tiltman's Fourth BOURBON Meeting, 25 January 1946 (TSC); NSA/CSS Archives, Accession No. 29450, location G05-0302-3. TICOM was the acronym for Target Intelligence Committee, a joint U.S.-U.K. effort after the war to investigate all phases of German and Japanese cryptologic operations and organizations. TICOM teams of U.S. and British officers scoured the German and Japanese countrysides, locating

their former enemies' COMINT centers and intercept stations, appropriating any COMINT materials and cryptographic hardware, and interrogating as many German and Japanese cryptologic personnel as they could identify and locate.

35. (U) STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 1 March 1946 (~~TS~~); CCH Collection, Series, IV.AA.6.1.

36. (U) STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 16 March 1946 (~~TS~~); CCH Collection, Series IV.AA.6.1.

37. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 12-46, 16 August 1946 (~~TS~~), NSA/CSS Archives, Accession No. 759, location G16-0407-3.

38. Senior USLO, LSIC Newsletter No. 13-46, 25 August 1946.

39. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 27-46, 18-20 December 1946 (~~TS~~), NSA/CSS Archives, Accession No. 759, location G16-0407-3. Another name used for this material was Stella Polaris.

40. (U) Wenger memorandum for Op-20, subject: Russian Interest in U.S. Communications, 13 September 1946 (~~TSC~~); NSA/CSS Archives, Accession No. 8449, location G16-0410-4.

41. Ibid.

42. (U) WDGAS-96 memorandum from Mr. Stephen L. Wolf, T/A Specialist, to Rowlett, Chief, Operations Division, Subject: Reports of Visit of Mr. Stephen L. Wolf, WDGAS-96-E, to London and Frankfurt, 26 February 1947 (~~TSC~~); CCH Collection, Series V.C.2.10. Hereafter, Wolf.

**Chapter 13: Old BOURBON, The Third Year - 1947**

1. (U) JPAG memorandum from Rowlett to Op-20-N-2 and CSGAS-90, subject: Standing Operating Procedures for the Special Russian Coordinator, 27 October 1947 (~~TSC~~); CCH Collection, Series V.R.1.3.

2. (U) JPAG Monthly Status Report, December 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 42466, location H10-0106-3.

3. (U) Although there was a great deal of 1946 correspondence concerning the planned trip to Washington, D.C., no 1947 information could be found to confirm the actual visit. Since Travis made a confirmed trip to the United States less than a year later (in December 1947), it is likely that the January 1947 visit to Washington was cancelled.

4. (U) JLG memorandum for  signed by P.J. Karl, Lt. USN, JLG, subject: Radio Channels for Liaison between SUSLO, LSIC, and Coordinator for Joint Operations, Washington, 7 January 1947 (~~S~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.

5. (U) USLO memorandums to JICG, subject: USTALO Informal Report No. 1, 20 January 1947 (~~S~~), No. 2, 24 January 1947 (~~TS~~), and No. 3, 7 February 1947 (~~S~~); NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

6. (U) Interview with Dr. Tordella, 28 February 1994, who recalled that "it was the coldest winter on record in England" in 1947. "There was virtually no electric power in London" while he was there because the "ice in the rivers prevented the coal barges from reaching the local power plants."

PL 86-36/50 USC 3605

7. (U) ASA memorandum, subject: Marston Report on Tour of Duty at LSIC, 21 February 1947 ~~(TSC)~~; CCH Collection, Series V.J.2.9.

8. Wolf.

9. (U) ASA (WDGAS-90) cover memorandum for D/Coordinator for Liaison from Frank B. Rowlett, Chief, Operations Division, subject: Report on Tour of Duty as Special BOURBON Representative at LSIC dated 28 January 1947 ~~(TSC)~~, 10 February 1947 ~~(TSC)~~; NSA/CSS Archives, Accession No. 5333, location G20-0208-3.

10. Howe, JOP study, 28.

11. (U) JICG (J.R. Dennis) memorandum for Op-20-N-2, subject:

29 May 1947 ~~(TSC)~~; NSA/CSS Archives, Accession No. 1496, box CPBP65.

12. (U) LSIC Monthly Status Report, May 1947 ~~(TSC)~~; NSA/CSS Archives, Accession No. 2006N, box CBQI45.

13. (U) JPAG memorandum to Op-20-N-2, subject: LSIC Monthly Status Report, May 1947, 7 July 1947 ~~(TSC)~~; NSA/CSS Archives, Accession No. 8449, location G16-0410-4.

14. (U) LSIC Minutes of S Section Meeting, 1 July 1947 ~~(TSC)~~; NSA/CSS Archives, Accession No. 5494, box CPBI51.

15. (U) Rowlett memorandum to CJO, subject: Review of Current U.S.-British Collaboration in the Communications Intelligence Field, 5 August 1947 ~~(TSC)~~. An undated, unsourced draft is available in the NSA/CSS Archives, Accession No. 1377, box CBPB57. A heavily annotated version is available in CCH Collection, Series V.J.2.7. Hereafter Rowlett Review.

16. Howe, JOP study, 70.

17. Rowlett Review.

#### **Chapter 14: Beyond BOURBON, The Fourth Year - 1948**

1. Burns, 440-441.

2. Howe, JOP study, 169.

OGA  
EO 1.4.(c)

5. Ibid.

6. Burns, 61.

7. ~~(S)~~ The Stone Report, actually a majority report and an accompanying minority position, failed to reconcile conflicting views of the various USCIB members. Following the naming of a new secretary of defense, Louis A. Johnson, the issues were resolved, and on 20 May 1949, AFSA, was formed; the goal of effective centralization was not successful, however, and the National Security Agency replaced AFSA three years later in 1952. See Burns, 61-65.

8. (U) H.L. Conley memorandum to Chief, CSGAS-90, subject: Conduct of [redacted] Problem, 14 December 1948 (~~TSC~~); NSA/CSS Archives; Accession No. 5505, box CBNI22. Hereafter, Conley Memorandum.

9. Ibid.

10. Ibid.

11. (U) JPAG Monthly Status Reports, January-December 1948 (~~TSC~~); NSA/CSS Archives; Accession No. 42466, locations H10-0106-3 and H10-0106-4.

12. Conley Memorandum.

13. Howe, JOP study, 125-126.

14. Conley Memorandum.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

15. (U) JLG memorandum for CJO, subject: Activity Report, 1 April 1947-31 March 1948, 23 March 1948 (~~S~~), CCH Series V.J.1.

16. ~~TC~~ (Wenger) memorandum for USCICC, subject: Estimated USCIB [redacted] 1 February 1948; dated 25 Feb 1948 (~~TS~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.

17. ~~C~~ JICG (H. Johnson, Acting Deputy Coordinator for Intercept Control) Memorandum for the Record, subject: LSIC Diversion of Facilities to the Russian problem, 27 May 1948 (~~S~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.

18. (U) George F. Howe, *The Narrative of AFSA/NSA*, Part IV, Final Draft, Chapter XX, 3, April 1963 (~~TSC~~); CCH General Collection.

19. Howe, History, Part IV, Chapter XX, 5.

20. (U) Rowlett's 12 July 1948 note to Colonel Hayes, covering LSIC/USLO (Lt. Fred Bright) letter of 5 July 1948 to Rowlett (~~TSC~~); NSA/CSS Archives; Accession No. 4978, location G05-0405-5.

21. Howe, History, Part IV, Chapter XX, 12.

22. ~~TS-CCO~~ Senior British Liaison Officer (SBLO) memorandum for Chairman, USCIB, on the subject of [redacted] 7 July 1948 (~~TSC~~); NSA/CSS Archives; Accession No. 8223, location G15-0510-5.

23. Ibid.

24. ~~TS-CCO~~ USCIB memorandum for SBLO, subject [redacted] 9 July 1948 (~~TSC~~); NSA/CSS Archives; Accession No. 8223, location G15-0510-5.

25. (U) Originator unknown; unaddressed paper, entitled: Comments of OMGUS Berlin Cable, 25 January 1949 (~~TSC~~); NSA/CSS Archives, Accession No. 5193, location H01-0301-4.

26. ~~S~~ USAF memorandum for Captain J.N. Wenger, USN, from George C. McDonald, Major General, USAF, Director of Intelligence, Office of D/Chief of Staff, Operations, subject: Collaboration with British on Electronic Reconnaissance, 29 March 1948 (~~TS~~); CCH Collection, Series V.J.2.3.

27. (C) JLG memorandum signed by P.J. Karl, Lt. USN, D/Coordinator for Liaison, to Chief, ASA and OP-202, subject: Abolition of British Secret Titles, 15 October 1948 (S); NSA/CSS Archives, Accession No. 1375, location G16-0406-3.

28. Howe, JOP study, 141.

29. (C) JLG memorandum for Chief, AS-90, subject: [redacted] t ASA, 24 July 1947 (TSC); cited in Howe, JOP study, 140.

30. Ibid., 141-144. Howe added: "By September 1949, the effort on [redacted] communications was absorbing the efforts of 36 people, of whom 12 were engaged in cryptanalysis of 5 systems."

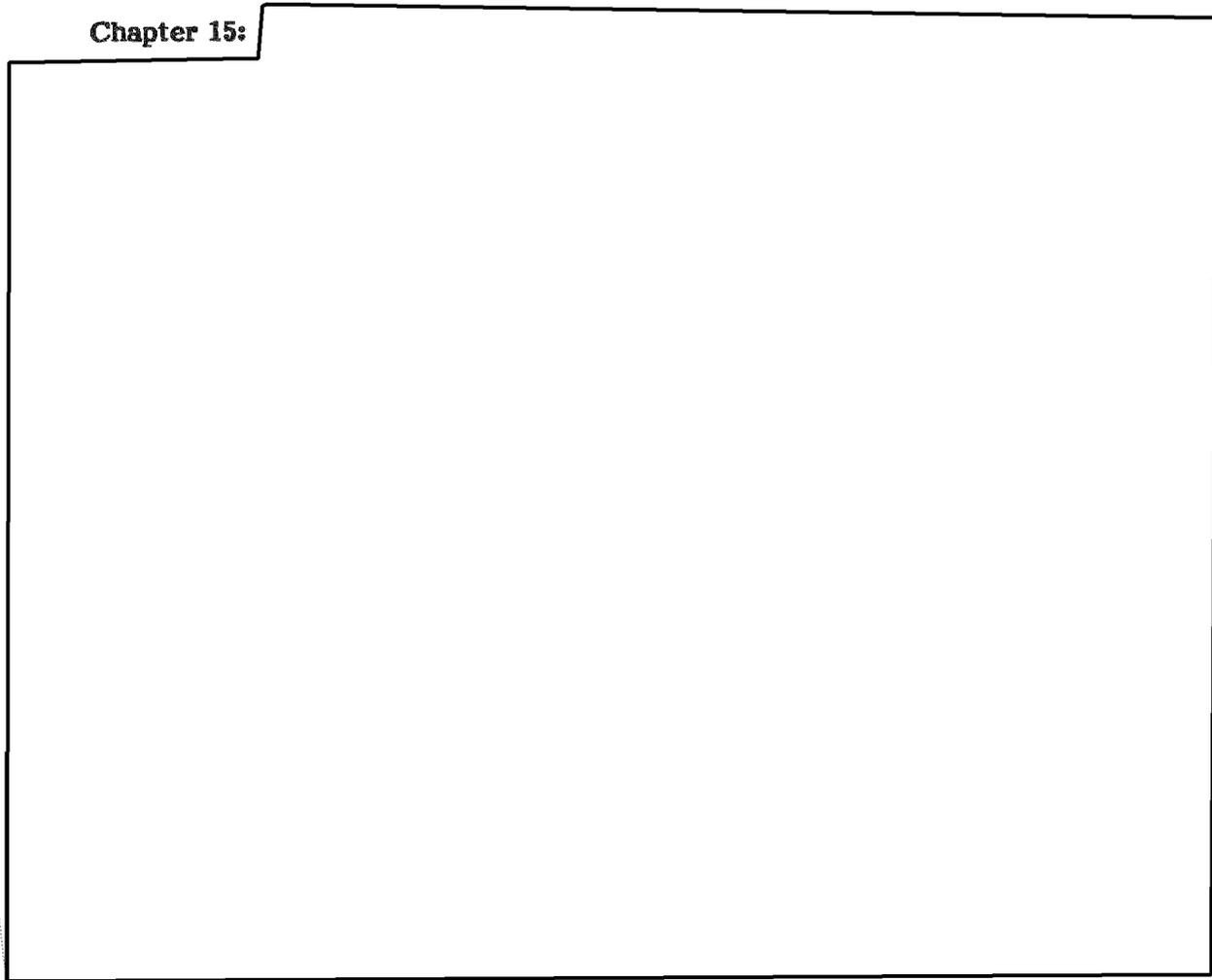
31. (U) GCHQ Monthly Status Report, October 1948 (TSC); NSA/CSS Archives; Accession No. 2006N, box CBQI 48.

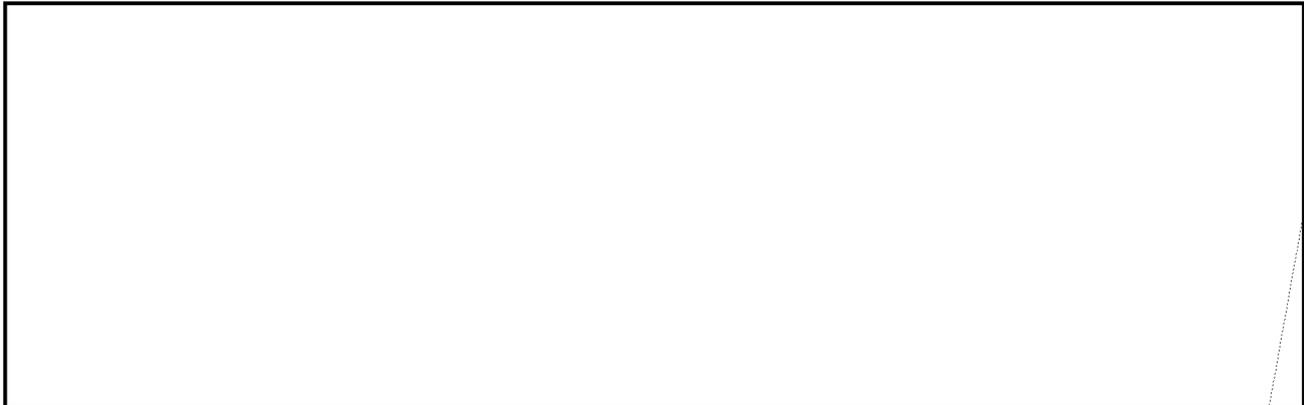
32. (S) [redacted] USSR #14. Title: Flight Unit (LETNAYa ChAST); location: [redacted] 30 April 1948 (TSC); NSA/CSS Archives, Accession No. 9268, location G16-0211-4.

OGA  
EO 1.4.(c)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

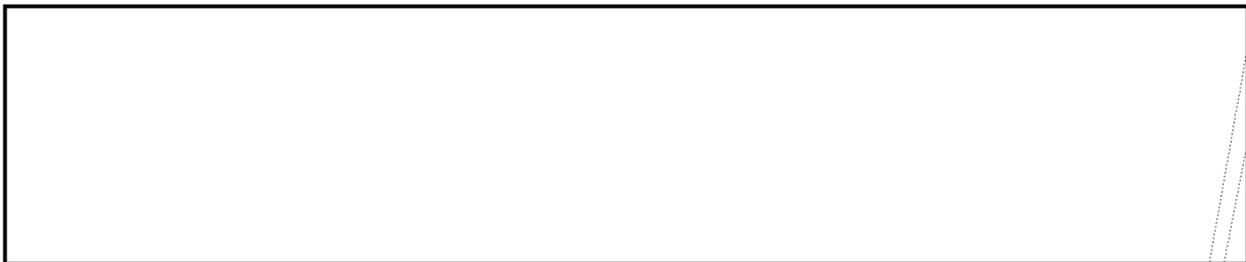
**Chapter 15:**



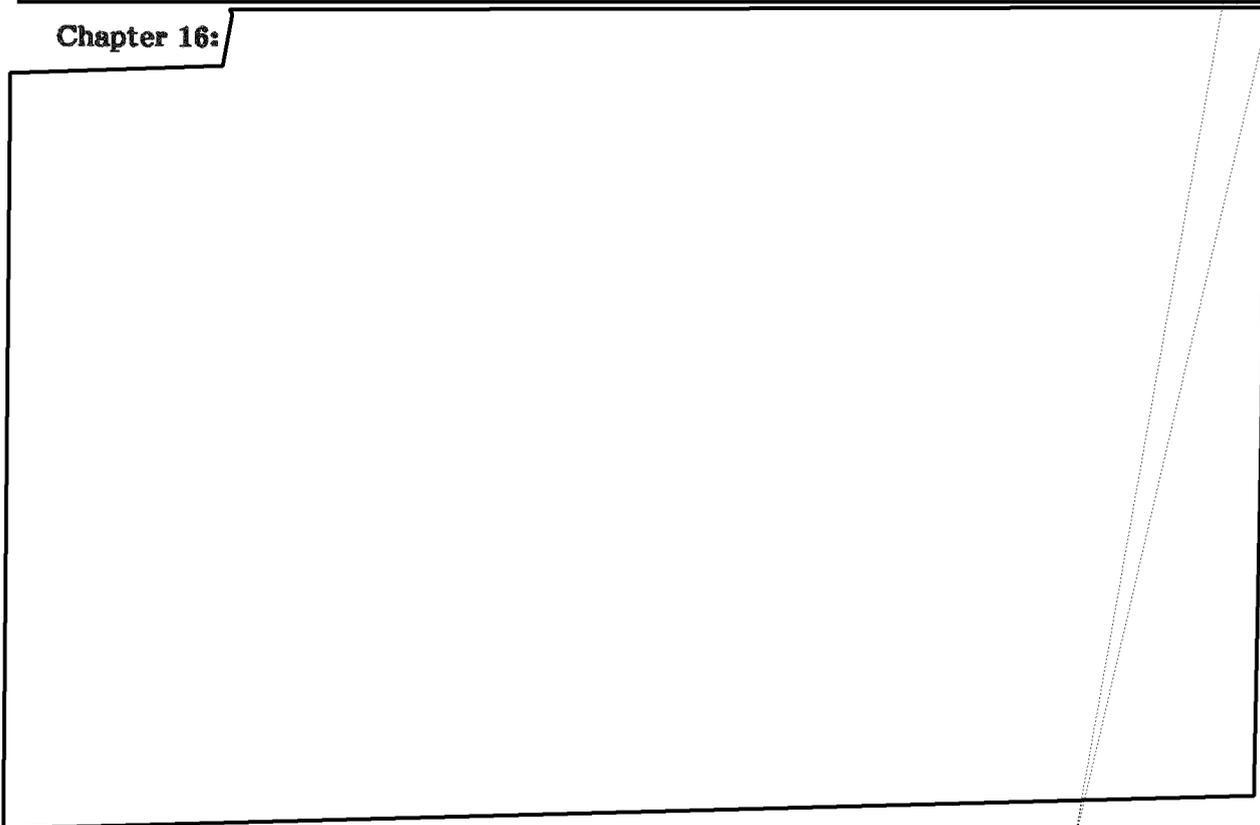


15. Howe, JOP study, 81.

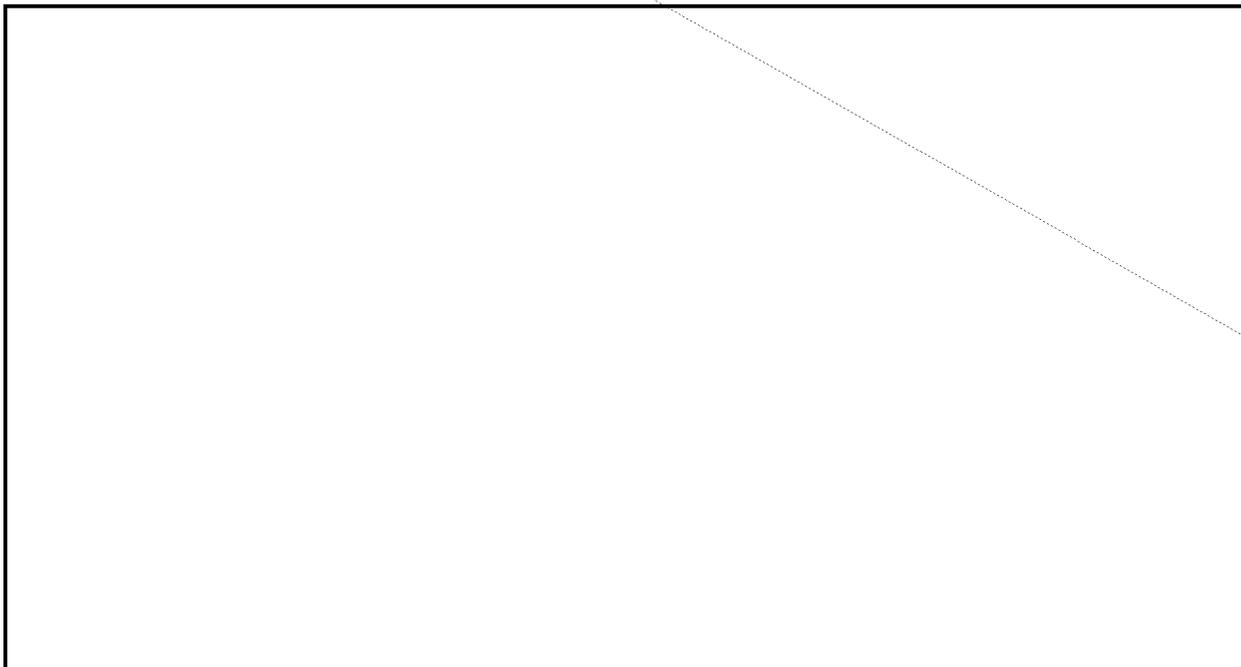
16. Ibid., 79.



**Chapter 16:**



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

**Chapter 17: Personnel Resources, 1946-1948**

1. (U) JPAG Monthly Status Reports, May-December 1946 ~~(TS)~~; NSA/CSS Archives; Accession No. 42466, location H10-0106-1. Also JPAG Monthly Status Reports, December 1947, and 1948.
2. (U) WDGAS-9 (Personnel) message to NY-1-A, 9 September 1946 ~~(TS)~~; NSA/CSS Archives, Accession No. 30886, location G05-0302-3.
3. JPAG Monthly Status Reports, December 1946, 1947 and 1948.
4. JPAG Monthly Status Report, February 1948.
5. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USCIB Newsletter No. 7-46, 2 July 1946 ~~(TS)~~, NSA/CSS Archives, Accession No. 759, location G16-0407-3.
6. Senior USLO, LSIC Newsletter No. 12-46, 16 August 1946.
7. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 19-46, 21 October 1946 ~~(TS)~~, NSA/CSS Archives, Accession No. 759, location G16-0407-3.
8. (U) LSIC Monthly Status Reports, May-December 1946 ~~(TS)~~; NSA/CSS Archives; Accession No. 2006N, boxes CBQI43 and 44. The number  traffic analysts (per Wolf).
9. (U) In addition to pertinent JPAG Monthly Reports for U.S. statistics, British statistics are found in LSIC and GCHQ Monthly Status Reports, December 1946, 1947, and 1948; NSA/CSS Archives, Accession No. 2006N, boxes CBQI44, 46 and 48.

PL 86-36/50 USC 3605  
EO 1.4.(c)

**Chapter 18: Field Operations**

1. (U) Handwritten note stating: "From a desc[ription] of cryptanalytic situation in Feb. 1946 in Wenger files;" CCH Collection, Series IV.AA.6.
2. JPAG Monthly Status Reports, May-December 1946.
3. (U) Op-20-G manual, entitled: BOURBON Non-Morse Glossary, 1 January 1946 ~~(TS)~~; CCH Collection, Series V.B.2.1.
4. (U) Op-20-G working aid, BOURBON Non-Morse Communications Procedures, 1 February 1946 ~~(TS)~~; CCH Collection, Series IV.AA.14 and V.B.2.2.
5. JPAG Monthly Status Report, May 1946.
6. (U) Unsigned ASA study entitled: BOURBON PROJECT: Survey of Machine Requirements, undated but produced circa June 1946 ~~(TS)~~; NSA/CSS Archives, Accession No. 45812, location G03-0401-7.
7. JPAG Monthly Status Report, August 1946.
8. JPAG Monthly Status Report, September 1946.
9. (U) Navy memorandum to unidentified, subject: Intervals between TOI and TOR NEGAT for Adak BOURBON intercepts, 2 April 1946 ~~(S)~~; NSA/CSS Archives, Accession No. 8449, location G16-0410-4.
10. Collins. (U) Red Forms were a carryover from the Enigma intercept forms of World War II; see David Kahn, *PL 86-36/50 USC 3605*  
*Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (Boston: Houghton Mifflin Co., 1991), 141.
11.  memorandum to Director GC&CS, subject: BOURBON Keyboards and Transliteration Systems, 5 March 1946 ~~(TS)~~; NSA/CSS Archives, Accession No. 30886, location G05-0302-3.
12. Senior USLO, LSIC Newsletter No. 7-46, 2 July 1946.
13. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 8-46, 12 July 1946 ~~(TS)~~, NSA/CSS Archives, Accession No. 759, location G16-0407-3.
14. Senior USLO, LSIC Newsletter No. 24-46, 22 November 1946.
15. (U) These are consensus numbers developed by the author. Conflicting numbers can be found in Wolf, in Rowlett Review, and in Minutes of an LSIC "S" Section Meeting held on 19 May. 30 May 1947 ~~(TS)~~; NSA/CSS Archives, Accession No. 5494, box CBPI51.
16. Rowlett Review.
17. Wolf.
18. Rowlett Review.
19. Ibid.
20. Ibid.
21. (U) JPAG Monthly Status Report, January 1947 ~~(TS)~~; NSA/CSS Archives, Accession No. 42466, location H10-0106-1.

22. (U) Op-20-2 (Goodwin) memorandum for The Secretary of the Navy and Fleet Admiral C.W. Nimitz, subject: Report of joint Army-Navy progress in BOURBON Communication Intelligence; July, August, and September, 1947, 3 October 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 9449, G16-0410-4. Also, Op-20-2 memorandum for The Secretary of the Navy (&) Fleet Admiral C. W. Nimitz, subject: Monthly (May and June combined) Report of joint Army-Navy progress in BOURBON Communication Intelligence, 18 July 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 8449, location G16-0410-4. EO 1.4 (b) PL 86-36/50 USC 3605

23. ~~JICG~~ (Rubin) cover memorandum to A/Deputy Coordinator for Liaison, subject:

27

March 1947 (~~S~~); NSA/CSS Archives, Accession No. 1358, location G16-0406-2.

24. (U) JICG/2.32/4.4 (Dennis) memorandum (for the Record), subject: Report on Russian Amateur Radio Operators, 26 September 1947 (~~S~~), with cc: Op-20-2, Op-32-Y-1, JICG (Lt. Dickey), and JLG; NSA/CSS Archives, Accession No. 1496, box CBPB65.

25. (U) LSIC Monthly Status Report, January 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 2006N, box CBQI44.

26. (U) USLO memorandum, thru JLG, to JICG, subject: USTALO Informal Report No. 6, 31 March 1947 (~~TSC~~), NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

27. (U) USLO memorandum to JICG, Washington, subject: USTALO Informal Report No. 14, 17 September 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

28. (U) LSIC Monthly Status Report, August 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 2006N, box CBQI46.

29. (U) LSIC Monthly Status Report, January 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 2006N, box CBQI44.

30. Wolf.

31. Ibid.

32. Ibid.

33. Ibid.

34. (U) Informal technical note to Phil Patton, from Herb Conley, SUSLO, LSIC., 24 September 1947 (~~S~~); NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

35. (U) CNO memorandum from G.P. McGinnis, Lt. Cdr, USN, for Herb Conley, subject: Direction Finding Activities. 25 September 1947 (~~S~~); NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

36. ~~S~~ TICOM is the acronym for Target Intelligence Committee, a joint U.S.-U.K. effort after the war to investigate all phases of German and Japanese cryptologic operations and organizations. TICOM teams of U.S. and British officers scoured the German and Japanese countrysides, locating their former enemies' COMINT centers and intercept stations, appropriating any COMINT materials and cryptographic hardware, and interrogating as many German and Japanese cryptologic personnel as they could identify and locate.

37. (U) WDGAS-93B memorandum signed by Oliver R. Kirby, Captain, Signal Corps, Executive Officer, WDGAS-93B, to Chief, AS-90, subject: New Non-Morse Processing Equipment, 18 March 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 45812, location G03-0401-6. (~~S-CCO~~) Information that CSAW's Dr. Tordella and ASA's Captain

Kirby worked closely together to develop Soviet printer collection and processing equipment in the late 1940s was provided by Mr. Cecil Phillips, recalling statements made by Dr. Tordella during oral history interviews.

38. (U) Revised WDGAS-93B memorandum signed by Oliver R. Kirby, Captain, Signal Corps, Executive Officer, WDGAS-93B, to Chief, AS-90, subject: New Non-Morse Processing Equipment, 22 April 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 45812, location G03-0401-6.

39. (U) U.S. Liaison Office (hereafter USLO) memorandum, signed by a P.J. Patton, to JICG, Washington, subject: USTALO Informal Report No. 1, 20 January 1947 (~~S~~); and Report No. 2, 24 January 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

40. (U) USLO memorandum, signed by a P.J. Patton, to JICG, Washington, subject: USTALO Informal Report No. 3, 7 February 1947 (~~S~~); NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

41. (U) USLO memorandum, thru JLG, Washington, to JICG, Washington, subject: USTALO Informal Report, No. 5, 17 March 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

42. (U) USLO London memorandum for CJO (USCIB), subject: [Soviet] Radio Communications, 6 June 1947 (~~S~~); NSA/CSS Archives, Accession No. 1363, location G16-0406-2.

43. (U) Intercept site listing of unknown but probable authoritative source, 28 April 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.

44. Howe, JOP study, 145-148.

45. (U) JICG/B.5 Intercept Operators Summary, period 1-15 October 1948; 25 October 1948 (~~S~~); CCH General Collection.

46. Howe, JOP study, 152.

47. Rowlett Review.

48. Ibid.

49. Rowlett Review, Tab A-2.

50. Howe, JOP study, 156.

51. (U) CJO (Wenger) memorandum for USCICC, subject: Estimated USCIB Intercept Terminal Requirements, 1 February 1948; dated 25 Feb 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.

52. (U) JICG memorandum for Col. P. Marr-Johnson (British Liaison Officer), subject: Missions to be Assigned to Station USM-36, 19 March 1948 (~~S~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.

53. (~~S~~) AS-93 memorandum to AS-10, subject: Reclassification of Russian  29 AFQ 1.4.(c)  
1948 (~~TSC~~); NSA/CSS Archives, Accession No. 5333, location G20-0206-2. EO 1.4.(b)

PL 86-36/50 USC 3605

54. Howe, JOP study, 71.

55. (U) JICG (P.J. Patton) memorandum for USTALO, subject: Forwarding of Information, 12 July 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.

56. (U) LSIC/USLO (Norman Boardman) letter to "Dear Mr. Rowlett," 4 September 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 4978, location G05-0405-5.

57. (U) LSIC Monthly Status Report, August 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 2006N, box CBQI48.

58. (~~S~~) JPAG Interim Report #4495, Section RU#1719, subject: Op-20-NT-1 Russian Traffic Analysis Bulletin #27, 13 October 1948 (~~SC~~); NSA/CSS Archives, Accession No. 46470, location H07-0111-2. Also Op-20 Memorandum for Op-202-T and 202-L, thru N-2, Subject  Transmissions, 19 October 1948 (~~TSC~~); CCH Collection, Series V.R.1.8.

59. Ibid.

PL 86-36/50 USC 3605  
EO 1.4.(c)

60. Ibid.

### Chapter 19: "Ferret" Airborne Reconnaissance Plans and Early Operations

1. (U) USLO London memorandum to JICG, Washington, subject: USTALO Informal Report No. 2, 24 January 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 5494, location G15-0201-2.

2. (U) C.T.R. Adams' *Aide Memoire*, subject: "Ferret" Activities, 17 July 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 1496, box CBPB65. The abbreviation C.I. has been used in various contexts to mean either communications intelligence, crypto-intelligence, and counterintelligence. Believe Adams' use of C.I. means the first of the three expansions.

3. (U) Op-20-S (R.T. Kelly, Lt. USN, Acting) memorandum for Op-20-2 via Op-20-T, subject: Current Army Ferreting Operations, 11 August 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 1496, box CBPB65.

4. Jeffrey Richelson, *American Espionage and the Soviet Target* (New York: Morrow, 1987), 120.

5. William E. Burrows. *Deep Black: Space Espionage and National Security* (New York: Random House, 1986), 58-59. Also, Jeffrey Richelson. *American Espionage and the Soviet Target* (New York: Morrow, 1987), 111.



### Part Four

## BOURBON Cryptanalysis

### Chapter 20

### Core Cryptologic Task

#### LARGEST ANALYTIC WORK FORCE

Solid monthly statistics became available in June 1946 for the numbers of both the U.S. and British cryptanalysts dedicated to the Soviet problem. The following chart shows not only the large number of cryptanalysts already employed but the increase in these resources over two and one-half years:

PL 86-36/50 USC 3605  
EO 1.4.(c)

Month	U.S.	U.K.	Total
June 1946			
December 1946			
December 1947			
December 1948			

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

The reader can also infer from the chart the level of emphasis being placed on Soviet cryptanalysis. Starting with growth rates of 20 percent and 18 percent through 1947, right in the face of general demobilization and reduction of resources in both the American and British defense establishments. An appreciation for the importance placed on cryptanalysis as the core cryptologic skill can be gained, too, when it is understood that by 1947 the number of cryptanalysts exceeded the total number of traffic analysts and linguists combined [redacted]

Things began to change in 1948, however, coinciding with the loss of the major readable Soviet cryptosystems. For the first time since the start of the BOURBON project, the number of people in a career field fell, albeit by only 4.8 percent. Nevertheless, the decrease in the number of American cryptanalysts working the Soviet target from [redacted] in December 1947 to [redacted] by December 1948 is significant, particularly in light of the increase of 59 percent in people working the Soviet target generally.

This drop in American cryptanalytic resources in 1948 was swept away by a continuing [redacted] increase in British cryptanalysts dedicated to the Soviet problem, giving a small Allied growth in cryptanalysts of [redacted]. The American figure actually rose briefly to a high of [redacted] in March 1948 before dropping back to [redacted]. Even the British numbers turned downward, however, as the high-water mark for their cryptanalysts was [redacted] in September 1948.<sup>2</sup>

PL 86-36/50 USC 3605  
EO 1.4.(c)

**A SOBERING STATISTICAL OVERVIEW OF THE EFFORT**

Detailed statistics also became available in mid-1946 concerning the number of identified Soviet cryptosystems being observed, the number of messages copied each month, and the results of cryptanalytic effort against those systems, specifically numbers for decrypts, translations, and summary reports. The statistics varied wildly from month to month, from agency to agency, probably the result of backlogs building up and being cleared up wholesale aperiodically because of [redacted] being revised and refined or systems becoming obsolete and dropped from the accounting. However, generally speaking, each nation each month [redacted] in use, received about [redacted] messages (of which there was much duplication) to work, [redacted] from [redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Sobering are the conclusions one can draw from these general statistics; namely, that only about [redacted] g [redacted] Besides remembering that it generally takes the mining of a lot of ore to extract a little gold, it is important to point out that, valid as these general statistics might be, there were also relatively productive exceptions. For example, in August 1946 GCHQ [redacted] messages, while American [redacted] production rose steadily from [redacted] by December 1946.<sup>4</sup>

EO 1.4.(c)  
EO 1.4.(b)

Another way to look at the statistics is comparing the number of [redacted] systems. A revealing body of statistics for March 1946<sup>5</sup> shows that [redacted] being worked by ASA and [redacted] by CSAW, of which only [redacted] were [redacted] While this [redacted] percent [redacted] ratio seems low, it's important to remember that the BOURBON project was only about six months old at the time. By December 1946, in the U.S., [redacted] were classified [redacted] (with another [redacted] and [redacted] were labeled as [redacted] But another [redacted] allowing the statistician to conclude that almost [redacted] percent of the systems were [redacted] Again, showing how statistics can be misleading, about [redacted] systems were obsolete or of very low volume.<sup>6</sup>

36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

[redacted] COMINT on the Soviet services from 1945 through 1948. Much of the diagnostic research on [redacted] families, the [redacted] was done in 1946. In addition, [redacted] appeared in 1946.

At GCHQ each month in 1947, some [redacted] were under various levels of cryptanalytic attack. Some [redacted] with the [redacted] using most of the systems. Monthly averages varied considerably, but GCHQ received about [redacted] Soviet

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

EO 1.4.(c) messages per month, [redacted] of them, translated [redacted] and produced  
EO 1.4.(b) reports on about [redacted] a month.<sup>8</sup>  
PL 86-36/50 USC 3605

With more than twice the cryptanalytic resources applied than GCHQ, Americans [redacted] per month, [redacted] Soviet services. ASA and CSAW cryptanalysts reviewed [redacted] pages of [redacted] per month (probably including duplicates of what the U.K. was reviewing), produced monthly about [redacted] of which about half were translated [redacted] per month, [redacted] of which were from [redacted] which the British did not work), and issued almost [redacted] summaries a month.<sup>9</sup>

PL 86-36/50 USC 3605

Combining the British and American figures gives a complete statistical picture for 1947. Assuming probably total duplication of effort on the review of traffic, but very little in the [redacted] Allied cryptanalysts reviewed monthly at least [redacted] pages of traffic, [redacted] messages, translated over [redacted] and issued summary reports on almost [redacted] translations. Of course, it was never solely a cryptanalyst's show; traffic analysts helped identify the units, and linguists and/or cryptolinguists translated [redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

EO 1.4.(c)

In August 1947, Frank Rowlett, in his role as the deputy coordinator for processing allocation, JPAG, reviewed the cryptanalytic situation on the Soviet target. The [redacted] [redacted] under study by both partners were placed in four general categories:

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

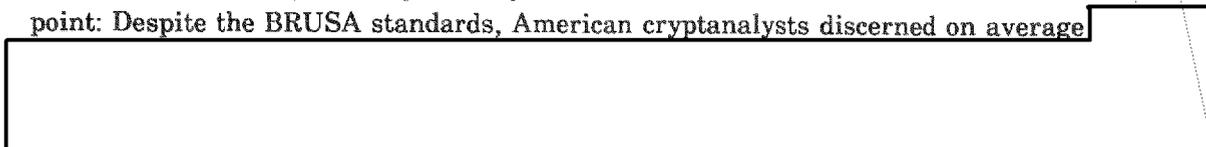
- (1) [redacted] was in progress, but not presently [redacted]
- (2) [redacted] used throughout the USSR on [redacted] the military, naval and police organization. About [redacted] had not yet been achieved;
- (3) [redacted] military radio [redacted] links within the USSR; [redacted] and special production techniques were under study; and
- (4) All other, all military, naval, police and internal [redacted] most of these [redacted] are of operational value only, but together they make an important contribution to the sum total of knowledge of the Russian set-up from a long range point of view; many of these [redacted] and many more are being worked on [redacted]

Rowlett gave credit to the British for major diagnostic research contributions on [redacted] allocating most credit to the U.S. for its basic research on [redacted]

[redacted]



Incidentally, while British and American cryptanalysts saw many things alike, they performed their analysis independently and often came to different conclusions. Case in point: Despite the BRUSA standards, American cryptanalysts discerned on average

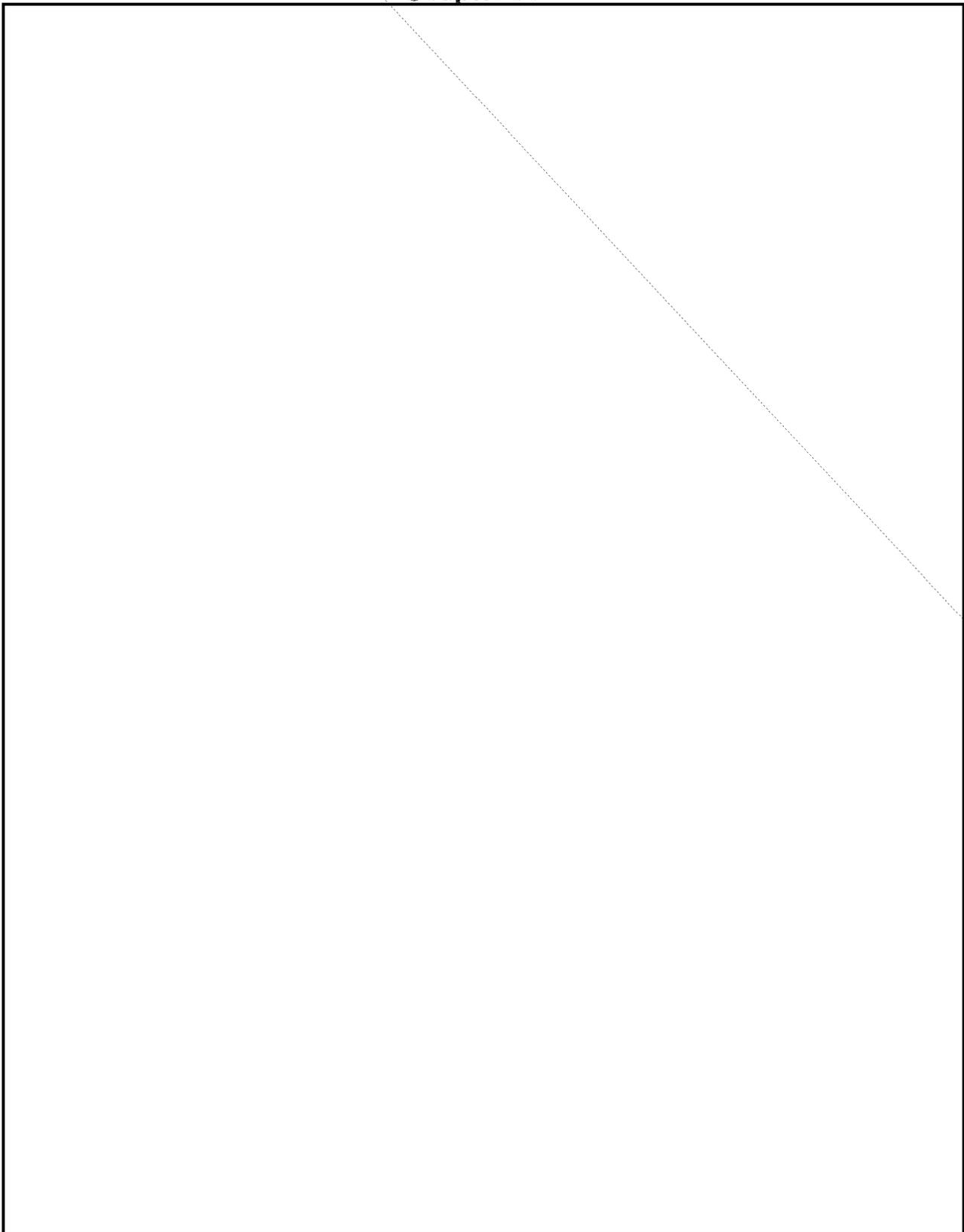




EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



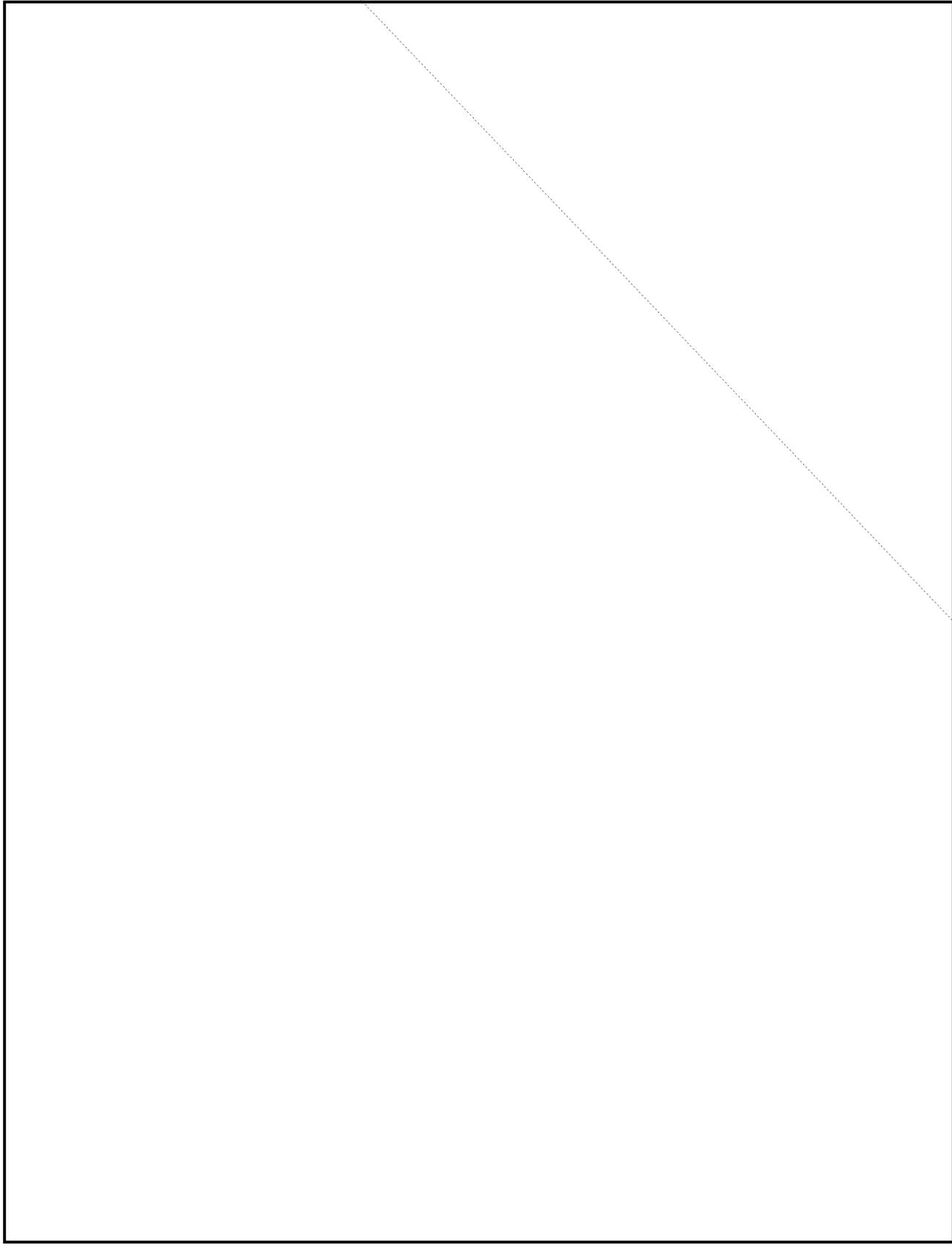
## Chapter 21

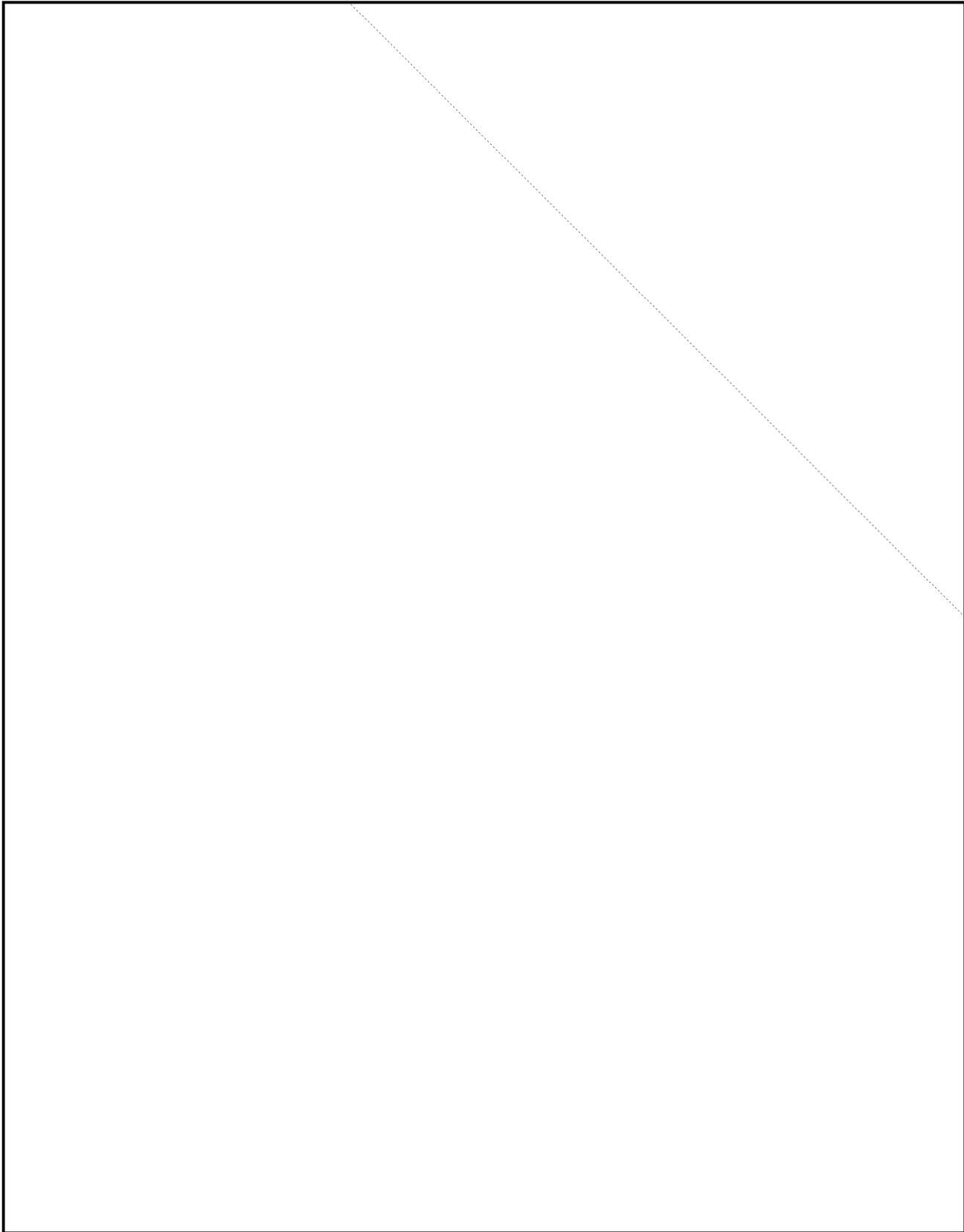


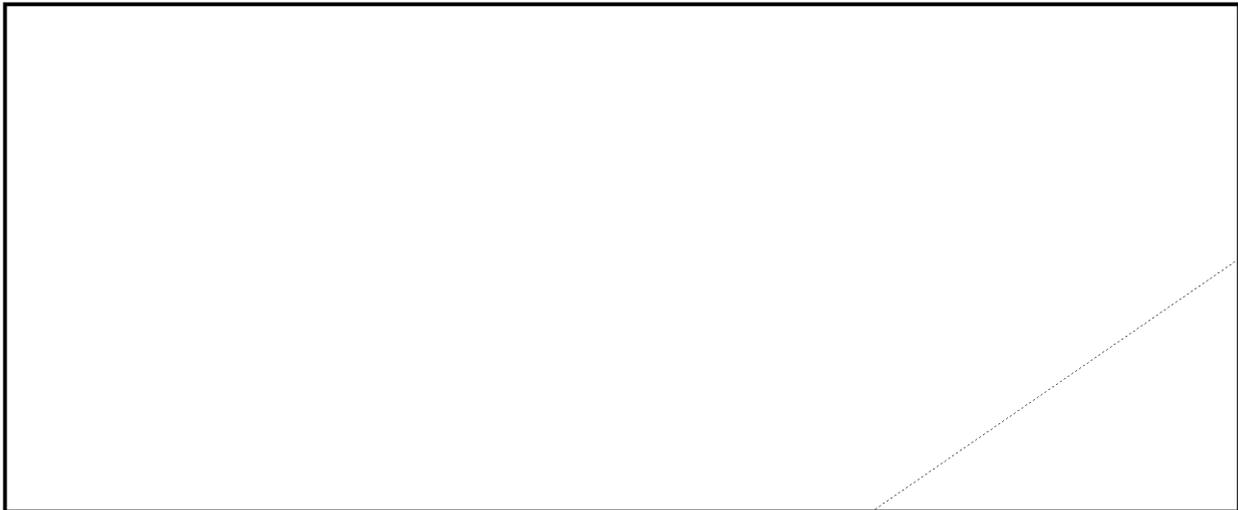
DOCID: 4314365

~~TOP SECRET UMBRA~~

EO 1.4.(c)  
EO 1.4.(b)

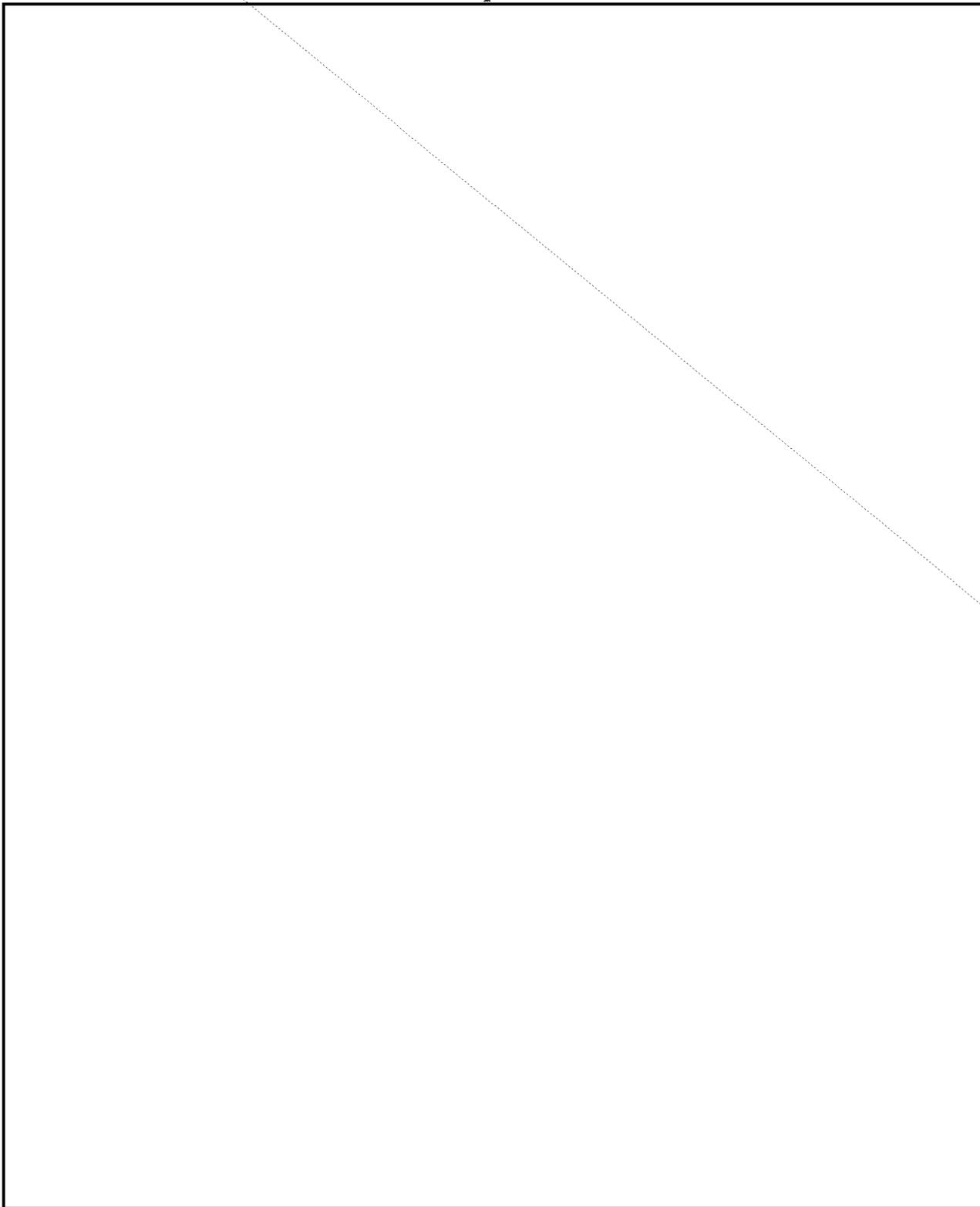






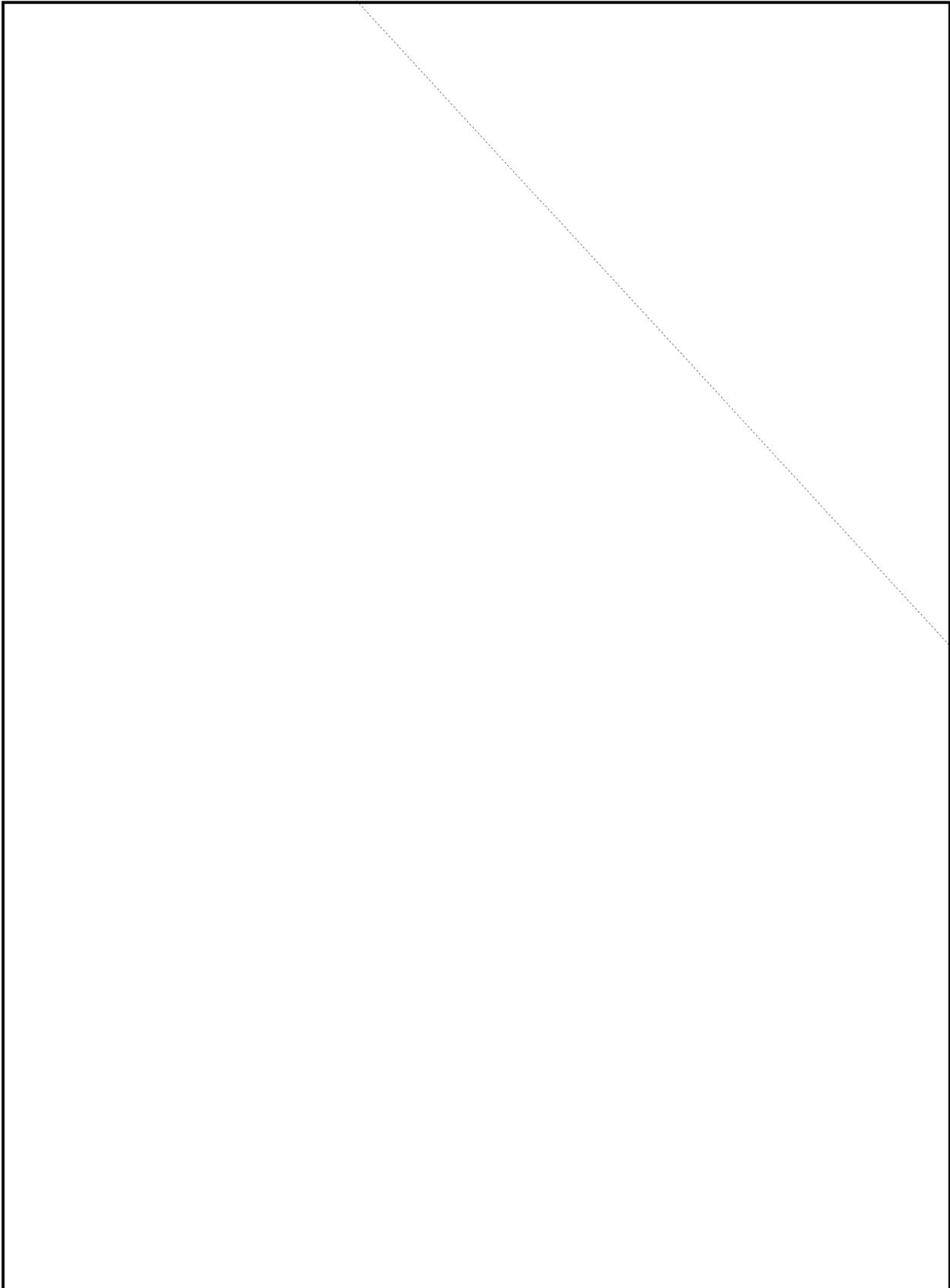
EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

### Chapter 22

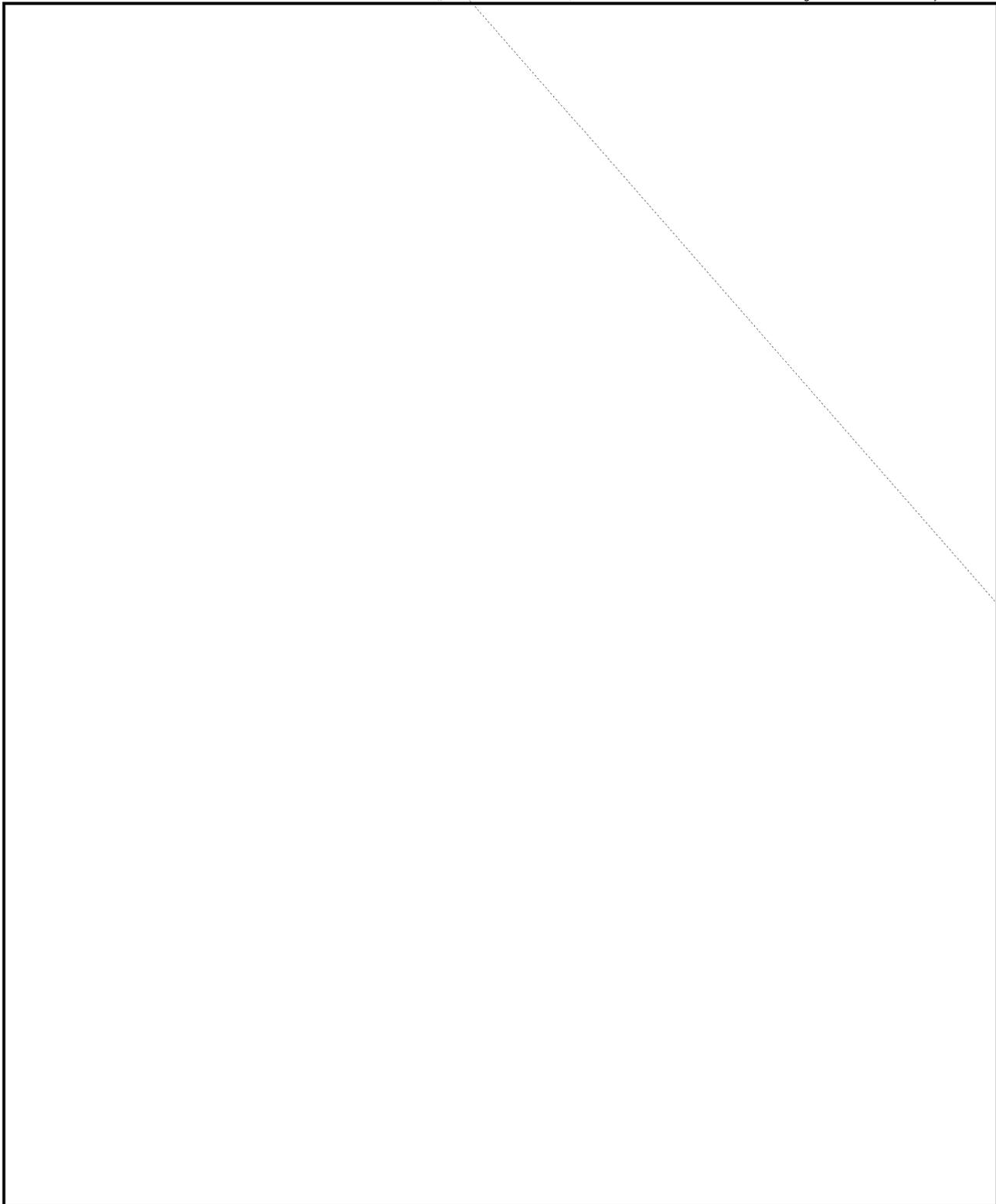


DOCID: 4314365

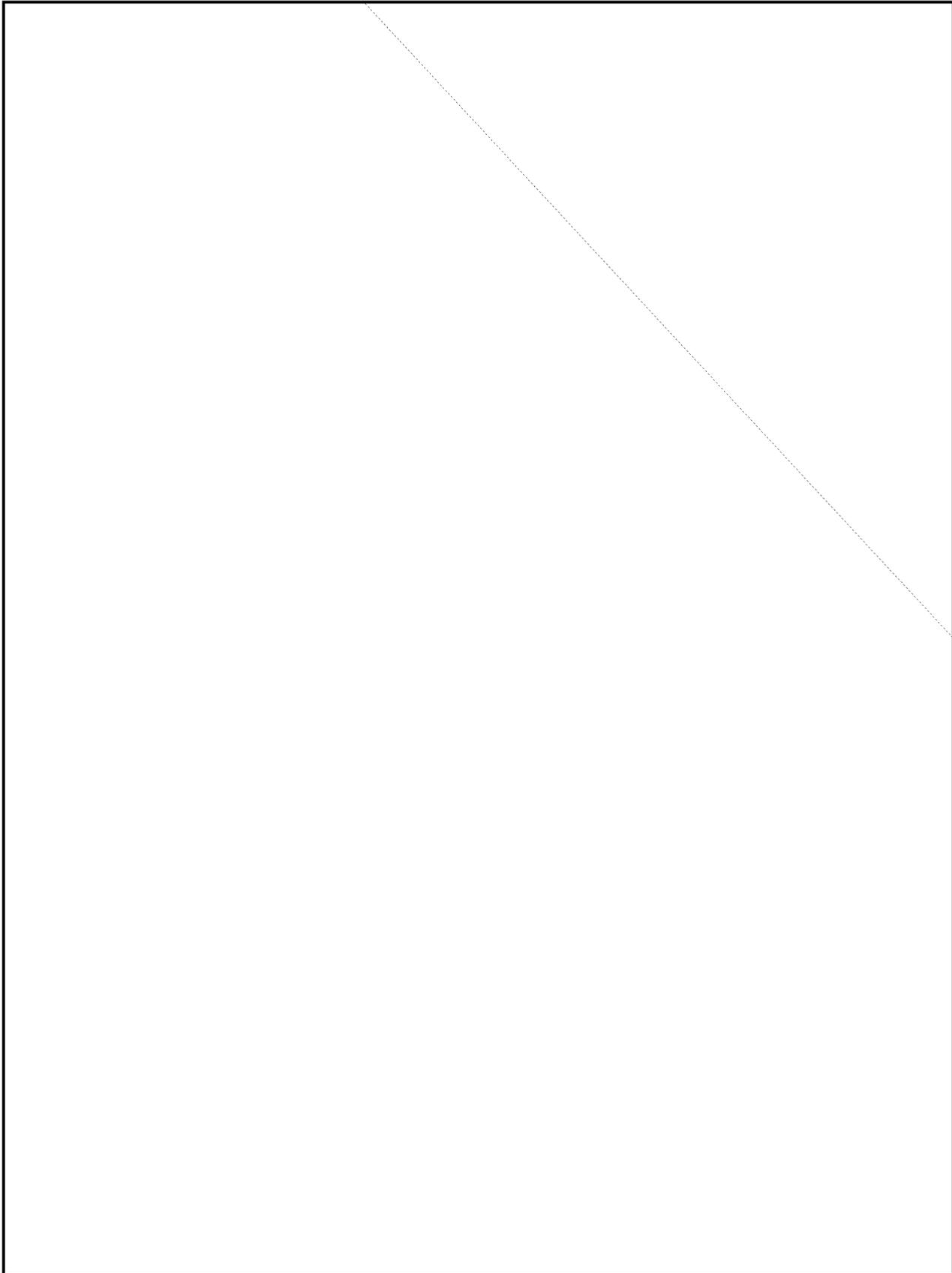
~~TOP SECRET UMBRA~~

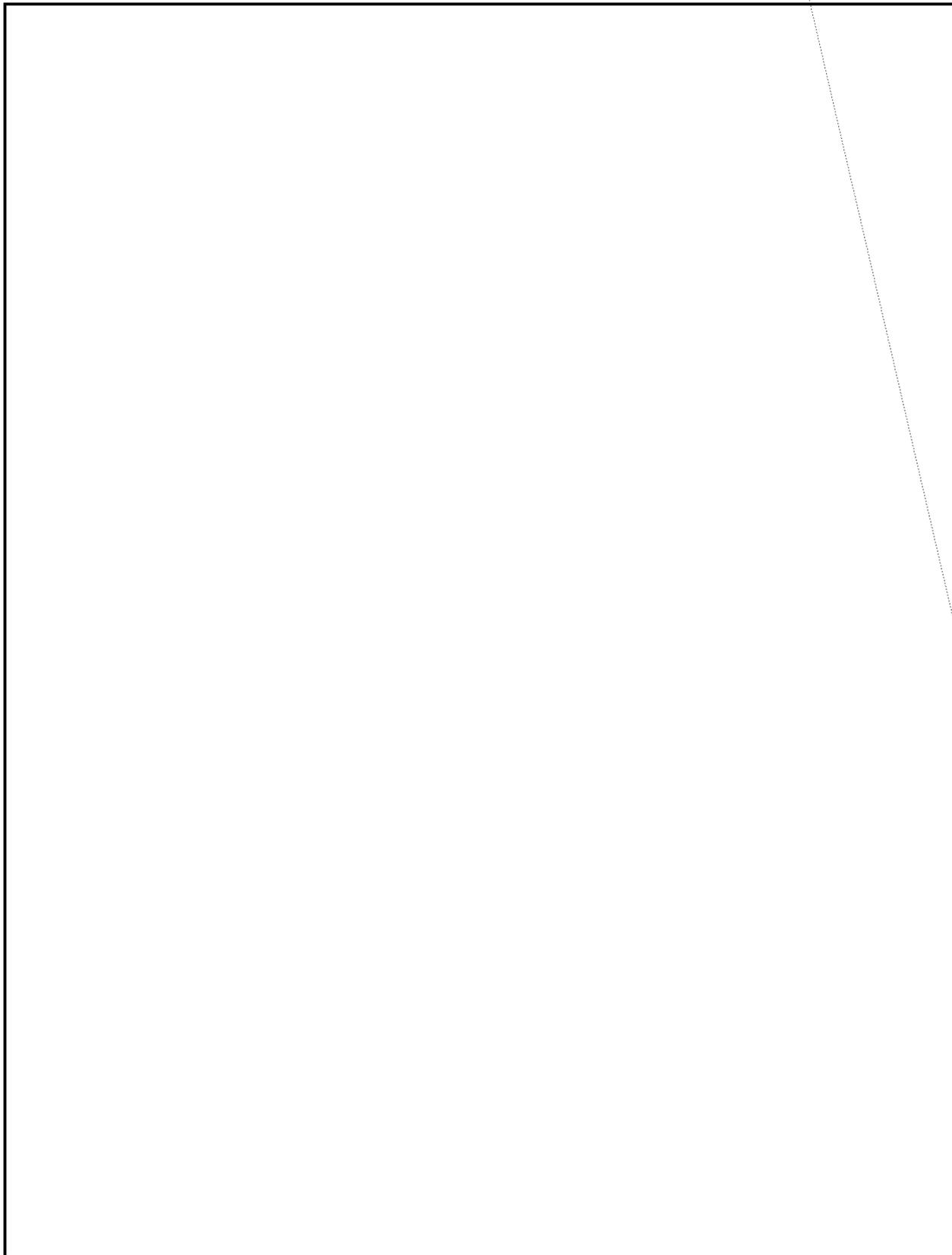


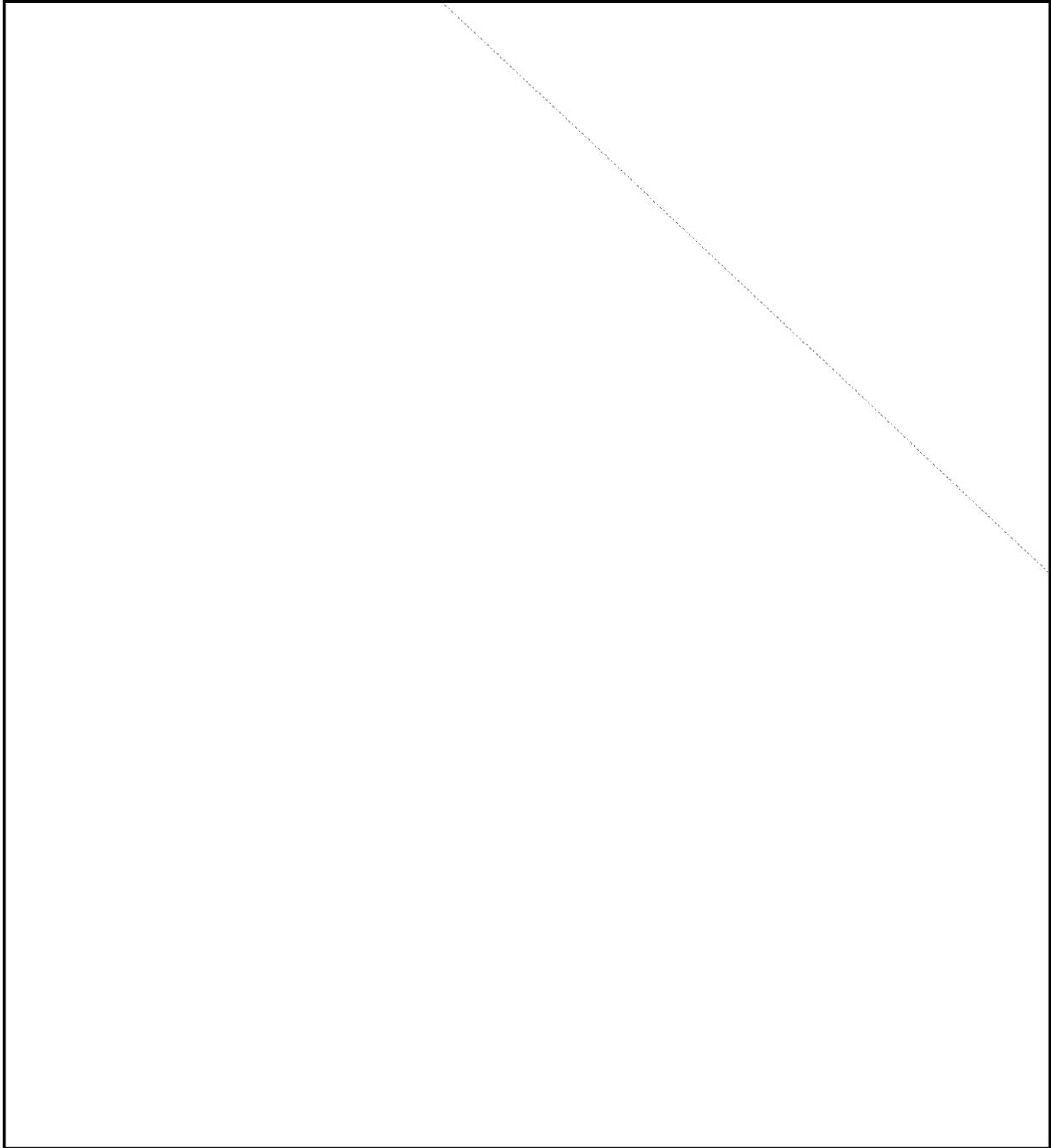
In August, Frank Raven, who in the 1960s and early 1970s rose to senior executive ranks at NSA (he was chief of G Group, 1966-1974), was in 1946 a U.S. Navy commander,









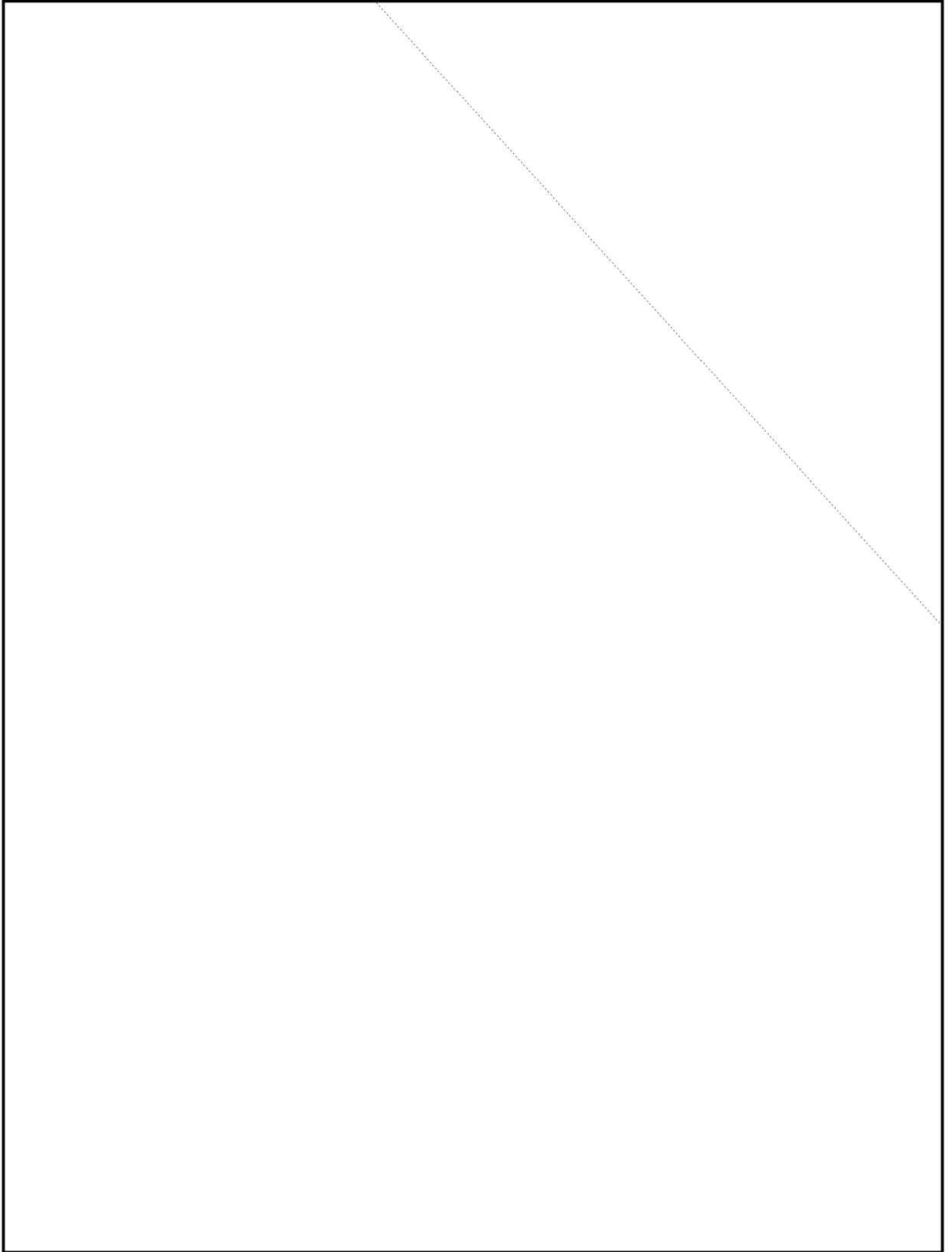


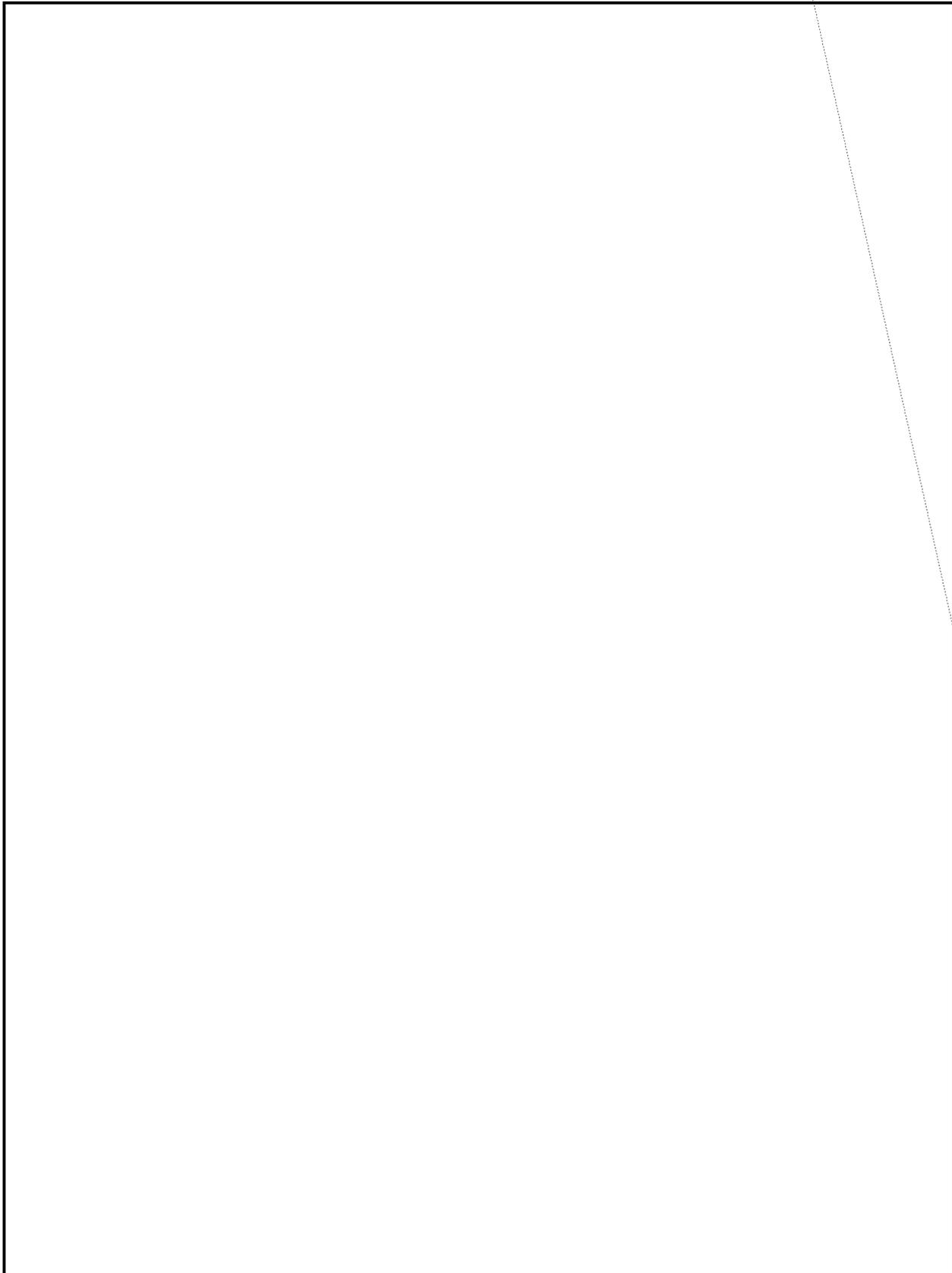


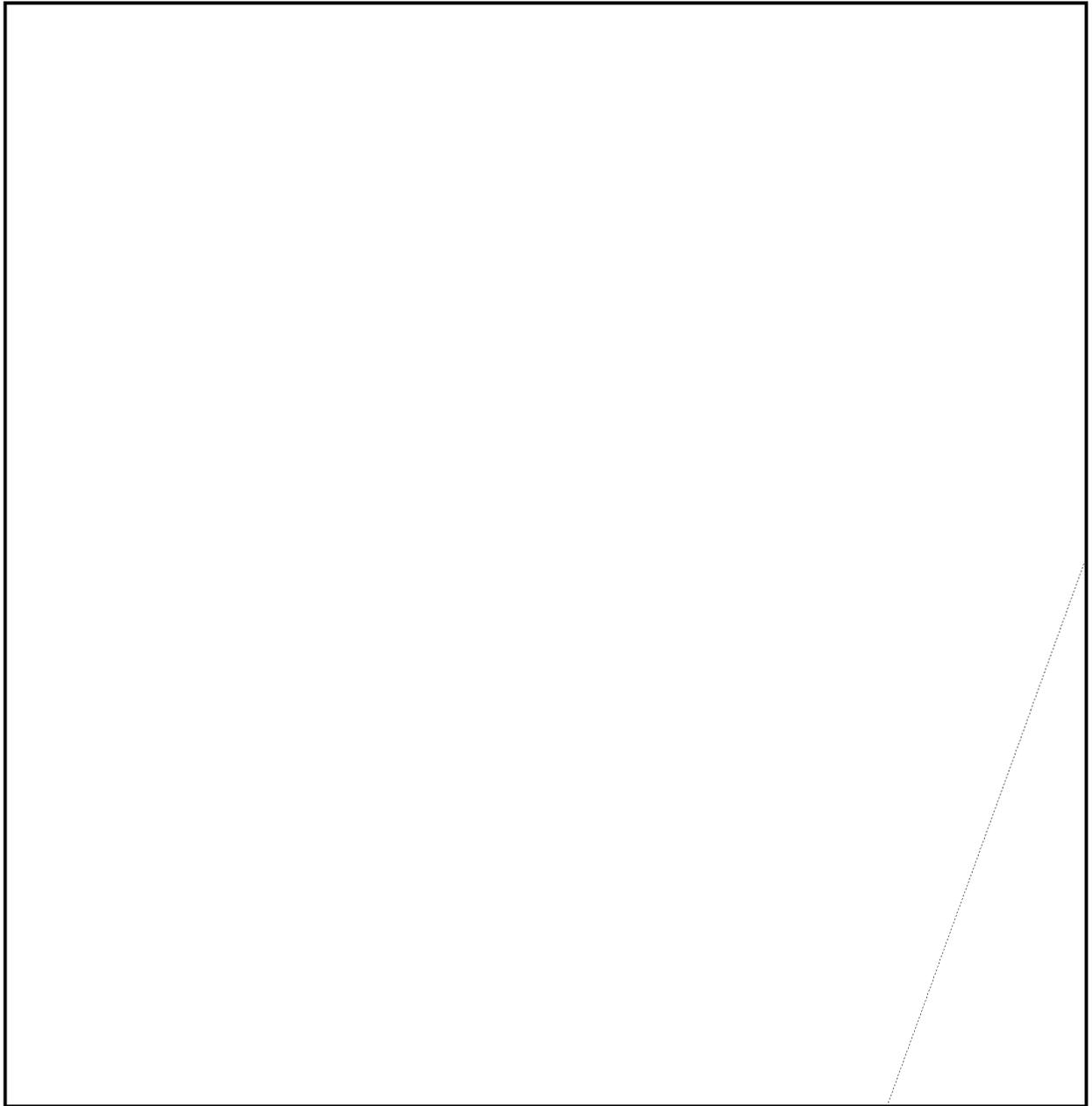
### Chapter 23







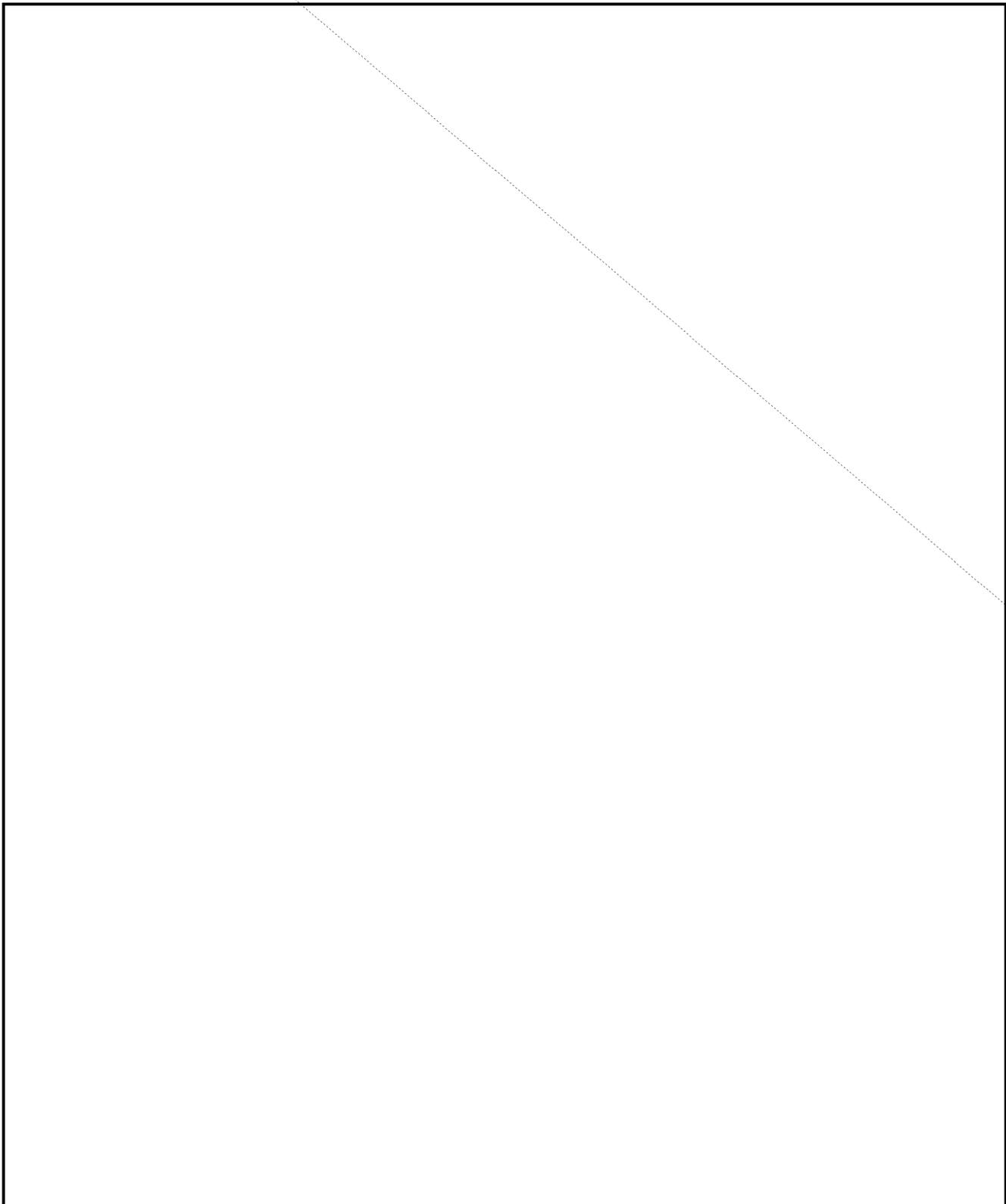




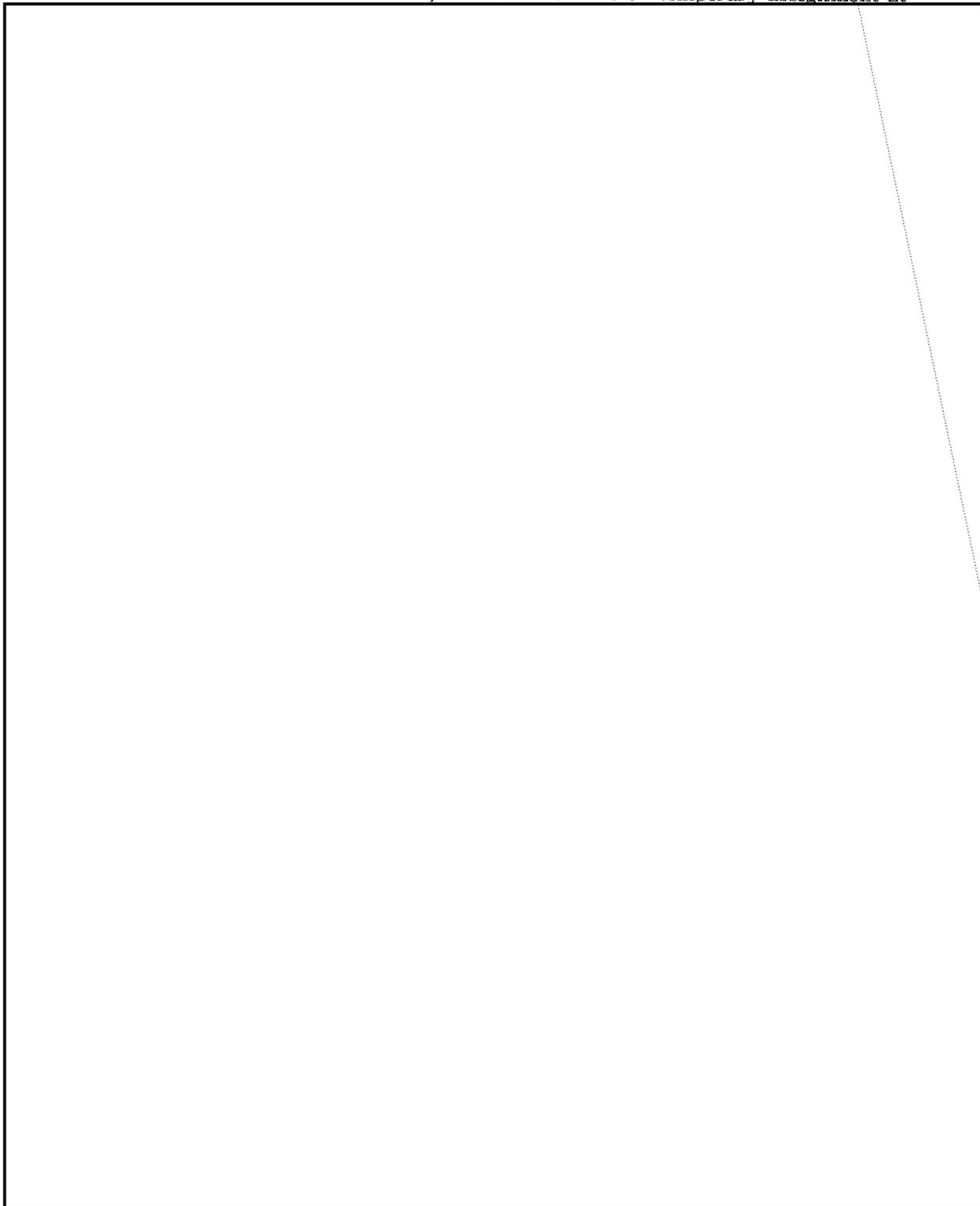
EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

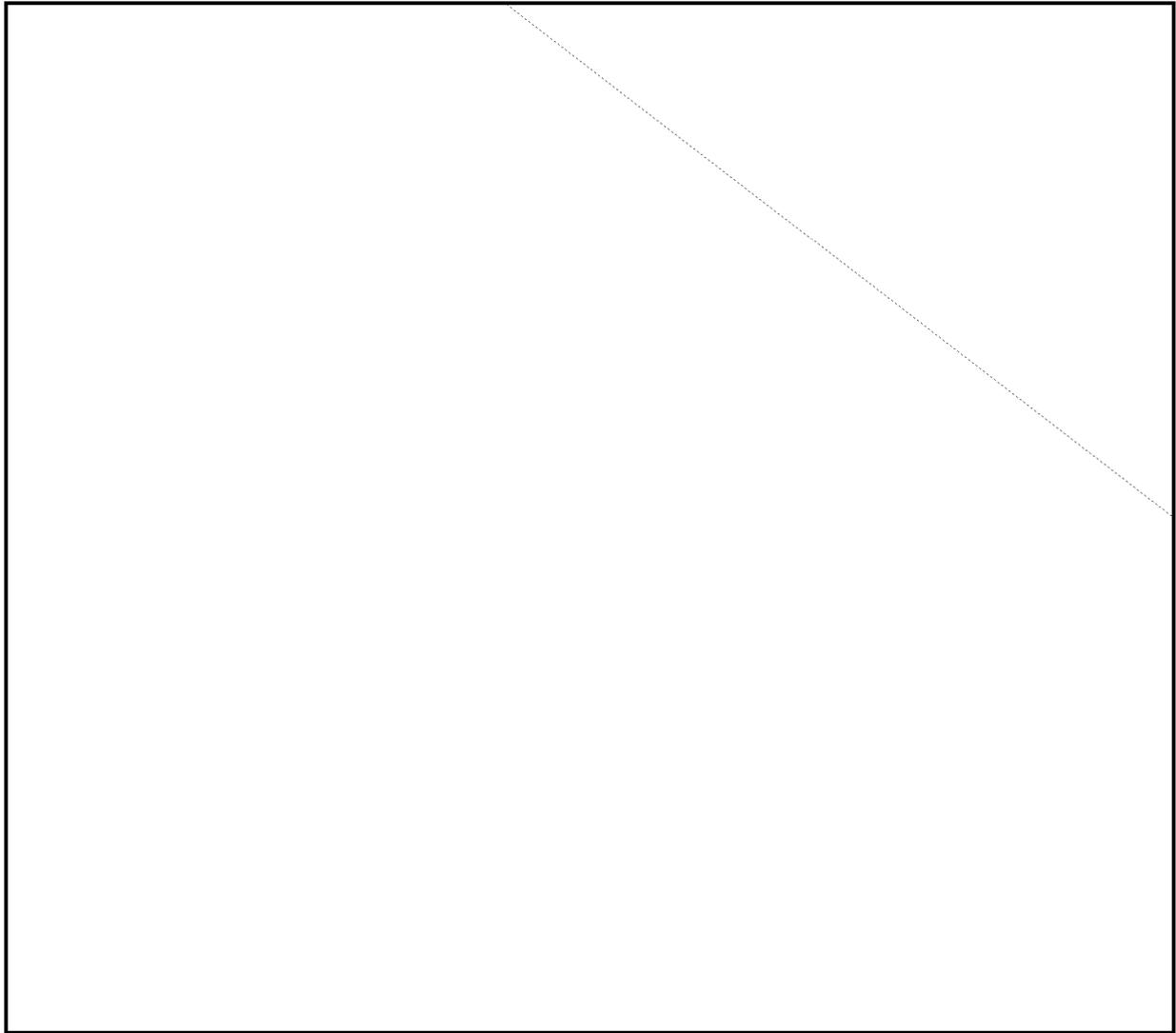


### Chapter 24



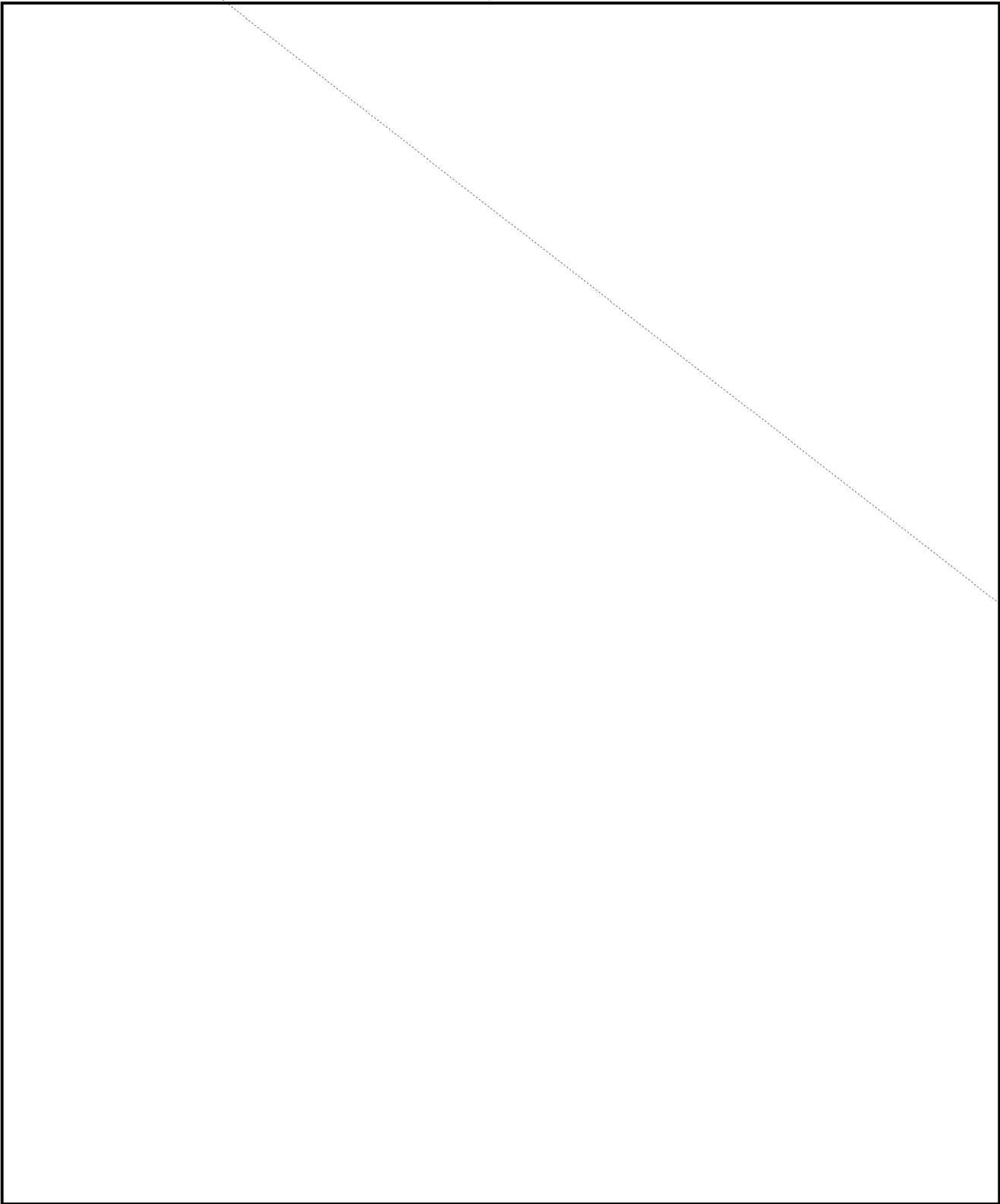
Commander Prescott H. Currier, who had begun his U.S. Navy cryptologic career as a radio operator and Japanese cryptanalyst in the 1930s and who later rose to the rank of captain as SUSLO London in the 1950s, was in June 1947 on temporary assignment at



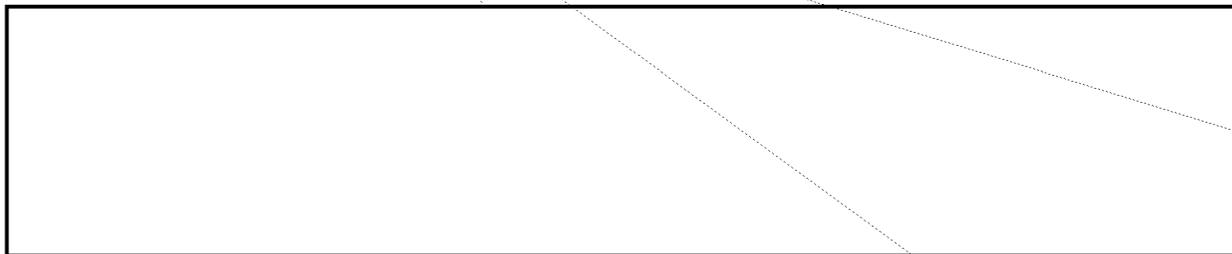


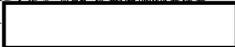


### Chapter 25

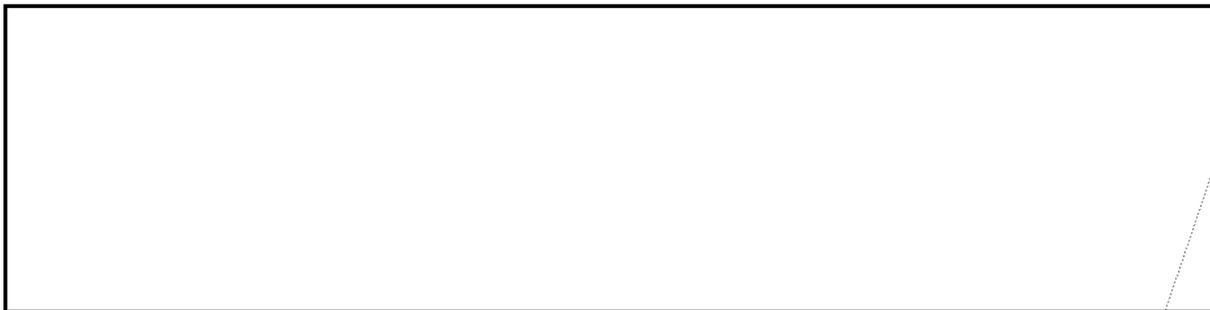






the meeting was Miss Ann Caracristi, who had joined ASA as a cryptanalyst on Japanese military manual systems in 1942 and who would later serve as chief,  Group (A Group), from 1975 to 1980 and as NSA's (first and so far only female) deputy director from 1980 to 1982.





EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Chapter 26

IBM and RAM Contributions to Cryptanalysis

PL 86-36/50 USC 3605  
EO 1.4.(c)

Electromechanical tabulating equipment produced by the International Business Machine (IBM) Corporation, the only company producing such equipment, played an important role in the Soviet cryptanalytic effort throughout the 1940s. No IBM computers per se were employed on the Soviet problem during this period, as there were none,<sup>1</sup> but IBM's tabulating machines, punched card readers, and electronic calculators were the hardware used to do statistical studies [redacted]

[redacted] generally in enciphered texts. The abbreviation IBM became synonymous with its hardware and permeated all equipment-related correspondence of the period.

With one exception. Rapid Analytical Machines (RAM) also played an important part in the Soviet effort at this time. RAM applied to specially built hardware designed to do very specific diagnostic tasks, such as looking for depths in traffic. RAM equipment, however, usually used IBM card-punch readers and tabulators and so on as major components but added such elements as photo-electric cells, specialized projectors and cameras, special tape readers, and other input and output devices. RAM systems looked

[redacted] Classic examples of RAM systems were the bombes used in World War II against such cryptosystems as the now-famous German ENIGMA cipher machines.<sup>2</sup>

As early as January 1946, IBM machines were printing out worksheets of Soviet [redacted] Later in January, among the material sent to GCHQ were "IBM listings of [redacted] which are in the process of recovery."<sup>4</sup>

In May, ASA used IBM processing on an [redacted] [redacted] "Messages have been incorporated into a machine run in order to study [the] code."<sup>5</sup> Also in May, GCHQ also used IBM equipment, in one case against [redacted] traffic: "The resulting 40,000-50,000 figures of [redacted] are being machine indexed by [the] IBM section, and will be analysed in various ways."<sup>6</sup> In June, IBM equipment helped ASA attack Soviet [redacted]

At about midyear, ASA surveyed its use of and need for machine support to the Soviet problem. Not surprisingly, machines were found to be used primarily in four areas: Non-Morse (Baudot) processing, and in [redacted]

Basic non-Morse processing equipment, called "IBM regeneration units," were composed of a tape reader, typewriter, punch, and a junction box. They produced a duplicate perforated tape (most collection sites copied the [redacted] [redacted] Baudot signals on perforated tape, but considerable collection was on undulator tape as well) and pageprint for sharing with the Navy. Currently, ASA was operating

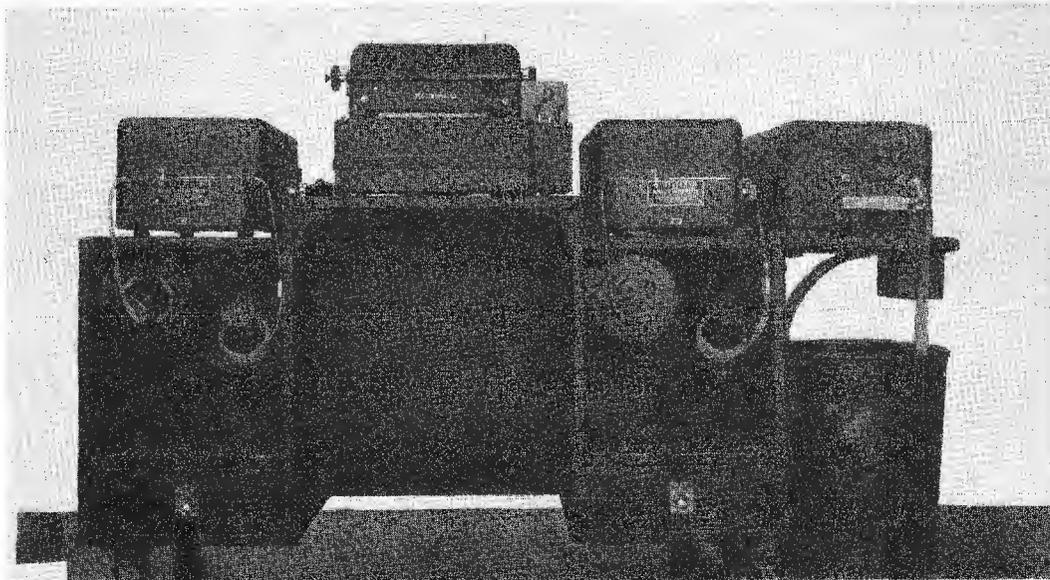
EO 1.4.(c)  
PL 86-36/50 USC 3605  
EO 1.4.(b)

EO 1.4.(b)  
PL 86-36/50 USC 3605

three units, with three more on order. Because of the expected increase in non-Morse collection, ASA believed it now needed ten more units. ASA also stated a requirement for eight IBM units to produce pageprint and punched tape (for follow-on machine cipher analysis) from undulator tape.<sup>9</sup>

On the [redacted] problem, the need for machine cryptanalytic aids was deemed "extremely pressing." At that time, only one "decoding machine" and a [redacted] counter" was being used, with an "analogue" in the final stages of construction, a special "fractionating unit" on order, and a "starwheel generator" being built in-house. The latter unit, however, needed a "double headed IBM reader" at \$1,400 to eliminate synchronization problems that plagued the current design, which used two single-headed readers. Finally required for the [redacted] problem was a [redacted] composed of one double-headed IBM reader and seventy-two counters, at an estimated cost of \$2,600.<sup>10</sup>

The [redacted] problem was receiving no help from machine cryptanalytic aids in the middle of 1946. A machine used on the [redacted] problem for stripping key<sup>11</sup> would work on [redacted] but was occupied full time on the former system. Nothing was on order. ASA proposed, at the cost of \$10,000 a unit, a modified "Mathew Machine,"<sup>12</sup> constructed of one of those double-headed IBM readers, an IBM typewriter and punch, a selector circuit, additive circuit "for a 32x32 alphabet square," a standard IBM plugboard, and an "enciphering or deciphering keyboard." The trouble was, however, in addition to cost, no such machine was available, would take a year to procure and another month to modify.<sup>13</sup>



Mathew Machine

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Equipment then available to aid [redacted] cryptanalysis consisted of the aforementioned "IBM regeneration units" some (number not specified) of which had been modified to interpret "all combinations of perforations on the tapes as lower case letters, or as symbols representing functions such as shift to upper case or shift to lower case, and by printing a special symbol to indicate the exact number of letter intervals where the original transmitter paused during transmission." Nothing was currently on order, but further work on [redacted] was deemed dependent on the acquisition of a "good [redacted] [redacted] to compare [redacted] Again, the ASA research and engineering people were designing a "simple but satisfactory high speed [redacted] expected to process 2,000 to 5,000 positions per minute. At an estimated cost of \$1,000 per unit, ASA wanted one unit built and, if it worked, maybe another unit "at a later date." Finally, an "essential" machine for [redacted] cryptanalysis also was a [redacted] (two, actually) at \$3,600 each.<sup>14</sup>

Also in July, Captain C.P. Collins, U.S. Army, who had been a deputy to the SUSLO, London, until late June, reported gloomily on the status of GCHQ's machine efforts, compared with U.S. work:

*IBM.* It has been [LSIC] policy not to depart from standard IBM machine procedures. Consequently the plethora of special gadgets and auxiliary equipment found on U.S. IBM are absent at LSIC. This is to the great detriment of LSIC.

*RAM.* Since the end of the war LSIC has dropped to practically zero in the RAM field, [redacted] problem cannot be done by hand or limited IBM, it is not done. All the ENIGMA Bombes except about a dozen have been dismantled. The dozen remaining are out of use.<sup>15</sup>

EO 1.4.(c)  
PL 86-36/50 USC 3605

Back in America in August, [redacted] messages were being subjected to IBM processing:

IBM log of all traffic received [which amounted to 6,198 messages]. . . IBM work started on search for [redacted] to all messages, and [redacted] study of result...Received pad number sort of IBM log to facilitate search for [redacted] . . .<sup>16</sup>

In September, IBM methods focused on Soviet [redacted] again:

All completed [redacted] listings were sent to IBM for punching and sorting. . . In [redacted] all [redacted] text is being copied from the [redacted] for use by IBM in preparing messages prints, [redacted]

By December 1946, IBM machines were heavily involved in improving the exploitation of Soviet [redacted]

- a. IBM [redacted] resulted in a large increase in solutions. Cited as proof: of the 760 messages intercepted on the Far Eastern links [redacted]
- b. New IBM prints for [redacted] revealed a relationship between [redacted]

- c. Preparation of an IBM index on [redacted] material was well under way for the attack on this problem; and
- d. An IBM job was proposed which would bring forth [redacted] more quickly.<sup>18</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

By June 1947, a new [redacted] single coordinate deciphering analog" was being wired up for operational use.<sup>19</sup> By September, it was reported to be running "reasonably well, without any redesign."<sup>20</sup>

RAM support of the [redacted] problem included development of an Alphabetic Substitution Device, which by August had been "used with good results in the [redacted] project. This device makes it possible to [redacted] all in a single operation. The resultant possible plaintext fragments are examined for good text."<sup>21</sup> By December, "high priority work had begun to develop a machine to aid in the cryptanalysis of [redacted]. The device would attempt to mechanize the process, now manual, to work an [redacted] of messages, and would, hopefully, be operated by any cryptanalyst having some knowledge of the Russian language."<sup>22</sup>

Machine applications also made headway against the [redacted] initially in May. Two devices were put into operation for the purpose of developing and studying [redacted] key. The first of these was a [redacted] which developed a series of cards. The second device calculated the key and recorded it into the [redacted] in the form of letter and baud notation."<sup>23</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Planning in September focused on developing procedures and equipment for more rapid decryption of [redacted] traffic. IBM equipment was also combined into a [redacted] analog, which produced approximately 200,000 letters of key, with "the best time achieved so far . . . 3,000 keys [sic; probably meaning letters of key] an hour."<sup>24</sup>

An example of how techniques developed for one cryptosystem could be applied to another occurred in September as well. "A pilot model of a [redacted] Decipherer, which should operate at several times the speed of the present one, has been discussed. It will use techniques derived from the [redacted] and the [redacted] coordinate analogue."<sup>25</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Among the machine applications in support of [redacted] was a new model of the IBM [redacted] Analogue, in operation by October, which generated and checked 6,000 letters of key per hour. A pilot model of even a faster [redacted] analog was under construction.<sup>26</sup>

Progress in machine applications to [redacted] exploitation continued in December 1947 when construction of a general-purpose relay gate was completed. The gate contained 100 four-point wire contact relays, and its first use was to test [redacted] key streams for the "identification of single wheels." The [redacted] analog was demonstrated successfully at the rate of three keys per second. Plans were to adjust the clutches in hopes of successfully running the machine at five keys per second (18,000 per hour).<sup>27</sup>

The [redacted] problem also received IBM applications' support, beginning in May. For processing [redacted] tapes, a "revised tape reader and analyzer unit" was under construction. The new unit would consist of (1) a double-headed reader - "a Transmission Distributor, Model 14, was converted for this purpose"; (2) analyzing circuits for converting baud coding to IBM coding; and (3) combining circuits for calculating [redacted] as the tapes were read. It was claimed that this new unit would permit a "more effective cycle determination because [redacted]"

IBM and RAM contributed to general Soviet cryptanalytic problems as well. In May, for example, modifications were being made to the "Alphabetic Substitution Unit" for the "purpose of facilitating plugging of the 32x32 substitution matrix."<sup>29</sup> In June, the "70 millimeter comparator" was being tested with a motor that drove it over twice its former speed, later specified as 850 frames per second. Also, a pilot model of a "desk size frequency counter, made from surplus components," was ready for testing.<sup>30</sup>

Machine applications were not limited to cryptanalysis. IBM lent a hand on the HF Direction Finding (DF) problem as well. For example, in September, "an IBM method of processing D/F studies . . . has been developed. Compared to manual methods, this procedure gives from a 3:1 to a 10:1 gain in man hours required to prepare the reports."<sup>31</sup>

In an effort to "acquaint those persons who may have occasion to request the services of the" Rapid Analytical Machines, the Chief of Naval Operations published in October 1947 a booklet entitled *Brief Descriptions of RAM Equipment* containing detailed information on twelve systems. The descriptions included logic diagrams, photographs, listings of current and potential cryptanalytic applications, and methods of use. Most of the dozen machines were being, or could be, applied to Soviet cryptanalytic problems.<sup>32</sup>

CSAW in 1948 provided insight into the relative use of and RAM resources against the Soviet target. Over a thirteen-month period ending January 1948, the ten-person naval IBM/RAM unit devoted from 416 to 982 manhours per month (averaging 761 manhours per month) on Soviet-related tasks. Based on manhours available to the unit, these numbers represented between 33 percent and 55 percent, averaging out at 43.5 percent of the available work force. In short, four to five of the unit's ten people worked on the Soviet target at all times.<sup>33</sup>

Also in the U.S., in February a third [redacted] was ready to be installed, "as soon as frames now under construction are completed."<sup>34</sup>

Despite the Soviets having pulled [redacted] off the air in September, the machine people in October 1948 used a [redacted] which "proved quite successful in [redacted] In November IBM procedures had been developed to assist in locating [redacted]"

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



## Chapter 27

### GCHQ Proposal for Division of Cryptanalytic Effort

Early in 1946, GCHQ addressed its perception of a problem of duplication of Allied cryptanalytic effort on the Soviet target. Brigadier John Tiltman, titular head of the Soviet problem at GCHQ at the time, asked the U.S. to furnish him with a list of the cipher systems being exploited, as GCHQ was "contemplating the use of this [list] in preparation of a plan for eliminating duplication of work."<sup>1</sup>

The list was provided, but nothing further happened until early November, when Commander Sir Edward Travis, director, GCHQ, began preparing for his trip to Australia and America. Essentially re-opening the case, Travis discussed where he wanted to go with a division of effort with Commander Manson, SUSLO, London, who passed the word back home on 4 November: "Among other things that [Travis] will propose during his discussions in the States will be implementation of a program for division of work between the two centers."<sup>2</sup>

Manson reported on the issue again two weeks later, while Captain Wenger, chief, Op-20-G, was TDY to London. It was now called "an allocation program":

The question of LSIC's taking the initiative in discussing an allocation program with USCIB . . . is apparently foredoomed to failure unless it takes the curious bias I mentioned in my last to you. In any case, the subject will no doubt come up for discussion between Capt. Wenger and the Director these next few days as they range over the various future LSIB-USCIB concerns, and the Captain will give the Director the necessary warning.<sup>3</sup>

A week after that, on 22 November, Manson wrote further on GCHQ's proposed "allocation program," indicating a change of direction as a result of American intransigence:

Now, a word further about the Director's desire to discuss an allocation program while in Washington. I have, of course, your vigorous denial of any such wish on the part of Washington Comint Center; but, as the matter was broached in conversation with Capt. Wenger by Sir Edward, and as the Captain had the latest information from USCIB and Col. Hayes's views, it was he who gave the Director warning that all might not be smooth sailing. Sir Edward at once understood the situation, and has now come up with a new idea which he plans to present: namely, the institution of a series of monthly prognosis charts, similar to those now prepared by the intercept people, showing what each Center plans to continue and/or undertake along cryptanalytic lines for the coming month. This scheme, being short of actual allocation, the Director hopes will receive some support and will eventually amount to a virtual program of division of labor without making commitments.<sup>4</sup>

The last words of 1946 on GCHQ's "allocation program" were, as usual, Commander Manson's, written on 18 December. Initially, Manson was reporting on the departure for the States of  the assistant to the head of cryptanalytic Group for

organization, GCHQ, who was to join the Travis party in Washington when it arrived from Australia in January 1947:

[redacted] is leaving, alone, for the States by sea about the first of the month. Since the discussions which took place concerning the reluctance of Washington Comint Center to entertain proposals for an allocation program [redacted] has been instructed by the Director to . . . make no propositions and no commitments, and just to put his ear to the ground and listen. . . .<sup>5</sup>

PL 86-36/50 USC 3605

The final disposition of GCHQ's "allocation program" must await a historical review beyond 1948. Suffice it to say, if the U.S. view held firm, little of substance probably came from the British proposal, other than perhaps the periodic exchange of lists of ongoing projects.

## Chapter 28

## Espionage or Normal Cryptographic Developments?

[redacted] there followed much soul-searching by the COMINT agencies on both sides of the Atlantic Ocean.<sup>1</sup> One of the first documented reports

[redacted] Although the possibilities of espionage were acknowledged, CSAW in an internal memorandum concluded that the most probable cause was "normal development of Soviet security program, requiring no specific knowledge of U.S. or British COMINT successes for its basic motivation, but quite probably hastened by deductions based on external evidence which is necessarily susceptible to their observations."<sup>2</sup>

The issue surfaced at the USCIB level in November, when its members discussed the possible reasons [redacted] First, the board reviewed a letter on the subject received from LSIB. It offered four possibilities: (1) preparation for war; (2) methodical drive to improve communication security; (3) temporary pulling off the air to remedy defects; and (4) reaction to a leak. LSIB ruled out the first possibility, but could not confirm or deny the last three.<sup>3</sup>

Next, the chiefs of the "technical agencies" (i.e., ASA and CSAW), Colonel Hayes and Captain Wenger were asked their views. Interestingly, they disagreed as to the causes. Colonel Hayes was "strongly inclined toward the belief that leakage of information had been the primary cause." Captain Wenger believed that "further development in the Soviet security program was . . . the most probable motivating factor although none [of the other possibilities] could be definitely ruled out." USCIB decided to refer the problem to its Committee on Security for study and to make recommendations for action.<sup>4</sup>

The issue was first addressed at a meeting of USCIB's Security Committee on 21 December 1948. The participants agreed to proceed on the assumption of Soviet penetration of Allied COMINT successes and draft a report accordingly.<sup>5</sup>

At the second meeting on 4 January 1949, the first draft was discussed. Recommendations were to compartment [redacted] plain language. There was much disagreement about what actions to take. The committee did agree, however, that "since the Russian problem [redacted] special emphasis must be placed on the security thereof by all disseminating and operating agencies." A decision was made to re-draft the report.<sup>6</sup>

On 11 January 1949 the Security Committee submitted to USCIB its report, citing the following facts bearing on the problem:

During 1948 the Russians adopted various successive communication security measures the reasons for which cannot be positively determined but which could have resulted from leakages of information [redacted] EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Accordingly, the committee submitted a draft USCIB Directive No. 4 (approved on 14 January 1949), which assumed a leak and took measures to reduce the damage of future betrayals. It reaffirmed the "need-to-know" principle for the processing agencies, directing that producers of each COMINT field and task "shall be sequestered and compartmented from other operations to the greatest extent practicable without undue detriment to the operational efficiency and effectiveness," and "reports of progress in each general field of COMINT effort shall be separate from similar reports covering other fields. . . ." Secondly, it directed, for producers and consumers alike, that a COMINT clearance and indoctrination did not entitle one to receive "COMINT from all fields and tasks, or even all COMINT from any one field or task, unless he [or she] specifically requires it." Moreover, a COMINT clearance "shall not be regarded as entitling [one] to receive detailed information on the specific technical successes and processes which have led to its production."<sup>8</sup>

GCHQ came aboard in April 1949, when the Allies agreed that added security would be obtained by the "complete separation of work on Non-Russian from that on Russian," excluding the early stages of intercept, intercept control, and traffic handling, but incorporating "all phases of traffic analysis, cryptanalysis, translation, publication, evaluation, distribution, dissemination, intelligence appreciation within both the processing and consumer agencies, and exchange of information between the technical agencies." USCIB rejected the recommendation to use a "subsidiary" code word to distinguish the Soviet material from other COMINT.<sup>9</sup>

The wisdom of the operating assumption (a leak) and these actions were confirmed a few years later. At least two Soviet spies were subsequently determined to have known that the Allies were achieving some success in reading Soviet cryptosystems. One was Kim Philby, who worked for Britain's MI6 and was a COMINT customer of at least GCHQ's product reports.<sup>10</sup> The other was William Weisband, who worked for ASA as a Russian linguist during the mid- to late 1940s and, though not convicted of spying per se, was strongly suspected of being a Soviet agent.<sup>11</sup> Either or both could have and probably did blow the whistle on the Allied successes.

Regardless of the reasons for the disappearance of these systems, [redacted] [redacted] were not again employed operationally by the Soviet military until 1952.<sup>12</sup> Well, at least there was traffic analysis and plain language to keep the Allies in business.

Notes

Chapter 20: Core Cryptologic Tasks

1. (U) JPAG Monthly Status Reports, June–December 1946, and December 1947 and 1948. Also, LSIC/GCHQ Monthly Status Reports, June–December 1946 (~~TSC~~), and December 1947 (~~TSC~~) and 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 2006N, boxes CBQI43 to CBQI48.

2. (U) LSIC/GCHQ Monthly Status Reports, January–December 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 2006N, boxes CBQI47 and CBQI48.

3. (U) JPAG Monthly Status Reports, May 1946–December 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 42466, locations H10-0106-1 to H10-0106-4. Also, LSIC/GCHQ Monthly Status Reports, May 1946–December 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 2006N, boxes CBQI43 to CBQI48.

4. LSIC/GCHQ Monthly Status Report, August 1946; JPAG Monthly Status Reports, January–December 1946.

5. Howe, JOP study, 14.

6. JPAG Monthly Status Report, December 1946. By September 1949, a time frame beyond the scope of this study, the numbers were: [redacted] Soviet systems; ASA [redacted] and Op-20-G, [redacted] and under a new classification system, ASA had [redacted] and [redacted] and Op-20-G had [redacted] and [redacted] [redacted] (Ibid., 24.)

7. (~~SC~~) The number of messages includes estimates of [redacted] traffic which was actually counted in intercepted characters, ranging from [redacted] per month, estimated to be equivalent to an average of 50,000 "pages" of traffic per month.

8. LSIC Monthly Status Reports, January–December 1947.

9. JPAG Monthly Status Reports, January–December 1947.

10. Rowlett Review.

11. Ibid.

12. (~~C~~) JLG memorandum to Chief, ASA, and OP-20-2, subject: LSIC study "The Effort on Russian Signal Intelligence in Relation to That on Other Signal Intelligence Tasks," 25 May 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 757, location G16-0406-5.

13. JPAG and LSIC/GCHQ Monthly Status Reports, January–December 1948.

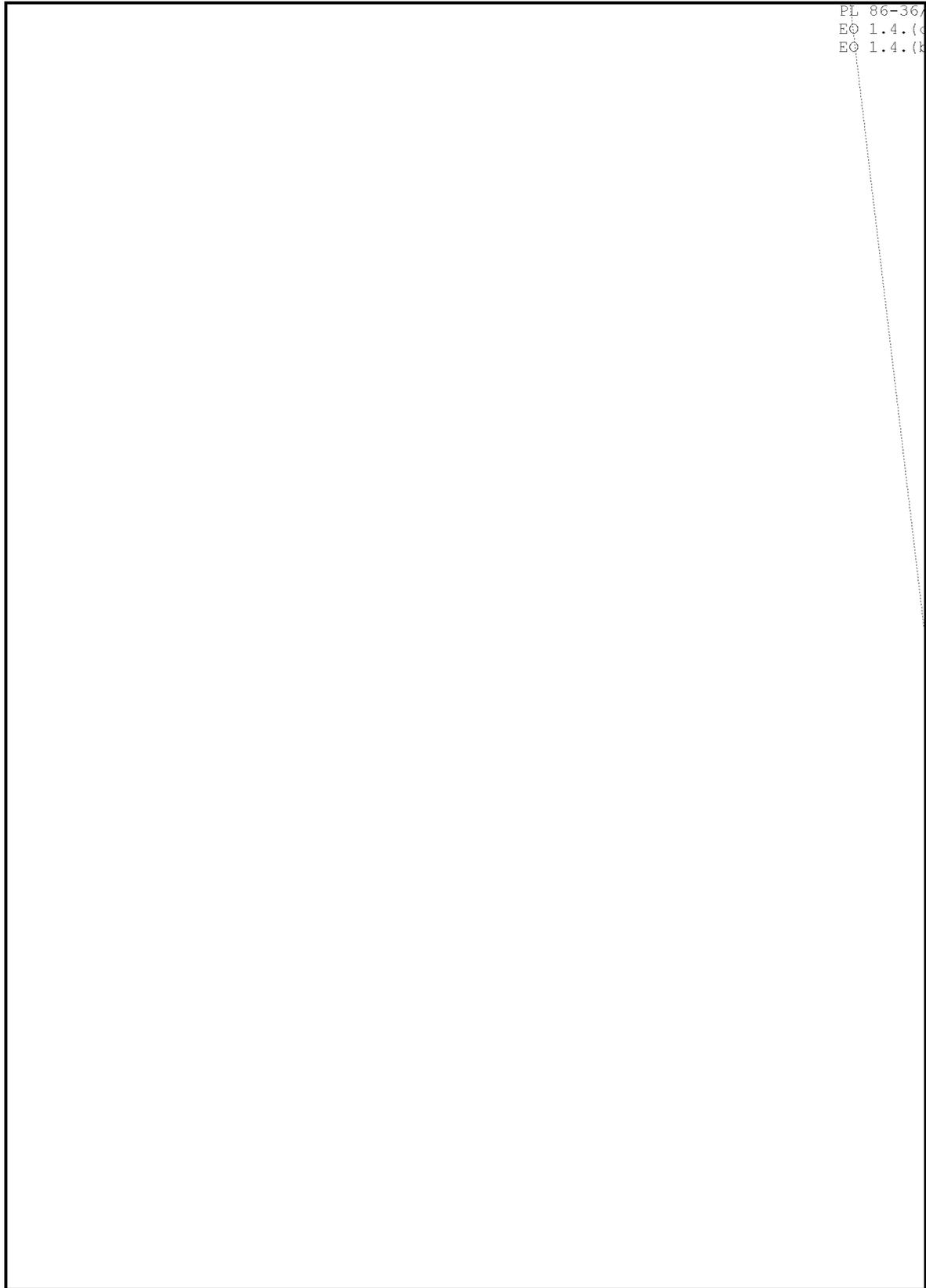
14. Ibid.

15. JPAG Monthly Status Reports, January–December 1948.

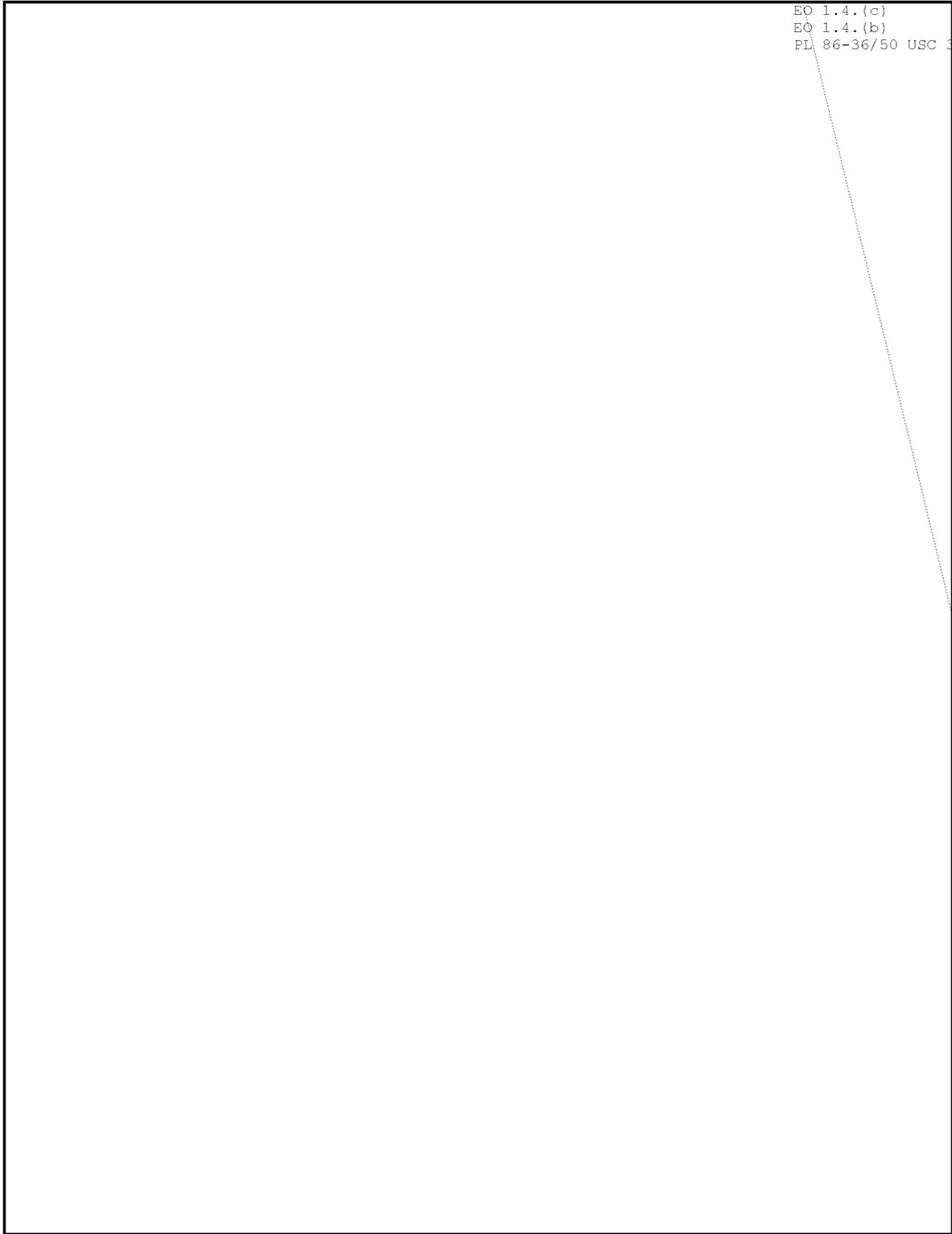
16. LSIC/GCHQ Monthly Status Reports, January–December 1948.

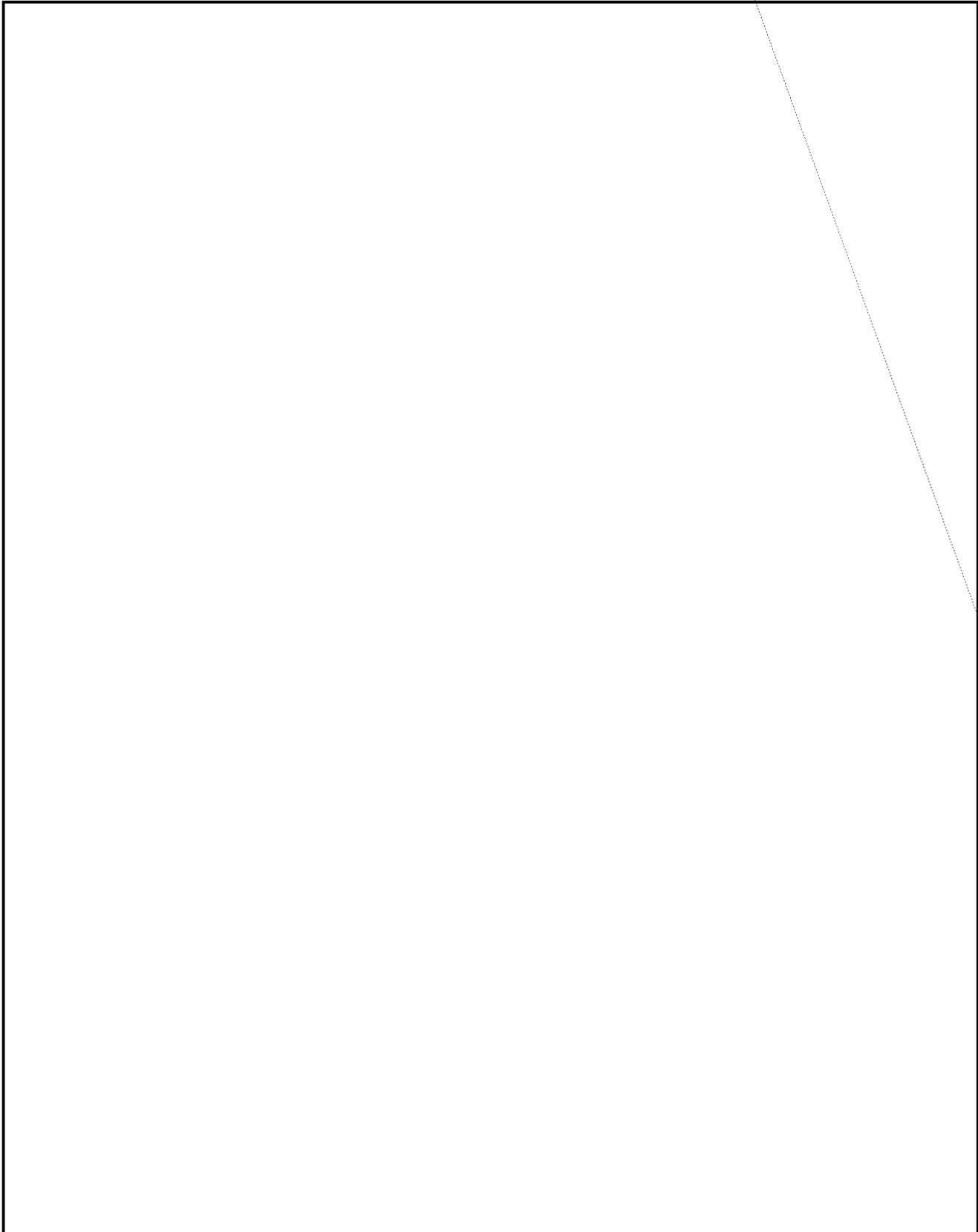
EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

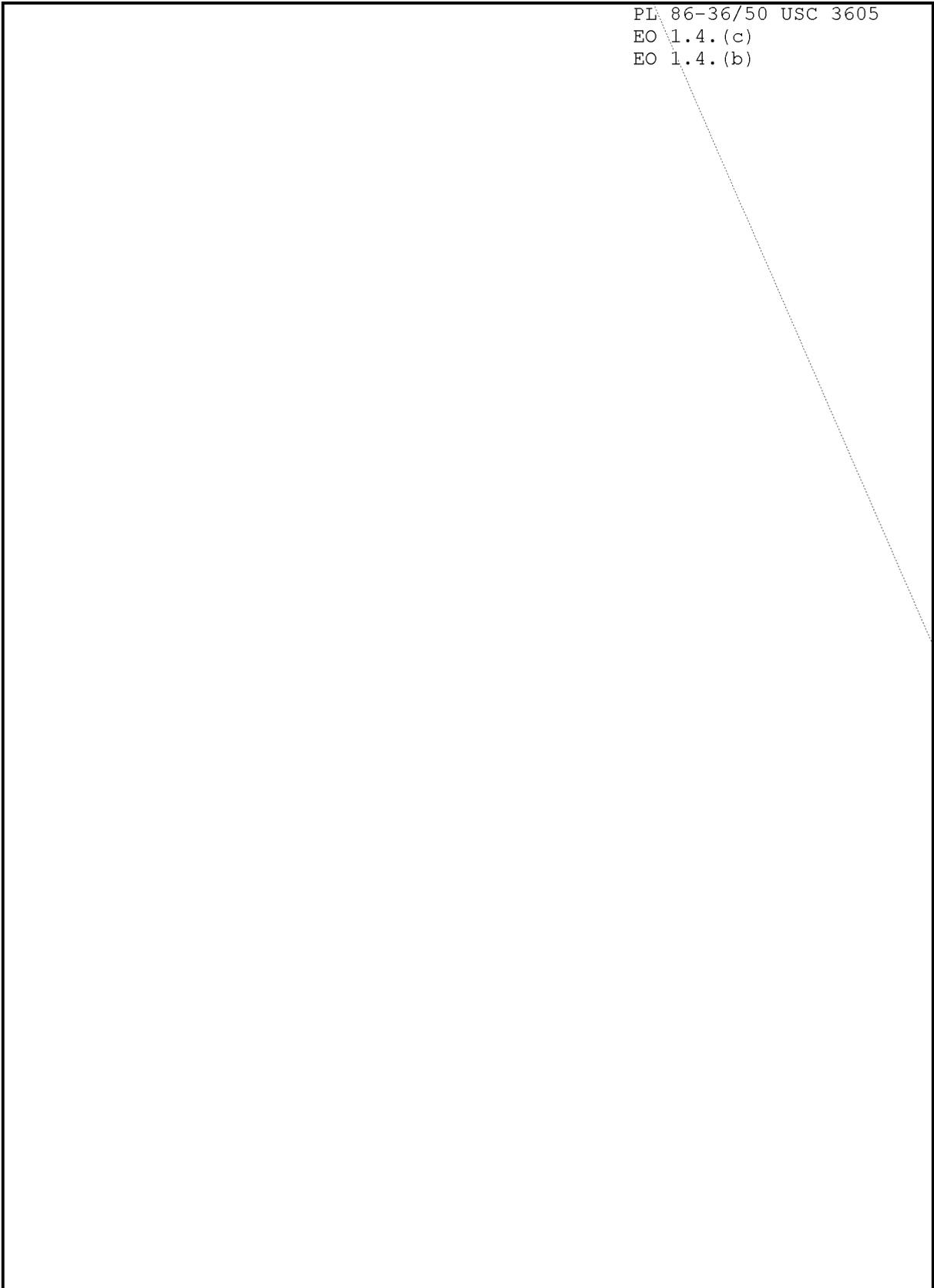
PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)



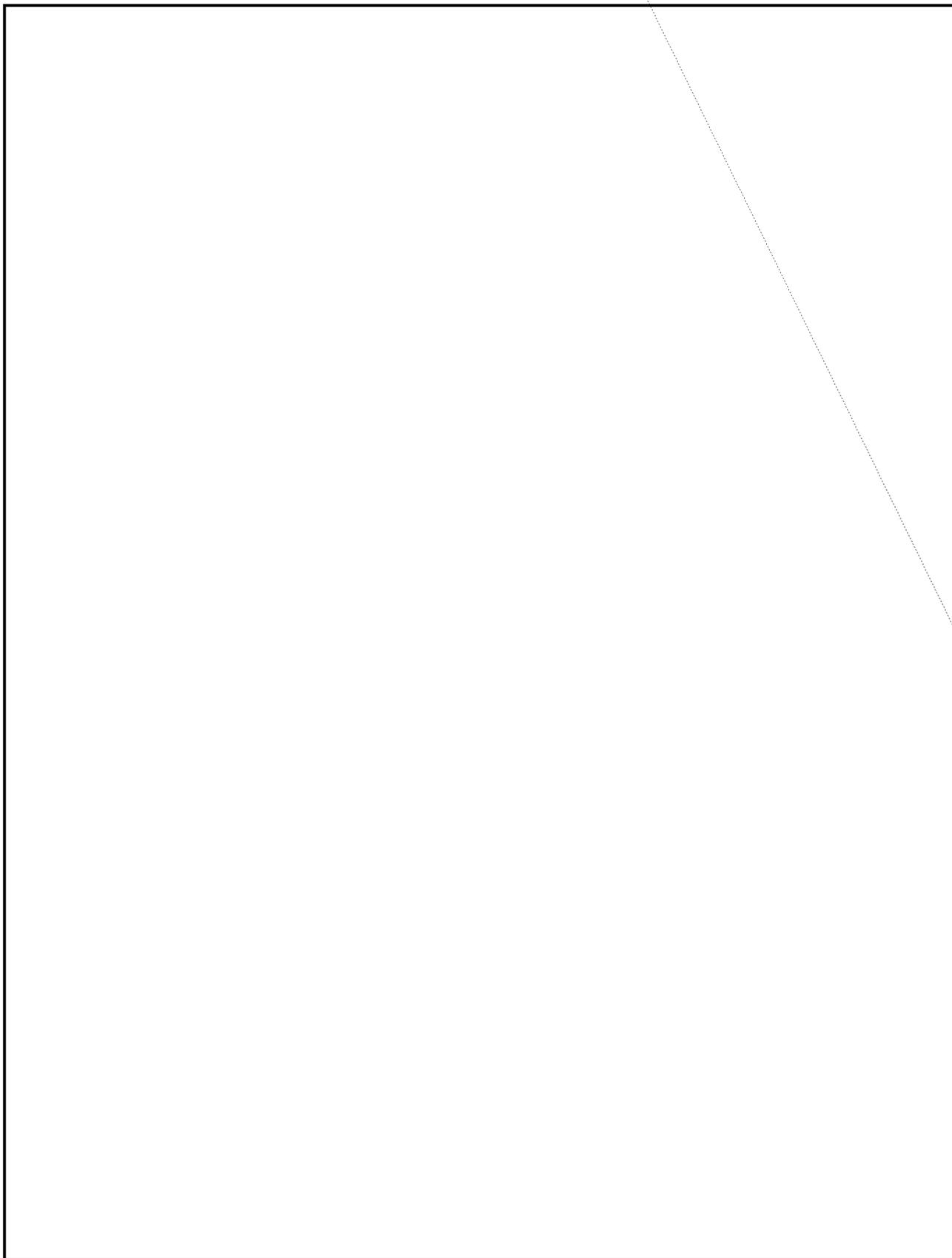
EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 1605

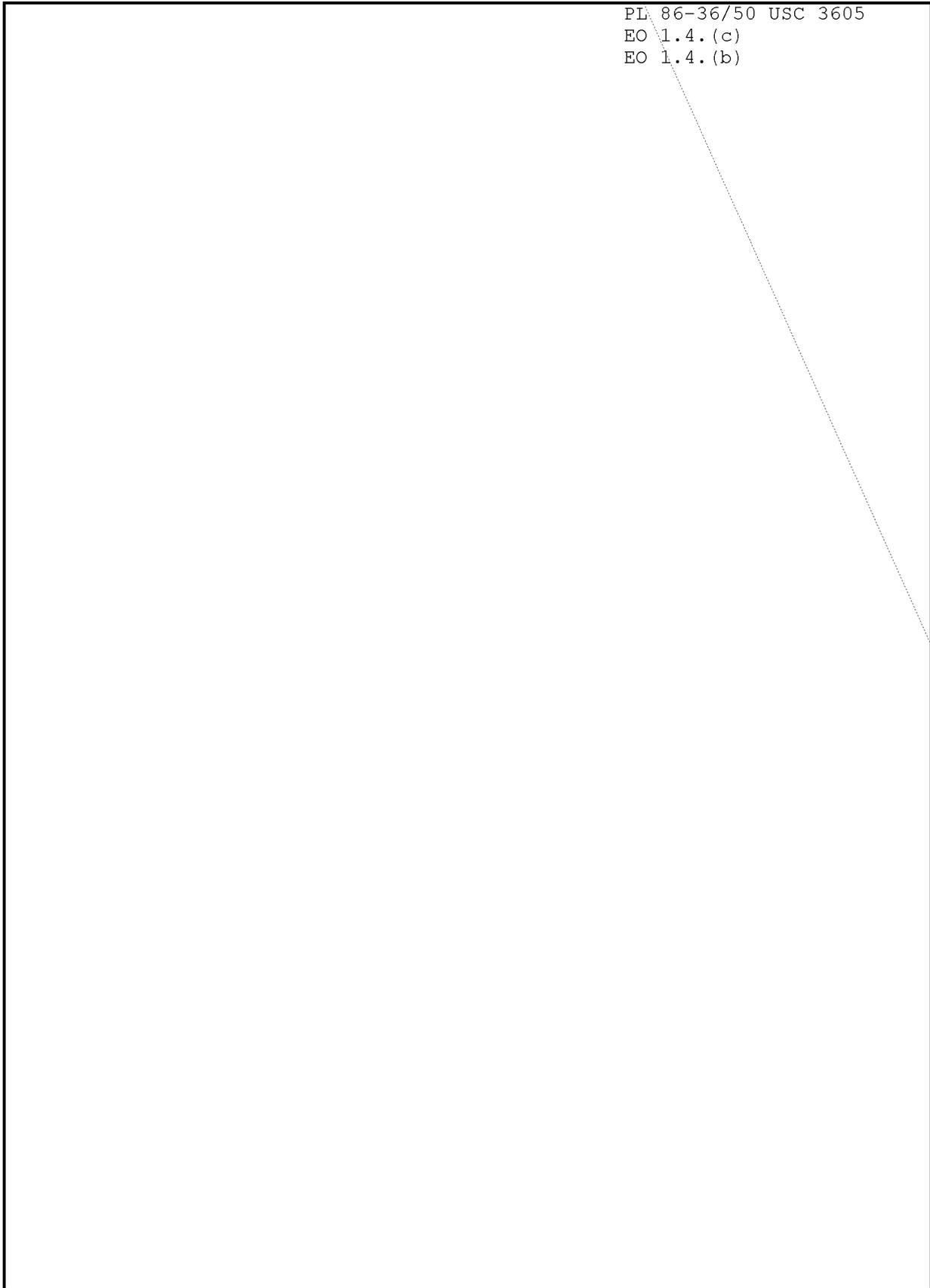






PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)





PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)

PL 86-36/50 USC 3605

EO 1.4.(c)

EO 1.4.(b)





### **Chapter 26: IBM and RAM Contributions to Cryptanalysis**

1. (U) In fact, IBM was still introducing calculating machines, putting on the market for the first time in 1946 its Type 603 electronic calculator. *The Origins of Digital Computers: Selected Papers*, Edited by Brian Randell; Third Edition. (New York: Springer-Verlag, 1982), 233. IBM, secure in the world of commercial calculating hardware, came late to the computer business, not introducing its first real computer, the IBM 701, until 1952. (Ibid, 194.)
2. ~~(S)~~ According to Cecil Phillips [11 August 1993 interview], who worked with both IBM and RAM equipment in the 1940s, there was always tension between the IBM and RAM people, because the IBM people believed that they could do anything the RAM team and equipment could do.
3. (U) STANCICC Liaison Officers, Special Project (BOURBON) memorandum for STANCICC, subject: Semimonthly Report on BOURBON, 16 January 1946 ~~(TS)~~; CCH Collection, Series IV.AA.6.1.
4. (U) STANCICC Liaison Officers, Special Project (BOURBON) memorandum for STANCICC, subject: Semimonthly Report on BOURBON, 31 January 1946 ~~(TS)~~; CCH Collection, Series IV.AA.6.1.
5. JPAG Monthly Status Report, May 1946.
6. LSIC Monthly Status Report, May 1946.

7. JPAG Monthly Status Report, June 1946.
8. (U) BOURBON Project: Survey of Machine Requirements.
9. Ibid.
10. Ibid.
11. Ibid. (X) Although called a "decoding" machine in the study, it should, according to Cecil Phillips (21 December 1993 discussion), more accurately be described as a "decrypting" machine, because it stripped key from the cipher text, uncovering the plain text.
12. (U) According to Cecil Phillips (2 December 1993 interview), Juanita Moody and Paul Reimers thought up the concept for the machine which was named after Mitford Mathews (with one "t" each) who constructed it. Incidentally, the names of later modifications took on the New Testament appellations Mark, Luke and John.
13. BOURBON Project: Survey of Machine Requirements.
14. Ibid.
15. Collins.
16. JPAG Monthly Status Report, August 1946.
17. JPAG Monthly Status Report, September 1946.
18. JPAG Monthly Status Report, December 1946.
19. JPAG Monthly Status Report, June 1947.
20. JPAG Monthly Status Report, September 1947.
21. JPAG Monthly Status Report, August 1947.
22. JPAG Monthly Status Report, December 1947.
23. JPAG Monthly Status Report, May 1947.
24. JPAG Monthly Status Report, September 1947.
25. Ibid.
26. JPAG Monthly Status Report, October 1947.
27. JPAG Monthly Status Report, December 1947.
28. JPAG Monthly Status Report, May 1947.
29. Ibid.
30. JPAG Monthly Status Report, June 1947.
31. JPAG Monthly Status Report, September 1947.
32. (U) CNO U.S. Naval Communications publication, *Brief Descriptions of RAM Equipment*, (Washington D.C., Navy Department, October 1947), 30 October 1947 (TSC); CCH Collection, Series VI.1.23.

- 33. (U) Op-20-NS-1 memorandum, signed by F. W. Cameron, Lieutenant, USN, to Op-20-N-22, subject: Percentage of NS-1 Man Hours Devoted to BOURBON [last time used] Production, 28 January 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 8449, location G16-0410-4.
- 34. JPAG Monthly Status Report, February 1948.
- 35. JPAG Monthly Status Report, October 1948. (U) Isomorphs are, in this case, cipher sequences exhibiting repeat patterns identical with cipher sequences of other messages.
- 36. JPAG Monthly Status Report, November 1948.

**Chapter 27: GCHQ Proposal for Division of Cryptanalytic Effort**

- 1. Semimonthly Report on BOURBON, 1 January 1946 (TS).
- 2. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 21-46, 4 November 1946 (~~TSC~~), NSA/CSS Archives, Accession No. 759, location G16-0407-3.
- 3. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 23-46, 18 November 1946 (~~TSC~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.
- 4. Senior USLO, LSIC Newsletter No. 24-46, 22 November 1946.
- 5. Senior USLO, LSIC Newsletter No. 27-46, 18 December 1946.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

**Chapter 28: Espionage or Normal Cryptanalytic Developments?**

- 1. (U) Many discussions with Cecil Phillips, beginning on 1 December 1992, lasting through April 1994.
- 2. (~~SC~~) N-2 memorandum to 202, N, signed by R. Mason, subject: **The Pattern of Soviet Conduct in Connection with Service Cryptography and Communications**, discussing [redacted] and exploration of the various causes [redacted] 26 October 1948 (~~TSC~~); CCH Collection, Series IV.AA.16.
- 3. (U) Minutes of 35th Meeting of USCIB, held on 16 November 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 2256N, location G16-0608-8.
- 4. Ibid.
- 5. (U) Agenda item 2 of the minutes of the First Meeting of the USCIB Security Committee held on 21 December 1948 (~~TSC~~); NSA/CSS Archives; Accession No. 26073N, location G16-0704-7. (U) Members present were Navy: Captain E.S. L. Goodwin, Chairman, and Commander A. Cole, Jr.; State: Mr. Grant C. Manson; Army: Lt. Colonels A.C. Peterson and C. H. Hiser; CIA: [redacted] USAF: Lt. Colonel H.H. Towler and Lt. H.T. Danilson, and Secretary: Lt. E. J. Rowett, U.S. Navy.
- 6. (U) Agenda item 2 of the minutes of the Second Meeting of the USCIB Security Committee held on 4 January 1949 (~~TSC~~); NSA/CSS Archives; Accession No. 26073N, location G16-0704-7.

EO 1.4.(c)

7. (U) USCIB Security Committee Special Report No. 2-49, subject: Measures for the Protection of COMINT, 11 January 1949 (~~TSC~~); NSA/CSS Archives; Accession No. 26073N, location G16-0704-7.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

8. Ibid.

9. (U) USCIB cover memorandum for the Chairmen, Intelligence and Security Committees of USCIB, subject: Joint Report on USCIB Policy on Dissemination of COMINT to Recipients in Critical Areas, and Protection of COMINT by Such Recipients, 27 April 1949 (~~TSC~~), with enclosures; NSA/CSS Archives; Accession No. 26073N, location G16-0704-7. Also, Minutes of the 41st Meeting of the USCIB held on 17 June 1949 (~~TSC~~); NSA/CSS Archives; Accession No. 26073N, location G16-0704-7.

10. (~~SC~~) GC&CS [redacted] 28 February 1946 (~~TSC~~); NSA/CSS Archives, Accession No. 1664N, location G14-0207-7.

11. (~~S~~) Suspected of being a Soviet agent as far back as World War II, William Weisband was first interviewed by the FBI on 9 May 1950 and was suspended from AFSA on 12 May; he was eventually convicted of contempt of court on 1 November and served one year in prison. Weisband was never tried for espionage. For further details on the Weisband case, see *History of VENONA* by Robert Louis Benson and Cecil James Phillips, National Security Agency, 1995 (~~TSC~~), 113-139.

12. (~~S-CCO~~) NSA ADVA 111 publication: *Russian Scrambler Manual*, July 1958; CCH General Collection.

### Part Five

## BOURBON Traffic Analysis

PL 86-36/50 USC 3605  
EO 1.4.(c)

### Chapter 29

#### From the Shadow of Cryptanalytic Support

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

#### RESOURCE OVERVIEW

A review of both traffic analysis tasks and personnel numbers shows that in 1946 the traffic analysis career field (as well as the language speciality) was principally a support effort to the core task of cryptanalysis. But this situation was changing quickly. In the two American cryptologic organizations, traffic analysts numbered [ ] in May 1946, growing to [ ] by December 1946, a 17 percent increase in six months.<sup>1</sup>

GCHQ organized its traffic analysts differently than the U.S., forming traffic analysis teams which dealt with groups of geographically contiguous countries. For example, GCHQ employed between [ ] traffic analysts in one team that worked not only the Soviet Union, but Eastern and Western Europe, Near East and Far East as well. Mr. Stephen Wolf, a senior traffic analysis specialist at ASA, visited GCHQ in August 1946 (see details below) and reported that [ ] traffic analysts (between 58 and 68 percent of the team's total) worked on the Soviet target.<sup>2</sup>

The following chart summarizes the growth of Allied people power dedicated to traffic analysis of the Soviet target from 1946 through 1948, showing increases of 30 percent and 47 percent annually:

	U.S.	U.K.	Approximate Total
December 1946	[ ]	[ ]	[ ]
December 1947	[ ]	[ ]	[ ]
December 1948	[ ]	[ ]	[ ]

\*Number in August 1946.  
\*\*Number in March 1948.

Let's briefly compare the size of the traffic analysis work force with its cryptanalytic counterpart. By the end of 1947, the Allied traffic analysis work force dedicated to the Soviet target remained considerably smaller than the corresponding cryptanalytic work force [ ] but was growing faster (by about 30 percent per year as opposed to 18 percent). The number of American traffic analysts on the Soviet problem actually increased 39 percent in 1947.

By the end of 1948, the Allied traffic analysis work force dedicated to the Soviet target remained considerably smaller than the corresponding cryptanalytic work force [ ]

[redacted] but was growing faster (by about 47 percent per year as opposed to 7 percent). The number of American traffic analysts on the Soviet problem actually increased 50 percent in 1948, with the growth in British traffic analysts greater than [redacted] percent.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

**EARLY TRAFFIC ANALYSIS ON SOVIET TARGET COMMUNICATIONS**

Modest progress in traffic analysis against Soviet communications began to be made as early as January 1946. For instance, a traffic analytic technique, not described but allegedly used successfully against Japanese traffic during the war, was adopted "to provide reports on individual [Soviet] systems which will give all facts known from preamble and other external analytic sources."<sup>4</sup> By July, the relationship between the Soviet Morse and non-Morse nets was so obvious that plans were being made to have the same analysts work both types of nets.<sup>5</sup>

Traffic analysis continued to produce results. Eleven traffic analysis reports were sent [redacted] It was becoming increasingly evident that the Soviet "Pacific Fleet Net" was employing a system of [redacted]

Although the connection between Soviet Morse service nets and their parallel printer links was pretty much taken for granted in later years, in March 1946 it was news that in traffic analysis the "study of [Soviet] non-Morse links shows increasing tie-ups with Morse nets."<sup>7</sup>

Finally, there appeared another hint of things to come in the growing career field of traffic analysis, something that would eventually be taken for granted, but again in May 1946 was a new discovery:

The most important development in traffic analysis during the month is the identification of several [Soviet] units mentioned in operators' chatter in non-Morse transmissions. These identifications provide battle order information on the same level as that derived from

[redacted]

Traffic analysis soon began to show progress in producing reportable COMINT information. ASA traffic analysts emphasized identifying the controls and outstations on the Morse nets and link ends on the "Military Baudot" printer circuits. Still in May, analysis of both Morse and printer net operations indicated, for example, that the Soviet 10th Air Army Headquarters was located at Toyohara (later changed to Yuzhno Sakhalinsk) on Sakhalin Island in the Far East. ASA traffic analysis had also begun on Soviet "6 and 9 channel Baudot" (i.e., printer) traffic as well on Morse nets.<sup>9</sup>

For their part, Op-20-G traffic analysts identified, based on callsign analysis, a new Soviet sub-tender, which if confirmed would "increase the total of known sub-tenders in the Far East to three." There was also tentative evidence that [redacted] circuits in the Far East" were undergoing a reorganization.<sup>10</sup>

British traffic analysts were apparently a multiskilled group. In May, for example, they filled in at GCHQ for a shortage of Russian linguists: "some Russian messages in low grade systems are translated by personnel of the traffic analysis group."<sup>11</sup> Also in July 1946, Commander Manson, SUSLO, London, reported on GCHQ's traffic analysis progress, wherein:

... summary conclusions which LSIC had drawn from a study of Soviet intercepts known to have been passed over Soviet Naval channels; they are not yet sensational in their revelations, but it can be easily seen that a start has been made to codify the known units of the Soviet Fleet [redacted] Certain warship and naval transport movements in the Baltic are set forth, and of particular interest is . . . evidence of Soviet Naval Reorganization in the Baltic from data gathered in March and April 1946.<sup>12</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Traffic analysis on the Soviet target was of sufficient importance to warrant a three and one-half month temporary duty assignment (August–November 1946) to Britain and Germany by Wolf. Although the primary motivation for the trip was [redacted] (about which, more later), Wolf used the visit as an opportunity to study British traffic analytic operations at GCHQ and at field stations in the U.K. where, apparently, most British traffic analysis was performed. He also spent a month and one-half in Frankfurt, headquarters of ASA-Europe (ASAE), where he visited several ASA field stations and taught traffic analysis courses for the purpose of "upgrading TA capabilities of ASAE personnel." Interestingly enough, according to Wolf, none of the six intercept stations subordinate to ASAE copied Soviet traffic. However, the ASAE Intelligence Branch had a Soviet Analysis section that "was directed toward reading and digesting of [redacted] ASAE copy and primary analysis were apparently focused on [redacted] [redacted] The major problem, according to Wolf, was lack of experienced operators and analysts."<sup>13</sup>

PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)

At the request of the U.S., GCHQ included for the first time a traffic analysis section in its monthly status report, showing the growing, albeit scattered, recognition of the value of traffic analysis on the Soviet problem. GCHQ took pains to point out that much traffic analysis was done at its field stations and by other groups and that British traffic analysts also performed collection management tasks:

Certain tasks normally regarded in U.S. as of a TA nature such as Russian [redacted] [redacted] are in LSIC carried out by Crypt[analysis] Group personnel. The TA Group in LSIC is responsible for all interception and task allocation; these are not normally regarded as TA in U.S.<sup>14</sup>

U.S. traffic analysis continued to produce reportable intelligence and to add new targets to its focus. In June, ASA traffic analysts completed "a study of [redacted] [redacted] Among other things, this study "permitted reevaluation of previous [redacted] locations." ASA was also continuing the study of externals of traffic from the "6 and 9 Channel Non-Morse" circuits, "with a view to determining their intelligence value."<sup>15</sup>

IBM equipment, which was primarily tasked against cryptanalytic problems, occasionally provided support to the traffic analytic effort. For example, in June Op-20-G produced "an IBM run containing all the [redacted] observed to date" as used by the Soviet [redacted] in an effort to uncover further evidence of systematic assignment.<sup>16</sup>

In August, traffic analysis provided tentative identification of two new Soviet [redacted] [redacted] in the Far East. Moreover, the study of callsigns showed a possible total of forty-four Soviet naval vessels, of which nine were identified as tankers. Also in August, ASA planned to expand its traffic analytic "effort in the study of routine messages . . . as an aid to the cryptanalytic effort." Op-20-G planned "as soon as practicable" to set up traffic analytic teams to exploit the Soviet Baltic, Black Sea and other fleets, "in addition to our present Pacific Fleet assignment."<sup>17</sup> A Soviet Black Sea naval traffic analysis desk was indeed set up by Op-20-G in September.<sup>18</sup>

ASA traffic analysis, aided by direction finding, developed more reportable intelligence in September. For example, it was determined that headquarters of the Soviet 126th Rifle Corps moved from Anadyr to Provideniya early in the month. And the headquarters of the Soviet 126th Rifle Corps was found to be located at Magadan. Additionally, the headquarters of the "Transbaikal-Amur" MD was identified at Khabarovsk.<sup>19</sup>

By October, U.S. traffic analysis was beginning to pay large dividends as regards production of intelligence information. Traffic analysts were rapidly filling gaps in the Soviet order of battle; for example:

- a. [redacted] identified the 52nd Rifle Corp in Far East, indicating also that it was subordinate to "Maritime" MD at Voroshilov;
- b. [redacted] indicated the existence of the 74th Artillery Military Depot identified in Moscow;
- c. [redacted] was identified as the 255th Rifle Corps at Petropavlovsk on the Kamchatka Peninsula;
- d. Appearance of four new outstations [redacted] on police networks indicated the expansion of [redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Meanwhile, as autumn descended on the British Isles, U.K. traffic analytic resources were diminishing. In October, GCHQ lost [redacted] of its total headquarters complement of [redacted] traffic analysts to demobilization and posting to U.K. field stations. Despite reduced resources, British traffic analysis produced intelligence information that Soviet Baltic Fleet forces were conducting tactical exercises off Swinemunde. British traffic analysts also determined that certain [redacted] on a Soviet [redacted] Morse group were allocated to [redacted]. Furthermore, the routings of certain Soviet printer message traffic indicated that sometime near the end of August the Soviet "2nd Air Army" had moved (presumably its headquarters) from the general Vienna area to Berlin.<sup>21</sup>

In November, GCHQ took another major personnel hit, losing [redacted] more traffic analysts, presumably to further demobilization and field station postings.<sup>22</sup> The impact of

these losses on the Soviet target is not known, but because of the Soviet target's number one priority, the negative impact was probably minimal, with other targets such as [redacted] taking the more damaging blows.

One of the fundamental duties of traffic analysis continued to be, of course, the support of cryptanalysis. American traffic analysts found in November, for example, that a Soviet 39th Army "Weekly Communications Report," originating from the headquarters at Dairen, was initially passed in [redacted] traffic, but since 8 August it had been transmitted to MD headquarters in the [redacted] system.<sup>23</sup>

Finally, in December 1946 U.S. traffic analysis produced numerous intelligence information "inferences" (as they were then called), a sample of which are these:

- a. SMERSH<sup>24</sup> garrisons were found to be located at Sverdlovsk, Bryansk, Saratov, Krasnodar, and Vinnitsa;
- b. A Soviet Major General of Artillery named Pochitalin was identified at Port Arthur;
- c. The move of the headquarters of the Soviet 39th Army from Dairen to Port Arthur was confirmed; and
- d. A Soviet Naval command afloat was tentatively identified, based on evidence that traffic was being routed to a "Commander [of] Cruisers, Pacific Fleet" in the Kalinin area, where cruisers were known to be at sea.<sup>25</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



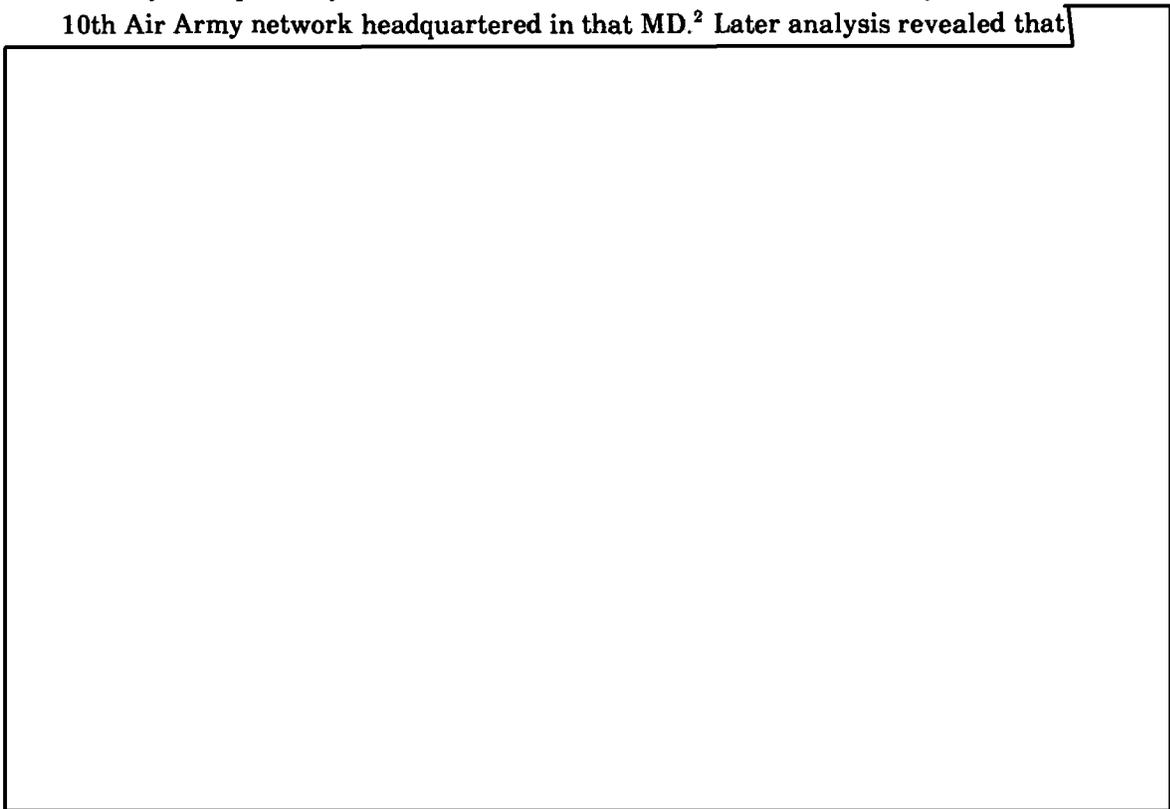
## Chapter 30

### Into the Sunlight of Independent Contributions

Traffic analysis in 1947 made major strides in building the Soviet military order of battle (OB). Allied traffic analysts identified and located no less than

- a. 11 Military Districts (MD) and their headquarters;
- b. 11 Armies, 3 Rifles Corps and a Brigade;
- c. 2 numbered Fleets in the Soviet Far East, and 2 River Flotillas;
- d. 9 Air Armies, 2 Bomber Air Corps (one in northern Korea), and 2 Air Divisions;
- e. 1 Long Range Aviation headquarters in Moscow, with 1 Air Army and 2 Air Corps subordinate;
- e. 2 Fleet Air Forces, 1 Fleet Air Division and 7 Fleet Air Regiments;
- g. 4 Antiaircraft Air Defense (PVO) headquarters and 1 PVO Fighter Air Division; and
- h. 3 SMERSH units, subordinate to the MVD.<sup>1</sup>

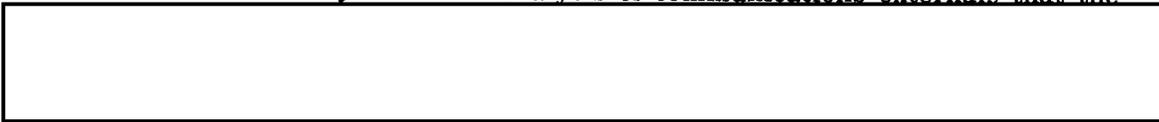
In addition to joining with GCHQ in establishing the existence of these sixty-five Soviet military and state security police organizations, American traffic analysts in January 1947 partially reconstructed the Far Eastern MD net and fully reconstructed the 10th Air Army network headquartered in that MD.<sup>2</sup> Later analysis revealed that



PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)



American traffic analysts in February partially reconstructed a Soviet civil air net operating out of Yakutsk, based on a "great deal of plain-text [messages] on these links." It was also determined by means of analysis of communications externals that the



PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)

On the Soviet merchant marine  target, a variety of communications nets were gradually being resolved in February into three fairly distinct organizations:

- a. Merchant Marine (MORFLOT);
- b. Fishing Group (RYBPROM); and
- c. North Sea Route (GLAVCEVMORPUT).<sup>7</sup>

EO 1.4.(c)  
PL 86-36/50 USC 3605

U.S. Navy traffic analysis found in March that the [redacted] was establishing a communications link directly with all his major unit commanders. Also, CSAW traffic analysts were beginning to detect and follow reorganizations, an indication of a maturing analytic capability against Soviet communications:

PL 86-36/50 USC 3605  
EO 1.4. (c)  
EO 1.4. (b)

Since the first of the year, changes have become apparent in the organization of the Naval Forces in the Far East including the Shore Net, the Forces Afloat, and the Air Forces. The extent of the changes cannot yet be determined since their institution has been gradual and progressive rather than all inclusive and immediate. . . . The Coast Defense organization in particular appears to be fermenting. . . .<sup>8</sup>

GCHQ traffic analysts achieved a breakthrough in April against Soviet Navy communications' externals: [redacted] This opens up a wide field of research since [redacted] are usually allocated very systematically."<sup>9</sup>

EO 1.4. (c)  
EO 1.4. (b)  
PL 86-36/50 USC 3605

EO 1.4. (c)  
PL 86-36/50 USC 3605

Meantime, in May 1947 U.S. plans were under way for the "BOURBON Traffic Analysis Section," [redacted] strong if the Army and Navy personnel were added together, to emphasize research on Soviet military nets in Europe. Study would also begin on [redacted] incidentally, the Soviet [redacted] was allocated its own [redacted] in May.<sup>10</sup> On Soviet [redacted] communications, the entire Far Eastern (Pacific Fleet) network had been reconstructed. It included three links to Moscow, one each from Vladivostok, Sovetskaya Gavan' and Khabarovsk. Also, communications by the 7th Fleet, with headquarters at Sovetskaya Gavan', were activated on 1 May.<sup>11</sup>

U.S. traffic analysis was beginning to pay off in June with the reconstruction of the Soviet Far Eastern naval air net, and work on the solution of [redacted] had progressed satisfactorily.<sup>12</sup> GCHQ traffic analysis of Soviet Baltic Fleet [redacted] proved fruitful, too, in June: [redacted] used by battleship[s], cruisers, destroyers and submarine tenders in the Baltic have been isolated and most of them identified."<sup>13</sup>

GCHQ traffic analysts discovered in July that Soviet [redacted] of aircraft in the Baltic Fleet revealed the [redacted] as a result, the previously unknown unit, the "69th Air Regiment," had been identified as a "North Baltic" unit. GCHQ also continued the reconstruction of the Soviet civil communications landline map; expected benefits were knowledge of [redacted] and "a comprehensive catalogue of main links with traffic loading, interceptibility, and value of traffic." Finally, GCHQ traffic analysts identified [redacted]

[redacted]

U.S. traffic analysis in August identified [redacted] Traffic

analytic detection of the use of new covernames by the probable Soviet 12th Air Army at

Chita was believed by GCHQ in August to be connected with a reorganization going on in the Far East.<sup>16</sup>

GCHQ looked into restructuring its traffic analysis operations in September. Currently, it had two traffic analysis sections: a Soviet and a non-Soviet section. Herbert Conley, SUSLO London staff officer, speculated that GCHQ would decide to amalgamate the Soviet traffic registry unit, the callsign unit and the fusion unit, because they were tied closely to the Soviet Traffic Analysis Section.<sup>17</sup> GCHQ also continued to monitor the growing Soviet [redacted] a new transmission schedule for control and new outstations was intercepted in September.<sup>18</sup>

And in Soviet Black Sea Fleet waters, GCHQ observed that "further classes of submarines have been tentatively identified, namely [redacted] Traffic analysis at GCHQ in September uncovered more Soviet naval tactical activity:

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Unusual activity was observed between the Flagship of the South Baltic Battle Squadron and PILLAU Naval Base from 19th to 21st Sept. During this period [redacted] as well as [redacted] was passed. This is the first time [redacted] has been heard on this link. This was followed by air exercises in the PILLAU area from 24th to 27th Sept, with which the Flagship was concerned.<sup>19</sup>

American traffic analysts uncovered more than OB items in September. They found evidence that "a new Baudot 2-channel [Soviet] air link has been established. This link probably serves Marshal Malinovski's staff for Air at Khabarovsk and the 10th Air Army at Otani." Also, traffic analysis detected three 9th Air Army units relocating to airfields in northern Korea. Finally, traffic analysis followed night operations by mobile units (including five submarines) of the Soviet Black Sea Fleet.<sup>20</sup>

ASA and CSAW traffic analysts had also begun to reconstruct the Soviet [redacted] in the Soviet Union and its outlying areas. In October, the most northern limit of that system was determined to be 72 degrees north latitude. On the Soviet naval target, Moscow's instructions to Vladivostok on a Morse link to inform the commander in chief (CinC), 7th Fleet at Sovetskaya Gavan', to use [redacted] for transmission of service messages to Moscow resulted in the discovery of a previously undetected two-channel Baudot teleprinter link.<sup>21</sup>

EO 1.4.(c)  
PL 86-36/50 USC 3605

At GCHQ, increased communications activity indicated that joint Soviet naval surface and air activity from 24 to 27 October constituted an exercise; a flagship, two destroyers and an unspecified number of unidentified surface units were known to have taken part. Naval air units thought to have been involved in the exercise were the 15th Air Regiment, Koenigsberg area, the 51st Mine and Torpedo Regiment from Palanga, and the 8th Mine and Torpedo Division, also from the Koenigsberg area.<sup>22</sup>

In November, GCHQ noted a second straight month of a generally high level of communications activity on [redacted] It was perhaps no coincidence that the non-Communist Bulgarian government fell in December 1947.<sup>23</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

U.S. traffic analysts in November determined that mobile units believed to be M-class submarines, which had been active in tactical operations since August, ceased activity in September. In addition, "heavy increases in radio circuit activity between Sevastopol' and Evpatoriya . . . indicate that these maneuvers were conducted off the West Coast of the Crimean Peninsula." ASA published a report which "delineated the staff organization of the Soviet Armed Forces as reflected by net structure and routing patterns."<sup>24</sup>

American traffic analysts in December 1947 detected the presence of a new two-channel radioprinter link serving the Soviet Air Forces headquarters in Moscow and the 14th Air Army at L'vov. December 1947 reporting on the Soviet naval target provided an early but still effective traffic analysis argument on the technical benefits of maintaining cover on military HF Morse links:

The Moscow-Sovetskaya Gavan (CinC 7th Fleet Headquarters) Morse link . . . has become virtually a pilot frequency for the radio-printer link between these two locations. Although the amount of traffic intercepted on pilot links is extremely small, [it is] very important and must be closely guarded because

EO 1.4.(c)  
86-36/50 USC 3605

[redacted] For instance, a recent conversation between operators concerning radio-printer communication [redacted]  
[redacted]

GCHQ traffic analysis of Soviet Fleet Air Forces Morse networks revealed in December that "some reorganisation is taking place in the Black Sea." Moreover, "there is evidence of a combined [Soviet] naval-naval air exercise having taken place on 27th and 28th November in the Tallinn area, chiefly involving . . . North Baltic Fleet Air Force-Tallinn, 19th Air Division-Borki and its subordinate Air Reg[imen]ts. Minesweepers were also concerned."<sup>26</sup>

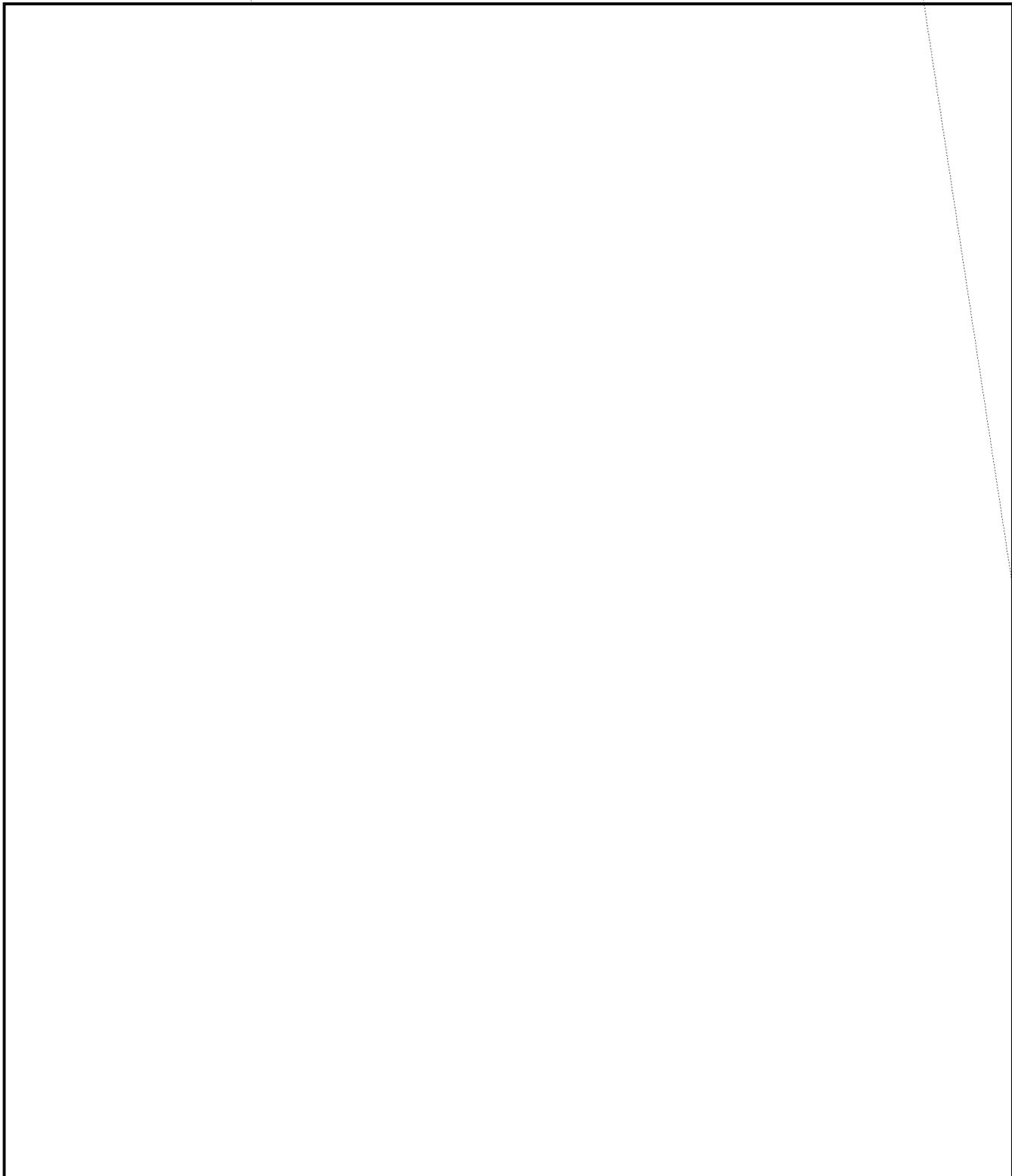


**Chapter 31**  
**Reaching Analytic Mastery**

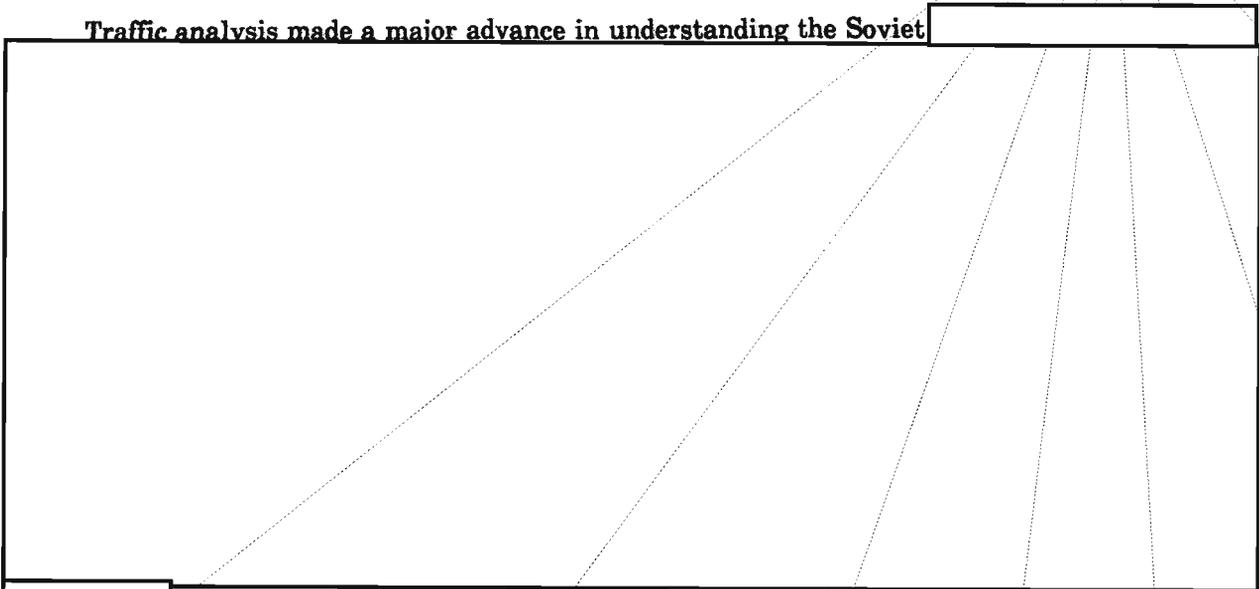
EO 1.4.(c)  
EO 1.4.(b)  
PI 86-36/50 USC 3605

While undoubtedly all the analytic career fields played their part in the more sophisticated COMINT analysis of Soviet military organizational developments and capabilities, it was the traffic analysis reports that often reflected such strides.





Traffic analysis made a major advance in understanding the Soviet



was allowing the following of the movements of major merchant vessels along the Northern Sea Route.<sup>6</sup>

Meantime, GCHQ traffic analysts discovered [redacted] that some Soviet air defense nets were subordinate to other nets; previously, they had been assumed to be on equal levels organizationally.<sup>7</sup> GCHQ also concluded in February, [redacted] [redacted] that the former Soviet 17th Air Army had been downgraded from an air army, probably to an air division. Furthermore, GCHQ's monitoring of the reporting of a Soviet air surveillance unit in the northwestern USSR was providing useful and timely COMINT information on aircraft movements, by type of aircraft, in the Baltic, and between "East Prussia" and Germany.<sup>8</sup>

An example of the natural tension, healthy if held within reason, between traffic analysis and cryptanalysis surfaced in April at ASA. It seems that one of the traffic analysis teams had been monitoring since January communications between the Soviet Central Group of Forces (CGF), presumably in Czechoslovakia, and military authorities in the Carpathian MD. Based in part on a sudden and significant increase in the communications exchanges, the traffic analysts concluded that impending movement of Soviet troops from CGF to or through the Carpathian MD was in the offing, and they had a report in preparation to that effect. But before it could be published, ASA cryptanalysts [redacted] discussed arrangements for the transfer of Soviet artillery troops from the CGF to the Carpathian MD, and they reported that fact. Scooped but undaunted, the traffic analysis team chief published a memorandum for the record "to reaffirm the validity of Traffic Analysis techniques based on traffic flow and volumes (as opposed to the Traffic Analysis techniques already completely confirmed), and to place in [the Traffic Analysis section's] internal records an interesting item not published formally."<sup>9</sup>

Traffic analysts at GCHQ also complained in April about insufficient collection of certain targets:

In almost all cases . . . it will be seen that each system is partly or completely appreciated but the full details can not be produced because of lack of intercepted data. This lack is due both to incomplete cover and to low activity on part of the links. Although Research is mainly satisfied in exposing a system it nevertheless, appreciates that sufficient data must exist to make the answer operationally useful.<sup>10</sup>

A traffic analysis highlight for the Americans in April was the discovery that a "new 2-channel radioprinter link [was] intercepted working between Hq Far Eastern MD, Yuzhno Sakhalinsk, and Hq, 31st Rifle Brigade, Anadyr, representing the first RP link below corps level in the Far East."<sup>11</sup> Charts 4 and 5 illustrate the state of reconstruction of two Soviet Far East Morse and Communications Nets:

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

GCHQ made more headway into the [redacted] in May. Concerning the Soviet military in general, GCHQ cited "two important discoveries which will produce operational Intelligence as data accumulates." The first was the understanding of the way the Soviets were using [redacted] and "the second is the use of [redacted] On Soviet air target: "The main Air Command network . . . [redacted]

[redacted]

Further, "Since 1 May, [redacted]

[redacted] Some identities have been recovered."<sup>14</sup>

Traffic analysts were routinely following the training activities of Soviet forces by July. For example, GCHQ watched the Soviet Navy in the Baltic: "On 3 July there was interworking between [redacted] of 2 destroyers and unidentified submarines in the Libau area. On the same date a further destroyer was in direct contact with several aircraft of an

PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)

unidentified air unit in the S. Baltic. In both cases activity was on the destroyers' frequency." Also, "The submarine group in the N. Baltic . . . was very active between 7-13 July. On 10 and 12 July, there was interworking between ...[an element of the possible] (69th Air Regt. N. 'Paernu' Bay area) and unidentified submarines."<sup>15</sup> GCHQ also watched the Black Sea: "On 10 July an operation of one day's duration took place in the Black Sea involving five major mobile units, the control of a group of submarines, 5 naval-air units, and the Black Sea Fleet naval-air H.Q. . . . C-in-C Black Sea Fleet was [probably] on board 326 (major mobile unit) from 15-21 July. From 29-31 July unusual activity was noted from major mobile units. There was also direct working between these vessels and aircraft. Nine submarines were also active on 29 July."<sup>16</sup>

GCHQ monitored more Soviet naval and naval air activity in August and September. In the Baltic Sea from 20-26 August, a Soviet naval force involving one cruiser, four destroyers, nine submarines and five unidentified vessels carried out training operations. There were daily movements of Soviet naval vessels between the Baltic and Barents Sea during September. Also, from 3-16 September, a major naval and naval air exercise, conducted in three phases, took place in the Baltic Sea.<sup>17</sup>

GCHQ also noted some [redacted] The 9th Air Army in the Far East, having for a year used [redacted]. On 17 August, on HF Morse, and on one air-ground net, the "majority of aircraft discontinued using [redacted] for reporting Departures and Locations in [redacted]."

PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)

ASA traffic analysts detected in August the first of many occurrences over the years of setting up special communications to support field training exercises:

A special net, established in the Far Eastern MD, was operating in August during the period of maneuvers in that MD. It served the District maneuver HQs at Etorofu, Petropavlovsk and Provideniya. The net using [redacted] apparently used the transmitters that are regularly used for normal communications by Yuzhno Sakhalinsk, Etorofu, Petropavlovsk, and Provideniya.<sup>19</sup>

GCHQ also found that "a study of [Soviet] [redacted] has been made, and from identities available from traffic analysis before March 1947, [redacted] other records, it has been possible to identify the following classes [of submarines]: K, M, M100, M200, Shch 300, Shch 400, S and N."<sup>20</sup>

Flight following, the concept of real-time (or near real-time) monitoring of Soviet military flight activity [redacted] was a common feature of the intelligence business, especially the SIGINT business, during most of the Cold War. This capability developed in the 1950s, particularly the real-time aspect, but a hint of its origins can be found as early as 1948. The capability was there then, carried out days after the fact rather than minutes. For example, the Soviets began [redacted] to notify ground stations of their

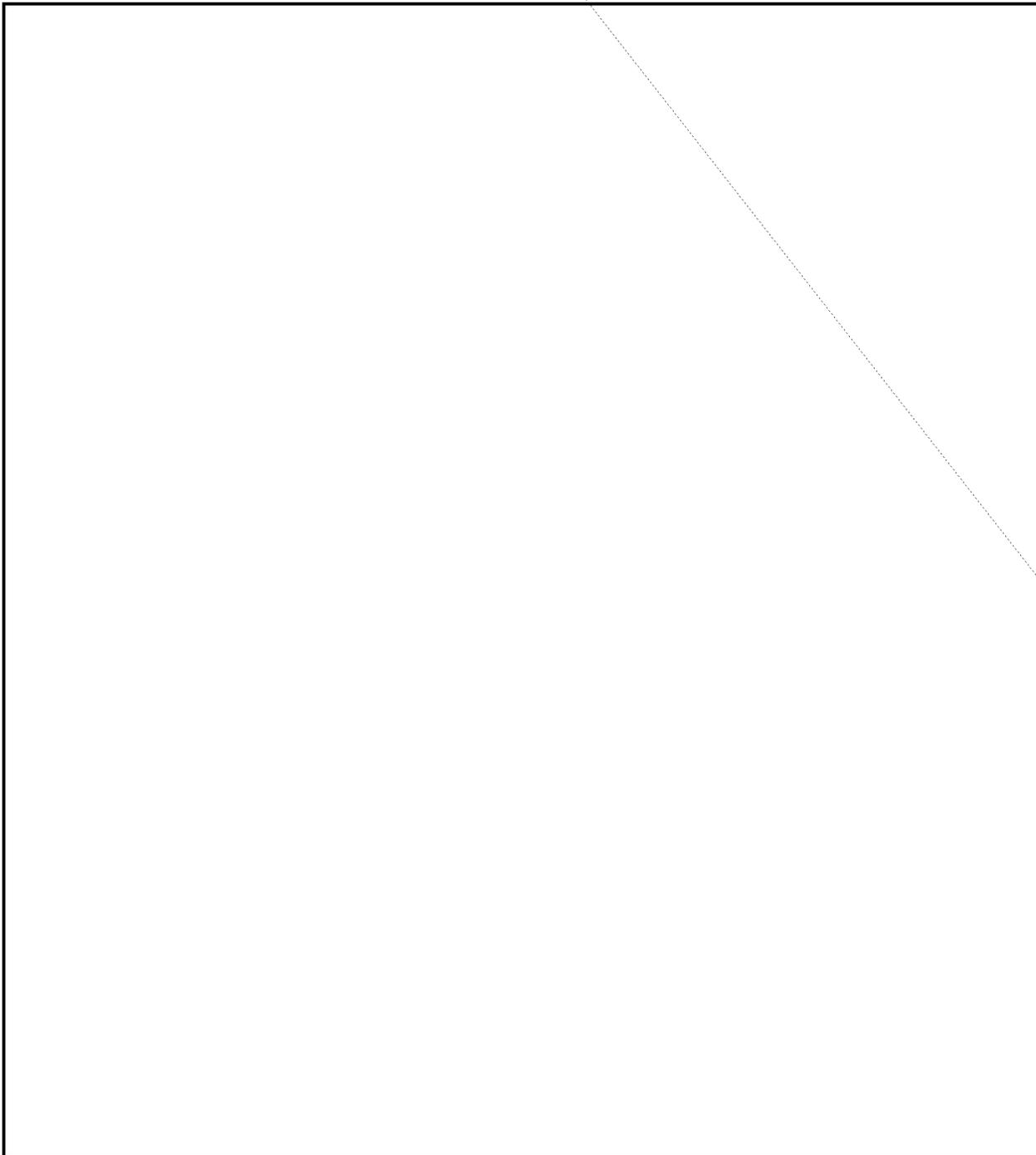
PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)

~~TOP SECRET UMBRA~~

approach, and when they crossed state borders, etc.; for example

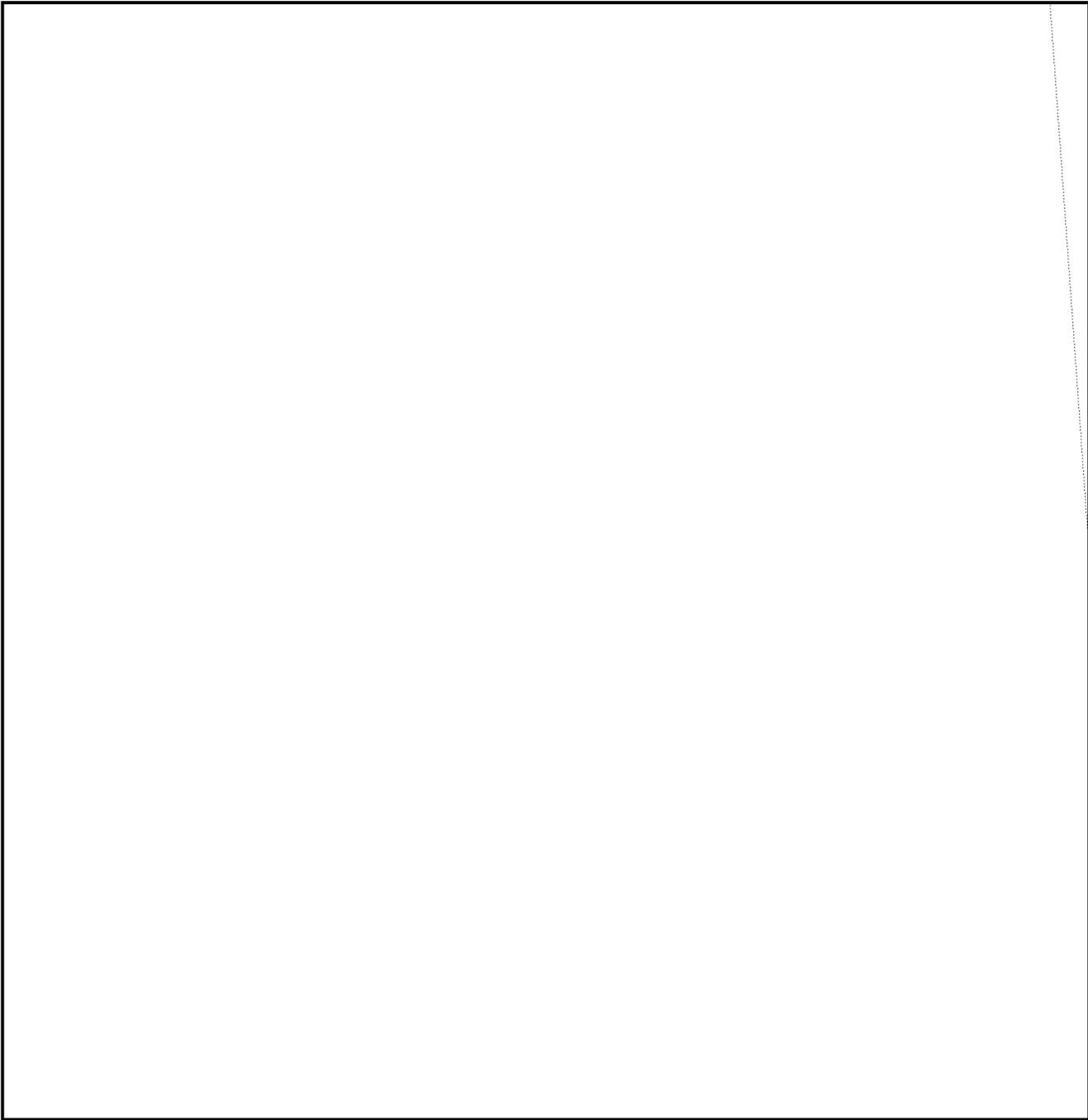
[redacted] Along with this, GCHQ began to monitor flight activity, particularly in the Baltic Sea: "On 9th December nine aircraft moved from Smolensk to Brusterort. The flight was controlled by Kaliningrad Naval air Station [redacted]

[redacted]



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

Chapter 32

[Redacted]

**"Removed from Normal SIGINT Procedure"**

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

This is a cautionary tale of an early post-World War II relationship between Allied COMINT producers and one primary COMINT customer.<sup>1</sup> It was a very strained relationship. It put American and British cryptologists directly at odds with a British Army general, who was, unfortunately for them, the director of Military Intelligence in the British War Office.

This general in 1946 had taken over ownership if not physical possession of a large database of Soviet military intelligence, which he naively and incorrectly viewed as equally valuable as the German ENIGMA intelligence of World War II. He consequently slapped extremely tight, ULTRA-like security controls on the material, limiting access especially to the one intelligence-information-producing source which could contribute most to the validation of its accuracy and to the maintenance and enlargement of its quantity, that is, COMINT.

The situation took over two years to resolve, becoming an object lesson to all cryptologists, demonstrating how the importance of a target problem, distorted and blown out of proportion to its true value by a powerful senior official with little understanding of the SIGINT process, can interfere with common-sense exploitation.

One of the projects under the BOURBON umbrella was called [Redacted] It concerned the COMINT exploitation of [Redacted]

[Large Redacted Area]

[Redacted]

Sometime in 1946, the document came to the attention of British Army general Sir Gerald Templer, director of Military Intelligence (DMI), War Office in London. He reportedly found the collection as valuable as "the solution to the German 'E' [presumably Enigma] problem" in World War II.<sup>6</sup> For example, in August 1946 the War Office estimated that the Soviets had 280 divisions [Redacted]

[Redacted] Templer promptly placed the material under the greatest possible security controls, established an extremely small DMI group to process all [Redacted] data, and arranged to share the findings with its American counterpart, MID, on an "Eyes Only" basis.

GCHQ and ASA<sup>8</sup> were brought into the picture originally in the hope that cryptanalysis might provide a solution to the basic method of [Redacted] used by the Soviets. If there was a logical scheme, and it was understood, one could divine the size and perhaps composition of the overall Soviet force structure. Apparently, General Templer thought that COMINT could provide little new material, as only a few people in each cryptologic agency were given access to the problem initially. Later, when it was realized that COMINT could contribute to the validation, maintenance, and the enlargement of the [Redacted] beyond the European theater, more cryptologic personnel were cleared for

ASA's involvement in [Redacted] began in July 1946, but with the project under another covername. Frank Rowlett, who was then chief of ASA's Operations Division, conveyed to Colonel Hayes, chief, ASA, what the U.S. knew about the [Redacted] Rowlett introduced, initially under the covername NICKELODEON, the subject in a tone which proved unduly optimistic based on what happened subsequently:

[Redacted]

The topic surfaced again later in July, this time brought up by Commander Manson, SUSLO, London. Manson reported on a conversation he had had with Commander Travis, director of GCHQ. It had to do with two ASA analysts coming to London in August:

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

BOURBON problem [redacted] men.<sup>10</sup>

to engage the attention of these

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

Clearly, something was not right with this project. Why did Manson have to be told "confidentially" by a British official about the reason for the two Americans coming to London? Why hadn't Washington already told Manson the purpose of two ASA analysts' trip?

The answers, apparently, had to do with the fact that Manson was not supposed to be let in on the [redacted] secret, that it was not a cryptologic matter. GCHQ was plainly unhappy about how things were going, however, and Travis would not leave Manson out of the loop. Notice in the following quotation from one of Manson's newsletters to Washington how he speaks gingerly on the hush-hush subject that is [redacted]

Major Linn and Mr. Stephen Wolf have been in town for about ten days now and they are using this office as a sort of general headquarters, although the locale of their actual job is apparently the War Office under [British Army] Brigadier Hirsch's [deputy director, Military Intelligence, War Office] cognizance. Everybody has observed to the best of his ability the unilateral nature of their assignment, and other than the practical considerations of their stay in London, in which this office has offered some help, there has been no discussion between us until very lately. The Director [i.e., Travis], however, has touched upon their mission in talks with me; in spite of my stating to him that I had no official connection with it, he seems to deplore it and to want to talk to me about it.<sup>11</sup>

Meanwhile, ASA produced a second NICKELODEON report, undated, but probably issued during the summer of 1946. The [redacted] had been analyzed from a cryptanalytic perspective and from a geographic viewpoint in an effort to detect any patterns of allocation. None were found at that time.<sup>12</sup> Two years later, Rowlett modified that view somewhat, indicating that "at the time of allocation, there was probably a useful pattern of assignment, but that the activation, deactivation, and transfer of units had so disrupted any original methodical plan that an operationally useful solution was impossible."<sup>13</sup> Still later, in 1962, traffic analysis determined that there indeed had been a logical pattern in the original assignments [redacted] and some analytic usefulness was to be found in understanding the allocation scheme.<sup>14</sup>

In August 1946, Colonel Hayes tried to ride to the rescue of GCHQ specifically and of the COMINT business generally. He would try to break [redacted] but of the War Office's restrictive security confines. Wearing a second hat as the U.S. cryptologic community's coordinator for joint operations (CJO), Colonel Hayes was authorized to speak for the United States Communication Intelligence Board (USCIB). He was rumored in June to be planning a trip to Britain. It was officially laid on in late July, and Hayes arrived in London for a week's visit on 22 August. Although not made clear before hand, high on his agenda was the transfer of the [redacted] liaison effort from MID to USCIB control.<sup>15</sup>

Manson later reported extensively on the saga of Colonel Hayes' dealings with the War Office on the [redacted] project. The meeting between the principals started off satisfactorily, according to Manson:

Wednesday [28 August] was very full. We began again with early conferences in my office and then Col. Hayes and I proceeded to the War Office in Whitehall for our 1100 [hour] appointment with Col. Gore and Brig. Hirsch [subordinates of General Templer], where a definite scheme for turning over to USCIB liaison on the [redacted] project was discussed and eventually approved.<sup>16</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

But not all was rosy. It seemed the War Office did not want Manson, who was USCIB's permanent representative and most senior liaison officer in London, to liaise on [redacted]

Col. Hayes encountered some reluctance on the part of MI3 [British War Office] to deal me into the picture, this reluctance being generated by the extraordinary secrecy which Gen. Templer has been trying to draw around the project. The Coordinator [i.e., Hayes] dealt briefly with this reluctance by merely stating that no more secure channel than the USCIB channel could possibly be offered.<sup>17</sup>

After solving that problem, Colonel Hayes deftly finessed another of General Templer's demands, to keep [redacted] an Army possession. Templer wanted Hayes to subscribe to the restriction that [redacted] intelligence not be disseminated to anyone in Washington but MID. According to Manson, "This of course raised the specter of [redacted] being a USCIB affair in London but an [M]ID affair in Washington." Here again, however, Hayes disposed of General Templer's objections by asking whether the War Office had not divulged [redacted] information to the other ministries in London. When Colonel Gore admitted that such revelations had of course taken place but, "only on the highest level," Hayes said that it was on the same level that he proposed to pass the information to other departments in Washington.<sup>18</sup>

GCHQ was still not an equal partner in the [redacted] effort. General Templer treated GCHQ very badly and was getting away with it. Incredibly, Manson was *not* to deal directly with GCHQ on [redacted] as he explained:

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

It was interesting to note MI3's great resistance to LSIC as a cognizant party of the [redacted] project. *Gen. Templer has apparently won the first skirmish and has managed to remove [redacted] from normal SIGINT procedure [emphasis added] to a large extent. Thus, Eastcote's share in these workings is confined to the efforts of 2 or 3 people, and it is ruled that there are to be no direct dealings between Eastcote and me - my only contact is to be Col. Gore.*<sup>19</sup>

GCHQ was unhappy with the situation and had put up a fight but apparently had yielded, agreeing to bow out of any direct liaison on the [redacted] project. Manson commented: "Whatever followed was no affair of mine, but I should not be surprised if words passed shortly afterward between LSIC and MI3. It is most apparent that a long struggle has gone on between LSIC and War Office in regard to [redacted] and criticism at Eastcote of Gen. Templer's method of handling the matter is thinly veiled."<sup>20</sup>

Meanwhile, ASA analysts scanned "a small percentage" of Soviet six- and nine-channel printer traffic, finding twenty [redacted] of which [redacted] [redacted] Mr. Wolf later estimated that approximately [redacted] were culled weekly.<sup>22</sup>

[redacted] of cipher and certain plaintext traffic. Scanning of Far Eastern military Morse and two-channel printer traffic, for example, revealed no [redacted] however, Soviet Red Army Far Eastern MD off-line cipher system decrypts yielded [redacted]

Despite continuing to view the War Office regulations on the [redacted] effort as being unduly restrictive, ASA in September sounded a note of optimism: "If security can eventually be relaxed it would seem desirable to handle intelligence from [redacted] [redacted] sources by normal signal intelligence methods and through standard signal intelligence channels. . . ."23

In early October, Manson reported further on the battle between GCHQ and the War Office over [redacted]

[Royal Air Force] Grp. Capt. [Eric M.] Jones [head of Intelligence [redacted] GCHQ] told me most frankly that he failed to see eye-to-eye with Gen. Templer in regard to [redacted] problem, and it was seriously discussed by the Eastcote Directorate as to whether LSIC would do battle with the General. It was at length decided to say nothing - but Jones tells me with grim satisfaction that MI3 is now requesting the same sequestered handling of [redacted] No decision has been taken and I shall be kept informed.<sup>24</sup>

In other words, General Templer, not content with clamping tight security restrictions on Soviet [redacted] now wanted to do the same thing on the [redacted] and, as we'll see shortly, [redacted] targets. Washington would have none of that nonsense, as Manson applauded later in October:

I was pleased to have your dispatch vetoing further expansion of the [redacted] agreement. Not only did Gen. Templer request such handling for the [redacted] material, but Grp. Capt. Jones informed me on Friday [18 October] that the same has applied to some [redacted] now appearing! USCIB's veto was so phrased that I was able to tell Jones straight off that the answer on [redacted] was also 'no', and he was most relieved. No one fights this battle more heartily or consistently than he.<sup>25</sup>

On 31 October 1946, the War Office published an elaborate memorandum instructing the Allied intelligence community on the proper classification and handling of [redacted] material.<sup>26</sup> The memorandum appeared to give both GCHQ and ASA sufficient latitude to get the SIGINT job done. But problems persisted. The War Office remained the British focal point for the processing and evaluation of [redacted] data, GCHQ was still being shunted outside the liaison chain, and restrictions on [redacted] remained tight.

Early in 1947, ASA tried to bring GCHQ more actively into a project. After commenting substantively on a War Office [redacted] report, ASA said that in the future, U.S. [redacted] reports would be sent to SUSLO, London, for distribution "to both MI3 and LSIC."<sup>27</sup>

In February, Colonel Hayes, dispatched a [redacted] status report to GCHQ, via U.S. Army colonel William Bartlett, the new SUSLO, London, reporting that the "present

monthly intercept of [Soviet] plaintext from Baudot [teleprinter] 6-channel links" was 3,500 messages, from high-speed Morse links, 25,000 messages, that all plaintext Soviet traffic from any type of circuit was scanned [redacted] and that the U.S. was planning to expand collection of [redacted] traffic by building fifteen nine-channel Baudot intercept machines and increasing Morse intercept "as rapidly as operators become available."<sup>28</sup> ASA issued another report on [redacted] directly to GCHQ in March.<sup>29</sup>

In April, the issue of separate "all-source" and [redacted] Soviet military order of battle databases came up between the British War Office and ASA. The War Office felt that the separate OBs were required. The implication was that "all source" information polluted the pure waters of the [redacted] data. ASA countered that [redacted] data should be considered "just one more source of intelligence, albeit an important one."<sup>30</sup> It was apparently a futile gesture. In July, ASA deferred to the War Office's wishes, promising that a [redacted] OB would be produced in the "near future."<sup>31</sup> Four months later, in November 1947, ASA assured the War Office that the future was still near, but claiming personnel resource losses had set back plans for production of a [redacted] OB.<sup>32</sup>

Amazingly, [redacted] problems and War Office's interference were still with ASA a full two years after the issue arose. On 16 June 1948, Rowlett forwarded to Colonel Hayes a memorandum prepared by one of his branch chiefs, a Mr. Theodore Squier. The Squier memorandum<sup>33</sup> recapped the early problems with [redacted] indicating that there was still no regular exchange of [redacted] data between ASA and GCHQ.

Squier outlined the current Soviet [redacted] processing situation at ASA. He explained that IBM machine methods had been used to "most easily and economically" handle the problem, despite the fact that "considerable time and effort has been expended in establishing machine procedures." First, the "basic [redacted] Document" was punched onto cards. Each card contained the [redacted] and the unit to which it was assigned. A distinction was made between new [redacted] [redacted] with the latter added by "cleared personnel of Eurasian Branch, [M]ID."

"Special" [redacted] reports (not further defined) were "prepared directly by card operated electromatic typewriters." [redacted] OBs, on the other hand, were "prepared by comparing the deck of occurrences, listing all hits," and manually producing the document.

All this background led to the last two sections of the Squier memorandum. The penultimate section was titled "Difficulties inherent in the current situation," and it made crystal clear the consequences of General Templer's restrictive policies. ASA had been forced to work under "unnecessarily stringent" security requirements not justified by the source of the information:

[redacted] are believed by U.S. personnel concerned to be no more significant than covernames or any other of a score of T/A 'handles' for units.<sup>34</sup>

Squier claimed that working under these restrictions wasted manpower, detracting "considerably from the value of the finished intelligence product." Moreover, what Squier considered "carrying the procedure to ridiculous extremes" led to the following ridiculous consequences – Three different OBs would be produced: a limited-distribution [redacted] version, a Top Secret Codeword-level book, and a Secret Codeword rendition.

The final section of the memorandum is somewhat puzzling. Squier offered two alternative solutions to the problem, neither of them very realistic in the face of what had happened during the previous two years. The most satisfactory solution, in Squier's view, was removing [redacted] material from the War Office's special handling restrictions, arguing that this action could be dictated on the basis of "the original possession of the document by the U.S." Wouldn't Hayes and Rowlett have already considered this move? Squier added that the War Office could then be persuaded (he didn't say how) to conduct (c) future exchanges between itself and MID through GCHQ.

EO 1.4.(b)  
PL 86-36/50 USC 3605

Squier then suggested his second solution, which seems on its face equally simplistic and unfeasible. MID and ASA would break off liaison arrangements with the War Office, "while partially respecting present security standards." They would then downgrade the classification of [redacted] documents to CAT III, disguising the source by reference to "local records or some similar subterfuge."<sup>35</sup> Seems simple enough. What happened next?

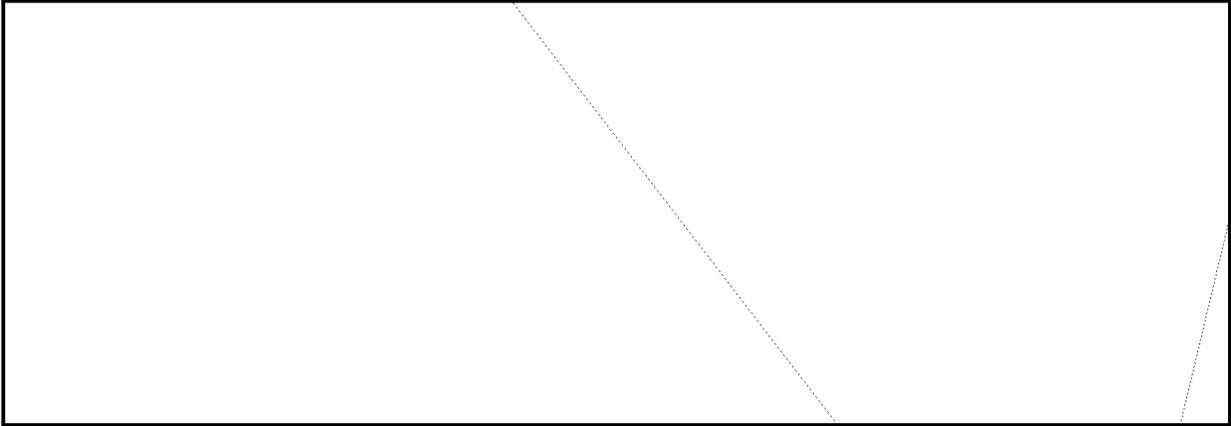
Available historical records do not directly document the consequences of Squier's memorandum nor the specific outcome of this issue. However, by December 1948 a joint ASA-MID intelligence report,<sup>36</sup> classified Top Secret Codeword, began thusly: [redacted] evidence suggests the location of the [Soviet] 96th Rifle Division at Kazan (55°48'N - 49°10'E) in the Volga MD. . . [redacted] identified as the 350th R Regt of the 96th R Div, has been observed. . . ." From this it could be inferred that in the U.S. at least, [redacted] had been broken out of the War Office straitjacket of unnecessarily restrictive compartmentation, into the comparatively free arms of Top Secret Codeword handling. If this inference is accurate, it took two and one-half years to undo the actions of a British general with little understanding of the SIGINT business but with a great deal of power to influence Allied SIGINT processing practices.

Two "lessons learned" come quickly to mind. First, educate the customer. The entire [redacted] problem began because of "a certain unsophistication on the general's part where SIGINT is concerned." There was no indication of a problem on the U.S. side, where the Army's Military Intelligence Division analysts had always worked closely (often in the same room) with ASA analysts. Of course, this lesson was learned long ago. Educating the customer has long been SIGINT community policy, and the [redacted] situation is a reminder of why it has been so.

Moreover, an educated customer would have already learned the second lesson. Strike a balance quickly between concern for keeping the secret and the need to clear enough people to get the job done. This absence of balance *was* the problem with [redacted] British War Office restrictions over how many SIGINT personnel could be cleared for the Soviet [redacted] problem, meant that many ASA and GCHQ analysts did not know when they

came across a [redacted] in traffic that it might be as significant as the Soviet [redacted] It meant great difficulty for GCHQ and ASA to merely exchange [redacted] findings. Granted, arriving at this balance is always a tough call. Clear too many folks for the secret, and someone's loose lips will eventually sink somebody's ships. Finding the proper relationship, particularly on a new secret, will always take some time. But taking over two years to strike the [redacted] balance was a bit too long, as everyone involved then seemed to understand, except the general.

[redacted] Until 1993, [redacted] were available to the Intelligence Community in a [redacted] file on the Community On-Line Intelligence System (COINS), but because the file was not accessed sufficiently, it was pulled off-line and individual [redacted] and their equations to specific units are now published in hardcopy only.<sup>37</sup>



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

## Notes

**Chapter 29: From the Shadow of Cryptanalytic Support**

1. JPAG Monthly Status Reports, May and December 1946.
2. Wolf.
3. JPAG and LSIC/GCHQ Monthly Status Reports, Decembers 1946, 1947 and 1948.
4. Semi-Monthly Report on BOURBON, 31 January 1946.
5. JPAG Monthly Status Report, May 1946.
6. Semi-Monthly Report on BOURBON, 16 February 1946.
7. Semi-Monthly Report on BOURBON, 16 March 1946.
8. Semi-Monthly Report on BOURBON, 1 May 1946.
9. JPAG U.S. Monthly Status Report, May 1946.
10. Ibid.
11. LSIC Monthly Status Report for May 1946.
12. Senior USLO, LSIC Newsletter No. 8-46, 12 July 1946.
13. Wolf.
14. LSIC Monthly Status Report, September 1946.
15. JPAG Monthly Status Report, June 1946.
16. Ibid.
17. JPAG Monthly Status Report, August 1946.
18. JPAG U.S. Monthly Status Report, September 1946.
19. Ibid.
20. JPAG Monthly Status Report, October 1946. (S)   
 thereafter simply calling all such entities "police" circuits, etc.
21. LSIC Monthly Status Report, October 1946.
22. LSIC Monthly Status Report, November 1946.
23. (U) JPAG Interim Report #326, subject: BOURBON Traffic Analysis Cryptanalytic [Note] #15, 5 November 1946 (~~TSC~~); P1 Collection, box CC013, file S-7040.
24. (U) Acronym for the Russian phrase SMERT ShPIONAM or "Death to Spies." By 1946, a section of the NKGB/MGB specializing in terror tactics outside the USSR. The term ceased to be used after 1946. *Espionage-Sabotage-Conspiracy: German and Russian Operations, 1940 to 1945*. Excerpts from the files of the German Naval

EO 1.4.(c)  
 EO 1.4.(b)  
 PL 86-36/50 USC 3605

Staff and from other Captured German Documents; Office of Naval Intelligence (Undated); CCH General Collection. And Buranelli, Vincent and Nan: *Spy/Counterspy: An Encyclopedia of Espionage* (New York: McGraw-Hill, 1982).

25. JPAG Monthly Status Report, December 1946.

**Chapter 30: Into the Sunlight of Independent Contributions**

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

1. JPAG and LSIC Monthly Status Reports, January–December 1947.

2. JPAG Monthly Status Report, January 1947.

3. JPAG Monthly Status Report, March 1947.



6. JPAG Monthly Status Report, February 1947.

7. Ibid.

8. JPAG Monthly Status Report, March 1947.

9. LSIC Monthly Status Report, April 1947.

10. JPAG Monthly Status Report, May 1947.

11. JPAG Monthly Status Report, June 1947.

12. Ibid.

13. LSIC Monthly Status Report, June 1947.

14. LSIC Monthly Status Report, July 1947.

15. JPAG Monthly Status Report, August 1947.

16. LSIC Monthly Status Report, August 1947.

17. (U) Dear Captain Dennis letter, from Herb Conley, USLO, 24 September 1947 (TS); NSA/CSS Archives, Accession No. 5494, box CBPI51.

18. LSIC Monthly Status Report, September 1947.

19. Ibid.

20. JPAG Monthly Status Report, September 1947.

21. JPAG Monthly. Status Report, October 1947.

22. LSIC Monthly Status Report, October 1947.

23. LSIC Monthly Status Report, November 1947.

24. JPAG Monthly Status Report, November 1947.
25. JPAG Monthly Status Report, December 1947.
26. LSIC Monthly Status Report, December 1947.

### Chapter 31: *Reaching Analytic Mastery*

1. (U) JPAG Interim Report #3743, Section RU #1275, subject: Traffic Analysis Diagram #32, 4 June 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0110-2.
2. LSIC Monthly Status Report, January 1948.
3. (U) JPAG Interim Report #3571, Section RU #1188, subject: Traffic Analysis Diagram #31, 3 May 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0110-1.
4. (U) JPAG Interim Report #4142, Section RU #1491, subject: Traffic Analysis Diagrams #38-40, 16 August 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-3.
5. LSIC Monthly Status Report, January 1948.
6. JPAG Monthly Status Report, January 1948.
7. LSIC monthly Status Report, February 1948.
8. LSIC Monthly Status Report, March 1948.
9. (U) Theodore L. Squier, Jr., Chief, 93-B-2 Memorandum for the Record, subject: Traffic Analysis Intelligence, 16 April 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 45812, location G03-0401-3.
10. Ibid.
11. JPAG Monthly Status Report, April 1948.
12. (U) JPAG Interim Report #4142, Section RU #1491, subject: Traffic Analysis Diagrams #38-40, 16 August 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-3.
13. Ibid.
14. LSIC Monthly Status Report, May 1948.
15. LSIC Monthly Status Report, July 1948.
16. LSIC Monthly Status Report, August 1948.
17. LSIC Monthly Status Reports, August and September 1948.
18. LSIC Monthly Status Report, August 1948.
19. JPAG Monthly Status Report, August 1948.
20. Ibid.
21. GCHQ Monthly Status Report, December 1948.
22. GCHQ memorandum on

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

23. (U) C. Garofalo, "A Brief Quarter Century of Soviet Crypto/Traffic Analysis," 1971 (TSC); as published in Vera R. Filby, *A Collection of Writings on Traffic Analysis*, Center for Cryptologic History, NSA, 1993..

24. GCHQ memorandum of [redacted]

25. Garofalo.

26. LSIC Monthly Status Report, April 1948.

27. Garofalo.

28. JPAG Monthly Status Report, October 1948.

29. GCHQ Monthly Status Report, December 1948.

30. GCHQ Monthly Status Report, November 1948.

31. (S) A61 CTR #7-68, title: Soviet Armed Forces Signal Operation Instructions, 14 August 1968 (TSC); CCH General Collection; original provided by [redacted] A/D/Chief, [redacted] January 1994.

32. JPAG monthly Status Report, November 1948 (dated 10 December 1948).

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

**Chapter 32: Project [redacted] "Removed from Normal SIGINT Procedure"**

1. (U) This chapter first appeared as an article by the same name in the Fall 1994 issue of *Cryptologic Quarterly*.

2. (TSC) [redacted] Working Aid 02-90, title: [redacted] 1 May 1990 (TSC), 1; copy available in A241.

3. (U) [redacted] interview of [redacted] [redacted] A241, on 6 April 1994.

4. (S) NSA serial [redacted] [redacted] (TSC). (U) Also, [redacted] [redacted] (TSC), 1; copy available in A241.

5. (U) Chief CSGAS-90 (Rowlett) memorandum for Chief, ASA, subject: [redacted] Processing; 16 June 1948 (TSC); NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

6. Ibid.

7. Wolf.

8. (S,CCO) The Soviet Navy and Naval Air Force also used [redacted] story apparently excluded the British Admiralty and the U.S. Navy's Office of Naval Intelligence and its communications intelligence organization, Op-20-G, except perhaps as customers of the [redacted] data. No historical documentation could be found for their involvement in the processing of [redacted] data during the period 1946-1948.

9. (U) Rowlett note to Col. Hayes, covering attachment prepared by R. Ferner, W. Jacobs and Mr. Squire, entitled: Project NICKELODEON, 15 July 1946 (TS-Special CREAM); NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

10. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 10-46, 26 July 1946 (TS); NSA/CSS Archives, Accession No. 759, location G16-0407-3.

- 11. Senior USLO, LSIC Newsletter No. 12-46, 16 August 1946.
- 12. (U) Probable ASA-produced report, subject: Second NICKELODEON Report, undated but issued circa June 1946 ~~(TS)~~; NSA/CSS Archives, Accession No. 6403, G20-0208-5.

13. (U) Chief CSGAS-90 (Rowlett) memorandum for Chief, ASA, subject: [redacted] Processing; 16 June 1948 ~~(TS)~~; NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

14. ~~(S/CCO)~~ NSA serial [redacted] ~~(TS)~~. Based on an understanding of the original [redacted] allocation scheme, it was possible in 1962 to correct erroneous [redacted] credited to some Soviet units and to assume with some confidence th [redacted] other units for which [redacted] had not yet been noted.

- 15. Senior USLO, LSIC Newsletter No. 13-46, 25 August 1946.
- 16. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 14-46, 2 September 1946 ~~(TS)~~, NSA/CSS Archives, Accession No. 759, location G16-0407-3.

- 17. Ibid.
- 18. Ibid.
- 19. Ibid.
- 20. Ibid.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

21. (U) NICKELODEON Report No. 3 [redacted] in U.S. Intercept, September 1946 ~~(TS)~~; NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

22. Wolf.

23. NICKELODEON Report No. 3.

24. (U) Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 17-46, 7 October 1946 ~~(TS)~~; NSA/CSS Archives, Accession No. 759, location G16-0407-3.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

25. Senior USLO, LSIC Newsletter No. 19-46, 21 October 1946.

26. (U) War Department memorandum for Chief, ASA, subject [redacted] 31 October 1946 ~~(TS)~~, covering a British War Office-produced paper entitled: Method of Handling SIGINT Material on [redacted] and the Intelligence Derived Therefrom, unsigned and undated; NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

27. (U) WDGAS-90 memorandum dated 6 January 1947 to MI3c, subject: Comment on MI3c [redacted] II/88, dated 18 November 1946, reference to U.S. First [redacted] Report dated 19 October 1946, ~~(TS)~~; NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

28. (U) USLO LSIC (Channel 409S) dispatch from CJO, EYES ONLY for Bartlett from Hayes TopSec [redacted] 19 February 1947 ~~(TS)~~; NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

29. (U) WDGAS-90 (Rowlett) cover memorandum to Colonel Hayes (AS-10), with proposed answer to Bartlett re [redacted] paper prepared by Stephen Wolf on 4 March 1947 ~~(TS)~~; NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

30. ~~(T)~~ ~~(C)~~ GAS-10 (Hayes) memorandum to Directorate of Military Intelligence, (British) War Office, subject: M.I.3c [redacted] 116, dated 7 April 1947 (~~TS~~); NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

31. ~~(T)~~ ~~(C)~~ GAS-90 (Hayes) memorandum for Lt. Col. D.W. Price, Directorate of Military Intelligence, British War Office, subject: M.I.3c [redacted] 40 (dated 6 June, which see above), 8 July 1947 (~~TS~~); NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

32. (U) CSGAS (Hayes) memorandum to Directorate of Military Intelligence, (British) War Office, subject: [redacted] Report, 20 November 1947 (~~TS~~); NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

33. (U) CSGAS-90 (Rowlett) memorandum for Chief, ASA, subject: [redacted] Processing; 16 June 1948 (~~TS~~); NSA/CSS Archives, Accession No. 6403, location G20-0208-5.

34. Ibid.

35. Ibid.

36. ~~(S)~~ RU-TAF-MIL-I #287 (Prepared by ASA, ID), subject: 96th Rifle Division, Kazan', Volga MD, 30 December 1948 (~~TS~~); NSA/CSS Archives, Accession No. 9281, location G16-0211-6.

37. (U) Interview with [redacted] [redacted] Analyst, A241, 6 April 1994.

38. Ibid.

39. Ibid.

PL 86-36/50 USC 3605

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

# Part Six

## BOURBON Language Processing

### Chapter 33

#### Language Support to Cryptanalysis

EO 1.4.(c)  
PL 86-36/50 USC 3605

#### RESOURCE OVERVIEW

Russian language skills were required to assist in [redacted] the Soviet [redacted] Throughout most of 1946 and 1947, in America at least, most translations of available Russian plain language telegrams were used [redacted]

ASA employed [redacted] Russian linguists and Op-20-G, [redacted] for an American total of [redacted] in May 1946.<sup>1</sup> ASA supplemented its language force by establishing a Russian language training program for qualified cryptanalysts in August:

An intensive and accelerated language training program has been initiated for carefully selected candidates with an adequate linguistic background. It is hoped within a period of six to nine months to develop in these candidates a limited competence in the translation of stereotyped and less complex traffic.<sup>2</sup>

Consequently, by December 1946 ASA claimed [redacted] Russian linguists, while the Navy had lost one of their [redacted] probably to demobilization. The American total had nevertheless grown to [redacted] a 25 percent increase in seven months.<sup>3</sup>

ASA continued its training program in 1947. A select group of [redacted] officers and [redacted] enlisted personnel at ASA began extensive Russian language and cryptanalytic training in March in preparation for field station assignments in the European and Pacific theaters.<sup>4</sup>

GCHQ statistics are harder to come by. Limited statistics available for GCHQ carried [redacted] dropping to [redacted] [redacted] These numbers are small probably because at GCHQ Russian linguists were so labeled only if they were simply linguists, and most were also trained in cryptanalysis. The relatively large complement of Russian linguists [redacted] depicted in the following chart were assigned to the GCHQ's Ryder Street operation (about which, more later):

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

	U.S.	U.K.	Approximate Total
December 1946	[redacted]	[redacted]	[redacted]
December 1947	[redacted]	[redacted]	[redacted]
December 1948	[redacted]	[redacted]	[redacted]

In summary, the above chart shows that American language resources dedicated to the Soviet target grew annually by 55 percent and 131 percent, while Allied language resources grew by 22 percent and 80 percent in two years.

### DEALING WITH THE SHORTAGE OF RUSSIAN LINGUISTS

In June 1947 the available number of Russian linguists in the two American cryptologic agencies were deemed to be insufficient. The shortage caused ASA to use cryptanalysts with limited language skills to exploit [redacted] traffic. Although the [redacted] messages was viewed as a task requiring strong language skills and some cryptanalytic expertise, because of the shortage of capable Russian linguists at ASA, it was deemed necessary to use cryptanalysts with more limited knowledge of the Russian language. It was thought that by using numerous reading aids [redacted] and with the aid of a competent language consultant, such personnel could produce a worthwhile number of [redacted] in a given period, "although they are admittedly slower than individuals with a good knowledge of the language."<sup>8</sup>

CSAW used a July report to the secretary of the navy on the status of Soviet COMINT production to highlight its difficulties in acquiring and keeping adequately trained Russian linguists. CSAW stated that although current technical progress was in their view highly satisfactory and encouraging, the shortage of linguists continued to be a serious handicap, "a direct result of which is the continuous loss of potentially available intelligence." CSAW's efforts to date to procure more Russian linguists had resulted merely in a trickle of half-trained language course graduates.<sup>9</sup>

A USCIB-level review in August of U.S.-British collaboration made a case for the need for more Russian linguists [redacted] reminding readers that GCHQ's language resources were contributing substantially to the Allied effort.<sup>10</sup>

While the case was being made to senior authorities for more language resources, ASA continued to grow its own, at least for supporting cryptanalytic tasks. Planned for October was a Russian language course, organized within the [redacted] section and "adapted to the special needs of the problem." Study material was to be taken directly from [redacted] and classes would be conducted "under the cooperative supervision of the translators assigned to the section." Six cryptanalysts from the [redacted] group were to participate probably in this course as well.<sup>11</sup>

### RUSSIAN LANGUAGE TRAINING AT GCHQ

Meanwhile, across the Atlantic, GCHQ was enlarging its language work force by also training its own employees. In February 1947 GCHQ began a six-month intensive, three-day-a-week, Russian course for [redacted] personnel [redacted] cryptanalysts and [redacted]

In April high interest in Russian language studies continued at GCHQ. Russian language study groups of GCHQ employees were being organized to meet "out of office

hours."<sup>13</sup> GCHQ's Russian language study groups met for the first time in May and had arranged "conversation and readings in Russian and rehearsals of Russian plays during the lunch hour."<sup>14</sup>

GCHQ in September continued its in-house training program, starting a second Russian language class for [ ] members of the cryptanalytic team and [ ] members of the reporting section; the class would meet twice a week until the end of March 1948.<sup>15</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



**Chapter 34**  
**U.S. Plain-Language Processing**

PL 86-36/50 USC 3605  
EO 1.4.(c)

**FROM CRYPTOLINGUISTICS TO PLAIN LANGUAGE**

Just as the primary function of all Russian linguists was to support cryptanalysis, so too the Russian *plain* language effort began as an adjunct to cryptanalysis. Often plain language was interspersed between encrypted messages, making plain text a valuable source of [redacted] as well as, occasionally, containing information of direct intelligence value. Mr. Jacob Gurin, who headed up the early ASA Soviet plain language problem, recalled: "The function in those days, 1946 and 1947, of plain text was to serve as [redacted] Eventually, Allied collection tapped into a wealth of plain language telegrams not directly of a military nature but of great value for economic and military-related information if processed in sufficient volume. Though not made explicitly clear by the end of 1948, when this study ends, its importance was confirmed in November 1949, by none other than Rear Admiral R.H. Hillenkoetter, U.S. Navy, the director of Central Intelligence, who wrote:

EO 1.4.(c)  
PL 86-36/50 USC 3605

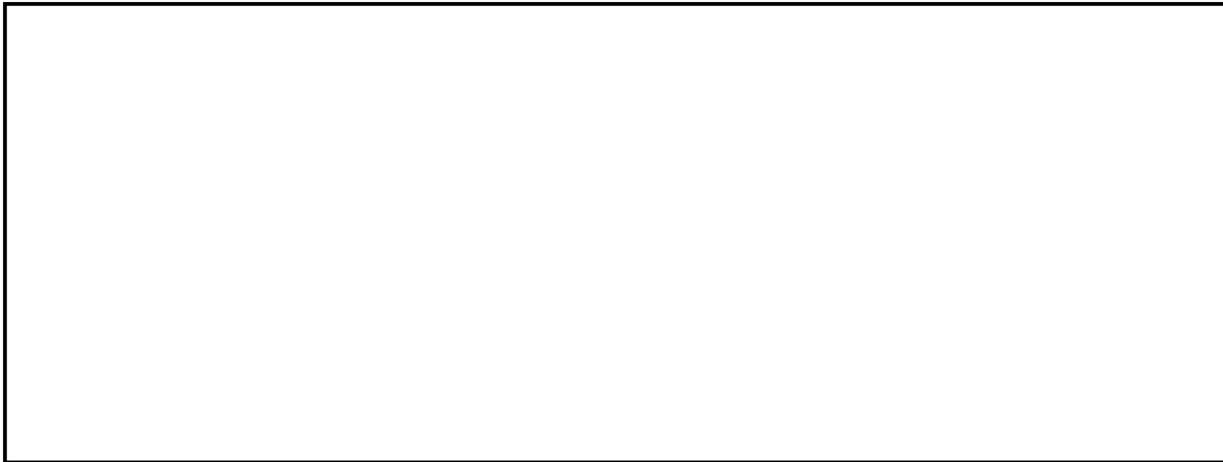
[redacted] OGA

In 1946, however, Russian linguists worked mostly in support of cryptanalysis, merely nibbling at the edges of a plain language effort. In May, for example, [redacted]

[redacted]

Despite Gurin's recollection that plain language was used only for [redacted] in 1946 and 1947, in actuality by midyear 1946 sufficient Soviet plain language material was available apparently to necessitate the provision of scanning guidelines for analysts. In June, Op-20-G and ASA combined to produce two lists of essential elements of information (EEIs) that plain language scanners should look for in Soviet traffic. The "general list" contained such items as "any mention of units of the armed forces, e.g., naval vessels, . . . aircraft, armies, divisions, etc." The list also included references to departments of government, technical weapon system information, economic data, personnel, research facilities, communications data, hydrographic data, and cryptographic information. In the

PL 86-36/50 USC 3605  
EO 1.4.(c)



**A QUESTION OF PRIORITIES**

Because a shortage of linguists was a factor, the priority of translation effort went to [redacted] apparently to provide [redacted]. Apparently the issue of whether to do plain language or work to maintain continuity went to the secretary of defense, first in August 1945 at the birth of Project BOURBON and again in August 1946; his vote went to continuity.<sup>7</sup>

But as early as December 1946, the director, GCHQ, had discussed the issue with Washington, probably trying to persuade the U.S. to apply more resources to Soviet plain language exploitation. When Travis brought up the issue again in February 1947, asking for American assistance, the issue came to the attention of USCICC. Committee meetings were held throughout 1947, and everyone agreed that more processing should be applied to plain language, in March that there was an "urgent" need for Russian translators, by September that the situation was "desperate." ASA presented monthly the status of its "plans" for a special plain-language group. Captain Wenger agreed that the project was of great importance, promising that "CSAW would assist as soon as personnel became available." Finally, in December 1947, "as a result of change in [redacted] [redacted] additional personnel became available at ASA and a new P/L unit was established."<sup>8</sup>

**SPECIFIC LANGUAGE TARGET:** [redacted]

Meantime, the August 1947 USCIB-level review of U.S.-British collaboration identified two important categories of Soviet traffic for [redacted]



EO 1.4. (c)  
EO 1.4. (b)  
PL 86-36/50 USC 3605

OGA  
EO 1.4. (c)

CSAW, as promised to USCICC, in a status report to the secretary of the navy in October, reemphasized the the significance of Soviet plaintext traffic vis-a-vis [redacted] and the consequent need for linguists:

BOURBON plain-language has emerged as an extremely important source of intelligence. The

[redacted]

As if the August USCIB review and CSAW's October status report to the secretary of the navy weren't enough, CSAW wrote again to the navy secretary, making an all-out pitch primarily for more Russian linguists, directly linking the requirement to the need to

[redacted]

CSAW provided background for the linguist requirement, describing in considerable detail the difficulty in acquiring Russian linguists through normal Navy personnel channels. At best, CSAW's most optimistic expectation was to have "41 BOURBON translators in May 1948," but it was considered "almost certain that the actual number will prove to be substantially smaller."

CSAW then recommended to the secretary of the navy a short-range solution:

- (a) Through provision of adequate inducements, procure 200 reasonably well qualified and reasonably acceptable students, officers or civilians, men or women, and commence their intensive training in the Russian language. This excess should provide for the expected attrition. Investigations and eliminations for security reasons can proceed while training is being prosecuted. . . .
- (b) Provide categorically by means of a written directive that the strength of CSA shall be raised to that approved by the Secretary of the Navy and kept there regardless of the strength of the Navy as whole. CSA is now at 62% of complement and losing ground.<sup>12</sup>

Finally, CSAW offered a long-range plan for increasing the production of Soviet COMINT through the acquisition of even more linguists:

- (a) Provide for a continuing program of Russian language training by the Navy adequate to keep filled the CSA complement of 100 translators.
- (b) Provide for increased emphasis on Russian language training at the U.S. Naval Academy and encourage and promote the study of Russian language in civilian colleges, particularly among NROTC [Naval Reserve Officers' Training Candidate] students.
- (c) Provide that the needs of CSA, as they change in light of changing conditions and problems, shall be examined and revised and, upon approval by the Secretary, promptly filled.<sup>13</sup>

~~TOP SECRET UMBRA~~

**ASA'S POWER GRAB FOR EXCLUSIVE RIGHTS TO THE PLAIN TEXT**

Despite the widely perceived shortage at year's end, recruitment and training efforts throughout 1947 by both ASA and CSAW had increased America's Russian language work force from [redacted]. But ASA's Russian language work force outnumbered CSAW's by [redacted] so ASA made a play to acquire the entire plaintext problem for itself.

It turns out that ASA had acquired such a relatively large work force [redacted]

[redacted] In a 17 December JPAG memorandum to his boss, the CJO, Frank Rowlett requested that ASA be allocated *exclusive* responsibility for "processing Russian plaintext messages."<sup>15</sup>

The proposal to centralize Russian plaintext processing at ASA had initially surfaced in a lengthy 10 December ASA memorandum for the record which detailed ASA's extensive and elaborately organized efforts to date. ASA had at the time two units engaged in processing Russian plain text messages:

- a. The Pentagon Unit - The Pentagon Unit consists of [redacted], some of whom are uncleared. The unit has no scanning responsibilities. It translates in full messages provided to it by a fully cleared, expert group of linguists in the Plain Text Unit at ASA.
- b. The Plain Text Unit - The Plain Text Unit is an experimental unit established by Operations Division, ASA, in collaboration with Special Research Branch, [Military] Intelligence Division [G-2], in an attempt to devise new methods of processing the unprecedented volume of Russian Plain Text messages. The unit is physically located at ASA [i.e., Arlington Hall], an organic part of the ASA Russian Section. It consists of [redacted] linguists, [redacted] traffic analysts, and [redacted] clerks....<sup>16</sup>

EO 1.4.(c)  
PL 86-36/50 USC 3605

[Large redacted block]

OCA  
EO 1.4.(c)  
PL 86-36/50 USC 3605

A week later, the ASA-drafted memorandum was forwarded to Captain Wenger, the CJO, touted as a formal JPAG proposal from the USCIB's neutral deputy coordinator for processing allocations, who just happened to be Rowlett.<sup>18</sup>

CSAW likely was not pleased with the ASA proposal. Captain Wenger, the CJO, decided that Rowlett's proposal should go to a joint ad hoc committee for study. Not surprisingly, agreement could not be reached, the committee was dissolved, and an informal arrangement was worked out. As might be expected, the informal plan provided that "each agency would continue to process P/L as before, but would exchange traffic of mutual interest and notify each other of contemplated intelligence reports based on P/L."<sup>19</sup>

~~TOP SECRET UMBRA~~

Significantly, for the first time, USCIB approved as accepted U.S. COMINT reporting policy that plain-language-based COMINT reports would contain full translations of some messages, summaries of others, all with comments derived from pertinent collateral. Previous reporting policy had essentially prohibited the summarization of related messages and the inclusion of comments based on collateral.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

**USCIB REVIEW OF SOVIET PLAIN-LANGUAGE PROBLEM**

In response to Travis' continuing efforts to get more U.S. help on the problem [redacted]

[redacted] ASA and CSAW began to increase resources on the plain language problem. And in February 1948 the USCIB met and discussed whether action was desirable to more effectively exploit Soviet plain language. As much a debating society as a policy board, USCIB began the discussion by arguing over the wording of [redacted]

[redacted] Admiral Stone, commander, Office of Naval Communications (ONC), insisted that from his reading of the paragraph it was not a criticism of the direction of the effort, but that the "field of Plain Language is so large that the present facilities are insufficient." Mr. Armstrong, State Department, diplomatically identified the problem as arising from the "utilization of the intelligence, which . . . is inadequate." He did note, however, that from his "brief conversations with the British, he has received the impression that the U.S. facilities are behind those of the British." [redacted]

OGA  
EO 1.4.(c)  
PL 86-36/50 USC 3605

Colonel Hayes, chief, ASA, took the opportunity to cite estimates of traffic volume - a monthly total of one million plain language messages, with ASA scanning "4 to 5 thousand messages a day." Captain Wenger, chief Op-20-2, added that GCHQ was scanning "100,000 messages per week."<sup>21</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

[redacted] could take two forms, said Wenger: first, translation of individual messages, gists of texts, and summaries; second, "since it is frequently uneconomical to translate item by item that such information could be available in summary form." Wenger added that Travis favored an exchange of summaries but not of [finished] intelligence studies. [redacted]

[redacted] The director of intelligence, U.S. Army, General Chamberlin, wanted the technical experts to get together and produce a plan which would "outline the degree of collaboration, the methods and procedures for allocation of work and other pertinent factors concerning the working level functions."<sup>22</sup>

The U.S. Air Force was finally heard from when General Cabell stated that the Air Force considered plain language exploitation of "infinite value . . . a project that should be enthusiastically supported." He said further that "because of lack of information

concerning Russian internal structure, USCIB should do all in its power to increase the production of pertinent plain language translations and the utilization thereof." When asked if the Air Force had any Russian linguists to contribute, Cabell replied "that his Department is as yet in the process of organization but that every effort will be made to augment the number of translators in that particular field."<sup>23</sup> (The USAF had been established in September 1947, about four months earlier.)

Next, the subject of whether or not plain language could be worked at a lower classification level than encrypted texts was brought up by Admiral Stone, who also noted that the British used "such personnel" (i.e., [redacted] Colonel Hayes said that plain language "must be processed in a different manner," and he agreed to look into the possibility. Finally, the USCIB agreed to form an ad hoc committee under the leadership of the CJO, prepare a study, and submit recommendations to USCIB.<sup>24</sup>

PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)

### ASA'S PLAIN-LANGUAGE EFFORT

Excellent statistics are available for ASA's plain-language effort during 1948. Actually beginning in December 1947 with [redacted] Russian linguists dedicated to the plain-language project, ASA acquired, trained, and assigned on average eight additional Russian linguists per month throughout 1948, ending the year with [redacted] (see Appendix A).<sup>25</sup> ASA took steps in September to exceed even this number, in part by starting an intensive six-month Russian language training course in September, with thirty-one students.<sup>26</sup>

Beginning in January 1948 with a strength of [redacted] Russian linguists, ASA in the first month scanned about 67,000 plain-language messages, extracted information from over 4,000 messages, "processed" (meaning typing information onto IBM cards) about a 1,000 messages, and issued one report and sixteen supplements.<sup>27</sup>

Those numbers rose rapidly throughout the year until in December 1948, [redacted] Russian linguists at ASA scanned over 221,000 messages in one month, extracted information from 25,400 of them, processed on IBM almost 7,000 messages, issuing 139 translations and 70 supplements to earlier reports and translations.<sup>28</sup>

For the year, ASA scanned over two million Russian plain-language messages, extracted information from 380,000 messages, and IBM-processed 52,000 messages (or about 2.4 percent of the number scanned). Moreover, during 1948 ASA published 28 COMINT reports, 436 translations, and 560 supplements.<sup>29</sup>

EO 1.4.(c)  
PL 86-36/50 USC 3605

### CSAW'S PLAIN-LANGUAGE EFFORT

CSAW had [redacted] Russian linguists in December 1947 and [redacted] doing language work by December 1948, an annual growth rate of 261 percent.<sup>30</sup> While CSAW likely allocated a substantial number of Russian linguists to plaintext work, it apparently did not (as ASA did) publish during 1948 what portion of its growing linguist population was [redacted] how many were working the plain-language target.<sup>31</sup> (In

1949, CSAW had [redacted] Russian linguists doing plain-language work, but on this occasion its total Russian language force was not given.)<sup>32</sup>

That CSAW linguists were working the plaintext problem there is no doubt; however, because the number of messages scanned and translated there was impressive, as the following statistics show:

PL 86-36/50 USC 3605  
EO 1.4.(c)

Month/Year	Scanned	Translated
May 1946	281	70
December 1946	829	185
May 1947	[redacted]	[redacted]
March 1948	[redacted]	[redacted]

PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)



## Chapter 35

## British Plain-Language Processing

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

## GCHQ TAKES OVER THE RYDER STREET OPERATION

The British took a different tack in processing Russian plain-language traffic. [redacted]

[redacted] It is believed to be the first of its kind in Allied cryptologic circles, and it most likely served as the model for several similar American projects in later years.<sup>1</sup> The Ryder Street operation was initially run by MI6, independently of GCHQ, probably because General Sir Stuart Menzies, who was both the director-general of MI6 and the boss of the director of GCHQ, wanted to insure complete separation of the cleared personnel at GCHQ and the [redacted]

[redacted] This Soviet plaintext language processing program had apparently been a going concern for some time, for months if not years. At some point in 1946 it was brought under the GCHQ tent, at least administratively. The British did not seem to be hiding this operation from the Americans, but they were slow to show. December 1946 had rolled around before an American cryptologic official finally had his arms around this unusual British effort.

Commander Grant Manson, SUSLO, London, first got an inkling of the size and scope of the Ryder Street operation in August:

I have also learned a few specific facts about the 'special BOURBON problem', one or two of which I feel that it might be wise to pass on to you. I am surprised to hear that LSIC has assembled a translating squad of 60 people, working in the [redacted] in Ryder Street under the leadership of Bonsall, who used to be the special intelligence officer for BOURBON under the old regime at Bletchley Park. The reason for the *cordon sanitaire* that has been drawn around the Ryder St. activity [redacted]

[redacted] and it is therefore essential that they should not be given any [redacted] inadvertent knowledge of the link existing between them and LSIC. The job undertaken by these men is straight translating; any by-products that verge upon the spheres of cryptanalysis or T/A are quietly withdrawn from Ryder St.<sup>2</sup>

In September Manson had occasion to pursue inquiries into the Ryder Street operation with RAF Group Captain Eric Jones, head of GCHQ's Intelligence Group. After a brief discussion of the [redacted] project (see chapter 32), the meeting got around to Ryder Street:

Since the [redacted] project brushed up against the activities at Ryder Street, which have hitherto been somewhat of a mystery to us all, I found that I had a ready-made opportunity to ask questions. Jones explained to me both the old and the new work at Ryder Street, by which I mean that he is now in process of bringing the Ryder Street activity into the LSIC family.

The unit at Ryder Street was first established as a sort of off-the-record group working on certain aspects of BOURBON [redacted]

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

[redacted] It flourished in a clandestine way under the aegis of [redacted]

[redacted] The raw material upon which they worked was mostly non-Morse BOURBON traffic. . . . I have Jones's absolute assurance that as of today nothing produced in Ryder Street will be concealed from USCIB.<sup>3</sup>

There was nothing more on the Ryder Street group until December 1946, when Manson addressed the subject again:

There are a few more facts concerning the Ryder Street setup which I can now add. . . . In the course of time, thanks to the accretion of vetted linguists as a result of the [redacted] [which concluded that GCHQ and its intercept stations needed [redacted] people to do their mission], Eastcote may assemble enough of this kind of personnel to enable it to do without the Ryder Street party altogether - but Jones believes this might take a year or two to accomplish.<sup>4</sup>

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

Commander Manson was relieved of duty as SUSLO, London, on 3 January 1947, but just before the new year, he was given an extensive tour of the Ryder Street operation, possibly the first American to actually view the working spaces there.<sup>5</sup>

**GCHQ'S EARLY WORK ON RUSSIAN VOICE LANGUAGE TARGET**

Most British plain-language work in 1946 was graphic translation efforts done on unenciphered telegrams [redacted] at Ryder Street. But the Soviet voice target began to emerge late in the year. In October 1946, GCHQ reported on its radio telephone (R/T) intercept research:

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

Wire recordings of Russian R/T transmissions intercepted at [redacted] [redacted] early in the summer are being analysed by a linguist who has been detached to research on them [redacted] [redacted] A summary of the recordings is being written up in the form of logs and sent to L.S.I.C. for examination.<sup>6</sup>

November saw GCHQ continuing to pursue this potential new source of COMINT on the Soviet target:

Recorded reels of Russian Air R/T traffic taken by . . . [redacted] have been played off and R/T logs prepared. The logs are being studied, by arrangements with Intelligence Group, by someone who was engaged in German R/T during the War, in order to form an estimate of the value of the material and to suggest a plan for dealing with it in future. Reels of Russian R/T taken by [redacted] are to be studied next. There has been confirmation from a signals service message on a naval group that R/T is in fact in current use by the Russian Navy.

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

It has been reported that [the] normal Moscow [redacted] link has occasionally gone over to R/T and passed a normal commercial message or so, verbally.

Some R/T messages on [redacted] have been taken experimentally.<sup>7</sup>

Briefly, GCHQ's pursuit force was diverted to cryptanalytic support:

The linguist detached to examine wire recordings of Russian R/T transmissions intercepted at

[redacted] has completed his task and has now been attached to the [redacted] [cryptanalytic] party.<sup>8</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

By December 1946, however, GCHQ was back on track:

Preliminary plans have been made in conjunction with Intelligence group and Special [i.e., Soviet] group for the formation of a combined party to work on the miscellaneous traffic on all Russian Air links and in particular air-ground and air-air W/T and R/T. It is intended that [redacted] should do the preliminary processing and T/A; details will be fixed after visits to [redacted] early in the New Year.<sup>9</sup>

British intercept stations began in 1947 to get a handle on Soviet probably HF tactical voice (radiotelephone) communications; the intercepts were sparse but reflected the operational use of these communications by three Soviet entities - [redacted]

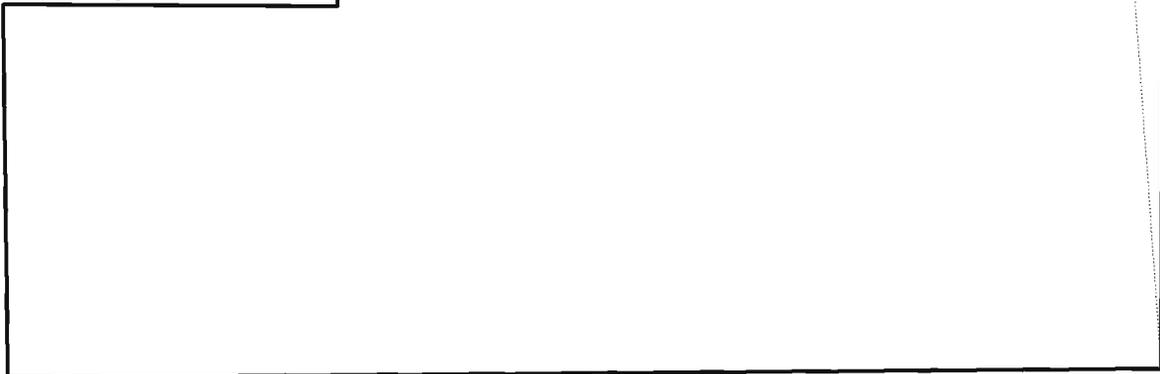
[redacted] In January 1947, for example, radiotelephone communications were noted [redacted]

In July radiotelephone communications were taken for the first time on a [redacted] [redacted] with Moscow probably the control, its outstation unidentified and unlocated.<sup>11</sup>

And in November a new [redacted] was found to be using Morse and radiotelephone communications, with control at [redacted] and one outstation in [redacted]

Finally, suggesting indications and warning capabilities to come, in December 1947 the British intercepted radiotelephone communications being used by Soviet military units "believed to be on manoeuvres."<sup>13</sup>

Lieutenant Fred Bright, SUSLO London staff officer, discovered in June 1948 that GCHQ had included the [redacted]



During the summer of 1948 GCHQ found further indications that the Soviets were using radiotelephone, as well as Morse, communications (presumably in the HF range) in support of their field training exercises in occupied Germany. A special British Army

intercept detachment had deployed to the "eastern limits of the British Zone of Germany," and "considerable success was obtained on both R/T and W/T, and four [Soviet] groups were covered which almost certainly represented formations on manoeuvres. These groups provided the first up-to-date information on combined R/T and C.W. communication, traffic types, callsign usage, etc., of Russian lower-level formations in the fields." GCHQ called on the U.S. to join with them in establishing a collection capability and "leave no stone unturned in the effort to intercept and examine low-level Russian military and air networks and traffic types . . ." despite "the difficulty common to both parties [i.e., the British and U.S.] being a shortage of competent R/T linguists."<sup>15</sup> No specific U.S. response has yet been found in the historical record, but it is clear from forty years of Allied cryptologic history, that ultimately the Allies established numerous



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Chapter 36  
London Technical Conference of 1948

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Only two years after a technical conference was held in London to follow up on the 1946 BRUSA Agreement, GCHQ called for another, this time with a major focus on the emerging Russian plain-language target.

GCHQ's Ryder Street plain-language group was still active in February 1948. Lieutenant Colonel William G. Bartlett (downgraded in rank from colonel like hundreds of other officers after World War II), SUSLO, London, informed Washington in February that Mr. Arthur W. Bonsall, who as Sir Arthur would serve as director of GCHQ from 1973 to 1978, [redacted] and would be relieved in April by John Beaumont. GCHQ was considering sending Bonsall to the States after his relief, to discuss the "Russian [redacted] language problem"<sup>1</sup>

In March, about fourteen months after the first American visit (U.S. Navy Commander Grant Manson, the first SUSLO London, visited the Ryder Street facility on 31 December 1946), a First Lieutenant Frederic J. Bright, U.S. Army, a new SUSLO London staff officer, paid a visit to GCHQ's Soviet plain language operation on Ryder Street, London (GCHQ organizational designator [redacted])

A few weeks later, Lieutenant Bright alerted Washington to GCHQ's proposal for a conference. He explained that GCHQ's director, Sir Edward W. Travis, had first planned to send a party to Washington to discuss the plain-language issue but changed his mind. Now, he was going to send Washington a "complete report on both the intercept and the processing of the traffic," then call for a conference to be held in London "this summer to discuss the problem."<sup>3</sup>

The very next day, 2 April, Travis, writing for the chairman of the London Signal Intelligence Board (LSIB), sent a formal memorandum to the chairman, USCIB (Rear Admiral Thomas B. Inglis U.S. Navy, director, Naval Intelligence), on the subject of "our limited effort on Russian Plain Text traffic [which] has produced most important information." The memorandum expressed concern over British loss of information as a result of lack of manpower and limitations on collection. Travis also mentioned that a report of a survey GCHQ made on the problem was enclosed. He thereupon formally proposed a joint British-U.S. effort, with details to be discussed at a special conference to be held in London.<sup>4</sup>

This call for for Soviet plaintext collaboration included an increase in the scope of Allied collaboration as spelled out in the BRUSA Agreement of 1946. The agreement limited the exchange to selected intercepts and translations. This British call became a plan and, eventually, [redacted] Its main outlines covered [redacted]

unwanted material. Inglis wrote LSIB on 3 June 1948 that the British plan was acceptable to USCIB. It would be approved at the London Conference.<sup>5</sup>

The GCHQ survey forwarded to Washington by Travis in April came in two parts, beginning with Enclosure A, a general description of the target:



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Enclosure B contained GCHQ's proposal for expanded exchange:



Enclosure B also included a much more detailed history on British efforts against Soviet plain text; for example, "British exploitation of Russian plain-text as an entity began in September, 1946, in a section of 30 persons . . .," suggesting the original size of the Ryder Street operation.<sup>8</sup>

Two weeks later, Colonel Hayes, once again the CJO, informed USCIB that ASA and CSAW had agreed on a plan to coordinate their exploitation of "Russian Plain Language Processing" which would maximize production and minimize duplication of effort.<sup>9</sup>

In May, GCHQ forwarded to Washington another study which, among other things, assessed their plain-language effort:



In June, Frank Rowlett, chief, ASA's Operations Division, sent a package of documentation on the Allied plain-language program to Lieutenant Bright in London. One was the "write-up on the ASA Russian Plain Text Unit previously promised you. It was delayed longer than I had anticipated." Another in the package was a copy of the British proposals. Rowlett also identified for Bright the ASA/MID contingent coming to

the London Conference: "Colonel Hayes is bringing [Mr. Benson K.] Buffham and [Mr. Oliver R.] Kirby and [probably Charles F.] Hiser [Lieutenant Colonel, ASA, stationed in 1946 at ASA-Europe in Frankfurt, Germany]. Colonel Peterson, from [U.S. Army] ID, will also attend."<sup>11</sup>

Preparations for the London Conference continued in July. Speaking for SUSLO London, and perhaps also GCHQ, Lieutenant Bright informed Rowlett and Colonel Hayes that he considered the ASA write-up "comprehensive," covering the field "very well." He also reported that [redacted] the Rider Street office, "was very pleased with the formal USCIB proposals, so that the work of that conference committee should be greatly simplified."<sup>12</sup>

On the Soviet plain-language effort, the London Conference was apparently successful, producing one revised appendix plus a new one. [redacted] was revised so that the security and dissemination regulations applied to Soviet radiotelephone, [redacted] and the grading of plaintext messages. A new [redacted] was formulated to embody the results of a complete survey of the Soviet plain text and radiotelephone targets.<sup>13</sup>

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

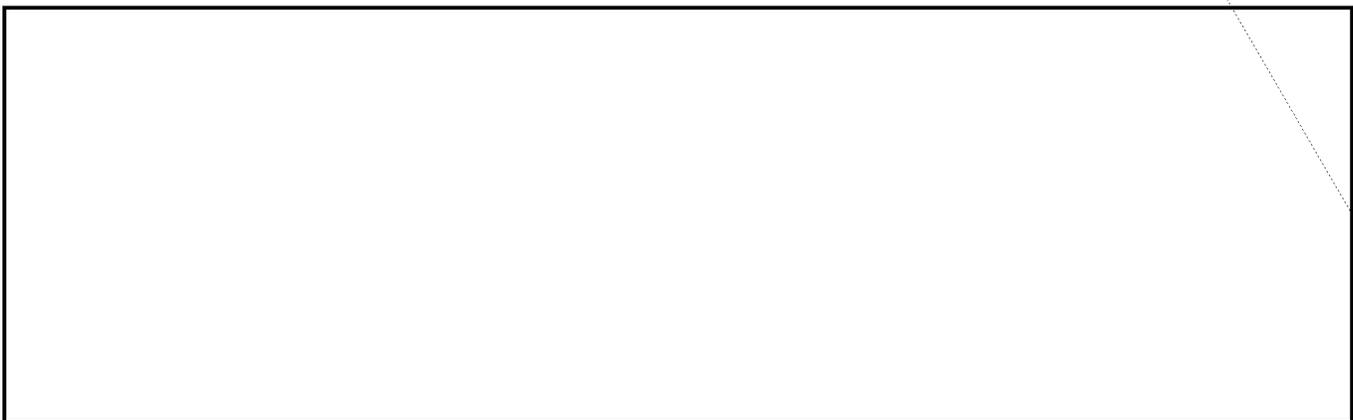
Notes

**Chapter 33: Language Support to Cryptanalysis**

1. JPAG Monthly Status Report, May 1946.
2. JPAG Monthly Status Report, August 1946.
3. JPAG Monthly Status Report, December 1946.
4. JPAG Monthly Status Report, March 1947.
5. LSIC Monthly Status Report, December 1946.
6. LSIC Monthly Status Report, December 1947.
7. LSIC Monthly Status Report, December 1948.
8. (U) JPAG Interim Report #1213, from WDGAS-93B, subject: Report on  Group at ASA, 12 June 1947 (~~TSC~~); P1 Collection, box CC013, file S-9237. EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605
9. (U) Op-20-2 memorandum for The Secretary of the Navy (&) Fleet Admiral C. W. Nimitz, subject: Monthly (May and June combined) report of joint Army-Navy progress in BOURBON Communication Intelligence; 18 July 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 8449, location G16-0410-4.
10. Rowlett Review.
11. JPAG Monthly Status Report, October 1947.
12. LSIC Monthly Status Report, February 1947.
13. LSIC Monthly Status Report, April 1947.
14. LSIC Monthly Status Report, May 1947.
15. LSIC Monthly Status Report, September 1947.

**Chapter 34: U.S. Plain-Language Processing**

1. (U) Jacob Gurin presentation, Cryptologic History Symposium, 14 November 1991. Audiotape available in OGA  
EO 1.4.(c)  
PL 86-36/50 USC 3605 CCH General Collection.



[Redacted]

OGA  
EO 1.4.(c)  
PL 86-36/50 USC 3605

7. (U) CJO memorandum for the Record, subject: Resumé of Progress on Russian P/L Problem, 3 February 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 2256N, location G16-0608-6.

8. Ibid.

[Redacted]

12. Ibid.

13. Ibid.

14. (U) CJO memorandum for the Record, subject: Resumé of Progress on Russian P/L Problem, 3 February 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 1494, location G16-0407-3.

15. (U) Rowlett (DCA) memorandum for CJO, "Allocation of Processing Tasks - Russian Plain Text," 17 December 1947 ~~(TSC)~~; NSA/CSS Archives, Accession No. 21518, box CBJQ74.

[Redacted]

18. (U) JPAG memorandum to Coordinator of Joint Operations from Rowlett, D/Coordinator for Allocations, Subject: Allocation of Processing Tasks - Russian Plain Text; 17 December 1947 ~~(TSC)~~; NSA/CSS Archives, Accession No. 21518, box CBJQ74.

19. Howe, JOP study, 124.

[Redacted]

21. Ibid.

22. Ibid.

23. Ibid.

24. Ibid.

25. LSIC/GCHQ Monthly Status Reports, January-December 1948; it is believed that many of GCHQ's cryptanalysts were also linguists, and not counted among the language population.

26. (U) SUSLO London (Fred Bright) paper, entitled: Some Notes on Ryder Street, 16 April 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 4978, location G05-0405-6. The source of the number 60 is SUSLO London's LSIC

Newsletter No. 12-46, 16 August 1946. The title of the group can be found in USLO memorandum to JICG, subject: USTALO Informal No. 4, 26 February 1947 (~~TS~~); NSA/CSS Archives, Accession No. 5494, box CBPI51.

27. Howe, JOP study, 120.

28. JPAG Monthly Status Reports, December 1947–December 1948.

29. JPAG Monthly Status Report, September 1948.

30. JPAG Monthly Status Report, February 1948.

31. JPAG Monthly Status Report, December 1948.

32. JPAG Monthly Status Reports, February–December 1948. (~~SCCO~~) In September 1949, ASA linguists scanned 122,182 messages, of which about 15% percent (or some 18,300) were used, according to Howe, JOE study, 125–126.

EO 1.4.(c)  
PL 86-36/50 USC 3605  
EO 1.4.(b)

33. JPAG Monthly Status Reports, December 1947 and December 1948. (~~SCCO~~) Figures from September 1949 indicate that CSAW received over 380,000 plain language messages, of which about 30,000 were translated or summarized, and another 135,000 were read and filed.

**Chapter 35: British Plain-Language Processing**

1. (~~SCCO~~) It was apparently the genesis of



2. Senior USLO, LSIC Newsletter No. 12-46, 16 August 1946.

3. Senior USLO, LSIC Newsletter No. 14-46, 2 September 1946.

4. Senior USLO, LSIC Newsletter No. 27-46, 18 December 1946. A review of historical records through 1948, the last year of this body of research, shows no indication other than that the Ryder Street operation was still ongoing at years' end.

5. (U) Manson Memorandum for Coordinator of Joint Operations, Op-20-2, Attention Capt. E.S.L. Goodwin, Supplement to Newsletter #27-46, subject: Inspection of [redacted] Group by the former USLO, 30 January 1947 (~~TS~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

6. (U) Senior USLO, LSIC Memorandum to D/Coordinator for Liaison, USCIB, subject: USLO, LSIC Newsletter No. 1-48, 19 February 1948 (~~TS~~); NSA/CSS Archives, Accession No. 759, location G16-0407-3.

7. LSIC Monthly Status Report, October 1946.

8. LSIC Monthly Status Report, November 1946.

9. LSIC Monthly Status Report, December 1946.

10. LSIC Monthly Status Report, January 1947.

11. LSIC Monthly Status Report, July 1947.

12. LSIC Monthly Status Report, November 1947.

13. LSIC Monthly Status Report, December 1947.
14. ~~(S)~~ Chief, AS-90 (Rowlett) cover note to Chief, ASA (Hayes), passing along Fred Bright's 16 April 1948 letter to Mr. Rowlett about the Ryder Street operation, entitled: *Some Notes on Ryder Street, 29 April 1948* ~~(TSC)~~; NSA/CSS Archives, Accession No. 4978, location G05-0405-6.
15. ~~(S)~~ BLO (Colonel P. Marr-Johnson) memorandum (MOP 89) to The Coordinator, no subject, 3 November 1948 ~~(SC)~~; NSA/CSS Archives, Accession No. 4390, location G15-0501-6.

### **Chapter 36: London Technical Conference of 1948**

1. (U) Senior USLO, LSIC Newsletter No.1-48, 19 February 1948 ~~(TSC)~~.
2. (U) LSIC/USLO Memorandum (signed by Frederic J. Bright, 1st Lt. Sig. C.) for Chief, CSGAS-90, ASA, no subject, 22 March 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No.4978, location G05-0405-5.
3. (U)LSIC/USLO letter to "Dear Mr. Rowlett," from "Fred" [Bright], 1 April 1948 ~~(TS)~~; NSA/CSS Archives, Accession No. 4978, location G05-0405-5.
4. (U) AZ/6106, LSIB Memorandum from Travis, for Chairman, London Signal Intelligence Board (LSIB), to Chairman, USCIB, 2 April 1948 ~~(TSC)~~; CCH Collection, Series V.J.1.
5. Howe, JOP study, 124-125.
6. ~~(S)~~ JLG Memorandum (#0001969) for OP-20-2 and ASA, subject: Russian Plain Text Traffic, 9 April 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No.757, location G16-0406-5.
7. Ibid.
8. Ibid.
9. ~~(S)~~ CJO (Hayes) Memorandum to Members of USCIB, subject: Russian Plain Language Problem, 14 April 1948 ~~(TSC)~~; CCH Catalog, Tab 2C42.
10. ~~(S)~~ JLG Memorandum to Chief, ASA, and OP-20-2, subject: LSIC study "The Effort on Russian Signal Intelligence in Relation to That on Other Signal Intelligence Tasks," 25 May 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 757, location G16-0406-5.
11. (U) ASA Chief of Operations Division (Rowlett) Memorandum for Lt. Fred J. Bright, [USLO, London], no subject, 18 June 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 4978, location G05-0405-5.
- 12.(U) Rowlett's 12 July 1948 note to Colonel Hayes, covering LSIC/USLO (Lt. Fred Bright) letter of 5 July 1948 to Rowlett ~~(TSC)~~; NSA/CSS Archives, Accession No. 4978, location G05-0405-5.
13. Howe, History, 15.



## Part Seven

### BOURBON COMINT Reporting

#### Chapter 37

#### Early Reporting on Soviet Target

EO 1.4.(c)  
PL 86-36/50 USC 3605  
EO 1.4.(b)

Today, [redacted]

Certainly, SIGINT reports for the most part are as complete, comprehensive, and accurate as the reporters can make them; generally, however, the reports are limited to the SIGINT facts and intelligence source identification information. [redacted]

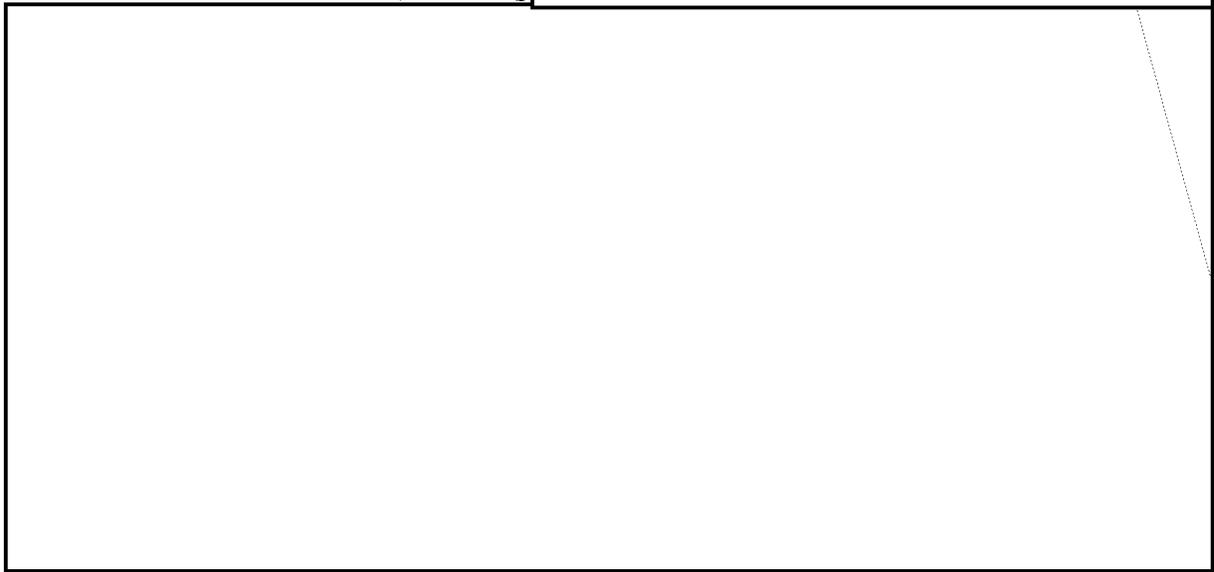
[redacted]

[redacted] and only when it has been clearly determined to be of value to the customer. SIGINT production information that reveals [redacted]

[redacted] is not included.

EO 1.4.(c)  
PL 86-36/50 USC 3605  
EO 1.4.(b)

These restrictions and prohibitions did not exist in the early 1940s nor did SIGINT reporting per se. There was COMINT reporting only and exclusively in the form of translations. There was no ELINT, or telemetry, or [redacted] etc., to qualify for the inclusive term SIGINT. From the start of the American effort against the Soviet target in the early 1940s, both the Army and Navy used 5x8-inch cards to document communications intelligence, specifically, translations of each decrypted message. Each card (or cards if the message was long) contained not only the translated text but all of the technical information available, including [redacted]



ASA "V-Series" intelligence card (1945)

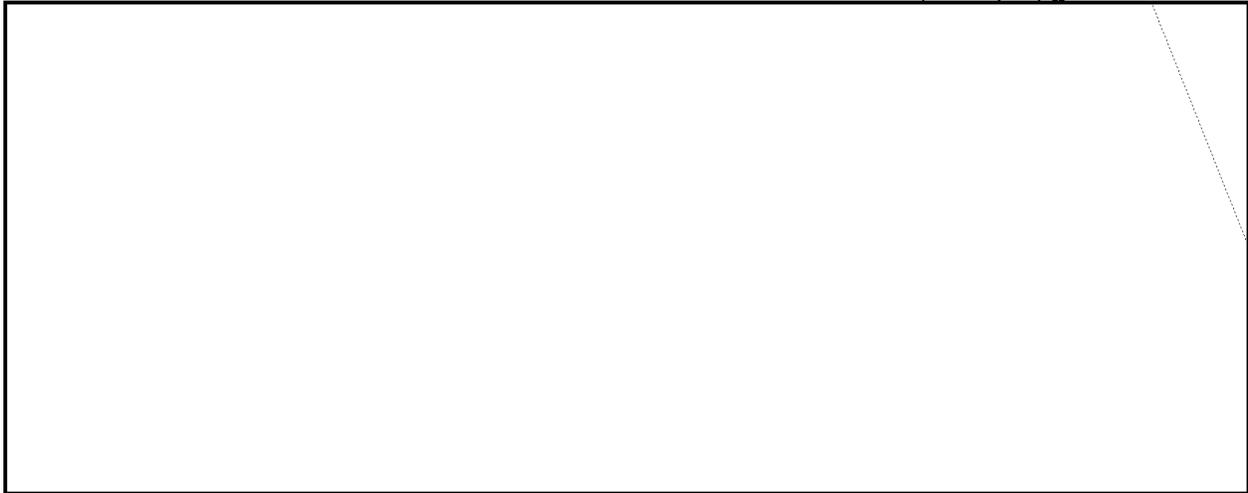
The Army began to serialize its Soviet cards in October 1945, identified by the letter V (believed in 1952 to be the transliterated first letter of the Russian word for military ("Voennyj")).<sup>1</sup> The example shown is a

The U.S. Navy's Russian Section had been producing intelligence in a so-called "Chronological Series" since May 1941. They serialized their cards, identified as G10-Z series, but filed them chronologically by date of intercept.<sup>2</sup>

EO 1.4.(c)

86-36/50 USC 3605

EO 1.4.(b)



Op-20-G "G10-Z/Chronological Series" intelligence card (1945)

Initially, American SIGINTers were restricted in their reporting practices. Reporters, who were at first simply the cryptanalysts, traffic analysts and linguists on the problem, who were given no special title by ASA, and who worked in "intelligence correlation" in the Navy, could comment on individual transcripts, suggesting expansion of abbreviations, adding unit identifications based on collateral, etc. But they were not permitted to indicate a connection between the given translation and an obviously related message sent, for example, the previous day. It was not until the emergence of the Russian plain-language problem in late 1947 and early 1948 that SIGINT analysts were permitted to report on a group of messages encompassing a period of time and covering the same topic.<sup>3</sup>

Concerning distribution, in the 1940s ASA was directly subordinate to the Army's Military Intelligence Division (G-2), and the SIGINTers worked in the same rooms at Arlington Hall Station with the G-2 intelligence analysts. As the primary customers, the G-2 analysts used the cards (with mimeographed copies to the Navy, GCHQ, State, primarily) to produce "all-source" intelligence reports and estimates. Therefore, the cards served not only as the SIGINT technical database but also as the intelligence product, read by the customer as needed.<sup>4</sup> The same procedure was probably used at Op-20-G, where the Navy and Army translations, collateral, and occasional G-2 and ONI intelligence reports were filed together by date.<sup>5</sup>

The British got into the formal SIGINT publication business earlier than the Americans. On 18 August 1945, the very same day that Admiral King and General Marshall approved the BOURBON project, the British began formal dissemination of BOURBON intelligence information. According to available records, GC&CS published its first translation on the subject of Soviet export activity. It was serialized [redacted]

and was entitled "Russian Exports from the Occupied Territories." It contained translated [redacted]

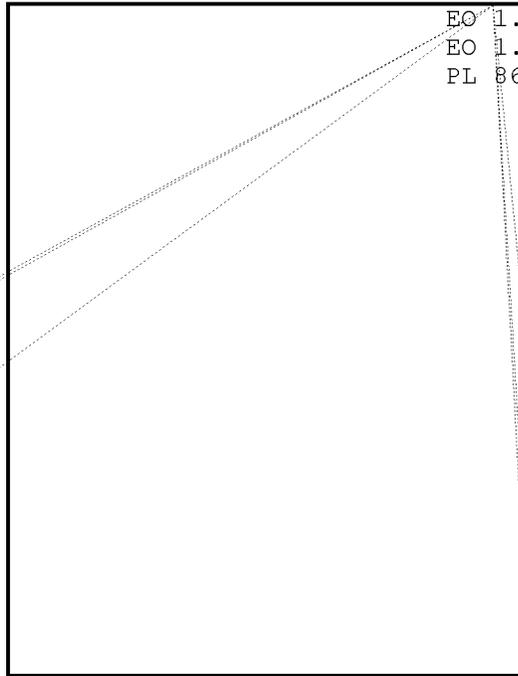
[redacted] messages originated by two Red Army transportation units (the 3rd and 4th Brigades, communicating with their rear services authority), probably in Poland. The messages had been copied during May, June, and July 1945, and most dealt with the day-to-day problems of shipping goods and maintaining serviceable trucks and sufficient drivers. One of the more interesting translations from the report, intercepted on 7 July 1945, talked about demobilization in the 3rd Red Army Brigade:

Brigade and its units have received orders to demobilize the older age groups during the period from 5/7 to 20/8/45. The necessary preparations for demobilization are being made by the units of the Brigade. There are due for demobilization: in the 39th Regiment - 182 men; in the 23rd Regiment - 37 men. As a result of this, the 39th Regiment will be short 105 drivers and the 23rd Regiment, 37. I request your instructions.<sup>6</sup>

According to the distribution page, this report was disseminated to [redacted]

[redacted] One of the two "spares" eventually made its way to the American liaison office.<sup>7</sup>

Most products were translations of one or more related messages (GC&CS also occasionally published "commentaries" to these translations). [redacted]



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

GC&CS product report cover sheet on a Soviet target (1945)

[REDACTED]

among other reasons such as G-2 pressure, Rowlett wanted a clearer picture of their partner's reporting effort. He asked Seaman in London to

Ascertain and expedite report stating quantity of translation in what systems now being produced by GCCS from crypt aspect and information relative [to] intelligence produced through traffic analysis. Particularly interested in the present staff required in evaluating BOURBON material and also how dissemination is made together with the scope of dissemination. Current information particularly desired on order of battle intelligence output. This information desired by MIS and suggest you pay particular attention to intelligence picture for discussion your return [to the U.S. in December].<sup>8</sup>

All told during 1945, ASA and Op-20-G each produced at least 100 intelligence items for their card files.<sup>9</sup> GC&CS had published perhaps only a dozen translations, but they were doing their share. For example, their third, fourth and fifth reports of Soviet military export activity contained the translations of no less than [REDACTED] messages of Soviet military transport units in occupied Germany and Poland. Many [REDACTED] were highly formatted [REDACTED] type messages, giving the daily status of serviceable equipment and tonnages of shipments, and so forth.<sup>10</sup> Of the others, several were of an obsequious nature typical of the Stalin era. For example, on 30 August 1945 one Razumovskij of the 18th (Military Transport) Regiment reported to a Colonel Stepanov:

My personnel are celebrating the Fourth Anniversary of [possibly the Unit] by fulfilling the August - [possibly September] Coal Export Plan before the due date. By their tenacious work and persistence, personnel will achieve high production indicators [REDACTED]. There has been transported [REDACTED] tons of coal.<sup>11</sup>

PL 86-36/50 USC 3605  
EO 1.4.(c)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

### Chapter 38 GCHQ Leading the Way, Formally Speaking

In this Allied cryptologic partnership in 1946, only the British had what might be called a formal COMINT reporting program; the United States was still for the most part in the card file business when it came to producing COMINT on the Soviet military and police forces. The British program had begun in August 1945, and most of the serialized reports, all in mimeographed (hard) copy vice electrically transmitted, consisted of one or more annotated translations of decrypted messages on related subjects; occasionally, the source of the translation would be labeled plaintext traffic. GCHQ (changed from GC&CS in 1946) also published serialized "commentaries," tying together a series of related translations.<sup>1</sup>

By January 1946, the publications department of GCHQ had up a full head of steam.

[Redacted]

The British reports were distributed "externally" to

[Redacted]

Other British offices were added based on topic. The U.S. received three to four "internal" distribution copies addressed by name to one of the American liaison officers.<sup>3</sup>

GCHQ serialized its Soviet reporting by topic.

[Redacted]

Like the Americans with their card files, GCHQ also published

[Redacted]

The reader can get a sense of the number of British COMINT reports issued in 1946 by reviewing the following statistics: GCHQ published

[Redacted]

The timeliness of GCHQ reporting, in terms of delay from date of intercept to date of publication, ranged from as long as seven months to mostly three months. GCHQ did, however, report more quickly on occasion; the activity in a few 1946 reports was less than a month old.

As indicated above, reporting subjects ranged from, for example, Soviet Naval Air Force organization and activity in the Baltic, and Soviet Air Forces' activity in the Kiev Military District, to initial references to the Soviet 4th and 5th Air Armies, to fall 1945 agricultural harvesting operations by the Red Army.<sup>7</sup>

In February, GCHQ published, among others, further reports on the Red Army's assistance to the fall 1945 agricultural harvesting campaign.<sup>8</sup> Reported also was evidence of the existence of a Soviet NKVD Air Force; the report included an interesting link to Kim Philby.

Kim Philby was the notorious British intelligence officer who spied for the Soviet Union and who is believed to have been especially active during the 1940s; he came under suspicion in 1951 and eventually defected to Moscow in 1963. The following story shows his early access to Soviet COMINT.

In February 1946, GCHQ published its sixteenth translation on Soviet Aviation activities, this one titled "Messages Referring to the NKVD Air Force," amplifying the single reference in a [redacted] with the following collateral:

It [i.e., the NKVD Air Force] is known from captured German documents to be an independent police air force involving liaison, reconnaissance, etc.<sup>9</sup>

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Perhaps the most interesting aspect about this particular report was the external distribution. It included the following add-on addressee:

[redacted]

Meanwhile, in 1947 GCHQ (and its American allies) were just beginning to make distinctions between what today we call technical reports and intelligence information (product) reports. The more important differences in 1947 seemed to be between the processing source of the intelligence information - [redacted]

[redacted]

GCHQ used a slightly different system of serialized reports based on analysis of Soviet [redacted] British traffic analysis reports were categorized by either

[redacted]

GCHQ published its Russian plaintext product [redacted] The British published at least eighty *traffic analysis* reports, both technical and intelligence, in 1947.<sup>13</sup>

On 30 June 1947, GCHQ made changes to its reporting serialization system. It

[REDACTED]

In December 1947, GCHQ introduced consumers to Soviet Military "activity" by reporting on a combined Soviet naval/naval air exercise in the Baltic Fleet area:

There is evidence of a combined naval-naval air exercise having taken place on 27th and 28th November in the Tallinn area, chiefly involving. . . North Baltic Fleet Air Force-Tallinn, 19th Air Division-Borki and its subordinate Air Reg[imen]ts . . . 66, 67, 68 . . . and . . . 69th Air Reg[imen]ts. Minesweepers were also [involved].<sup>15</sup>

In 1948, GCHQ issued at least 185 intelligence reports (or fifteen per month) on specific Soviet [REDACTED] in 1948.<sup>16</sup> GCHQ produced a total of 349 technical reports in 1948, or about twenty-nine each month of the year, in an almost baffling variety of series - Interim Reports for cryptanalytic progress, weekly traffic analysis summaries, Periodic Notes (S/S5/500 series), Weekly T/A Summaries which were actually produced at selected British field stations [REDACTED]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



### Chapter 39 American Card Files and Other Media

Soviet service (military and police) COMINT produced by the two American cryptologic organizations in 1946 continued to be mimeographed onto 5-inch by 8-inch cards, complete with all the technical details. Copies of these cards, also called bulletins, were distributed directly to their primary customers, the U.S. Army's Military Intelligence Division (MID), the U.S. Navy's Office of Naval Intelligence (ONI) and, when pertinent, to the State Department and FBI.

ASA produced more than 2,300 V-series serialized cards in 1946. Each card contained the translation of a [redacted] derived from one of at least [redacted]

[redacted] The cards also contained the date and time of intercept, the "to" and "from" callsigns, identification of the subscribers, if known, plus frequencies, case notations, [redacted] The footnoted annotations on the translations were the closest thing to actual COMINT reporting (as we understand the term today) that existed during this period.<sup>1</sup>

Op-20-G also published hundreds of, if not a few thousand, cards in 1946. Op-20-G was reading at least [redacted]

As with ASA, the Navy cards contained all the technical sources and methods data available.<sup>2</sup>

By 1947, ASA and CSAW were producing three basic types of "product" reports: (1) [redacted] (ASA/CSAW [redacted] series, on 5x8 inch cards); (2) plaintext translation series (also on cards); and (3) traffic analysis "fusion" items (V-TAF [Traffic Analysis Fusion] Items).

For comparison purposes, the following chart shows Allied *cryptanalysis-based* reporting on a representative month of May 1947; chart also shows incidentally that, while Soviet collection amounted to 75-92 percent of all Allied intercept (see above), because so [redacted] Soviet reporting apparently amounted to only 15 percent of all COMINT reporting by the Allies:

Target Country	British	U.S.	Total
Soviet Union	[redacted]	950*	[redacted]
All Other (62 entities)	[redacted]	382	[redacted]

\*Mainly Russian military messages (i.e. [redacted] in Far Eastern Area.<sup>3</sup>

A second snapshot, exclusively American, of cryptanalytic reporting statistics on Soviet service targets indicates that in 1947 the two cryptologic agencies apparently published [redacted] - a substantial output averaging [redacted]

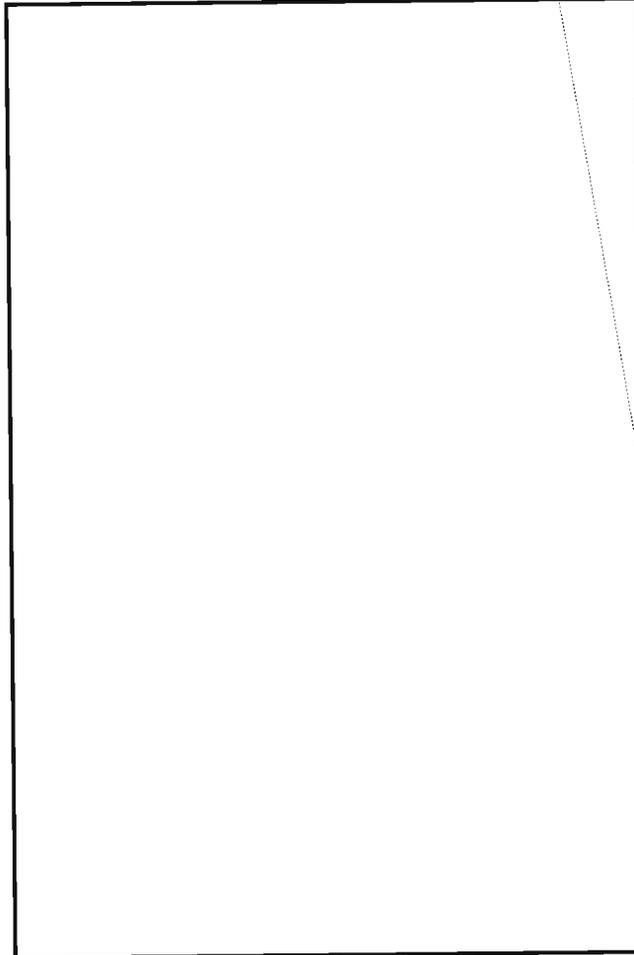
EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

In 1947 the Americans issued between twenty-five and fifty traffic analysis-based reports per month, also both technical and intelligence.<sup>5</sup>

With the Soviet military and state security police *order of battle* in good form, the *activity* of these forces could now be followed, even from telegrams. For example, in July CSAW reported evidence of the beginning of summer surface patrol activity by MVD border police craft in the Vladivostok, Sakhalin Island, and Petropavlovsk/Kamchatka areas of the Soviet Far East.<sup>6</sup>

In 1948, American COMINT reporting, or as it was more commonly called then, "dissemination," was the responsibility at ASA of the Information and Documents Branch (CSGAS-95). At CSAW, it was the Information Division (NI). Each unit received finished COMINT from the cryptanalytic and traffic analysis sections and passed it on to authorized consumers. Published translations (bulletins), prepared in a format standardized by the USCIB's Joint Processing Allocation Group (JPAG), was the principal means of reporting COMINT. All Soviet COMINT was published in a special series. All bulletins were exchanged with GCHQ, who in turn forwarded copies of all its bulletins to ASA and CSAW.<sup>7</sup>

EO 1.4.(c)  
PL 86-36/50 USC 3605  
EO 1.4.(b)



V-TAF-AIR-I item

Most significantly, COMINT consumers in 1948 acquired the right of access to virtually raw traffic:

In addition to receiving published bulletins, the consumer agencies were allowed to obtain raw translations and other unfinished COMINT products necessary for the fulfillment of their mission, and to place indoctrinated representatives within COMINT producing sections. These arrangements were sanctioned by USCIB on 27 April 1948, in connection with a request [redacted] for fuller access to COMINT activities, and were made applicable to all USCIB members. The exact categories of COMINT products and information to be made available could not be laid down in advance, but had to be left to the judgment of the individual consumers.<sup>8</sup>

OGA  
EO 1.4.(c)

This USCIB sanction was undoubtedly interesting, if not unsettling to COMINT producers, but its ramifications, if any, did not appear in the cryptologic archival record for 1948. Perhaps there was no problem at the time; the COMINT agencies were reporting all the technical details anyway.

PL 86-36/50 USC 3605  
EO 1.4.(b)

As in the three previous years, 1948 reports intended for the COMINT customers still contained [redacted]

The customer knew, for example, which reports came [redacted]

That said, the Allied cryptologic agencies produced a great volume of technical reports on the Soviet target in 1948. On the American side, under the JPAG banner, were published several series of essentially technical reports. These were, of course, the JPAG-issued Monthly Status Report, under the CJO's signature, which summarized virtually everything the U.S. processed during the month. Each monthly was an enormous document, always well over 100 legal-size pages, containing the numbers of each agency's personnel (by career field), processing and machine, and highlights, plans, a cryptographic summary, a traffic analysis summary, then detailed information of every specific foreign cryptographic system under study. The Soviet portion itself averaged twenty-five to thirty pages every month.

In addition, JPAG published several thousand "Interim Reports" every year, approximately 1,000 Soviet ones in 100 copies to a distribution of at least 6 and sometimes as many as 14 internal and external elements. Most of these were technical reports for the COMINT community, [redacted]

ASA and CSAW published Soviet-related Interim Reports, not only on Net Analysis Casebooks, but [redacted]

[redacted] Russian Operator's Manuals and periodic changes thereto,<sup>12</sup> listings of "Russian Naval Air Bases, Black Sea Area"<sup>13</sup>; or in the Far Eastern Area,<sup>14</sup> International Russian Callsigns,<sup>15</sup> Soviet "Military Daily" summaries,<sup>16</sup> "Russian Abbreviation File (Part 33) (Supplement #5)" updates,<sup>17</sup> [redacted]

[redacted] and so on.

Exceptions to these purely technical reports included the sanitized Secret non-codeword level weekly CSAW-produced "OP-20-NT-1 Russian Traffic Information Summary, period 2 through 8 February 1948"<sup>21</sup> which read, not surprisingly, like a weekly intelligence summary of Soviet naval and naval air activity, and included the commanders in chief, Pacific and Atlantic Fleets, on the distribution page. ASA's special report "Abnormal Water Levels of the Danube River System"<sup>22</sup> included the Special Research Branch of MID on distribution. Clearly, these were in effect product reports lumped in what was generally a technical reporting series.

As in 1946 and 1947, ASA and CSAW continued to publish [redacted] product reports in the RU Series 5x8 inch cards, and traffic analytically derived COMINT in the V-TAF Series reports. What was new in U.S. product reporting in 1948 was the plain-language reporting (see below).

As had been done since 1945, U.S. cryptologic agencies continued to include [redacted]

[redacted] when a single organization for the centralized evaluation and follow-on dissemination on COMINT was proposed; it was the Consolidated Information Dissemination Office or CONSIDO, of which details of its organization and operation are beyond the scope of this article.<sup>23</sup>

**U.S. PLAIN-LANGUAGE REPORTING**

In January 1948 USCIB established a RU-PLAI reporting series, for "Russian Plain Language Analysis Items," which would be made up of

individual identifications or organizations involved in economic activities, their titles, locations, subordination, personalities, and activities, derived from the analysis of plain text messages intercepted on various commercial radio circuits of the USSR. The date given at the right is the last appearance of the identification in messages. These items will serve to provide additional information on a current basis to supplement studies of the more important ministries and directorates of the USSR.<sup>24</sup>

Apparently, ASA produced these plain language reports in a joint effort with the U.S. Army's Military Intelligence Division (MID), as each report was annotated "Prep by ASA, ID." The first substantive report, produced on 5x8 inch cards, looked like this:<sup>25</sup>



Example of Russian Plain Language Analysis Item

Between 9 January 1948 and the end of the year, ASA published 734 reports. Despite activities in Soviet atomic energy being the number one COMINT requirement, a review of all 734 RUPLAI reports revealed no clearly identified items related to that requirement. What the RUPLAI reports did, however, was bring home to the intelligence community the enormous scope and breadth of centralization of the Soviet planned economy. These reports contained detailed information on several Academies of Science (USSR, RSFSR, Ukraine, Georgia) and no fewer than twenty-four USSR ministries: Armaments, Automobile and Tractor Industry, Aviation Industry, Chemical Industry, Coal Industry for Western Areas and Eastern Areas, Communications Industry, Electrical Industry, Electric Power Stations, Ferrous Metallurgy, Fish Industry, Health (USSR, RSFSR, and several SSRs), Heavy Machine Building, Internal Affairs (MVD), Light Industry, Medical Industry, Metallurgical Industry, Nonferrous Metallurgy, Oil Industry of Southern and Western Areas, Procurement, Railroad Transportation, River Fleet, Rubber Industry, Shipbuilding Industry, Trade, and Transport Machine Building.

It is important to remember that *each* of these ministries sat at the top of an organizational pyramid which included every conceivable type of directorate, department, institute, trust, combine, bureau, plant or factory, depot, station and oil field. In fact, for the Ministry of Aviation Industry alone, in 1948 RUPLAI reports discussed the activities of twenty-four numbered, subordinate production plants (including some major plants that are still open today building Russia's latest fighters, bombers, helicopters and airliners), flight test institutes, and another half-dozen aircraft parts supply, communications and weapons factories subordinate to other ministries.

Some of the Soviet [redacted] reports hearken back to the dark days of one of its subordinates, the [redacted] being informed by the [redacted] that following the abolition of rationing, [redacted] personnel would be supplied with food "against cash payment, without any ration cards" required.<sup>28</sup>

## CUSTOMER USE OF SOVIET COMINT

Customers of course combined COMINT with other intelligence sources and produced daily and weekly reports. The Department of State published a daily "Diplomatic Summary," which probably contained little Soviet information, [redacted]. [redacted] The Army published "Military Digest," likely containing much Soviet COMINT, and the Navy published a report strictly addressing the Soviet target called the "Soviet Intelligence Summary," which was probably based on Op-20-NT's weekly summaries. Of course, all agencies published special reports as well.

PL 86-36/50 USC 3605

EO 1.4.(c)

EO 1.4.(b)

**ADDITIONAL COMINT SUPPORT TO CUSTOMERS**

In March 1948, Captain Joseph N. Wenger, chief, Op-20-2 at CSAW, submitted to Rear Admiral Earl E. Stone, who was the chief, Op-20, Naval Communications, for his signature a memorandum for the "Chief of Naval Intelligence." Wenger reported that a survey had been made and the following information had been developed: "Soviet submarines use conventional hand Morse and standard Soviet Naval procedure . . ."

Apparently following up in August, trying to acquire more coverage on Soviet submarines, CSAW's technical branch (Op-20-T) informed Wenger's Op-20-2 what it knew about Soviet submarine communications, particularly in the Atlantic Ocean. It was necessary, for example,

Also, exclusive submarine circuits were believed to be found on specific HF frequencies (e.g., ) but these were all noted only when close to their bases.

Soviet submarines had never been detected on distant patrols, and

Op-20-T suggested that Navy direction finding sites begin copy of suspected frequencies, but more as training than actual monitoring. Op-20-T conservatively recommended that a large effort be deferred until there was actual evidence of Soviet submarines in the Atlantic.<sup>28</sup>

**A CAUTIONARY TALE OF THE "ABSURD ESTIMATE"**

EO 1.4.(c)  
PL 86-36/50 USC 3605

Jacob Gurin, Russian linguist and analyst from 1946-1952, who started the ASA Plain Language Exploitation Group and later rose to senior ranks as an Agency leader in the fields of language training and speech research generally, said once that all Soviet COMINT was highly valued by the intelligence community in the late 1940s, because on the Soviet target especially, "Everything was a secret."<sup>29</sup>

But as always, for the secrets to be of value, they had to get to the appropriate user. One particular incident in 1947 shows how one customer, the U.S. State Department, may have risked serious consequences by restricting the internal distribution of COMINT on the Soviet target.

In January, the State Department began a diplomatic initiative to bring about the restoration to Chinese Nationalist control of Port Arthur and Dairen (now called Lushun and Luda, both located in what is now northeast China on Korea Bay), which had been in Soviet military hands since the end of World War II. The Soviets, while giving lip service to the turnover, in fact supported Chinese Communist forces battling the Nationalist government, and therefore resisted the American effort, stalling the transfer.

On 23 March a Mr. Young, who was chief of the Far Eastern Section of the State Department's "SPS" (probably Special Projects Section, also probably the specific recipient of COMINT for the State Department) briefed a Mr. Penfield, who was the deputy director of the Office of Far Eastern Affairs at State. It seems that Chinese Nationalist forces were planning to conduct military operations in the Port Arthur area during the period 10-15

April, intending to "defeat Chinese Communist forces there before taking over the administration of Port Arthur and Dairen from Soviet authorities." The Soviet government voiced opposition to any fighting between the two Chinese forces in that area, and when Young informed Penfield that unspecified "secret" information showed that there were eight or nine Red Army divisions in the Port Arthur area to back up Soviet wishes, Penfield "considered this estimate absurd." Young thereupon complained to his own boss, Mr. T. Achilles Polyzoides, deputy director, SPS, that although Penfield was seriously underestimating the strength of Soviet forces capable of backing the Soviet position, he (Young) was unable because of security restrictions to use the "special CREAM" (i.e. [redacted]) to persuade Penfield of the true size of the Soviet presence.<sup>30</sup>

What action Polyzoides took is unknown. Presumably, it was the State Department's security policy not to share the [redacted] COMINT with Penfield. But this peek into one consequence of a customer's practice of maintaining security of COMINT, suggests that this particular kind of problem, i.e., occasionally prohibiting access of sensitive information to someone who apparently needs it, was with us back in 1947 and undoubtedly will continue to crop up from time to time.

EO 1.4.(c)  
PL 86-36/50 USC 3605

## Notes

**Chapter 37: Early Reporting on Soviet Target**

1. (U) NSA/CSS Archives, Microfilm Reel #3248.
2. (U) NSA/CSS Archives, Microfilm Reel #2157.
3. (U) Interviews with Oliver Kirby, 11 June 1993, and Cecil Phillips, 14 June 1993.
4. Ibid.
5. (U) NSA/CSS Archives, Microfilm Reel #2155-2157.
6. (U) As stated in text; NSA/CSS Archives, Accession No. 1665N, location G14-0207-7.
7. Ibid.
8. (U) ASA (WDGSS-93) memorandum from Rowlett to BOURBON Liaison Officer, subject: Proposed Message for Major Seaman, 26 November 1945 (TS), and subsequent NEGAT message to COMNAVEU (from Dennis for Seaman), 26 November 1945 (TS); NSA/CSS Archives, Accession No. 1664N, location G14-0207-7.
9. (U) AFSA 251 Pre-Merger Bulletin Series Histories & Microfilm Log Book (TSC), circa 1952; CCH General Cryptologic Series.
10. (SC) [redacted] subject: *Messages Dealing with Red Army M/T Activity (3 Brigade)*, 10 December 1945 (TSC), [redacted] subject: *Messages Dealing with Red Army M/T Activity (4 Brigade)*, 4 December 1945 (TSC), and [redacted] *Messages Dealing with Red Army M/T Activity (43 and 18 Regiments)*, 10 December 1945 (TSC); NSA/CSS Archives, Accession No. 1665N, location G14-0207-7.
11. (SC) [redacted] *Messages Dealing with Red Army M/T Activity (43 and 18 Regiments)*, 10 December 1945 (TSC); NSA/CSS Archives, Accession No. 1665N, location G14-0207-7.

EO 1.4.(c)  
PL 86-36/50 USC 3605

**Chapter 38: GCHQ Leading the Way, Formally Speaking**

1. (C) [redacted] . . . , various titles, dated between 7 and 20 December 1946 (TSC); NSA/CSS Archives, Accession Nos. 1664N and 1665N, location G14-0207-7.
2. Ibid.
3. Ibid.
4. (C) GCHQ paper, titled: Re-naming of L.S.I.C. [redacted] Publications, circa 30 June 1947 (TSC); NSA/CSS Archives, Accession No. 4390, location G15-0501-6.
5. (C) [redacted] . . . , various titles, dated between 7 and 20 December 1946 (TSC); NSA/CSS Archives, Accession Nos. 1664N and 1665N, location G14-0207-7.
6. (SC) GC&CS [redacted] title: *Messages Referring to Russian Factories*, publication date 18 March 1946 (TSC); NSA/CSS Archives, Accession No. 1664N, location G14-0207-7.
7. (C) [redacted] . . . , various titles, dated between 7 and 28 January 1946 (TSC); NSA/CSS Archives, Accession Nos. 1664N and 1665N, location G14-0207-7.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

8. ~~(S)~~ GC&CS [redacted] title: Further Messages Concerning Red Army Harvesting Operations, 2 February 1946 ~~(TSC)~~; NSA/CSS Archives, Accession No. 1665N, location G14-0207-7.
9. ~~(S)~~ GC&CS [redacted] subject: Messages Referring to the NKVD Air Force, 28 February 1946 ~~(TSC)~~; NSA/CSS Archives, Accession No. 1664N, location G14-0207-7.
10. LSIC Monthly Status Report, May 1947.
11. Ibid.
12. Senior USLO, LSIC Newsletter No.13-46, 25 August 1946; No. 14-46, 2 September 1946; and No. 27-46, 18 December 1946. Also, (U) Supplement to No. 27-46, 30 January 1947 ~~(TS)~~; NSA/CSS Archives, Accession No. 759, location G16-0407-3.
13. ~~(S)~~ Eighty traffic analysis reports were listed in the 12 LSIC monthly status reports for 1947.
14. ~~(S)~~ GCHQ paper, titled: Re-naming of L.S.I.C. [redacted] Publications, circa 30 June 1947 ~~(TSC)~~; NSA/CSS Archives, Accession No. 4390, location G15-0501-6.
15. LSIC Monthly Status Report, December 1947.
16. LSIC/GCHQ Monthly Status Reports, January–December 1948.
17. Ibid.

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

### Chapter 39: American Card Files and Other Media

1. (U) Microfilm record of ASA V-Series; NSA/CSS Archives, Reel Nrs. 3248-3249.
2. (U) Microfilm records of G10-Z and NY-1 serialized cards; NSA/CSS Archives, Reel Nrs. 2155-2158.
3. Howe, JOP study, 70. Also Rowlett Review.
4. JPAG Monthly Status Reports, January–December 1947.
5. Ibid.
6. [redacted]
7. Howe, JOP study, 168–169.
8. Ibid, 169.
9. ~~(S)~~ JPAG Interim Report, JPAG #4195, Section RU #1526, Net Analysis Casebook #59, Taper Air/Ground European Links, 24 August 1948 ~~(SC)~~; NSA/CSS Archives, Accession No. 46470, location H07-0109-3.
10. (U) JPAG Interim Report #3104, Section RU #942, subject: [redacted] 23 January 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 46470, location H07-0109-6.
11. (U) JPAG Interim Report #3177, Section RU #982, subject: BRUSA Nomenclature, 9 February 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 46470, location H07-0109-7.
12. ~~(S)~~ JPAG Interim Report #3080, Section RU #928, subject: Op-20-NT-1 Russian Operators' Manual (Change #2), 19 January 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 46470, location H07-0109-6.
13. ~~(S)~~ JPAG Interim Report #3069, Section RU #923, subject: Russian Naval Air Bases, Black Sea Area, 15 January 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 46470, location H07-0109-6.
14. ~~(S)~~ JPAG Interim Report #3241, Section RU #1016, subject: Russian Naval Air Bases, Far Eastern Area, 26 February 1948 ~~(TSC)~~; NSA/CSS Archives, Accession No. 46470, location H07-0109-7.

EO 1.4.(c)  
PL 86-36/50 USC 3605

CT  
EO 1.4.(c)  
OGA

15. (U) JPAG Interim Report #3180, Section RU #985, subject: Op-20-NT-1 Additions and Corrections to International Russian Callsigns, 9 February 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-7.

16. (U) JPAG Interim Report #4259, Section RU #1576, subject: [redacted] #377 Military Daily, 1 September 1948 (~~SC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-5

EO 1.4.(c)  
PL 86-36/50 USC 3605

17. (U) JPAG Interim Report #3225, Section RU #1010, subject: Russian Abbreviation File (Part 33) (Supplement #5), 24 February 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-7.

18. (~~S~~) JPAG Interim Report #3219, Section RU #1006, [redacted] (IBM Methods ASA), 11 February 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-7.

19. (~~C~~) JPAG Interim Report #3243, Section RU #1017, subject: Op-20-NT-1 [redacted] 27 February 1948 (~~SC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-7.

20. (~~C~~) JPAG Interim Report #3349, Section RU #1073, subject: [redacted] 18 March 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-7.

21. (~~S~~) JPAG Interim Report #3420, Section RU #1106, subject: Op-20-NT-1 Russian Traffic Information Summary, period 2 through 8 February 1948 (~~S~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-7.

22. (~~C~~) JPAG Interim Report #3371, Section RU #1090, subject: Abnormal Water Levels of the Danube River System, 23 March 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 46470, location H07-0109-7.

23. Howe, JOP study, 170-171.

24. (~~S~~) RU-PLAI #1, Russian Plain Language Analysis Items, 9 January 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 9268, location G16-0211-4.

25. (~~S~~) RU-PLAI #2, [redacted] USSR, 13 January 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 9268, location G16-0211-4. Presumably CSAW could and did publish RU-PLAI reports, but none could be found in available records.

26. (U) RUPLAI #616 [redacted] USSR #41, 22 November 1948 (~~TSC~~); NSA/CSS Archives, Accession No. 9268, location G16-0211-4.

27. (~~C~~) Op-20-2 Memorandum for the Chief of Naval Intelligence, originated by CAPT Wenger, signed by RADM Stone, subject: Status of our present ability to provide operational information on Soviet Submarines, 22 March 1948 (~~TSC~~); CCH Collection, Series V.B.2.7.

28. (~~C~~) Op-20-T Memorandum for Op-20-2, Subject: Russian Submarines in Atlantic, 16 August 1948 (~~TSC~~); CCH Collection, Series V.R.1.7.

29. (U) Jacob Gurin presentation, Cryptologic History Symposium, 14 November 1991. Audiotape available in CCH General Collection.

30. (~~SC~~) State Department Memorandum from Mr. Young to Mr. Polyzoides, subject: Effect of Limitations on the Use of All Available Cream Material regarding the Port Arthur Naval Base Area, 3 April 1947 (~~TSC~~); NSA/CSS Archives, Accession No. 9670, box CBDB38.

## Part Eight

### Afterword

#### Chapter 40

#### One for the Road

EO 1.4.(c)  
PL 86-36/50 USC 3605

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

As 1945 ended, the two allied nations had almost 400 analysts working the Soviet problem. This was already a lot of people, but the number would quadruple in the next three years. Soviet-dedicated intercept positions, numbering no more than about thirty-seven in early 1946, would grow to almost 600 by the end of 1948. The number of [redacted] pegged at seventy-eight in March 1946, would increase to more than 150 by 1948, even though early, [redacted] were being replaced by more [redacted] initially and crudely distinguished as either [redacted] would soon be precisely [redacted] [redacted] by 1948.

Early in 1946, [redacted] [redacted] which would be but the first of several to be exploited heavily for the next few years, made increasingly possible by the application of specialized "IBM machines," as they were usually called.

[redacted]

Russian linguists and traffic analysts would provide greater relative contributions as

[redacted]

By 1948, however, the Allied cryptologic agencies had developed a solid database on the Soviet Union. The entire Soviet military order of battle and much of the country's industrial structure had been reconstructed by Allied intelligence and was being further refined by extensive, serialized COMINT reporting, formal and otherwise. Military and civilian policymakers now had a wealth of hard data on the previously little-known strength of an adversary. Furthermore, COMINT would soon provide Allied defense officials with a continuous flow of information on Soviet [redacted]

[redacted]

BOURBON would be successful not in the same sense or to the same degree as the cryptologic triumphs in World War II, which directly helped achieve the victories over Germany and Japan (although it could be argued that the forty-five years of Allied SIGINT effort against the Soviet Union contributed in an important way to the successful

containment of communism). Rather, BOURBON would be successful in a lesser, still significant sense. Each partner would benefit from the other's efforts. The goal to [redacted] [redacted] gather previously unavailable intelligence on Soviet military and economic capabilities and intentions would be achieved to an important extent. Finally, the arrangements and procedures worked out for BOURBON would show the way for successful follow-on collaborations.

PL 86-36/50 USC 3605  
EO 1.4.(c)  
EO 1.4.(b)

While it may have seemed premature in 1945, the decision by Allied cryptologic officials to target the Soviet Union *numero uno* clearly had to be seen as a sound selection by the end of 1948. Nowhere could be found someone in authority to write: "We are going to target the Soviet Union because. . ." Rather, the fact of targeting the USSR seemed a foregone conclusion. All available historical correspondence, and there is much of it, both U.S. internal and exchanges between Great Britain and America, addressed in enormous detail not *whether* but essentially *how best* to exploit the communications of the Soviet Union. At least from hindsight, the decision seems visionary. Despite the fact that knowledgeable officials understood that in World War II the partnership with the Soviet Union was limited to an "anti-Hitlerian" alliance, lacking the political, social and cultural bindings that tied together Great Britain and the United States, it seems uncanny that by 1948, Stalinist Russia had emerged as the arch Cold War enemy. Only briefly in 1945, were the USSR [redacted] given equal weight on the COMINT requirements list; the Soviet Union quickly became the greater [redacted] gaining resources in abundance while the others sacrificed.

EO 1.4.(c)  
PL 86-36/50 USC 3605

[redacted] the maturation of Soviet traffic analysis, the substantially enlarged Russian linguist work force, the expanded collection and processing capabilities all put Allied cryptologists on a sound footing for the future. And a bit more scary it was. The first Soviet atomic bomb was exploded in 1949. The capitalized expression "Cold War" became for the first year in history an entry in the *Facts on File* index. The term "Soviet bloc" became common. In partial response, the Western Allies formed the North Atlantic Treaty Organization (NATO).

And, of course, as is well known, the Soviet target came to dominate, until the 1990s, the Agency's budget in terms of personnel, collection systems (driving requirements for all overhead assets), processing and reporting systems. Although the establishment of the National SIGINT Operations Center (NSOC) was given final impetus by the North Korean shutdown of the U.S. Navy EC-121, Group A was always the major player in real-time SIGINT support, at least until the fall of the Berlin Wall. A8's Current SIGINT Operations Center (CSOC) of the 1960s served as the model for NSOC.

A reader might ask if in fact the BOURBON project had been such a success in the 1940s, what was wrong with having two American COMINT agencies "coordinating" their separate processing tasks? Thomas Burns's *Origins of the National Security Agency, 1940-1952*, answers that question in detail. From a Soviet target perspective, Project BOURBON was successful *in spite* of the ASA-CSAW arrangement, not *because* of it. As early as 1948, as the Stone Board report shows, U.S. intelligence officials knew the existing arrangement

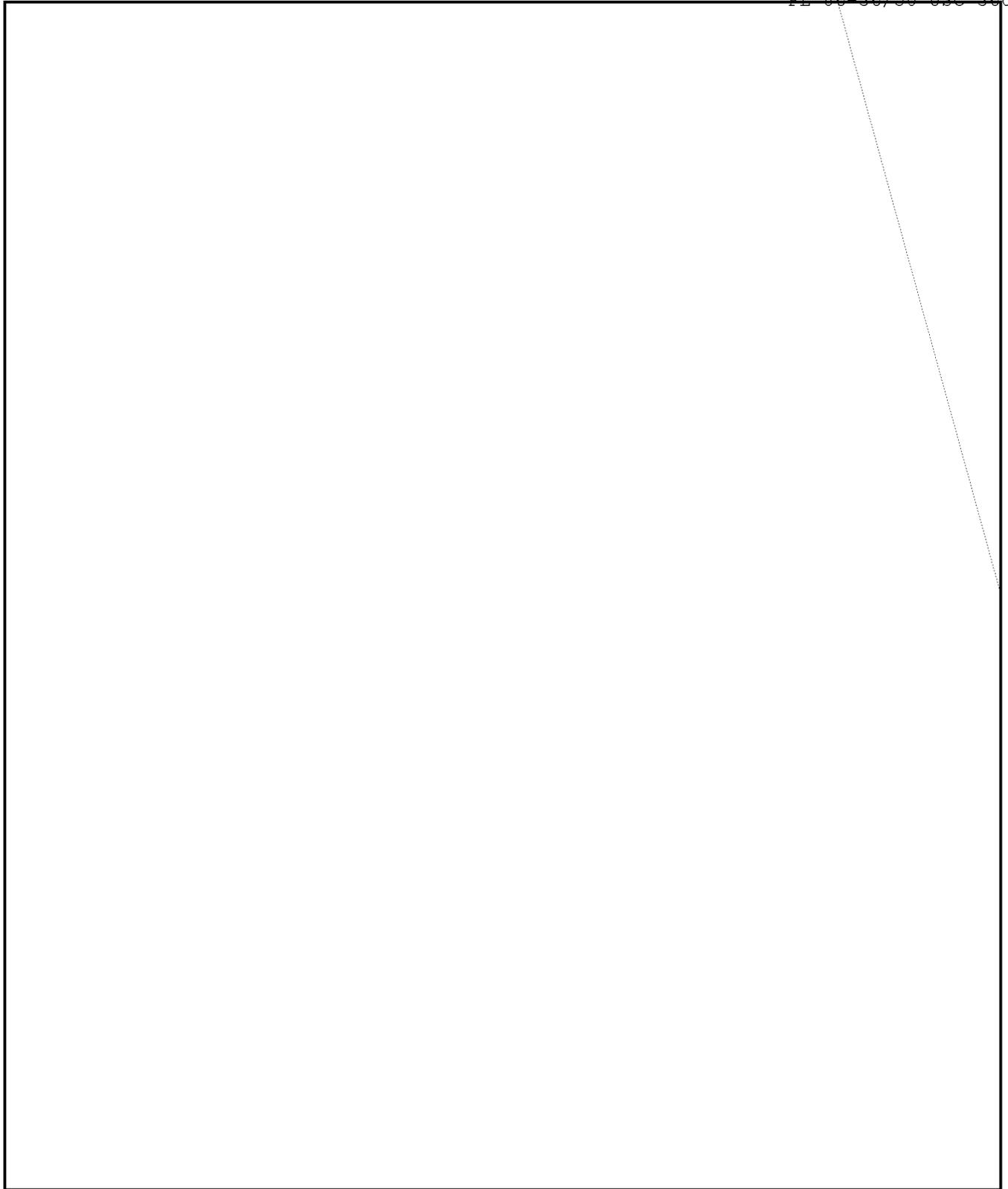
was not working well. The battle was, again, mostly over *how* to improve it, *how* to centralize processing, not *whether* it should be done. The creation of the Armed Forces Security Agency (AFSA) in 1949 was merely the first attempt. SIGINT processing problems surfaced by, among other things, the Korean War, brought about the establishment of the National Security Agency in 1952.

But one agency or two, the Soviet problem dominated the SIGINT business in America like no other for over forty years. Project BOURBON got us off to a good start, and the subsequent wide-ranging effort against the Soviet Union had even a better ending, topped off by the demise of the Soviet Union and the fall of the Berlin Wall. Like the successful efforts of World War II cryptologists against Germany and Japan leaving a legacy of professionalism for Cold War analysts, it is hoped that the enormous inheritance of Cold War cryptologic skills, innovative collection and processing techniques and technology, tradition, and dedication will be handed down in good shape to the Allied SIGINTers of the post-Cold War world.



**Appendix A**

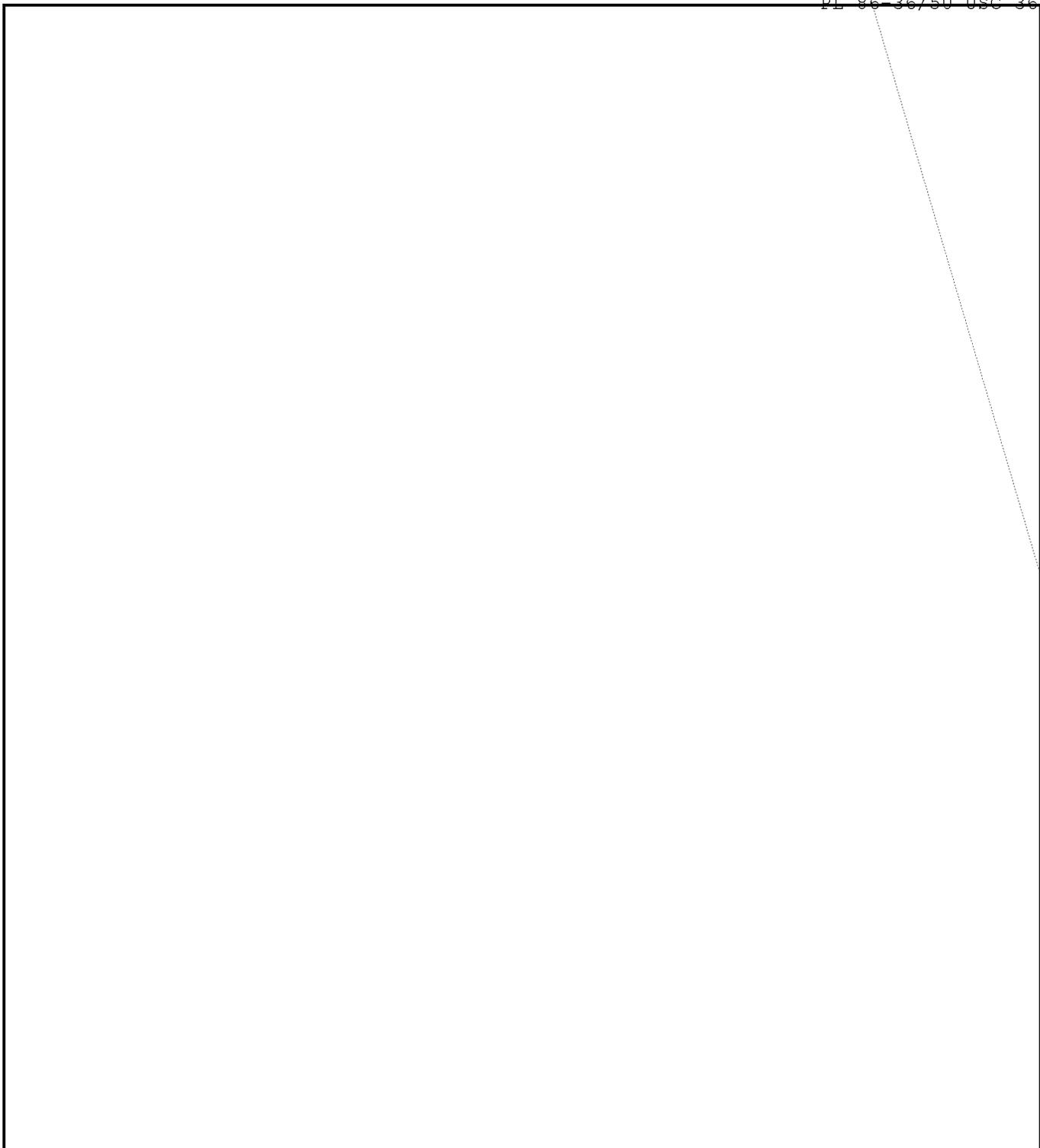
EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605





**Appendix B**

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605





Appendix C

ASA Russian Plain-Language  
Unit Strength & Output

Month/Year	Strength	Number of Messages					
		Scanned	Extracted	Processed	Reports	Xlations Supplements	
(Dec 1947 goal:		80-120K		5-7.5K		360)*	PL 86-36/50 USC 3605 EO 1.4.(c)
Nov 1947-							
Feb 1948**		235,000	15,248	3,752	3	-	55
(per month)		(67,000)	(4,357)	(1,072)	(1)	-	(16)
Mar-Apr 48		338,146	83,401	12,291	3	35	95
(per month)		(169,073)	(41,700)	(6,146)	(1.5)	(18)	(48)
May 1948		225,718	61,527	2,672	1	38	50
Jun 1948		223,307	56,039	2,895	2	-	-
Jul 1948		159,344	15,480	2,973	2	31	41
Aug 1948		163,563	25,344	4,857	6	32	22
Sep 1948		197,967	35,807	4,706	9	30	112
Oct 1948		276,790	43,893	6,083	-	-	-
Nov 1948	153,623	20,193	4,976	2	131	115	
Dec 1948	221,241	25,438	6,878	-	139	70	

\* JPAG Memorandum to Coordinator for Joint Operations, subject: Allocation of Processing Tasks: Russian Plain Text, 17 December 1947 (TSC); NSA/CSS Archives, Accession No. 21518, box CBJQ74.

\*\* JPAG Monthly Status Reports, November 1947-December 1948 (TSC); NSA/CSS Archives, Accession No. 42466, locations H10-0106-3 and H10-0106-4.

\*\*\* AFSA Strength figures for the Plain Language Unit rose from 167 in June 1950, to 183 in January 1951, to 269 in January 1952, and to 421 by January 1953 (per XXV-13, Part IV, of Dr. Howe's *The Narrative History of AFSA/NSA*). However, the value of plaintext traffic reportedly declined "abruptly" in November 1951, with its disappearance from radio, presumably a consequence of the traffic being transferred to landline. CCH General Collection.



## Appendix D

**Herbert Conley's Memorandum, Subject:  
Conduct of Russian Air Force and Army Problem\***

In December 1948, Mr. Herbert Conley, who had been a SUSLO London staff officer in 1947, possibly into 1948, and was currently an ASA supervisor involved in analysis and reporting on the Soviet target by late 1948, issued an extensive memorandum which not only presented intelligence highlights of the BOURBON problem in 1948, but summarized ASA's exploitation of the Soviet Red Army and Air Forces targets since September 1945. Here it is, essentially in its entirety:

1. At your verbal request, the following objective summary of the conduct of the Russian Air Force and Russian Army problems at Army Security Agency has been prepared. This summary has been coordinated with Mr. Kirby, of AS-97, and Mr. O'Gara of SRB, ID. Figures presented have been taken from JICG or JPAG reports.

2. A broad program of intercept and processing of Russian traffic was introduced at the Army Security Agency in September 1945. From that date to the present time the Army Security Agency has conducted the intercept and analysis of Russian Military and Russian Military Air traffic as one large interrelated and integrated problem. Emphasis on various portions or phases of this problem has been adjusted from time to time in order to obtain most effectively the greatest overall intelligence product from the facilities and personnel available. Emphasis has not, therefore, been determined by whether certain traffic was Military or Military Air, but whether the exploitation of this traffic would yield a large amount of intelligence or significant intelligence items.

3. In undertaking the Russian Military and Military Air problem, the Army Security Agency initially placed its greatest effort on the intercept and processing of Far Eastern traffic. This approach was adopted because the British effort was confined almost exclusively to European material and also because ASA intercept facilities were concentrated in the Pacific. After significant progress had been made in the processing of the traffic from Far East sources, work was intensified on high level material from all areas in Russia. Intercept and processing of this material consumed a large amount of the available facilities and personnel, but the effort was considered justified because [redacted] revealed plans, unit identifications, troop dispositions, air strength and training activities in all parts of the USSR.

[redacted] and the intercept and analysis of material passed on Far East circuits was continued. By mid-1948 the basic organization of the

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

\*H.L. Conley memorandum to Chief, CSGAS-90, Subject: Conduct of Russian Air Force and Army Problem; 14 December 1948 (TSC); NSA/CSS Archives, Accession No. 5505, box CBNI22.

Russian Military and Military Air Command had been determined and practically all major headquarters had been identified. In the Far East, unit identifications and dispositions were almost complete down to air regiment and army division levels, and in Europe a large number of lower level units had been identified and their strength had been computed. Continued attempts to build up intercept strength in Europe had made it possible by the summer of 1948 to begin intercept of Russian operational or low-level Military and Military Air circuits in this area. The intercept and analysis of such links has been increased during the past few months, with emphasis being accelerated as the Russians have reduced transmission of high level traffic. Operational air links employing radio-telephone transmissions have not been intercepted regularly, but cover of Morse links is extensive.

4. At the present date, Army Security Agency, Washington, is receiving daily by teletype all air defense and operational air traffic intercepted at U.S. Stations in Germany and at British stations in the U.K. Information on flights of Russian planes in Europe is available in Washington within a few hours after the flight has been scheduled. Material from [redacted] messages is integrated both at ASA Europe and at ASA Washington so that composite information on aircraft movement is available to intelligence consumers within a minimum of time. ASA Europe is presently issuing to USAFE, through SSO channels, current information on plane concentrations and plane movements in Europe.

5. Below is listed a comparison of current intercept, traffic analysis, and cryptanalytic effort being expended by ASA and CSAW on Military, Military Air and Naval problems:

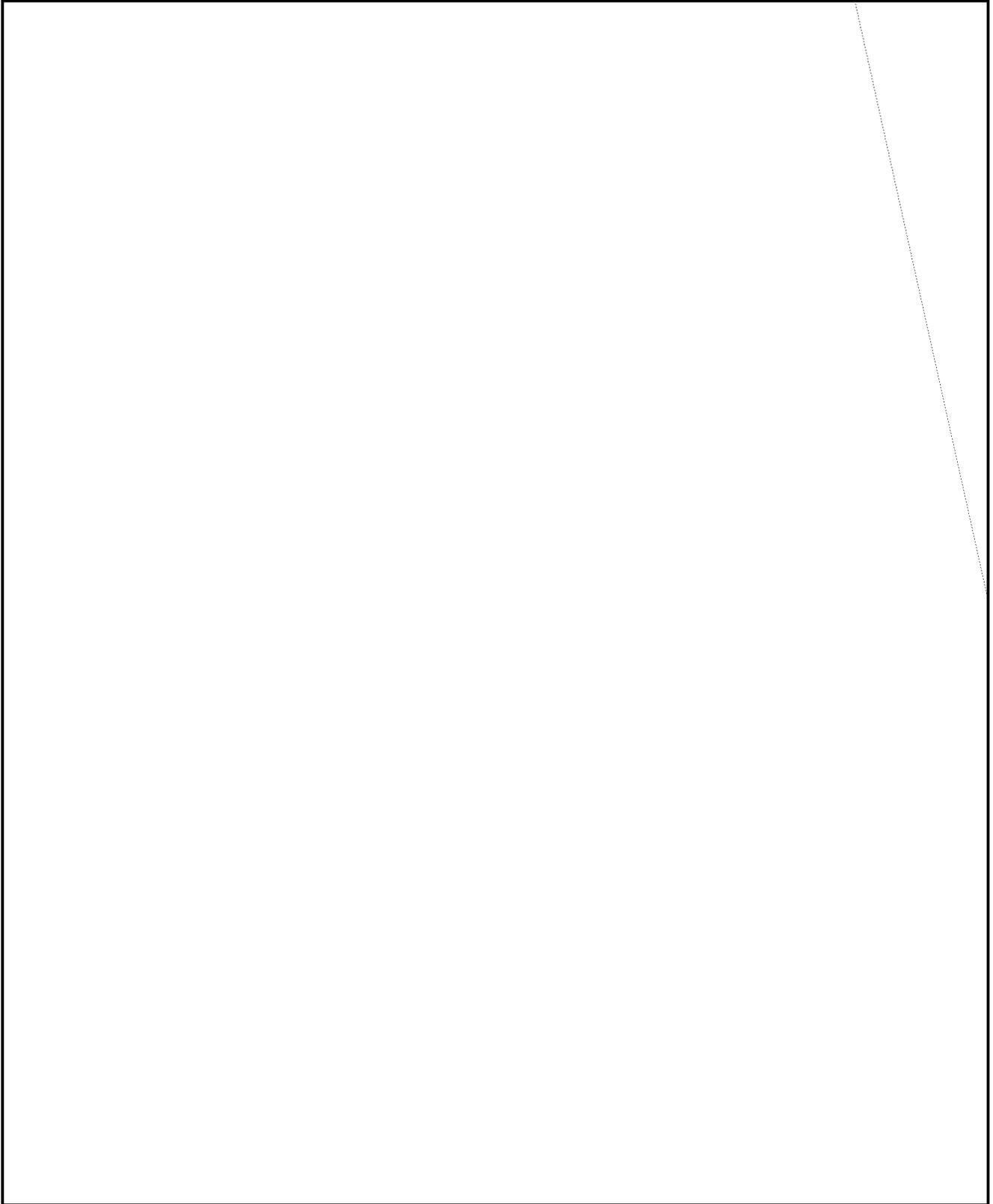
- a. Intercept Effort (Figures from JICG Report 15-30 November 1948): Operators Assigned to Military Air: [redacted] Military: [redacted] Naval & Naval Air: [redacted]
- b. T/A Effort (figures from U.S. Monthly Status Report, November 1948: Number of personnel engaged in analysis of networks - Military Air: [redacted] Military: [redacted] Naval & Naval Air: [redacted]

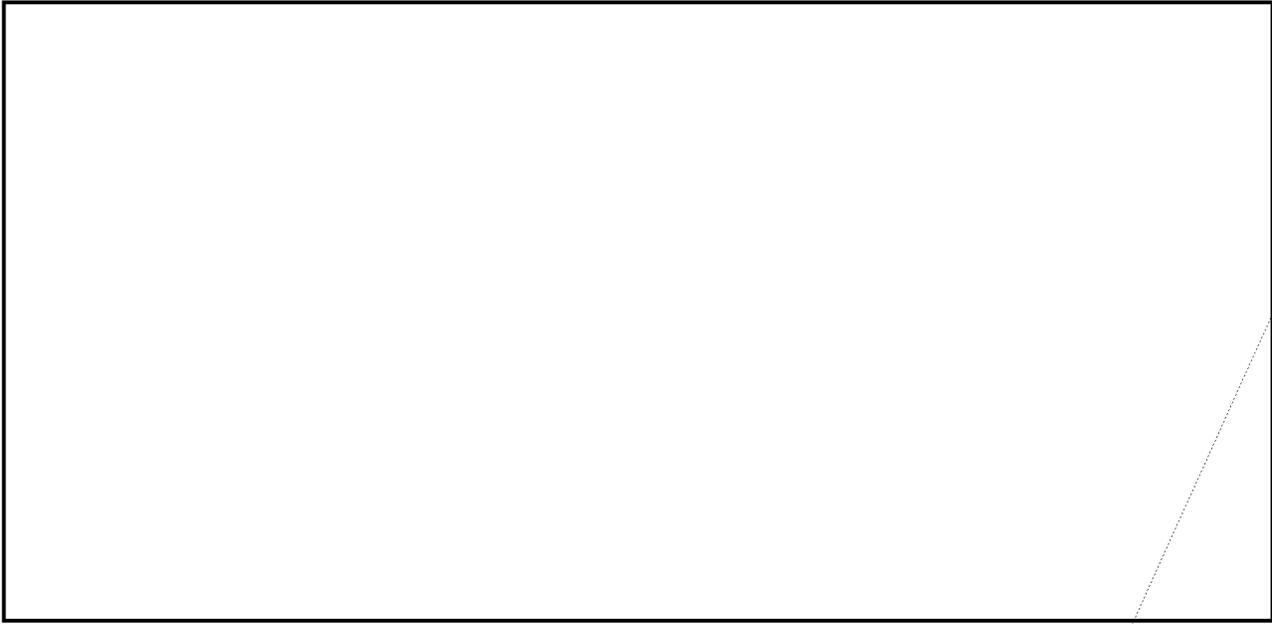
Crypt Effort (figures from U.S. Monthly Status Report, November 1948;

	Military Air	Military	Naval & Naval Air
Personnel	[redacted]		
[redacted]			
Intercepts [thereof]			
Translations:			
Gists:			
Intercepts [thereof]:			

EO 1.4.(c)  
PL 86-36/50 USC 3605  
EO 1.4.(b)

**Appendix E**





EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

# Bibliography

## Primary Sources

### SIGINT Product

- ASA, ID RU-PLAI #1, Russian Plain Language Analysis Items, 9 January 1948 (TSC)
- ASA, ID RU-PLAI #2, Ministry of Nonferrous Metallurgy USSR, 13 January 1948 (TSC)
- ASA, ID RUPLAI #154, [redacted] USSR #14 Title: Flight Unit (LETNAYa ChAST'); [redacted] 30 April 1948 (TSC)
- ASA, ID RUPLAI #616, [redacted] USSR #41, 22 November 1948 (TSC)
- ASA, ID RU-TAF-MIL-I #287, 96th Rifle Division, Kazan', Volga MD, 30 December 1948 (TSC)
- GC&CS [redacted] Messages Dealing with Red Army M/T Activity (4 Brigade), 4 December 1945 (TSC)
- GC&CS [redacted] Messages Dealing with Red Army M/T Activity (3 Brigade), 10 December 1945 (TSC)
- GC&CS [redacted] Messages Dealing with Red Army M/T Activity (43 and 18 Regiments), 10 December 1945 (TSC)
- GC&CS [redacted] Further Messages Concerning Red Army Harvesting Operations, 2 February 1946 (TSC)
- GC&CS [redacted] Messages Referring to the NKVD Air Force, 28 February 1946 (TSC)
- GC&CS [redacted] Messages Referring to Russian Factories, 18 March 1946 (TSC)
- [redacted] title: [Soviet] Telecommunications as of May 1948, 26 July 1948 (TSC)
- Microfilm record of ASA V-Series, 1945-1948 (TSC)
- Microfilm records of G10-Z and NY-1 serialized cards, 1946-1948 (TSC)
- NSA [redacted] Soviet [redacted] Initial and Current Methods of Assignment and Employment, 30 July 1962 (TSC)

EO 1.4.(c)  
PL 86-36/50 USC 3605

### SIGINT Technical Product

- Probable SSA Analysis titled "R-50," 12 April 1945 (TS)
- Probable ASA Report on the [redacted] 20 September 1945 (TSC)
- Rowlett paper, subject: Special Report on BOURBON [redacted] 15 October 1945 (TSC)

Probable Op-20-G Chart I-1, between pages 28 and 29 of U.S. Navy Communication Intelligence Organization, Liaison and Collaboration, 1941-1945 (~~S~~)

Op-20-G Manual, entitled: BOURBON Non-Morse Glossary, 1 January 1946 (~~TS~~)

Op-20-G Working Aid, BOURBON Non-Morse Communications Procedures, 1 February 1946 (~~TS~~)

Op-20 Handbook on BOURBON Non-Morse Communications Procedures, 1 February 1946 (~~TS~~)

IR #8220, Russian Systems, [hand-annotated 1946] (~~TS~~)

BOURBON Interim Report No. 1, 15 February 1946 (~~TS BOURBON~~)

BOURBON Interim Report No. 2, 15 March 1946 (~~TS BOURBON~~)

BOURBON Interim Report No. 3, 15 April 1946 (~~TS BOURBON~~)

BOURBON Interim Report No. 4, 15 May 1946 (~~TS BOURBON~~)

ASA Manual S-700, Cryptanalyst's Manual, Glossary of Terms, September 1946 (~~TS~~)

JPAG Interim Report #138 RU #084, [redacted] 17 September 1946 (~~TS~~)

JPAG Interim Report #300, RU #158, [redacted] 30 October 1946 (~~TS~~)

JPAG Interim Report #326, BOURBON Traffic Analysis Cryptanalytic [Note] #15, 5 November 1946 (~~TS~~)

Chart, source unknown, [Soviet] Baudot Two-Channel Links - Military, 1 February 1947 (~~TS~~)

LSIC Interim Report 31, [redacted] 14 March 1947 (~~TS~~)

JPAG Interim Report #988 RU #371, [redacted] Program at ASA, 22 April 1947 (~~TS~~)

JPAG Interim Report #1213, Report on [redacted] Group at ASA, 12 June 1947 (~~TS~~)

Probable CSAW report: [redacted] *An Exercise Manual for the Training of Personnel*, October 1947 (~~TS~~)

Chart, source unknown, [Soviet] Far Eastern Military Morse Links; undated but circa 1948 (~~TS~~)

JPAG Interim Report #3069, RU #923, Russian Naval Air Bases, Black Sea Area, 15 January 1948 (~~TS~~)

JPAG Interim Report #3080, RU #928, Op-20-NT-1 Russian Operators' Manual (Change #2), 19 January 1948 (~~TS~~)

JPAG Interim Report #3104, RU #942, [redacted] 23 January 1948 (~~TS~~)

EO 1.4.(c)  
PL 86-36/50 USC 3605  
EO 1.4.(b)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

JPAG Interim Report #3420, RU #1106, Op-20-NT-1 Russian Traffic Information Summary, period 2 through 8 February 1948 (~~S~~)

JPAG Interim Report #3177, RU #982, BRUSA Nomenclature, 9 February 1948 (~~TSC~~)

JPAG Interim Report #3180, RU #985, Op-20-NT-1 Additions and Corrections to International Russian Callsigns, 9 February 1948 (~~TSC~~)

JPAG Interim Report #3219, RU #1006 [redacted] (IBM Methods ASA) 11.4.(c)  
February 1948 (~~TSC~~) PL 86-36/50 USC 3605

JPAG Interim Report #3225, RU #1010, Russian Abbreviation File (Part 33) (Supplement #5), 24 February 1948 (~~TSC~~) EO 1.4.(b)

JPAG Interim Report #3241, RU #1016, Russian Naval Air Bases, Far Eastern Area, 26 February 1948 (~~TSC~~)

JPAG Interim Report #3243, RU #1017, Op-20-NT-1 [redacted] 27  
February 1948 (~~SC~~)

JPAG Interim Report #3349, RU #1073, [redacted] 18  
March 1948 (~~TSC~~)

JPAG Interim Report #3371, RU #1090, Abnormal Water Levels of the Danube River System, 23 March 1948 (~~TSC~~)

JPAG Interim Report #3571, RU #1188, Traffic Analysis Diagram #31, 3 May 1948 (~~TSC~~)

JPAG Interim Report #3660, RU #1244, [redacted] 17  
May 1948 (~~TSC~~)

JPAG Interim Report #3743, RU #1275, Traffic Analysis Diagram #32, 4 June 1948 (~~TSC~~)

JPAG Interim Report #4142, RU #1491, Traffic Analysis Diagrams #38-40, 16 August 1948 (~~TSC~~)

JPAG Interim Report #4195, RU #1526, Net Analysis Casebook #59, Taper Air/Ground European Links, 24 August 1948 (~~SC~~)

JPAG Interim Report #4259, RU #1576, Military Daily, 1 September 1948 (~~SC~~)

JPAG Interim Report #6123, RU #2544, [redacted]  
[redacted] 7 October 1949 (~~TSC~~)

GCHQ [redacted] Russian Interim Report Number 304 - [redacted]  
[redacted] Final Write-Up, 11 October 1948 (~~TSC~~)

JPAG Interim Report #4495, RU #1719, Op-20-NT-1 Russian Traffic Analysis Bulletin #27, 13 October 1948 (~~SC~~)

GCHQ [redacted] Russian Interim Report Number 316 - Final Report on [redacted]  
[redacted] 28 October 1948 (~~TSC~~)

NSA ADVA/111 Technical Report, [redacted] July 1958 (~~SC~~)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

NSA A61 CTR #7-68, Soviet Armed Forces Signal Operation Instructions, 14 August 1968  
(TSC)

NSA Basic Cryptologic Glossary, June 1971 (C)

NSA A27 TSR 02-89, Fifty Years of [redacted] 10 January 1989  
(TSC)

NSA A284 Working Aid 02-90, [redacted] Location Sort, 1 May 1990  
(TSC)

### Cryptologic Histories, Articles and Memoirs

AFSA publication: *History of* [redacted] 3 May 1951 (TSC)

Benson, Robert Louis, and Phillips, Cecil James. *History of VENONA*. Ft. Meade, MD: NSA/CSS, 1995 (TSC) EO 1.4.(c)  
MDL 86-36/50 USC 3605  
EO 1.4.(b)

Burns, Thomas L. *The Origins of the National Security Agency, 1940-1952*. Ft. Meade, MD: NSA/CSS, Center for Cryptologic History, 1990 (TSC)

Callimahos, Lambros D., and Friedman, William F. *Military Cryptanalytics, Part II*. Ft. Meade, MD: National Security Agency, 1959 (U)

*Data on Soviet Cryptographic Systems 1917-1933*, Serial TRQ-77, Washington, D.C.: Army Signal Security Agency, 1945 (TSC)

*The Friedman Legacy: A Tribute to William and Elizebeth Friedman*. Ft. Meade, MD: NSA/CSS, Center for Cryptologic History, 1992. (U)

Friedman, William F. *Brief History of U.S. COMINT Activities* (TSC). Memorandum for Mr. Grant Hanson, 20 February 1952 (TSC)

Garofalo, C. "A Brief Quarter Century of Soviet Crypto/Traffic Analysis," 1971; as published in Vera R. Filby, *A Collection of Writings on Traffic Analysis*. Ft. Meade, MD: NSA/CSS, Center for Cryptologic History, 1993 (TSC)

GC&CS History: *Army & Air Force SIGINT, Volume II - The Organisation and Evolution of British Army SIGINT-II* (TSC). Circa 1945 (TSC)

GC&CS History: *Army & Air Force SIGINT, Volume IV - The Organisation and Evolution of British Air Force SIGINT-I* (TSC). Circa 1945 (TSC)

GC&CS Histories: *Naval SIGINT, Volumes I & II - The Organization and Evolution of British Naval SIGINT, Part I - The Making of SIGINT* (TSC). Circa 1945 (TSC)

Howe, Dr. George F., and Watson, Dr. Robert J. *Historical Study of COMINT Under the Joint Operating Plan, 1946-1949*, April 1970 (TSC)

... *The Narrative of AFSA/NSA*, Final Draft, April 1963 (TSC)

Kirby, Oliver R. "The Origins of the Soviet Problem: A Personal View," ~~(TSC)~~, *Cryptologic Quarterly*, Winter 1992 ~~(TSC)~~

EO 1.4.(c)  
PL 86-36/50 USC 3605  
EO 1.4.(b)

Naples, Anthony F. [redacted] (Unpublished manuscript, drafted circa 1974, edited 1978.) ~~(TSC)~~

NCA (U.S. Naval Communications Activity) informal history entitled *Russian Language Section, July 1943-January 1948* ~~(TSC)~~, Undated ~~(TSC)~~

Peterson, Michael L. "Before BOURBON: American and British COMINT Efforts against Russia and the Soviet Union before 1945" ~~(TSC)~~, *Cryptologic Quarterly*, Fall-Winter 1993, 1-20 ~~(TSC)~~

... "Early BOURBON - 1945: The First Year of Allied Collaborative COMINT Effort against the Soviet Union" ~~(TSC)~~, *Cryptologic Quarterly*, Spring 1994, 1-40 ~~(TSC)~~

... "Middle BOURBON - 1946: The Second Year of Allied Collaborative COMINT Effort against the Soviet Union" ~~(TSC)~~, *Cryptologic Quarterly*, Summer 1994, 1-57 ~~(TSC)~~

... "Old BOURBON - 1947: The Third Year of Allied Collaborative COMINT Effort against the Soviet Union" ~~(TSC)~~, *Cryptologic Quarterly*, Fall 1994, 1-57 ~~(TSC)~~

... "Project [redacted] 'Removed from Normal SIGINT Procedure' " ~~(TSC)~~, *Cryptologic Quarterly*, Winter 1994, 1-12 ~~(TSC)~~

... "Beyond BOURBON - 1948: The Fourth Year of Allied Collaborative COMINT Effort against the Soviet Union" ~~(TSC)~~, *Cryptologic Quarterly*, Spring 1995, 1-57 ~~(TSC)~~

Phillips, Burton, and Snook, Suzanne. *A Brief History of Russian* [redacted] Circa 1946 ~~(TSC)~~

Remarks on British [redacted] (1917-1932) Washington, D.C.: Signal Security Agency, 2 May 1945 ~~(S)~~

Rowlett, Frank B. *Recollections of Work on Russian*, 11 February 1965 ~~(TSC)~~

Tiltman, John H. [redacted] ~~(TSC)~~ *NSA Technical Journal*, Fall 1963 ~~(TSC)~~

... "Experiences 1920-1933," ~~(TSC)~~ *NSA Technical Journal*, Summer 1992 ~~(TSC)~~

... "Some Principles of Cryptographic Security," ~~(TSC)~~ *NSA Technical Journal*, Summer 1974 ~~(TSC)~~

Tordella, Louis W. *Collection of Russian Transmissions by the Navy; My Recollections* ~~(TSC)~~, 5 May 1978 ~~(TSC)~~

Wenger, Joseph N. Informal history of BOURBON ~~(TSC)~~, February 1946 ~~(TSC)~~

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

DOCID: 4314365

~~TOP SECRET UMBRA~~**Oral Interviews, Discussions and Briefings**

Mr. Robert (Lou) Benson, 30 October 1992 and other occasions through early 1994 (TSC)

Mr. Jacob Gurin presentation, Cryptologic History Symposium, 14 November 1991 (TSC)

Mr. Oliver Kirby, 11 June 1993 (TSC)

[redacted] 6 April 1994 (TSC)

Mr. Cecil Phillips, 31 December 1992, 11 August, 14 June, and 2 December 1993, 12 January, and 16 March 1994 (TSC)

Dr. Louis Tordella, 28 February 1994 (TSC)

**Memoranda****Army-Navy Communication Intelligence Board (ANCIB)**EO 1.4.(c)  
PL 86-36/50 USC 3605

ANCIB memorandum from Admiral Hewlett Thebaud, Chairman, for General Bissell, Admiral Redman and General Corderman, subject: British Reply to U.S. Proposals regarding RATTAN (BOURBON), 15 August 1945 (TS)

ANCIB memorandum for General Marshall and Admiral King; subject: Signal Intelligence, 22 August 1945 (TS)

**Army-Navy Communication Intelligence Coordinating Committee (ANCICC)**

ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 15 August 1945 (TS)

ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Project Report, 31 August 1945 (S)

ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Project Report, 14 September 1945 (TS)

ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 2 October 1945 (TS)

ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 14 October 1945 (TS)

ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 7 November 1945 (TS)

ANCICC Liaison Officers, Special Project (BOURBON) memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 16 November 1945 (TS)

ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 1 December 1945 (TS)

~~TOP SECRET UMBRA~~

ANCICC Liaison Officers' memorandum for ANCICC, subject: Semi-Monthly Report on BOURBON, 16 December 1945 ~~(TS)~~

Secretariat, ANCICC memorandum to Colonel Rowlett, ASA, subject: Exchange of BOURBON Translations, 19 December 1945 ~~(TS)~~

**Army Security Agency (ASA and its predecessor, SSA)**

SSA (SPSIB-3) memorandum from Lt. Col. Rowlett for Colonel Hayes, subject: Comments on Navy proposal for RATTAN, 18 June 1945 ~~(TS)~~

SSA (SPSIS-1) memorandum from Robert T. Walker, Major, Signal Corps, Executive Officer, to Chief, Military Intelligence Division, subject: RATTAN Liaison, 26 July 1945 ~~(TSC)~~

SSA (Rowlett) memorandum for [redacted] 6 September 1945 ~~(TSC)~~

PL 86-36/50 USC 3605

SSA (SPSIS-9) memorandum from W. Preston Corderman, Brigadier General, USA, Commanding for Deputy Chief, MIS, subject: BOURBON Intercept, 14 September 1945 ~~(TSC)~~

ASA (WDGSS-93) memorandum from Rowlett to BOURBON Liaison Officer, subject: Proposed Message for Major Seaman, 26 November 1945 ~~(TS)~~

ASA memorandum for Col. Solomon, U.S. Army, at Pentagon, subject: History of BOURBON Problem, 12 March 1946 ~~(TS)~~

Probable ASA report, subject: Second NICKELODEON Report, undated but issued circa June 1946 ~~(TS)~~

Rowlett note to Col. Hayes, covering attachment prepared by R. Ferner, W. Jacobs and Mr. Squire, entitled: Project NICKELODEON, 15 July 1946 ~~(TS-Special CREAM)~~

Probable ASA NICKELODEON Report No. 3, [redacted] in U.S. Intercept, September 1946 ~~(TS)~~

WDGAS-90 memorandum dated 6 January 1947 to MI3c, subject: Comment on MI3c [redacted] 18 November 1946, reference to U.S. First [redacted] Report dated 19 October 1946 ~~(TSC)~~

ASA (WDGAS-90) cover memorandum for D/Coordinator for Liaison from Frank B. Rowlett, Chief, Operations Division, subject: Report on Tour of Duty as Special BOURBON Representative at LSIC, 28 January 1947 ~~(TSC)~~

ASA memorandum, subject: Marston Report on Tour of Duty at LSIC, 21 February 1947 ~~(TSC)~~

WDGAS-96 memorandum from Mr. Stephen L. Wolf, T/A Specialist, to Rowlett, Chief, Operations Division, Subject: Reports of Visit of Mr. Stephen L. Wolf, WDGAS-96-E, to London and Frankfurt, 26 February 1947 ~~(TSC)~~

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

WDGAS-90 (Rowlett) cover memorandum to Colonel Hayes (AS-10), with proposed answer to Bartlett re [redacted] paper prepared by Stephen Wolf on 4 March 1947 (TSC)

EO 1.4. (c)

EO 1.4. (b)

PL 86-36/50 USC 3605

WDGAS-93B memorandum signed by Oliver R. Kirby, Captain, Signal Corps, Executive Officer, WDGAS-93B, to Chief, AS-90, subject: New Non-Morse Processing Equipment, 18 March 1947 (TSC)

ASA Project Approval Sheet (Fiscal Year 1947), S.C. [i.e., Signal Corps] Project No. 4600, R.L. Project No. 4-3716, title: Analog for [redacted] signed by Harold G. Hayes, Colonel, Signal Corps, Chief, ASA, 26 March 1947 (TSC)

WDGAS-10 (Hayes) memorandum to Directorate of Military Intelligence, (British) War Office, subject: M.I.3c [redacted] dated 7 April 1947 (TSC)

Revised WDGAS-93B memorandum signed by Oliver R. Kirby, Captain, Signal Corps, Executive Officer, WDGAS-93B, to Chief, AS-90, subject: New Non-Morse Processing Equipment, 22 April 1947 (TSC)

WDGAS-90 (Rowlett) memorandum to Chief, WDGAS-93, et al., subject: Mechanism for Determination of Intercept Priorities, and inclusions, 25 June 1947 (TSC)

WDGAS-90 (Hayes) memorandum for Lt. Col. D.W. Price, Directorate of Military Intelligence, British War Office, subject: M.I.3c [redacted] 8 July 1947 (TSC)

Hezlep memorandum for Chief, AS-90, subject: Weather Processing at ASA, 24 July 1947 (TSC)

Rowlett memorandum to CJO, subject: Review of Current U.S.-British Collaboration in the Communications Intelligence Field, 5 August 1947 (TSC)

CSGAS (Hayes) memorandum to Directorate of Military Intelligence, (British) War Office, subject: [redacted] Report, 20 November 1947 (TSC)

Probable ASA memorandum for the Record, subject: Russian Plain-Text Processing at ASA, 10 December 1947 (TSC)

ASA (Theodore L. Squier, Jr., Chief, 93-B-2) memorandum for the Record, subject: Traffic Analysis Intelligence, 16 April 1948 (TSC)

Chief, AS-90 (Rowlett) cover note to Chief, ASA (Hayes), passing along Fred Bright's 16 April 1948 letter to Mr. Rowlett about the Ryder Street operation, entitled: Some Notes on Ryder Street, 29 April 1948 (TSC)

AS-93 memorandum to AS-10, subject: Reclassification of Russian [redacted] and Tables, 29 April 1948 (TSC)

Chief, CSGAS-93 (Hugh S. Erskine, Lt. Col., Signal Corps) memorandum for Record, no subject, 3 June 1948 (TSC)

Chief CSGAS-90 (Rowlett) memorandum for Chief, ASA, subject: [REDACTED]  
Processing; 16 June 1948 (TSC)

ASA Chief of Operations Division (Rowlett) memorandum for Lt. Fred J. Bright,  
[USLO, London], no subject, 18 June 1948 (TSC)

Rowlett's 12 July 1948 note to Colonel Hayes, covering LSIC/USLO (Lt. Fred Bright)  
letter of 5 July 1948 to Rowlett (TSC)

CSGAS-97E (Edward E. Christopher, Chief) memorandum to JPAG, subject: Joint  
Effort on [REDACTED] 25 October 1948 (TSC)

H.L. Conley memorandum to Chief, CSGAS-90, subject: Conduct of Russian Air Force  
and Army Problem, 14 December 1948 (TSC)

#### Chief of Naval Operations (CNO), U.S. Navy

CNO memorandum from G.P. McGinnis, Lt. Cdr., USN, for Herb Conley, subject:  
Direction Finding Activities, 25 September 1947 (S)

EO 1.4. (c)  
EO 1.4. (b)  
PL 86-36/50 USC 3605

#### Coordinator for Joint Operations (CJO)

CJO memorandum for Chief, ASA, subject: [REDACTED]  
[REDACTED] 2 July 1947 (TSC)

CJO staff member: C.T.R. Adams' *Aide Memoire*, subject: "Ferret" Activities, 17 July  
1947 (TS)

CJO memorandum for the Chairman, USCIB, subject: An examination of the  
[REDACTED] question in terms of U.S.-British collaboration under the BRUSA  
Agreement, 15 August 1947 (TSC)

CJO (Wenger) memorandum, subject: Russian Material for [REDACTED]  
13 November 1947 (TSC)

CJO (Wenger) memorandum for Colonel P. Marr-Johnson, British Liaison Office,  
subject: [REDACTED] by USCIB, 28  
January 1948 (TSC)

CJO memorandum for the Record, subject: Resumé of Progress on Russian P/L  
Problem, 3 February 1948 (TSC)

CJO (Wenger) memorandum for USCICC, subject: Estimated USCIB Intercept  
Terminal Requirements, 1 February 1948; dated 25 February 1948 (TS)

CJO (Hayes) memorandum to Members of USCIB, subject: Russian Plain-Language  
Problem, 14 April 1948 (TSC)

CJO memorandum for Director, London SIGINT Center, 6 July 1948 (TS)

CJO memorandum for Members of USCIB, subject: Request for GCHQ permission to transmit certain COMINT material of [redacted] 8 July 1949 (TSC)

[redacted]

OGA  
EO 1.4.(c)

**Government Communications Headquarters (GCHQ and predecessors)**

Minutes of Brigadier Tiltman's Fourth BOURBON Meeting, 25 January 1946 (TSC)

GCHQ [redacted] memorandum to SLO Washington (for Cdr. Barnett), subject: [redacted] 15 May 1947 (TSC)

GCHQ paper, titled: Re-naming of L.S.I.C. [redacted] Publications, circa 30 June 1947 (TSC)

LSIC minutes of [redacted] Meeting, 1 July 1947 (TS)

LSIC Monthly Status Reports, May 1946-September 1948 (TSC)

GCHQ Monthly Status Reports, October-December 1948 (TSC)

**Joint Intercept Coordinating Group (JICG)**

JICG (Rubin) cover memorandum to A/Deputy Coordinator for Liaison, subject:

[redacted] 27 March 1947 (S)

JICG (J.R. Dennis) memorandum for Op-20-N-2, subject: Exchange Request for [Soviet] Black Sea Naval Traffic, 29 May 1947 (TS)

JICG/232/44 (Dennis) memorandum (for the Record), subject: Report on Russian Amateur Radio Operators, 26 September 1947; with cc: Op-20-2, Op-32-Y-1, JICG (Lt. Dickey), and JLG (S)

JICG memorandum for Col. P. Marr-Johnson (British Liaison Officer), subject: Missions to be Assigned to Station USM-36, 19 March 1948 (S)

JICG (H. Johnson, Acting Deputy Coordinator for Intercept Control) Memorandum for the Record, subject: LSIC Diversion of Facilities to the Russian problem, 27 May 1948 (S)

JICG (P.J. Patton) memorandum for USTALO, subject: Forwarding of Information, 12 July 1948 (TS)

JICG/B.5 Intercept Operators' Summary, period 1-15 October 1948; 25 October 1948

~~(S)~~

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

**Joint Liaison Group (JLG)**

JLG memorandum from Rufus L. Taylor, Cdr., USN, D/Coordinator for Liaison, for Chief, ASA and Op-20-2, subject: Short Title LSIC, Security Classification and use of in Correspondence, 28 October 1946 ~~(S)~~

JLG memorandum for BOURBON Coordinator, subject: Baudot Traffic, 5 November 1946 ~~(TS)~~

JLG memorandum for the CJO, subject: [REDACTED]  
[REDACTED] 5 to 10 September 1946 ~~(TS)~~

JLG memorandum for Mr. Fred Griffin, LSIC, signed by P.J. Karl, Lt. USN, JLG, subject: Radio Channels for Liaison between SUSLO, LSIC, and CJO Washington, 7 January 1947 ~~(S)~~

JLG memorandum for CJO, subject: Cover Names, 24 February 1947 ~~(S)~~

JLG memorandum for Col. P. Marr-Johnson (Senior British Liaison Officer), subject: Russian T/A Reports, 9 April 1947 ~~(TS)~~

JLG (Hezlep) memorandum for JPAG, subject: USCIB [REDACTED]  
[REDACTED] 10 November 1947 ~~(TSC)~~

JLG (Hezlep) memorandum for the CJO, subject: Activity Report, 1 April 1947-31 March 1948; 23 March 1948 ~~(TSC)~~

JLG memorandum (#0001969) for OP-20-2 and ASA, subject: Russian Plain Text Traffic, 9 April 1948 ~~(TSC)~~

JLG memorandum for JPAG, subject: [REDACTED] 14 May 1947 ~~(TS)~~

JLG memorandum to Chief, ASA, and OP-20-2, subject: LSIC study "The Effort on Russian Signal Intelligence in Relation to That on Other Signal Intelligence Tasks," 25 May 1948 ~~(TSC)~~

JLG memorandum for Deputy Coordinator for Allocations, subject: COMINT Material for MSIC; 8 July 1948 ~~(TS)~~

JLG memorandum signed by P.J. Karl, Lt., USN, D/Coordinator for Liaison, to Chief, ASA and OP-202, subject: [REDACTED] 15 October 1948 ~~(S)~~

**Joint Processing Allocation Group (JPAG)**

JPAG memorandum for Captain Dyer, OP-20-N2, and Mr. Rowlett, Chief, WDGAS-90, ASA, subject: BOURBON Material [REDACTED] 18 March 1947 ~~(TSC)~~

JPAG memorandum to Op-20-N-2, subject: LSIC Monthly Status Report, May 1947, 7 July 1947 (TSC)

JPAG (Rowlett) memorandum for WDGAS-90 (ASA) and Op-20-N-2, subject: Sending BOURBON Interim Reports [redacted] 11 July 1947 (TS)

JPAG (Rowlett) memorandum to Op-20-N-2 and CSGAS-90, subject: Standing Operating Procedures for the Special Russian Coordinator, 27 October 1947 (TSC)

JPAG (Rowlett) memorandum to CJO, subject: Allocation of Processing Tasks - Russian Plain Text; 17 December 1947 (TSC)

JPAG Memorandum to CJO, subject: [redacted] 18 February 1948 (TSC)

EO 1.4.(c)  
PL 86-36/50 USC 3605

JPAG Monthly Status Reports, May 1946-December 1948 (TSC)

**London Signal Intelligence Board (LSIB)**

[redacted] LSIB memorandum from Travis, on behalf of Chairman, London Signal Intelligence Board, to Chairman, USCIB, 2 April 1948 (TSC)

**United States Communication Intelligence Board (USCIB)**

Minutes of the 28th Meeting of USCIB, held on 3 February 1948 (TSC)

Minutes of the 30th Meeting of USCIB, held on 27 April 1948 (TSC)

USCIB memorandum for SBLO, subject: [redacted] 9 July 1948 (TSC)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Minutes of the 35th Meeting of USCIB, held on 16 November 1948 (TSC)

USCIB memorandum for Brigadier Tiltman (SBLO), subject: [redacted] 18 October 1949 (TS)

**State-Army-Navy Communication Intelligence Coordinating Committee (STANCICC)**

STANCICC Liaison Officers' memorandum for STANCICC, subject: Semimonthly Report on BOURBON, 1 January 1946 (TS)

STANCICC Liaison Officers, Special Project (BOURBON) memorandum for STANCICC, subject: Semimonthly Report on BOURBON, 16 January 1946 (TS)

STANCICC Liaison Officers, Special Project (BOURBON) memorandum for STANCICC, subject: Semimonthly Report on BOURBON, 31 January 1946 (TS)

STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 16 February 1946 (TS)

STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 1 March 1946 (TS)

STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 16 March 1946 (TS)

STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 1 April 1946 (TS)

STANCICC Liaison Officers' memorandum for STANCICC, subject: Semi-Monthly Report on BOURBON, 1 May 1946 (TS)

**Joint Army and Navy**

Joint Ethier (Navy) and Wolf (WDGAS-90) memorandum for JPAG, subject: Cognizance List for Scanning of BOURBON Plain-language Traffic, 20 June 1946 (TS)

**Senior British Liaison Office (SBLO), Washington**

[redacted] memorandum to Director, GC&CS, subject: Japanese Work on Bourbon, 23 October 1945 (TSC) 86-36/50 USC 3605

British Joint Staff Mission (BJSMB) memorandum for STANCIB-STANCICC, subject: Treatment of BOURBON during Commonwealth Conference, 27 February 1946 (TSC)

[redacted] memorandum to Director GC&CS, subject: BOURBON Keyboards and Transliteration Systems, 5 March 1946 (TSC)

Marr-Johnson memorandum for Chairman, USCIB, 31 October 1946, referenced in Op-20-T memorandum for Op-20-2, subject: [redacted] 8 November 1946 (TSC)

BJSMB memorandum (MOP/464) for JLG, subject: Russian T.S. Reports, 28 February 1947 (S)

BJSMB memorandum (MOP/557) for CJO via JLG, subject: [redacted] 28 May 1947 (TS)

BJSMB memorandum (MOP/557) for CJO via JLG, subject: Russian T.A. [redacted] 28 May 1947 (TS), and BJSMB Memorandum (MOP/558) for CJO via JLG, subject: [redacted] 4 June 1947 (TSC)

BJSMB memorandum (MOP/558) for CJO via JLG, subject: [redacted] 4 June 1947 (TSC)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Senior British Liaison Officer (SBLO) memorandum for Chairman, USCIB, on the subject of [redacted] 7 July 1948 (TSC)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

SBLO (Colonel P. Marr-Johnson) memorandum (MOP 89) to The Coordinator, no subject, 3 November 1948 (SC)



**Office of Naval Operations (ONI), U.S. Navy**

ONI memorandum of 18 December 1945 to Chief of Naval Communications relative to priorities of interest to ONI for communications intelligence, cited in Op-23-Y memorandum to STANCICC, subject: Communications Intelligence, Priorities of Countries as to Interest to ONI, 24 April 1946 (TS)

**Op-20/Op-20-G/CSAW**

Op-20-3-G memorandum, unaddressed and unsigned, subject: Proposed plan for the coordination of U.S. Army-Navy Communication Intelligence effort on the RATTAN project, 13 June 1945 (TS)

Op-20-G (Wenger) memorandum for Op-20, subject: RATTAN Liaison, 16 July 1945 (TS)

OIC, Op-20-3, memorandum from Fabian to Seaman, subject: Questions on TICOM Documents, 1 August 1945 (TS)

PL 86-36/50 USC 3605

Op-20-G memorandum for Secretariat of ANCICC, subject: Progress Report on Special Project, 8 August 1945 (TS)

Op-20-3-G-10 memorandum for ANCICC, subject: Post War Collaboration with the British, 28 August 1945 (TS)

Fabian memorandum to Mr [redacted] subject: Minutes of the Meeting Regarding Exchange of British and American [redacted] Traffic, 10 October 1945 (TS)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Op-20-G memorandum for Brig. General Carter W. Clarke, subject: Exchange of BOURBON [redacted] with British, 4 December 1945 (TS)

Op-20-G memorandum for OIC, Station A, subject: BOURBON, 26 December 1945 (S)

Handwritten note stating: "From a desc[ription] of cryptanalytic situation in February 1946 in Wenger files" (TSC)

Navy (probably Op-20-G) memorandum to unidentified, subject: Intervals between TOI and TOR NEGAT for Adak BOURBON intercepts, 2 April 1946 (S)

Wenger memorandum for Op-20, subject: Russian Interest in U.S. Communications, 13 September 1946 (TSC)

Op-20-T memorandum signed by E.S.L. Goodwin, Captain, USN, for Op-20-2 [changed from Op-20-G], subject: [redacted] 8 November 1946 (TSC); [redacted] 14 October 1946 (TS)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Op-20-NT memorandum, subject: [redacted] 6 November 1946 (TSC)

Op-20-2 memorandum for The Secretary of the Navy (&) Fleet Admiral C. W. Nimitz, subject: Monthly (May and June combined) report of joint Army-Navy progress in BOURBON Communication Intelligence, 18 July 1947 (TSC)

NY-1 (E.W. Knepper) memorandum to N-22, subject: Additional source of [redacted] traffic, 18 July 1947 (TSC)

Op-20-S (R.T. Kelly, Lt.-USN, Acting) memorandum for Op-20-2 via Op-20-T, subject: Current Army Ferreting Operations, 11 August 1947 (TS)

Op-20-2 (Goodwin) memorandum for The Secretary of the Navy and Fleet Admiral C.W. Nimitz, subject: Report of joint Army-Navy progress in BOURBON Communication Intelligence; July, August, and September, 1947, 3 October 1947 (TSC)

Op-20-2 (Goodwin) memorandum for The Secretary of the Navy via Fleet Admiral C.W. Nimitz, subject; Needs of Navy Communication Intelligence, 3 October 1947 (TSC)

NY-7 (Raven) cover memorandum, thru NY, to N, subject: [redacted] Research, 6 November 1947 (TSC)

Op-20-NI-1 memorandum, subject: Dissemination of Russian Material [redacted] 25 November 1947 (TSC)

Op-20-NS-1 memorandum, signed by F. W. Cameron, Lieutenant, USN, to Op-20-N-22, subject: Percentage of NS-1 Man Hours Devoted to BOURBON Production, 28 January 1948 (TSC)

Op-20-2 (Wenger) memorandum for the Chief of Naval Intelligence, signed by RADM Stone, subject: Status of our present ability to provide operational information on Soviet Submarines, 22 March 1948 (TSC)

N-31 (H. Campaigne) memorandum to [Op-]20-L, subject: [redacted] History of, dated 8 June 1948 (TSC)

Op-20-T memorandum for Op-20-2, subject: Russian Submarines in Atlantic, 16 August 1948 (TSC)

Op-20 memorandum for Op-202-T and 202-L, thru N-2, subject: "Flash" Transmissions, 19 October 1948 (TS)

N-2 memorandum to 202, N, signed by R. Mason, subject: The Pattern of Soviet Conduct in Connection with Service Cryptography and Communications, 26 October 1948 (TSC)

**Op-23-Y**

Op-23-Y memorandum to STANCICC, subject: Communications Intelligence, Priorities of Countries as to Interest to ONI, 24 April 1946 (TS)

**Senior U.S. Liaison Officer, London (SUSLO)**

Seaman memorandum, subject: Bourbon, 8 August 1945 (TSC)

U.S. Liaison Officer memorandum for Cdr. Fabian, subject: BOURBON, 27 September 1945 (TSC)

LSIC/USLO cover memoranda from Christopher (for Manson) to Col. Rowlett, subject: BOURBON Reports B-89 to B-99, dated from 1 to 31 May 1946 (TSC)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: STANCIB Newsletter No. 2-46, 27 May 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USCIB Newsletter No. 6-46, 25 June 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USCIB Newsletter No. 7-46, 2 July 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USCIB Newsletter No. 8-46, 12 July 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USCIB Newsletter No. 10-46, 26 July 1946 (TS)

[C.P.] Collins memorandum, subject: Report on Liaison between United States Communications Intelligence Agencies and the London Signal Intelligence Centre, 25 July 1946 (TSC)

Senior USLO, LSIC, memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB "Special" Newsletter No. 11-46, 1 August 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USCIB Newsletter No. 12-46, 16 August 1946 (TS)

Enclosure A [to unspecified correspondence] entitled "Personnel on Duty with United States Communications Intelligence Liaison Center in Great Britain" and Enclosure B similarly entitled "in Washington," 16 August 1946 (not marked, but treated as Secret)

Senior USLO, LSIC, memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB Newsletter No. 13-46, 25 August 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 14-46, 2 September 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 17-46, 7 October 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 19-46, 21 October 1946 (TS)

Senior USLO, LSIC, memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB [sic] Newsletter No. 20-46, 27 October 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 21-46, 4 November 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB Newsletter No. 22-46, 12 November 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 23-46, 18 November 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison (USCIB), subject: USCIB Newsletter No. 24-46, 22 November 1946 (TS)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, subject: USLO, LSIC Newsletter No. 27-46, 18-20 December 1946 (TS)

USLO memorandum, signed by a P.J. Patton, to JICG, Washington, subject: USTALO Informal Report No. 1, 20 January 1947 (S)

USLO memorandum, signed by a P.J. Patton, to JICG, Washington, subject: USTALO Informal Report No. 2, 24 January 1947 (TS)

Manson memorandum for Coordinator of Joint Operations, Op-20-2, Attention Capt. E.S.L. Goodwin, Supplement to USLO Newsletter #27-46, subject: Inspection of Group by the former USLO, 30 January 1947 (TS)

EO 1.4.(c)

EO 1.4.(b)

PL 86-36/50 USC 3605

USLO memorandum, signed by a P.J. Patton, to JICG, Washington, subject: USTALO Informal Report No. 3, 7 February 1947 (S)

USLO LSIC (Channel 409S) dispatch from CJO, EYES ONLY for Bartlett from Hayes TopSec [ ] 19 February 1947 (TS)

USLO memorandum, subject: USTALO Informal No. 4 to JICG, 26 February 1947 (TS)

USLO memorandum, thru JLG, Washington, to JICG, Washington, subject: USTALO Informal Report, No. 5, 17 March 1947 (TS)

USLO memorandum, thru JLG, to JICG, subject: USTALO Informal Report No. 6, 31 March 1947 (TS)

USLO memorandum for CJO (USCIB), subject: [Soviet] Radio Communications, 6 June 1947 (S)

USLO memorandum from P.H. Currier to JPAG, subject: Notes on [redacted] 6 June 1947 (TSC)

USLO (Norman Boardman) letter to "Dear Mr. Rowlett," 4 September 1948 (PS)

USLO memorandum to JICG, Washington, subject: USTALO Informal Report No. 14, 17 September 1947 (TS)

"Dear Captain Dennis" letter, from Herb Conley, USLO, 24 September 1947 (PS)

Informal SUSLO (Conley) technical note to Phil Patton, 24 September 1947 (S)

USLO memorandum, signed by P.H. Currier, Commander, USN, to JPAG, subject: [redacted] 14 January 1948 (TSC)

Senior USLO, LSIC memorandum to D/Coordinator for Liaison, USCIB, subject: USLO, LSIC Newsletter No. 1-48, 19 February 1948 (TS)

USLO memorandum (signed by Frederic J. Bright, 1st Lt. Sig. C) for Chief, CSGAS-90, ASA, no subject, 22 March 1948 (TSC)

USLO letter to "Dear Mr. Rowlett," from "Fred" [Bright], 1 April 1948 (TS)

SUSLO London (Fred Bright) paper, Some Notes on Ryder Street, 16 April 1948 (TSC)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

**State Department**

State Department memorandum from Mr. Young to Mr. Polyzoides, subject: Effect of Limitations on the Use of All Available CREAM Material regarding the Port Arthur Naval Base Area, 3 April 1947 (TSC)

**United States Communications Intelligence Coordinating Committee (USCICC)**

USCICC memorandum for the Chairman, USCIB, subject: [redacted]  
[redacted] 15 April 1948 (TSC), enclosing [redacted]  
[redacted] 12 April 1948 (TSC)

**U.S. Army**

Memorandum for Wing Commander A.D. McDonald: A.I.3, [British] Air Ministry from Gordon D. Stott, 1st Lt, U.S. Army, subject: Soviet Air Force, 27 April 1945 (TSC)

**U.S. Army Air Force /U.S. Air Force**

USAF memorandum for Captain J.N. Wenger, USN, from George C. McDonald, Major General, USAF, Director of Intelligence, Office of D/Chief of Staff, Operations, subject: Collaboration with British on Electronic Reconnaissance, 29 March 1948 (TS)

**U.S. Navy**

U.S. Fleet, Hq. of the CIC, Navy Department memorandum from Capt. Smedberg (ANCICC staff officer) for Admiral Thebaud and General Clarke, subject: RATTAN, 16 June 1945 (TS)

**War Department**

War Department, Office of Chief Signal Officer memorandum (from Sinkov and Rosen) to Asst. Chief of Staff, G-2, subject: Report of Technical Mission to England, 11 April 1941 (S)

War Department memorandum for Chief, ASA, subject: [redacted] 31 October 1946, covering a British War Office-produced paper entitled Method of Handling SIGINT Material on [redacted] and the Intelligence Derived Therefrom, unsigned and undated (TS)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

**Originator Unknown**

Unaddressed paper, entitled: Comments of OMGUS Berlin Cable, 25 January 1949 (TS)

Memorandum for All Members, U.S. Delegation, CANUSA Conference, 1 November 1949 (TS)

**Messages****ASA (and its predecessors, SIS and SSA)**

SSA (SPSIS-1) message from Corderman to Seaman, 24 July 1945 (TS)

SSA Informal Rowlett message to Seaman, 25 August 1945 (TS)

WDGAS-9 (Personnel) message to NY-1-A, 9 September 1946 (TS)

**Chief of Naval Operations (CNO)**

CNO message for COMNAVEU, 26 July 1945 (S)

CNO messages (AO 56243, 56244, 56245 and 56246) to COMNAVEU for Seaman, 31 July 1945 (~~S~~)

CNO message (AO 58642) for COMNAVEU (for Seaman to pass to Manson), 8 August 1945 (~~TS~~)

**Commander U.S. Naval Forces, Europe (COMNAVEU)**

COMNAVEU message to Op-20-G (from Seaman to Fabian), 5 October 1945 (~~TS~~)

COMNAVEU message to Op-20-G (from Seaman to Fabian), 2 November 1945 (~~TS~~)

**Government Code & Cipher School (GC&CS)**

GCCS message from Seaman to SSA (SPSIS-9), 22 July 1945 (~~TS~~)

GCCS message from Seaman to Corderman, 7 August 1945 (~~S~~)

GCCS message to NEGAT (from Knepper to Fabian), 10 October 1945 (~~TS~~)

**Government Communications Headquarters (GCHQ)**

GCHQ message to NEGAT (220855Z) (~~TS~~)

**Op-20-G (NEGAT) and CSAW**

Op-20-G message for Seaman, 28 July 1945 (~~S~~)

NEGAT message to GCCS (from Fabian for Knepper), 3 October 1945 (~~TS Bourbon~~)

NEGAT message to COMNAVEU (from Dennis for Seaman), 26 November 1945 (~~TS~~)

NY-1 (Knepper) informal message (Nr. 653) to WDGAS-93B (Kirby), 20 August 1947 (~~TS~~)

**Studies**

ASA study, BOURBON Project: Survey of Machine Requirements, undated but produced circa June 1946 (~~TS~~)

ASA study, [redacted] 19 September 1946 (~~TS~~)

CNO U.S. Naval Communications publication, *Brief Descriptions of RAM Equipment*, (Washington D.C., Navy Department, October 1947), 30 October 1947 (~~TS~~)

Edgar C. Duin (Capt. Signal Corps) study, Russian [redacted] [redacted] 28 September 1948 (~~TS~~)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

EO 1.4.(c)  
PL 86-36/50 USC 3605

Joint CSGAS-97 and NY-1 study, *A Survey of Russian Cryptographic Systems*, 10 January 1949 (TSC)

NCA Research Library dissertation, [redacted] 2 July 1946 (TSC)

Op-20-2 (N51) study, [redacted] 14 December 1949 (TSC)

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

## Secondary Sources

### Books

Buranelli, Vincent and Nan. *Spy/Counterspy: An Encyclopedia of Espionage*. New York: McGraw-Hill, 1982

Burrows, William E. *Deep Black: Space Espionage and National Security*. New York: Random House, 1986

Hayes, Grace Person. *The History of the Joint Chiefs of Staff in World War II: The War Against Japan*. Annapolis, Maryland: Naval Institute Press, 1982

Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: The Macmillan Co., 1973

... *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*. Boston: Houghton Mifflin Co., 1991

Lamphere, Robert J., and Shachtman, Tom. *The FBI-KGB War: A Special Agent's Story*. New York: Random House, 1986

Manne, Robert. *The Petrov Affair: Politics and Espionage*. Elmsford, NY: Pergamon Books, Inc., 1987

Randell, Brian, Editor. *The Origins of Digital Computers: Selected Papers*, Third Edition. New York: Springer-Verlag, 1982

Richelson, Jeffrey. *American Espionage and the Soviet Target*. New York: Morrow, 1987

Smith, Bradley F. *The ULTRA-MAGIC Deals: And the Most Secret Special Relationship, 1940-1946*. Novato, CA: Presidio Press, 1993

*Stalin's Correspondence with Churchill, Attlee, Roosevelt and Truman, 1941-1945, Volumes One and Two*. Moscow: Foreign Languages Publishing House, 1957

Truman, Harry S. *Memoirs, Volume One: Year of Decisions*. New York: Doubleday & Co., 1955

West, Nigel. *The Sigint Secrets: The Signals Intelligence War, 1900 to Today*. New York: William Morrow and Company, Inc., 1988

Yardley, Herbert O. *The American Black Chamber*. Indianapolis: Bobbs-Merrill Co., 1931



**Index****A-2, 115****ABC Radio Network, 50****ABLE, U.S. Naval Station, Guam, 56, 63****Academy of Sciences, Georgia,****Academy of Sciences, RSFSR,****Academy of Sciences, Ukraine,****Academy of Sciences, USSR,****Adak, Alaska, 102****Adams, Lieutenant C.T.R., U.S. Navy, 115, 116, 129****Advanced Exploitation Unit, 92****AFSA (Armed Forces Security Agency), 46, 60 87, 121, 1378, 139, 184, 238, 258, 263, 269****A Group, 161, 212****Air Weather Service, USAF, 92****Albania, 67**EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605**Algiers, Algeria, 44****Alphabet Substitution Unit, 167****AMTORG Trading Corporation, 10, 11, 22****ANCIB (Army-Navy Communications Intelligence Board), 31, 35, 36, 39, 41, 42, 46, 55, 60****ANCICC (Army-Navy Communications Intelligence Coordinating Committee), 25, 31, 37,  
39, 46, 55, 58-66****Argentina, 66****Arlington Hall Station, Virginia, 12, 14, 15, 226****Armstrong, W. Park Jr., 87, 227****Army Signals Intelligence Section (SIS), 10, 11****Army Signals Security Agency (SSA), 11, 27, 33-35, 37, 38, 43, 44, 48, 54, 59, 61****ASA (Army Security Agency), 10, 12, 14, 22, 33, 48, 49, 54, 55, 63, 67, 69, 70, 72, 74, 81-83,**

86-88, 90, 92, 95, 96, 101, 106, 109-111, 113, 115-118, 121, 126, 132, 137-139, 141,  
143-145, 147, 149, 151, 152, 155, 156, 160-165, 171-173, 176-178, 181, 185, 187, 188,  
194, 195, 199, 204, 206, 208-212, 217, 2199, 220, 223-228, 236-241, 244, 246, 251-255,  
258, 262, 269, 271, 272

ASA Europe (ASAE), 76, 77, 89, 189, 237, 272

ASA Plain Language Exploitation Unit, 226, 236, 256, 272

[Redacted]

EO 1.4.(c)  
OGA

Austria, 6, 11

[Redacted]

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

B-17 reconnaissance aircraft, 117

[Redacted]

B-29 reconnaissance aircraft, 116, 117

[Redacted]

Baker Unit, 92

Balkans, 30, 32

Baltic states, 10, 11

Bainbridge Island, Puget Sound, Washington State, 13

[Redacted]

Bartlett, Colonel William G., U.S. Army, 209, 217, 235

[Redacted]

BAZIL, 7

Beaumont, John, 235

Benson, Robert L. (Lou), 25, 62, 118, 184

Bentley, Elizabeth, 85  
Bering Strait, 117  
Berkeley Street, 73  
Berlin, Germany, 9, 18, 31, 48, 85  
Berlin Wall, 263

[Redacted]

BIOGRAPH, 116, 117  
BIRTHSTONE file, 212  
Bissell, General Clayton L., U.S. Army Air Force, 60  
Black Chamber (also see Yardley), 7, 9, 10  
Black Sea Straits, 32  
Bletchley Park, England, 37, 38, 41, 53, 54, 71, 73, 101, 231  
BLUE, 37

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Boardman, Norman, 128

[Redacted]

PL 86-36/50 USC 3605

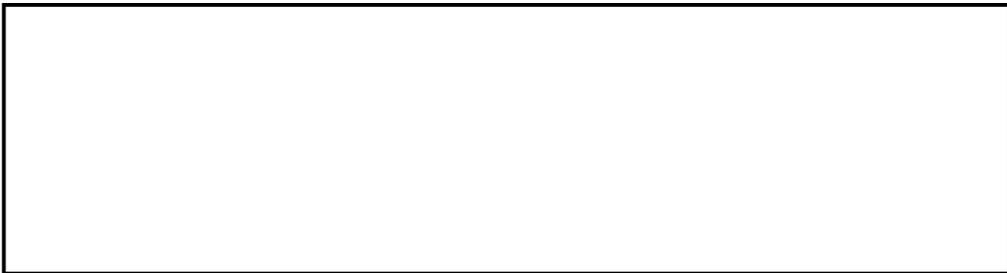
Bolshevik code, 10  
Bolshevik regime, 6  
Bolshevik Revolution, 9  
Bonsall, Arthur W., 231, 235  
Boulder, Colorado, 50  
Bright, First Lieutenant Frederic J., U.S. Army, 90, 122, 233, 235-237, 239, 241  
British Admiralty, 21, 216, 247  
British Air Ministry, 32  
British Army, 17-20  
British ciphers, 9  
British Directorate of Military Intelligence (MI1), 21  
British Foreign Office, 8, 21  
British General Headquarters, France, 21  
British General Staff, 18

British Joint Staff Mission (BJSM), 124  
 British Military Cipher Bureau, 21  
 British Secret Intelligence Service (SIS/MI6), 172, 232  
 British Security Service (MI5), 100  
 British-USA (BRUSA) Agreement (see BRUSA Agreement)  
 British War Office (MI3), 71, 205-211, 217, 218, 247  
 British "Y" Station, 19, 20  
 British Zone in Germany, 234



EO 1.4.(c)  
 EO 1.4.(b)  
 PL 86-36/50 USC 3605

BRUSA Agreement, 55, 70, 74, 89, 90, 95, 99, 124, 267  
 BRUSA Technical Conference, 1948 (see London Technical Conference)  
 "Brusterort" (unlocated near Kaliningrad), 203  
 Buffham, Benson K., 237  
 Bulgaria, 67, 79  
 Burns, Thomas L., 58, 59, 61, 118, 121, 262  
 Burrows, William E., 129  
  
 Cabell, General (probably Charles P.), U.S. Army Air Force, 227, 228  
 Callimahos, Lambros D., 175  
 Cameron, Lieutenant F.W., U.S. Navy, 183  
 Campaigne, Dr. Howard H., 153, 157, 178, 273



Caracristi, Ann Z., 161  
 Carpathian MD, 166, 191  
 Casablanca Conference, 1943, 15, 16

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Central Group of Forces (CGF), Czechoslovakia, 146, 199

[Redacted]

OGA  
EO 1.4.(c)

Central Intelligence Group (CIG), 80

Chadless tape, 111

Chamberlin, Major General Stephen J., U.S. Army, 86, 87, 227

Chambers, Whittaker, 86

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Chief of Naval Operations (CNO), 31, 41, 59, 60, 110, 167, 182

China, 6, 66, 85

Chinese Nationalists, 67, 256, 257

Chinese Communists, 67, 256, 257

Chita, USSR, 114, 194

Christopher, Edward E., 119, 181

Chronological Series Intelligence Card, 244

Chukotsk Peninsula, USSR, 117

Churchill, Prime Minister Winston , 16, 30-32, 65

Cipher Bureau (Yardley's), 9

Civil War, U.S., 6

CJO (Coordinator of Joint Operations), 70-72, 81, 90, 99, 113, 116, 119, 121-125, 128,  
207, 226, 228, 236, 240, 241, 253, 269

Clarke, Colonel Carter W., U.S. Army, 35, 36, 58, 63

[Redacted]

Cold War, 1, 2, 29, 65, 79, 85, 202, 205, 262, 263

Cole, Commander A., Jr. U.S. Navy, 183

[Redacted]

[Redacted]

Collins, Captain Charles P., U.S. Army, 73, 74, 119, 126, 165

Combined Chiefs of Staff (CCS), British, 42, 60

COMINTERN (Komintern), 10, 18

COMINTORG, 57

Commander U.S. Naval Forces, Europe (COMNAVEU), 59, 62, 63

Command Post Exercise (CPX), 76

[Redacted]

Community On-Line Intelligence System (COINS), 212

COMPARTY (Kompartei), 18

Conley, Herbert L., 83, 87-89, 110, 122, 127, 177, 194, 214, 271

CONSIDO, 254

Cooper's BOURBON party, 101

Coordinator of Joint Operations (see CJO)

CORBY, 49, 50

Corderman, Brigadier General W. Preston, U.S. Army, 38, 42, 44, 60, 61

[Redacted]

CREAM material, 124, 247, 248, 257, 260

[Redacted]

CSAW (Communications Supplementary Activity, Washington), 72, 81-83, 86-90, 92,

96, 97, 101, 109, 111, 114, 127, 132, 133, 144-147, 156, 161, 167, 171, 193, 194,

204, 220, 224-229, 236, 240, 251-256, 262, 272,

[Redacted]

Currier, Commander Prescott H., U.S. Navy, 156, 176, 179

Czechoslovak communications, 187

Czechoslovak Crisis of 1948, 212

Czechoslovakia, 11, 67, 85

Dairen, China, 256, 257

Danilson, Lieutenant H.T., U.S. Air Force, 183

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

PL 86-36/50 USC 3605

[Redacted]

Dennis, Captain J.R., U.S. Navy, 121, 127, 214, 258

Denniston, Alistair G., 17

Department of Defense, U.S., 87

[Redacted]

Department of State, U.S. (see State Department)

Dickey, Lt., 127

Direction Finding (see HFDF)

Director, GC&CS /GCHQ (see Travis)

Director of Central Intelligence (DCI), 80, 86, 238

Director of Military Intelligence (DMI), MI3, 206

[Redacted]

[Redacted]

Duin, Captain Edgar C., U.S. Army, 181

Dutch authorities, 10

Dyer, Captain Thomas H., U.S. Navy, 123

Eastcote, London, 71-73, 81-83, 101, 208, 231, 232

ELINT (Electronic Intelligence), 23, 66, 91, 243

ENIGMA bombes, 165

ENIGMA cipher machines, 163, 177

ENIGMA material, 19, 205, 206

Erskine, Lieutenant Colonel Hugh S., U.S. Army, 179, 180

Essential Elements of Information (EEI), 223

[Redacted]

Ethier, H.E., Lieutenant, U.S. Navy, 238

Evpatoriya, USSR, 195

Fabian, Rudolph J., 38, 41, 53, 54, 59, 61-63, 177

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

PL 86-36/50 USC 3605

Far East, 31, 46, 50, 67, 88, 109, 194

Far East MD, 137, 139, 191, 192, 199, 200, 202, 209

FBI (Federal Bureau of Investigation), 51, 86, 184, 251

FCC (Federal Communications Commission), 42

Ferner, Robert O., 216

Ferret flights, 66, 112, 115-117, 129

Fetterlein, Ernst C., 17, 18

[Redacted]

Finland, 11, 30

[Redacted]

[Redacted]

Fish, Hamilton, U.S. congressman, 10

[Redacted]

"Flash" transmissions, 66, 114, 129

[Redacted]

Forrestal, Secretary of Defense James V., 87

[Redacted]

France, 6, 66

Frankfurt, Germany, 44, 76

French ciphers, 9

[Redacted]

French cryptographic practices, 21

Friedman, Elizebeth S.,

Friedman, William F., 5-7, 10, 22-24, 27, 41, 175

Fulton, Missouri, 31

G-2 (Military Intelligence, U.S. Army), 22, 44, 244, 246

Garofalo, C., 216

GC&CS (Government Code and Cipher School), 17-19, 21-23, 26, 35, 37-39, 41, 42, 44,  
47-50, 53-56, 59, 62, 63, 71, 143, 245-247, 258, 259

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

OGA  
EO 1.4.(c)

GCHQ (Government Communication Headquarters), 3, 17, 35, 48, 71-75, 79-82, 84,  
89-92, 97, 101, 107-111, 113, 115, 123, 124, 132-135, 137, 144-147, 149-153, 156-161,  
163, 165, 169, 170, 172, 174, 175, 177, 181, 183, 185, 187, 188, 191, 193, 194, 197,  
199-204, 206-224, 227, 231-236, 239, 244, 247-249, 252, 258, 259, 265

General Cryptographic Branch, SSA, 12, 34

George, Prime Minister Lloyd, 17

German air traffic, 19

German communications, 20

German SIGINT information, 21

Germany, 6, 9, 11, 16

GLAVCEVMORPUT (Northern Sea Shipping Route), 192

[Redacted]

Goodwin, Captain E.S.L., U.S.Navy, 123, 127, 183, 239, 240

Gore, Colonel (probably Robert Gore-Browne), British Army, 208

Gouzenko, Igor, 49, 50

Government Code and Cipher School (see GC&CS)

Government Communication Headquarters (see GCHQ)

[Redacted]

Great Britain, 1, 3, 6, 30

Greece, 67

Green codes, 165

Group of Soviet Occupation Forces, Germany, 110

GRU (Chief Intelligence Directorate of the Soviet General Staff), 12

Guam, 92, 114

GULAG (Chief Directorate of Camps, MVD), 255

Gunn, Lieutenant Maximillan C., U.S. Navy, 97

Gurin, Jacob, 223, 238, 256, 260

[Redacted]

Hall, (Rear) Admiral (probably John L.), U.S. Navy, 21

EO 1.4.(c)  
EO 1.4.(d)  
PL 86-36/50 USC 3605

Harbold, General (probably Norris B.), U. S. Army Air Force , 115, 116

Hayes, Colonel Harold G., U.S. Army, 58, 72, 73, 81, 83, 86, 90, 96, 113, 116, 122, 151, 167,  
171, 178, 206-211, 216-218, 227, 236, 237, 241

Herzo Air Base, Germany, 113

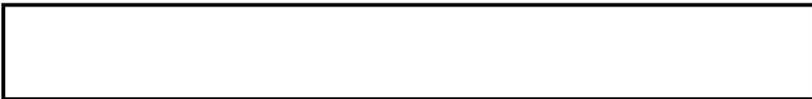
Hezlep, William H., Jr., 92, 96, 123, 124

HF (high frequency) communications, 50, 65-67, 92

HFDF (high frequency direction finding), 81, 91, 110, 167

HF (high frequency) Morse, 110, 114, 149, 195, 202

HF (high frequency) tactical voice, 233



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Hillenkoetter, Rear Admiral Roscoe H., U.S. Navy, 86, 87, 223

Hiroshima, Japan, 41

Hirsch, Brigadier, British Army, 207, 208

Hiser, Lieutenant Colonel Charles F., U.S. Army, 183, 237

Hiss, Alger, 86

Hitler, Adolph, 11, 16, 30, 31

HMS *Queen Elizabeth*, 53

HMS *Queen Mary*, 53, 55



Howe, Dr. George F., 60, 61, 63, 118, 121-124, 128, 173, 174, 180, 238-241, 259, 260, 269

Hungary, 67, 79

Hurt, John B., 10

IBM (International Business Machines), 36, 47, 72, 90, 111, 142, 151, 152, 163-167, 181,  
188, 206, 226, 228, 253, 260, 261



EO 1.4.(c)  
PL 86-36/50 USC 3605

Imperial Japan, 1, 2, 23, 27

Imperial Russia/n, 2, 5-7, 9

India, 17

[Redacted]

Inglis, Rear Admiral Thomas B., U.S. Navy, 87, 235, 236

Iran, 65

Iron Curtain, 1, 31

[Redacted]

EO 1.4.(c)  
PL 86-36/50 USC 3605

Italian air traffic, 19

Italian communications, 20

Italo-Abyssinian war, 8

Italy, 6, 11

IVORY, 248

Jacobs, Walter W., 216

Japan, 6, 9, 11, 16, 57

Japanese diplomatic communications, 22

JCS (Joint Chiefs of Staff), U.S., 60, 91

JICG (Joint Intercept Control Group), 70, 112, 120-122, 127-129, 240, 271, 272

Jilinski, General, Imperial Russian Army, 17

JLG (Joint Liaison Group), 70, 71, 91, 96, 99, 100, 118, 119, 122-125, 127, 128, 173, 180,  
241

Johnson, H., 122

Johnson, Secretary of Defense Louis A., 121

Jones, Group Captain Eric M., Royal Air Force, 41, 209, 231, 232

JOP (Joint Operating Plan), 60, 70

JPAG (Joint Processing Allocation Group), 70, 75, 83, 96, 97, 100, 101, 119, 121-126,  
129, 133, 138, 173-183, 213-216, 226, 238-240, 252, 253, 259, 260, 269, 271

Jugoslav (see Yugoslav)

[Redacted]

Kahn, David, 24, 126

EO 1.4.(c)  
OGA

Kaliningrad, USSR, 203

[Redacted]

Karelia, USSR, 224

Karl, Lieutenant P.J., Jr., U.S. Navy, 120, 123

Kelly, Lieutenant R.T., U.S. Navy, 129

Kennan, George F., 79

KGB (Committee for State Security), 8, 11, 145

Kiev MD, 248

King, Admiral Ernest J., U.S. Navy, 15, 31, 36, 42, 60, 245

King, Mackenzie, Canadian prime minister, 50

Kirby, Oliver R., 59, 111, 127, 128, 179, 237, 258, 271

Knepper, Lieutenant Commander Edward W., U.S. Navy, 42, 53, 54, 62, 70, 179, 180

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Koenigsberg, USSR, 194, 232

Kolyma River, USSR, 224

Komintern (see COMINTERN)

Kompartei (see COMPARTY)

KONGO, 7

Korrespondent numbers, 201

Kremlin, 19

Kullback, Dr. Solomon, 10

*La Chambre Noire*, 21

Lamphere, Robert J., 62

[Redacted]

Latvia, 9

Libau, USSR, 201

Lend-Lease Act, 107, 112

Lenin, Vladimir Ilich, 19

Leningrad MD, 91

Leningrad, USSR, 16

Levenson, Arthur J., 151

Lewis, Frank W., 41

[Redacted]

Linn, Major John K., U.S. Army, 206, 207

Liverpool, England, 54

London Technical Conference, 1948, 90, 235-237, 241

London Signal Intelligence Board (LSIB), 41, 70, 91, 99, 169, 171, 235, 236, 241

London Signal Intelligence Centre (LSIC) (see also GCHQ), 71, 73-75, 80, 82, 91, 101, 107, 110, 118, 126, 142, 165, 169, 173, 175-183, 187, 208, 209, 213-217, 231, 232, 236, 238-241, 259

[Redacted]

Luda (current name for Port Arthur), China, 256

Lushun (current name for Dairen), China, 256

L'vov, USSR, 195

[Redacted]

Malinovskij, Marshal Rodion Ya., USSR, 194

Manhattan Project, 12

Manne, Robert, 125

Manson, Commander Grant C., U.S. Naval Reserve, 38, 41, 59, 71, 74-76, 101, 107, 108, 119, 169, 183, 187, 206-209, 231, 232, 235, 240

Manson, Major John, U.S. Army, 53

Manual Morse (see Morse, manual)

Marshall Plan, 79, 85

Marshall, General George C., U.S. Army, 31, 42, 60, 245

Marr-Johnson, Colonel Patrick, British Army, 71, 74, 95, 123, 124, 128, 241

Marston, Major E. Dale, U.S. Army, 81, 121

MARTA, 7

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Mason, Redfield, 183

Mathew Machine, 164

Mathews, Mitford, 182

MC-88 typewriter, 47

McDonald, A.D., 58

McDonald, Major General George C., U.S. Army Air Force, 115, 116, 122

McGinnis, Lieutenant Commander G. P., U.S. Navy, 127

[Redacted]

Menzies, General Sir Stewart, British Army, 101, 231

Meteorological (MET) Party, GCHQ, 91, 92

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

MI3 (see also British War Office), 208, 209, 217

MI5 (see also British Security Service), 100

MI6 (see also British Secret Intelligence Service), 231, 247, 248

MI-8, 9

Middle East, 66, 67

Military Intelligence Division (MID), U.S. Army, 9, 67, 206-211, 236, 251, 253, 254

Military Intelligence Service (MIS; also G-2), 44

[Redacted]

PL 86-36/50 USC 3605

Minuend, 161, 181

Monster, 53

Moody, Juanita, 182

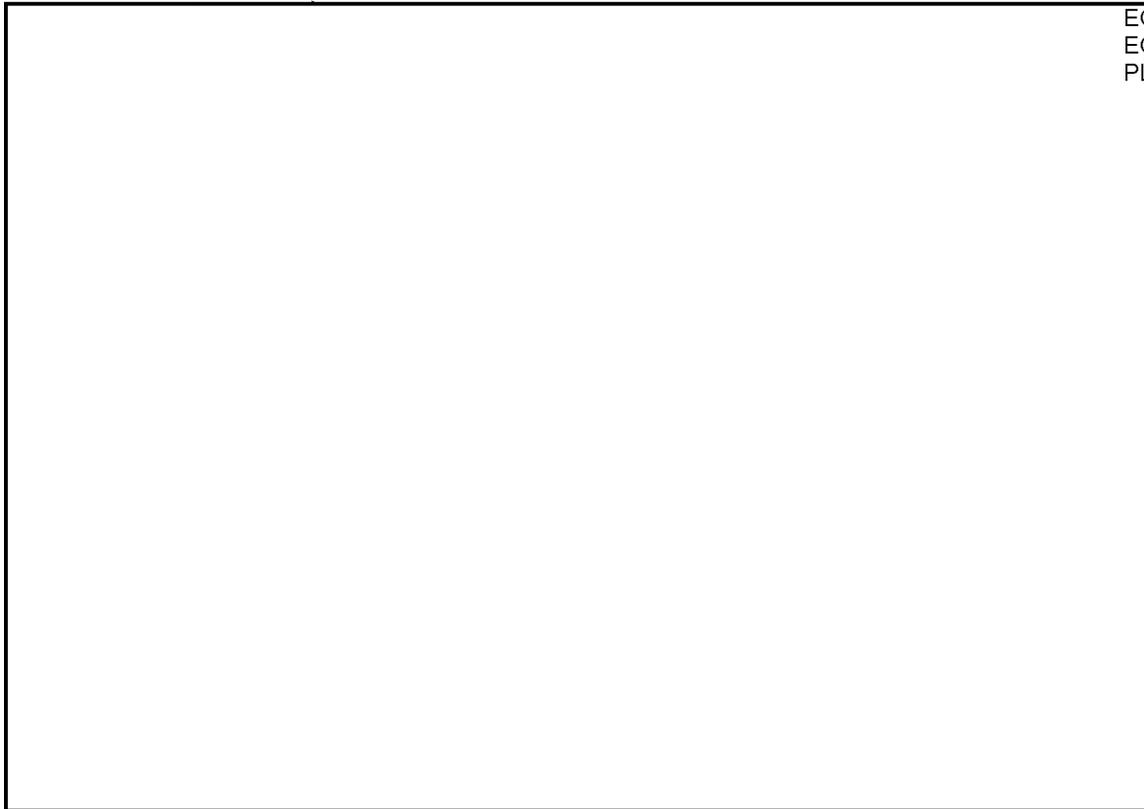
[Redacted]

MORFLOT (Soviet Merchant Marine Service), 192

Morse, manual, 44, 50, 52, 57, 65, 69, 109, 112, 113, 185, 233

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605



Nagasaki, Japan, 41

Naples, Tony, 24, 177

Napoleon, 7

National Intelligence Authority (NIA), 80

National Security Act of 1947, 80

National Security Agency (NSA), 41, 46, 87, 121, 143, 157, 161, 177, 184, 240, 262, 263,  
269

National Security Council, 80

National SIGINT Operations Center (NSOC), 262

Naval Communications Annex, Washington (NCAW), 13-15, 43, 50, 58-60, 62

Naval School of Oriental Languages, University of Colorado, Boulder, 15

Navy Code and Signal Section, 10

Nazi Germany, 1, 2, 11, 16, 20, 23, 29, 30

Near East, 66

NEGAT, 62, 126, 175

New York City, 9, 10, 54, 55

[Redacted]

NICKELODEON, 206, 207, 216, 217

Nimitz, Fleet Admiral Chester W., U.S. Navy, 76, 127, 238, 239

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

"Non-Morse" communications processing, 151, 163, 164, 186, 187

North Africa, 16

North Atlantic Treat Organization (NATO), 1

Northern Sea Route, 199

Norwegian fjords, 19

O'Conner, Colonel, British Army, 35

October Revolution, 17

Office of Naval Communications (ONC), U.S. Navy, 227

Office of Naval Intelligence (ONI), U.S. Navy, 10, 22, 66, 87, 118, 244, 251

Office of Strategic Services (OSS), 42

O'Gara, John F., 271

OGPU, 8

Okhrana, 7

[Redacted]

EO 1.4.(c)  
PL 86-36/50 USC 3605

OMGUS, Berlin, 122

Op-20-2, 72, 75, 123, 127, 129, 178, 238-240, 256, 260

Op-20-3, 59

Op-202-L, 129

Op-202-T, 129

Op-20-G, 13-15, 23, 33, 36, 37, 43, 44, 49-50, 58-60, 63, 70, 72, 95, 105, 106, 126, 137,

142-144, 149, 186, 188, 216, 219, 223, 224, 244, 246, 251

Op-20-N, 83, 121, 123, 129, 176, 183, 253, 255, 259, 260

Op-20-S, 129

Op-20-T, 123, 256, 260

Otani, USSR, 194

[Redacted]

Paernu Bay, USSR, 202

Palanga, USSR, 194

Paris Peace Conference, 1918, 21

Paschke, Dr., 41

PASSIONATE, 116, 117

Patton, Phillip J., 83, 112, 127, 128

Pearl Harbor, Territory of Hawaii, 1, 11, 29

Pearson, Drew, 50

Penfield, Mr., D/Director, Office of Far Eastern Affairs, State Department, 256, 257

Pentagon Unit, 226

Pershing, General John J., U.S. Army, 21

Peter the Great, 7

Peterson, Lieutenant Colonel Arthur C., U.S. Army, 183, 237

[Redacted]

EO 1.4.(c)  
OGA

Philby, Harold ("Kim"), 172, 248

Phillips, Burton, 24

Phillips, Cecil J., 25, 61, 62, 82, 118, 128, 156, 175, 179-184, 258

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Pillau, USSR, 194

PINK, 137

Pochitalin, Major General, Soviet artillery, 189

[Redacted]

Poland, 11, 19, 21, 30, 32, 67, 79

[Redacted]

Polyarnoe, USSR, 19

Polyzoides, T. Achilles, 257, 260

[Redacted]

Port Arthur, China, 256, 257

Port Lyautey, French Morocco, 50

Portuguese communications, 20

Price, Lieutenant Colonel D.W., British Army, 218

Pritchard's party, GCHQ, 101

[Redacted]

PT-43, 202

PT Tables, 160

PURPLE machine, 22, 34

PVO (Antiaircraft Air Defense), 191

[Redacted]

Radioprinter, 65, 90, 112, 113

Radiotelephone (also R/T), 65, 90, 232-234, 236, 237

[Redacted]

RAM (Rapid Analytic Machines), 90, 163, 165-167, 181, 183, 273

RATTAN, 33-35, 37, 39, 42, 49, 58-60, 141

Raven, Francis A., 83, 143, 144, 176

RAYON, 7

Red Army, 8, 16, 22, 31, 65, 132, 139, 142, 233, 245, 248, 271

Red Codes, 165

Red Forms (British), 107, 108

Redman, Admiral John R., U.S. Navy, 60

Reimers, Paul, 182

Remington Rand, 107

Richelson, Jeffrey, 129

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

EO 1.4.(c)  
PL 86-36/50 USC 3605

Rockex, Porter's, 90

Romania (also Rumania), 67, 79, 90

Rosen, Leo, 27

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Rowett, Lieutenant E.J., U.S. Navy, 183

Rowlett, Frank B., 10-13, 24, 27, 34, 35, 37, 38, 47, 49, 50, 58, 60-63, 82-84, 96, 110,  
118-123, 126, 128, 133, 173, 206, 210, 211, 216-218, 226, 236-239, 241, 246, 258, 259

Royal Air Force, 18, 247

[Redacted]

Royal Navy, 17

RSFSR Ministry of Health, 255

RU, 70

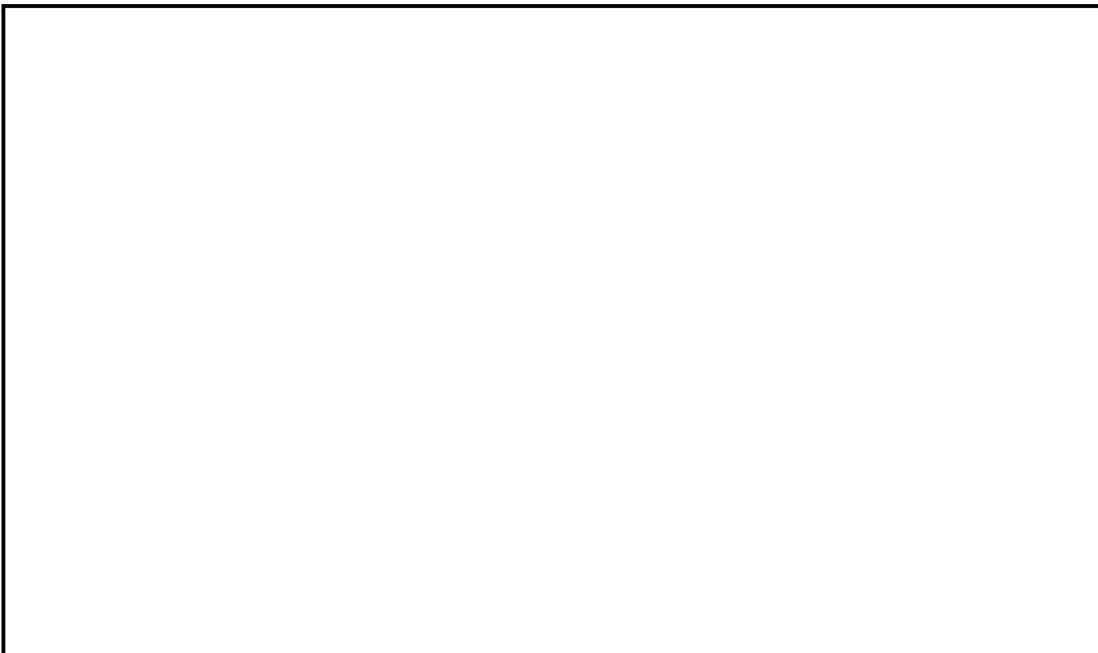
[Redacted]

Rubin, Morton, A., 127

[Redacted]



RUPLAI reports, 123, 254, 255, 260



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

[Redacted]

Russian Plain Language Analysis Item, 254

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

RYBPROM (Soviet Fisheries Group), 192

Ryder Street operation (GCHQ), 219, 231-237, 239-241, 247

Safford, Captain Laurance F., U.S. Navy, 10, 23

Sakhalin Island, USSR, 186

SALAMBO, 7

[Redacted]

Sarafand, Palestine, 18

Saratov, USSR,

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Scandinavia, 10, 67

[Redacted]

Scheyern, Germany, 113

Scrambler, 150-157, 161, 166, 184, 195, 210

Scytale, 6

Seaman, Major John N., U.S. Army, 37-39, 41, 42, 53, 59, 60, 62, 63, 246, 258

Senior British Liaison Officer (SBLO), Washington, 99, 122

SERIOZA, 7

Service Cryptologic Agency (SCA) (later, Service Cryptologic Element [SCE]), 87

Sevastopol', USSR, 195

Shachtman, Tom, 62

[Redacted]

EO 1.4.(c)  
PL 86-36/50 USC 3605

- Short signals, 66
- Siberia, USSR, 33, 49, 50, 109, 117
- Sicily, 15
- Signal Corps Radio (SCR), 112
- Simla, India, 18
- Sinkov, Dr. Abraham, 10, 27
- Skaggs Island, California, 15
- Smedberg, Captain W.R., III, U.S. Navy, 58
- SMERSH, 189, 190, 213
- Smith, Bradley F., 58
- Smolensk, USSR, 203
- Snook, Suzanne, 24
- Solomon, Colonel, U.S. Army, 25
- Source 267, 75, 76
- Sovetskaya Gavan', USSR, 114, 193-195

[Redacted]

- Soviet 2nd Air Army, 188
- Soviet 3rd Long Range Bomber Army, 199
- Soviet 4th Air Army, 248
- Soviet 5th Air Army, 248

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Soviet 7th Fleet, 193-195

[Redacted]

- Soviet 9th Air Army, 202
- Soviet 10th Air Army, 161, 185, 191, 194
- Soviet 12th Air Army, 193
- Soviet 14th Air Army, 195
- Soviet 17th Air Army, 199
- Soviet 31st Rifle Brigade, Anadyr', 200

- Soviet 39th Army, 189
- Soviet 52nd Rifle Corps, Far East MD, 188
- Soviet 56th Rifle Corps, Far East MD, 137
- Soviet 74th Artillery Military Depot, Moscow, 188
- Soviet 85th Rifle Corps, Far East MD, 137
- Soviet 96th Rifle Division, Kazan, 211, 218
- Soviet 126th Rifle Corps, Far East MD, 138, 188
- Soviet 137th Rifle Corps, Far East MD, 137
- Soviet 255th Rifle Corps, 188
- Soviet 350th Rifle Regiment, 211

[Redacted]

Soviet Air Force/s, 32, 142, 144, 159, 248, 271

Soviet "amateur" radio operators, 109, 127

Soviet Baltic Fleet, 68, 161, 188, 193, 194, 202, 204, 249

[Redacted]

Soviet Black Sea Fleet, 82, 114, 121, 144, 146, 188, 202, 204

[Redacted]

Soviet Border Troops, 8

[Redacted]

Soviet Communist Party, 10

Soviet Far East, 46, 117, 153, 174, 185, 186

[Redacted]

Soviet Fisheries Group (RYBPROM), 192

Soviet-German Nonaggression Pact, 11, 30

Soviet Ground Forces, 70

[Redacted]

Soviet Merchant Marine Service (MORFLOT), 192

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Soviet Military Attaché, Ottawa, Canada, 50

[Redacted]

Soviet Navy, 8, 16, 70, 132, 142, 188, 216, 248

Soviet Naval VHF, 113

[Redacted]

Soviet Northern Fleet, 204

Soviet Pacific Fleet, 186, 188, 204

[Redacted]

Soviet spies/spy rings, 12, 51

[Redacted]

SPARTAK, 7

"Special" CREAM, 257

Special Projects Section (SPS), State Department, 256, 257

Special Security Office/r (SSO), 89, 272

[Redacted]

Squier, Theodore L., Jr., 176, 210, 211, 214, 216

Stalin, Joseph, 11, 16, 65

Stalingrad, USSR, 16, 30

STANCIB (State-Army-Navy Communications Intelligence Board), 119

STANCICC (State-Army-Navy Communications Intelligence Coordinating Committee),  
118-120, 174, 181

State Department, U.S., 21, 35, 87, 244, 251, 255-257, 260

Stella Polaris, 120

Stettinius, Secretary of State Edward R. Jr., 32

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Stockholm, Sweden, 10

Stone, Rear Admiral Earl E., U.S. Navy, 87, 227, 256, 260

Stone (Board) Report, 121

Stott, Gordon D., 58

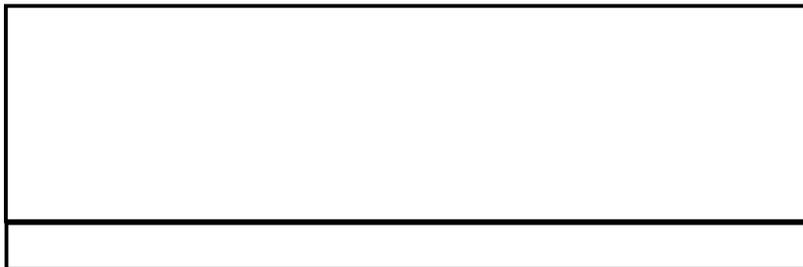
Subcommittee on Merger Planning, USCIB, 46

Substitution systems, 7, 8

Sudetenland, 112

SUSLOL (Senior U.S. Liaison Office/r, London), 71, 72, 89, 90, 105, 107, 112, 119, 120,

125-129, 156, 174, 179, 183, 209, 213, 231-233, 235, 239, 271



EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

EO 1.4.(c)  
OGA

Swinemunde, Poland, 188

Tallinn, USSR, 110, 195

Tannenberg, Battle of, 7



Target Intelligence Committee (see TICOM)

Tashkent, USSR, 224

TATIANA, 7

Taylor, Commander Rufus L., U.S. Navy, 72, 118

Telemetry, 23

Templer, General Sir Gerald, British Army, 206, 208-210

TEXTA, 72

Thebaud, Admiral L. Hewlett, U.S. Navy, 35, 36, 41, 58, 60

TICOM (Target Intelligence Committee), 39, 41-43, 49, 54, 56, 59, 75, 111, 119, 120,

127, 151

Tiltman, Brigadier John H., 17, 18, 26, 48, 50, 55, 75, 76, 119, 125, 169

Tordella, Dr. Louis W., 13, 15, 25, 81, 109, 110, 115, 120, 127, 128

Toshimoe, Etorofu Island, USSR,

Towler, Colonel H.H., U.S. Air Force, 183

[Redacted]

Traffic Analysis Fusion Items,

Transbaikal-Amur MD, 188

Transcaucasus, 19

Transmission Distributor, Model 14,

Trans-Siberian railroad, 33

Transposition systems, 7, 8

Travis, Commander Sir Edward W., Royal Navy, Director, GCHQ, 35-37, 42, 50, 55, 72, 80, 81, 101, 120, 169, 170, 206, 207, 235, 236, 241

Treasury Department, U.S., 42

Truman Doctrine, 32, 79

Truman, President Harry S., 30-32, 47, 50, 58, 80, 85

Tsar Alexander I, 7

Turkey, 6, 32

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

U-Boats, German, 19

Ukraine, 212

Ulan-Bator, Mongolian People's Republic, 192

ULTRA, 205, 245, 247, 258, 259

Unification Bill, 80

United Nations (U.N.), 30, 65, 79

U. N. Charter, 32

U. N. Conference, 32

[Redacted]

EO 1.4.(c)  
PL 86-36/50 USC 3605

U.S. Air Force (USAF), 80, 91, 92, 112

USAF Europe (USAFE), 89, 91, 272  
USAF Security Service (USAFSS), 87, 92  
U.S. Army, 30, 107  
U.S. Army Air Force (USAAF) Intelligence (A-2), 115, 116  
USCIB (U. S. Communications Intelligence Board), 70, 71, 75, 80, 82, 83, 86, 89, 91, 95-97,  
99, 100, 113, 115, 116, 119, 121-125, 128, 169, 171, 192, 183, 184, 207-209, 220, 224,  
225, 228, 232, 235-237, 239, 240, 252-254  
USCICC (U.S. Communications Intelligence Coordinating Committee), 116, 118, 122, 123,  
128, 224-227  
U.S. commander in chief, Mediterranean Fleet, 91  
U. S. Forces European Theater (USFET), 76, 77  
U.S. Liaison Office (USLO) (see SUSLO)  
USM-36, 128  
U.S. Navy, 30  
U.S. Navy Russian Section, 244  
USSR Ministry of Armaments, 255  
USSR Ministry of Automobile and Tractor Industry, 255  
USSR Ministry of Aviation Industry, 123, 255  
USSR Ministry of Chemical Industry, 255  
USSR Ministry of Coal Industry for Western Areas and Eastern Areas, 255  
USSR Ministry of Communications Industry, 255  
USSR Ministry of Electrical Industry, 255  
USSR Ministry of Electric Power Stations, 255  
USSR Ministry of Ferrous Metallurgy, 255  
USSR Ministry of Fish Industry, 255  
USSR Ministry of Health, 255  
USSR Ministry of Heavy Machine Building, 255  
USSR Ministry of Light Industry, 255  
USSR Ministry of Medical Industry, 255  
USSR Ministry of Metallurgical Industry, 255

USSR Ministry of Nonferrous Metallurgy, 255  
 USSR Ministry of Oil Industry of Southern and Western Areas, 255  
 USSR Ministry of Procurement, 255  
 USSR Ministry of Railroad Transportation, 255  
 USSR Ministry of River Fleet, 255  
 USSR Ministry of Rubber Industry, 255  
 USSR Ministry of Shipbuilding Industry, 255  
 USSR Ministry of Trade, 255  
 USSR Ministry of Transport Machine Building, 255

Vasilevskij, General Aleksandr M., Deputy People's Commissar of Defense Army, 205  
 V-E Day, 12, 31, 273  
 VENONA, 12, 25, 51, 62, 118, 184  
 Vichy France, 11  
 VIOLET, 7  
 V-J Day, 12, 69



V-Series Intelligence Card, 243, 251, 259  
 V-TAF-AIR-I Item, 251, 252, 254  
 VULCAN, 7



Wahiawa, Territory of Hawaii, 50  
 Walker, Robert T., 59  
 War Department, U.S., 21  
 Warsaw Pact, 1  
 Washington COMINT Center/s, 75, 170  
 Washington-to-Ladd Field, Alaska, landline, 12  
 Watson, Dr. Robert J., 60

EO 1.4.(c)  
 EO 1.4.(b)  
 PL 86-36/50 USC 3605



EO 1.4.(c)  
 PL 86-36/50 USC 3605

Weisband, William, 172, 184

Wenger, Captain Joseph N., U.S. Navy, 10, 14, 23, 25, 37, 59, 68, 72, 76, 81, 83, 90, 91, 96,  
99, 113, 115, 116, 118, 124, 126, 128, 160, 169, 171, 226, 227, 256, 260

West, Nigel, 17, 26, 27

[Redacted]

White Russian Front Stations, 48

[Redacted]

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605

Winter Harbor, Maine, 14

Wolf, Stephen L., 76, 81, 82, 110, 120, 121, 125-127, 185, 187, 206-208, 213, 216, 217, 238

World War I, 5, 6, 17, 20, 21

World War II, 1, 2, 8, 13, 14, 18-23, 29, 80, 95, 101, 112, 126, 163, 184, 205, 206, 235,  
261-263

Yardley, Herbert O., 9, 10, 21, 24, 27

[Redacted]

EO 1.4.(c)  
PL 86-36/50 USC 3605

Young, Mr., Far Eastern Section, State Department, SPS, 256, 257, 260

[Redacted]

Yuzhno-Sakhalinsk, USSR, 137, 139, 185, 200, 202

[Redacted]

Zeppelin, 21

[Redacted]

Zimmermann telegram, 21

EO 1.4.(c)  
EO 1.4.(b)  
PL 86-36/50 USC 3605





~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~