STUDY PROJECT

SIGNALS INTELLIGENCE SUPPORT TO U.S. MILITARY COMMANDERS: PAST AND PRESENT

BY

PENELOPE S. HORGAN
Department of Defense

USAWC CLASS OF 1991

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

Jnclassified
CURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

a. REPORT SECURITY CLASSIFICATION
Unclassified

1b RESTRICTIVE MARKINGS

a. SECURITY CLASSIFICATION AUTHORITY

3 DISTRIBUTION / AVAILABILITY OF REPORT
Approved for public release.
Distribution is unlimited.

b. DECLASSIFICATION / DOWNGRADING SCHEDULE

PERFORMING ORGANIZATION REPORT NUMBER(S)

5 MONITORING ORGANIZATION REPORT NUMBER(S)

a. NAME OF PERFORMING ORGANIZATION
U.S. Army War College

6b. OFFICE SYMBOL *(If applicable)*

7a. NAME OF MONITORING ORGANIZATION

c. ADDRESS *(City, State, and ZIP Code)*
Carlisle Barracks, PA 17013-5050

7b. ADDRESS *(City, State, and ZIP Code)*

a. NAME OF FUNDING / SPONSORING ORGANIZATION

8b OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

c. ADDRESS *(City, State, and ZIP Code)*

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

1. TITLE *(Include Security Classification)*
Signals Intelligence Support to U.S. Military Commanders:
Past and Present

2. PERSONAL AUTHOR(S)
Horgan, Penelope S.

3a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT *(Year, Month, Day)*	15. PAGE COUNT
Final	FROM _____ TO _____	1991 April 10	164

6. SUPPLEMENTARY NOTATION

7. COSATI CODES			18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
FIELD	GROUP	SUB-GROUP	

9. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

Intelligence, including signals intelligence, support to U.S. military commanders was not a subject covered extensively in the AY91 USAWC curriculum. In an attempt to overcome this shortfall, the USAWC hopes to publish a textbook on strategic intelligence for use in both Course 3 and Advanced Course(s) for AY92.

In order to fulfill the requirement for an unclassified chapter of this book on signals intelligence (SIGINT), this two-part study was produced.

Part One is a case study of SIGINT support to U.S. military commanders during World War II. Although not a complete historical compendium of SIGINT support during the war, these selective vignettes represent a reasonably balanced appraisal of the strengths and weaknesses of that support and some of the lessons learned about intelligence support during SIGINT's infancy.

Part Two represents some of the systemic improvements made, as a result of the lessons learned from World War II experiences, to expedite the flow of SIGINT to military commanders
(continued on reverse)

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS

21 ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL
Mr. D. H. Dearth

22b TELEPHONE *(Include Area Code)*
(717) 245-3921

22c OFFICE SYMBOL
AWCD

D Form 1473, JUN 86 *Previous editions are obsolete*

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

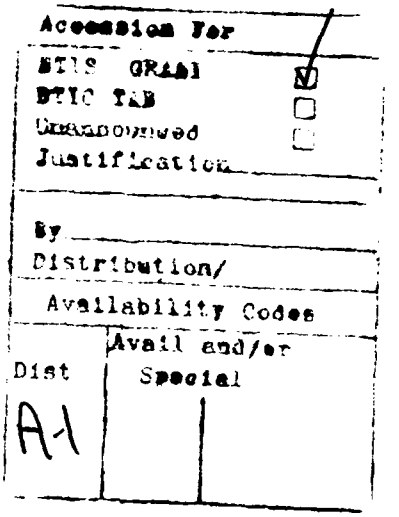
19. ABSTRACT (Continued)

in satisfaction of their requirements. Due to the unclassified text, the paper focuses primarily on the process as opposed to specific results and improvements in tasking, collection, processing, analysis, and reporting within the United States SIGINT System (USSS).

This text advises the U.S. military commander that the USSS is making every effort to provide timely and accurate reporting in a format, periodicity, and at a classification level which will best fulfill consumers' requests at all stages of the conflict continuum in accordance with the Joint Operation Planning and Execution System. To that end, the National Security Agency, the primary intelligence community producer of SIGINT information, was designated a combat support agency in 1988.

The text also provides a caution regarding the fragility of SIGINT, advising against inappropriate disclosures of SIGINT information which could compromise that perishable source. Lastly, the text encourages greater awareness and involvement by the military community in intelligence requirement submission and review, product review and feedback, and threat assessment of the "new international world order".

Much of the information of this text was taken and/or sanitized from previously classified information in an effort to make the SIGINT system more readily accessible to SIGINT consumers. Its contents were approved by the National Security Agency, Fort George G. Meade, Maryland.



USAWC MILITARY STUDIES PROGRAM PAPER

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

SIGNALS INTELLIGENCE SUPPORT TO U.S. MILITARY COMMANDERS: PAST AND PRESENT

by

Penelope S. Horgan
Department of Defense

Douglas H. Dearth
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Penelope S. Horgan

TITLE: Signals Intelligence Support to U.S. Military Commanders: Past and Present

FORMAT: Individual Study Project Intended for Publication as a Military Studies Program (MSP) study project.

DATE 10 April 1991 PAGES: 164 CLASSIFICATION: Unclassified

Signals intelligence (SIGINT) should be an integral part of U.S. military commanders' planning and execution at all levels of the conflict continuum. In order to facilitate a greater understanding of SIGINT support to U.S. military commanders and their operations, this two-part study was produced.

Part One is a case study of SIGINT support to U.S. military commanders, particularly during World War II. Although not a complete historical compendium of SIGINT support, these selective vignettes represent a reasonably balanced appraisal of the strengths and weaknesses of that support and some of the lessons learned about intelligence support during SIGINT's infancy.

Part Two represents some of the systemic improvements made, as a result of the lessons learned from World War II experiences, to expedite the flow of SIGINT to military commanders in satisfaction of their requirements. Due to the unclassified text, the paper focuses primarily on the process as opposed to specific results and improvements in tasking, collection, processing, analysis, and reporting within the United States SIGINT System (USSS).

This text advises the U.S. military commander that the USSS is making every effort to provide timely and accurate reporting in a format, periodicity, and at a classification level which will best fulfill consumers' requests at all stages of the conflict continuum in accordance with the Joint Operation Planning and Execution System. To that end, the National Security Agency, the primary intelligence community producer of SIGINT information, was designated a combat support agency in 1988.

The text also provides a caution regarding the fragility of SIGINT, advising against inappropriate disclosures of SIGINT information which could compromise that perishable source. Lastly, the text encourages greater awareness and involvement by the military community in intelligence requirement submission and review, product review and feedback, and threat assessment of the "new international world order".

Much of the information of this text was taken and/or sanitized from previously classified information in an effort to make the SIGINT system more readily accessible to SIGINT consumers. Its contents were approved by the National Security Agency, Fort George G. Meade, Maryland.

"In grateful appreciation to the men and women of

the National Security Agency

who have devoted their lives

to the service of their nation."

Ronald Reagan, President of the United States,
during a dedication ceremony of a new facility at
the National Security Agency, September 1986

TABLE OF CONTENTS

INTRODUCTION

Throughout history, rulers and military commanders have sought information on their adversaries, wanting to know their strengths, weaknesses, and intentions. Those leaders with such foreknowledge were thought to have the advantage, especially when opposing sides resorted to war to resolve their differences. Chinese strategist Sun Tzu extolled the value of "intelligence" in his martial classic 'Art of War':

> "Now the reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge."[1]

> "What is called 'foreknowledge' cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation."[2]

Carl von Clausewitz stated in Book One, Chapter Six of his On War that "Many intelligence reports in war are contradictory; even more are false, and most are uncertain. ... In short, most intelligence is false, and the effect of fear is to multiply lies and inaccuracies."[3] Regardless of how pessimistic von Clausewitz could be regarding the value of the intelligence received by 19th Century military commanders, he admitted that there was, indeed, a need for intelligence:

> "Finally, the general unreliability of all information presents a special problem in war; all action takes place, so to speak, in a kind of twilight, which, like fog or moonlight, often tends to make things seem grotesque and larger than they really are."
>
> "Whatever is hidden from full view in this feeble light has to be guessed at by lay talent, or simply left to chance. So once again for lack of objective knowledge, one

has to trust to talent or to luck."[4]

Dr. R.V. Jones, one of Britain's foremost scientists and head of British Scientific Intelligence during World War II, has suggested that "the ultimate object of Intelligence is to enable action to be optiimized."[5] Renown intelligence specialist Sherman Kent claimed that:

> "Intelligence means knowledge. ... the kind of knowledge our state must possess in order to assure itself that its cause will not suffer nor its undertakings fail because its statesmen and soldiers plan and act in ignorance."[6]

Michael Handel, one of the co-founding editors of the journal Intelligence and National Security, has examined leaders' use of intelligence to determine that:

> "The proper use of accurate, timely intelligence can significantly reduce uncertainty, thereby enabling political and military leaders to improve the quality of their decisions, develop more effective strategies, or conduct more successful military operations. The information provided by intelligence is thus only a means to an end - an instrument essential for the attainment of a leader's goals in the most efficient way."[7]

The birth of American intelligence began with the nation's quest for independence. George Washington can be considered the Father of American intelligence. Appalled by the poor intelligence he received as a militia officer with the British during the French and Indian Wars (1755-1763), Washington avowed that no man under his command would die because of intelligence failures. Consequently, several secret intelligence organizations were formed during the Revolutionary War. The Committee of Secret Correspondence was formed in 1775 as an intelligence arm of

the Continental Congress. Its five members included such noted statesmen as Benjamin Franklin, Benjamin Harrison, John Jay, John Dickinson, and Thomas Johnson. The Committee was later joined by James Lovell, a cryptologic expert who encrypted American colonial messages and decrypted British codes and ciphers. In this manner, Washington was able to provide his forces the intelligence they needed to defeat numerically-superior British military and naval forces. In 1777, Washington wrote to a friend:

> "The necessity of procuring good intelligence is apparent and need not be further urged. All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, Success depends in most Enterprises of the kind, and for want of it, they are generally defeated, however well planned and promising a favourable issue."[8]

From its beginning then, American intelligence has been shrouded in secrecy and perceived as an adjunct of military operations. The invention of electric telegraphy in the 1830's greatly increased the ability to acquire information on nations' political intentions and war plans. The art of intercepting these communications and exploiting them for strategic, operational, and tactical purposes has been termed "signals intelligence" or SIGINT.

The use and exploitation of telegraphic communications was in its infancy during the Civil War and the Spanish-American Wars. However, with the growth of wireless radio technology in World Wars I and II, there was a burgeoning of SIGINT collection, processing, and analysis in support of military commanders. For example, in World War II, SIGINT communications yielded the lucrative solutions and decryption of German and Japanese ciphers and codes, making their communications centers of gravity for

these nations and giving American military commanders previously unimagined advantages in their campaign planning.

The tremendous asset of SIGINT during the Cold War was praised by former CIA Director Allan Dulles when he claimed that it was "the best and 'hottest' intelligence that one government can hope to gather about another."[9] The SIGINT source of information and the methodolgy for processing that information is, understandably, highly protected.

It is the intent of this paper to unravel some of the myth and mystery about signals intelligence and the uniqueness of that intelligence source. This paper will also detail the process of tasking the United States SIGINT System (USSS), the flexibility of SIGINT's response, and various types of SIGINT product. The purpose of SIGINT is to fulfill the strategic, operational, and tactical intelligence needs of U.S. military commanders for planning, targeting, deception, command and control communications counter-measures (C3CM) and electronic warfare (EW), special operations, and weaponeering, throughout the conflict continuum. This type of SIGINT support is depicted in Figure 30. Signals intelligence supports joint operations, in accordance with JCS Pub 3-0; however, this chapter will primarily address SIGINT support of the Army. Further, it must be emphasized that the Department of Defense is just one, albeit a very important, consumer of SIGINT information. Other Executive Branch departments and agencies levy specific, and sometimes competing, reporting requirements upon finite SIGINT resources.

The first part of this paper highlights selective vignettes of SIGINT successes and support to military commanders, particularly during

World War II. The details of SIGINT support during that conflict have been declassified in recent years, with many of the key producers and consumers of that intelligence revealing the process, potential, and problems associated with support to strategic, operational, and tactical-level commanders. World War II support will be used as a framework to examine the lessons learned for improvement of the process in the 1990s.

By no means is this limited historical review a complete chronology of the war. Nor is its intent merely to extol the value of signals intelligence, thereby giving that discipline undue credit in the overall war effort. Bold, decisive, and informed military commanders won World War II; signals intelligence, however, had an important supporting role. These historical vignettes are simply meant to be illustrative, because current SIGINT support to military commanders cannot be discussed in such great detail in an unclassified document. Nevertheless, the process in place today produces even more timely intelligence information, thereby serving as an invaluable tool for the formulation of political strategy and military plans. However, the ability and inclination of the leader to use this tool have always been, and are still, the determining factor of its utility.

The second part of this paper will examine: the organizations responsible for the collection, analysis, and production of SIGINT; the role of the National Security Agency (NSA) within the Defense Department and the Intelligence Community; and the Executive and Legislative Branches' oversight of NSA. The chapter also will provide an overview of the procedures for requesting signals intelligence support and the types of

SIGINT provided today to military commanders in accordance with the deliberate and crisis action planning procedures of the Joint Operations Planning and Execution System (JOPES). NSA's designation in 1988 as a Combat Support Agency is also examined.

This paper will also discuss the fragility of the SIGINT source as a caution to SIGINT consumers about its potential perishability and the dangers of compromising sensitive sources and methods.

COMPONENTS OF SIGNALS INTELLIGENCE

Signals intelligence (SIGINT) is that category of intelligence information which comprises, either individually or in combination, all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), regardless of the means by which signals are transmitted.

COMMUNICATIONS INTELLIGENCE (COMINT)

COMINT is technical and intelligence information derived from exploitation of foreign communications by other than the intended recipient. COMINT is produced by the collection and processing of foreign communications passed by electromagnetic means and by the processing of foreign encrypted communications, however transmitted. Collection comprises search, intercept, and direction finding. Processing comprises range estimation, transmitter/operator identification, signals analysis, traffic analysis, cryptanalysis, decryption, study of unencrypted (plaintext) communications, the fusion of these processes, and the reporting of the results. COMINT does not include intercept and processing of press, propaganda, and other public broadcasts except for processing of encrypted or possible "hidden meaning" messages in those broadcasts.[10]

Concealment of communications from persons other than the intended recipients is usually accomplished by the use of codes and ciphers. Plaintext communications are encoded or enciphered by the sender to disguise their contents. The secret text or cryptogram must then be decoded or deciphered by the recipient. This process is accomplished through crypto-

graphers; the art is known as cryptography. Both the sending and receiving cryptographers must have an understanding of the procedures and devices and how these procedures and the crypto devices were used. The "what and how" of the process is known as the key. The key may consist of a set of rules, alphabets, or procedures; an ordinary book or a specialized code book may be the source of the keys. Cryptanalysis is the art of breaking or solving codes and ciphers without the key applied to the communications to alter their contents. The encryption systems are recovered for application against additional messages which may have been encrypted in the same or similar way. The plaintext is recovered for its potential intelligence value. Cryptography and cryptanalysis -- popularly termed code making and code breaking -- make up cryptology.[11]

Transformation of an unencrypted (plaintext) message into an encrypted message (cipher text) typically requires the use of a system or a set of mathematical procedures and a key which, for secure communications, should be known only to the transmitter and the legitimate recipient of the communication. In the encryption process, the same system or set of procedures is applied to the plaintext information and the key is employed to control how the information is encrypted. The inverse is true for the decryption process. The authorized recipient recovers the concealed information from the cipher by applying to the cryptogram the key or keys, usually in a reverse order.[12] Cipher systems use a process of transposition or substitution or a combination of both for securing communications in which the encryption is carried out on single characters or groups of characters without regard to their meanings.

Code systems are a specialized form of substitution in which the cryptographer may also replace single characters where necessary (through

a syllabary); however, the more frequent replacement is for syllables, words, phrases, and even whole sentences. Code systems employ code books which contain code groups for a large number of words and phrases in a specialized vocabulary (e.g., military operations terminology). Each plaintext meaning has its own code group, usually comprised of four or five digits or letters. Code books also include syllabary groups so cryptographers can encode groups that do not already have values in the code book.[13] Some code systems are further encrypted by a cipher system. This second encryption process, known as superencipherment or superencryption, is generally thought to be more secure.

Other communications intelligence information can be derived through the analysis of "communications externals" -- that part of message externals that deal with the sender, recipient, and manner of transmission of the communication. Using the analogy of a letter, communications externals pertain to that information which can be gleaned from studying the outside of the envelope. Therefore, even if the encrypted message inside the envelope cannot be read/understood, the communications externals enable the analyst to discern some things about the sender and recipient. In the case of military radio communications, such things as callsign and callwords, call up procedures among operators, chatter among operators, frequencies, message schedules of transmission, message serialization, message precedence, routing information (indicating where a message is to be sent), the crypt system key setting indicators, and other communications procedures are analyzed to determine communication net organization, traffic patterns, order of battle (type and organization), location, urgency, and the purpose of and the volume of the communication.[14] The study of communications externals is called

traffic analysis.

ELECTRONIC INTELLIGENCE (ELINT)

ELINT is technical and intelligence information derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonation or radioactive sources. ELINT is produced by the collection (observation and recording) and processing of these signals for intelligence purposes.[15] It does not include information derived from friendly radars or nuclear radiation. ELINT is divided into two sub-categories:

Operational ELINT (OPELINT) is the timely, high-priority electronic intelligence used to satisfy indications and warning (I&W) parameters and current intelligence requirements. OPELINT is also used to update a number of major intelligence data bases, including the Electronic Order of Battle (EOB) and the ELINT Parameters List. Specifically, OPELINT reporting meets the requirements of users who desire parametric data in machine-readable format to support electronic warfare (EW) applications or automatic processing or display routines on particular signals of interest. This is called OPELINT Data Forwarding. Other substantive, narrative OPELINT may be presented in the form of Tactical Reports (TACREP) reporting.[16]

Technical ELINT (TECHELINT) is concerned with signals characteristics, capabilities, functions, associations, limitations and performance, and the technology of foreign communications electronic systems. TECHELINT is used to identify the specific parametric values of non-communications emitters that are needed to estimate their primary functions, capabilities, modes of operation (including malfunctions), and their specific roles within a complex weapons system or defense network.[17]

FOREIGN INSTRUMENTATION SIGNALS INTELLIGENCE (FISINT)

Foreign Instrumentation Signals Intelligence (FISINT) is intelligence information derived from electromagnetic emissions associated with the measurement of the performance, testing, and operational deployment of non-U.S. aerospace, surface, and sub-surface systems which might have either civilian or military application. It includes but is not limited to signals from telemetry, beaconry, electronic interrogators, tracking/fusing/arming/command systems, certain video data links, and signals transmitted to and from earth satellite vehicles.[18] By analyzing each signal, information is developed about the emitter and its user. Integration of this information with that from other resources provides accurate targeting data and a basis for determining enemy intentions.[19]

HISTORICAL PERSPECTIVE OF SIGINT

WORLD WAR I AND BETWEEN THE WARS

Exploitation of military SIGINT came of age in World War I because of increased radio usage and increased cryptographic and cryptanalytic efforts. Germany experimented with a variety of ciphers and codes; it is said that virtually every cryptographic system of that time was used during the war. Cryptography and its impact on national-level decision making is probably best remembered during World War I for the British interception and decoding of the infamous Zimmermann telegram.

The German Foreign Minister, Arthur Zimmermann, sent a telegram to the German Ambassador to the U.S. on 16 January 1917 for retransmission to the German Ambassador to Mexico, proposing that Mexico could regain the "lost territory" of Texas, New Mexico, and Arizona if it would wage war against the United States. (see Figure 1) British "Room 40 O.B.", the British Naval SIGINT organization, succeeded in solving the cryptogram and contrived a means of passing the information to President Wilson, who made its contents public (without compromising the British success). The U.S. entered World War I for a variety of reasons; however, the outrage among the American people at the public disclosure of the Zimmermann telegram on 1 March 1917 certainly was a contributing factor[20], as the British intended.

The German proposal to Mexico so inflamed the U.S. because Mexican instability had been a primary U.S. concern since 1910, when a revolution rocked that country. By 1916, an American Punitive Expedition, under BGEN John J. Pershing, was sent to Mexico in an attempt to capture renegade leader Francisco "Pancho" Villa after his raid on Columbus, New Mexico.

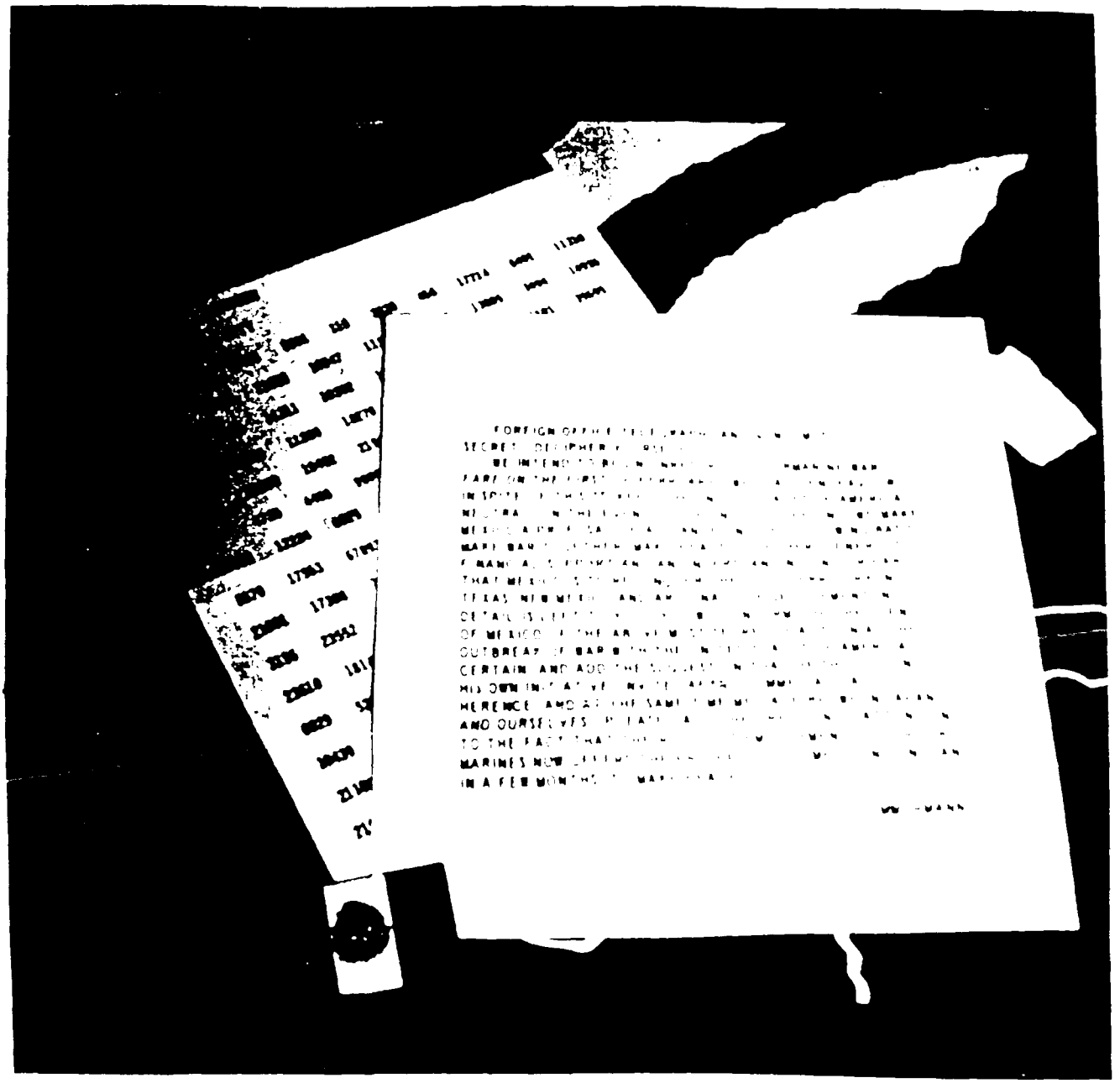


Figure 1

Encrypted and decrypted version of the Zimmermann telegram. Reprinted with permission of the Cryptologic History Office, National Security Agency

The U.S. Army's Military Intelligence Division (MID) assisted radio intelligence units, which had deployed to Mexico along with their mobile "radio tractors". Intelligence support to these forces included interception and goniometery, known currently as radio direction finding (RDF). In 1918, MID created the Radio Intelligence Service for operations along the Mexican border to monitor German diplomatic and agent activity.[21] (see Figure 2)

After the U.S. entry in World War I, MID Signal Corps intercept stations in the European theater provided intelligence support to U.S. military commanders of the American Expeditionary Force (AEF). Intercepted traffic was passed to radio intelligence units located within the two U.S. AEF field armies and General Headquarters where cryptanalysts and traffic analysts attempted to glean usable intelligence from message externals and message contents. Moreover, goniometric RDF was used to locate enemy positions.[22] (see Figure 2)

In 1918, MID established a Cipher Bureau (MI-8) under a former State Department code clerk, Herbert O. Yardley. Yardley's MI-8 worked closely with its British and French counterparts and broke a German agent cipher that led to the arrest of the only German spy to receive a death sentence in the U.S. during World War I.[23] When demobilization threatened to terminate MI-8's work, Yardley's operations were transferred to New York City, where they were jointly and covertly funded by the War and State Departments as America's "Black Chamber", a tiny, all civilian effort.

After World War I, diplomatic communications were a primary concern of a peacetime MI-8. The "Black Chamber's" greatest success for national policy makers was realized by the time of the 1921 Washington Conference

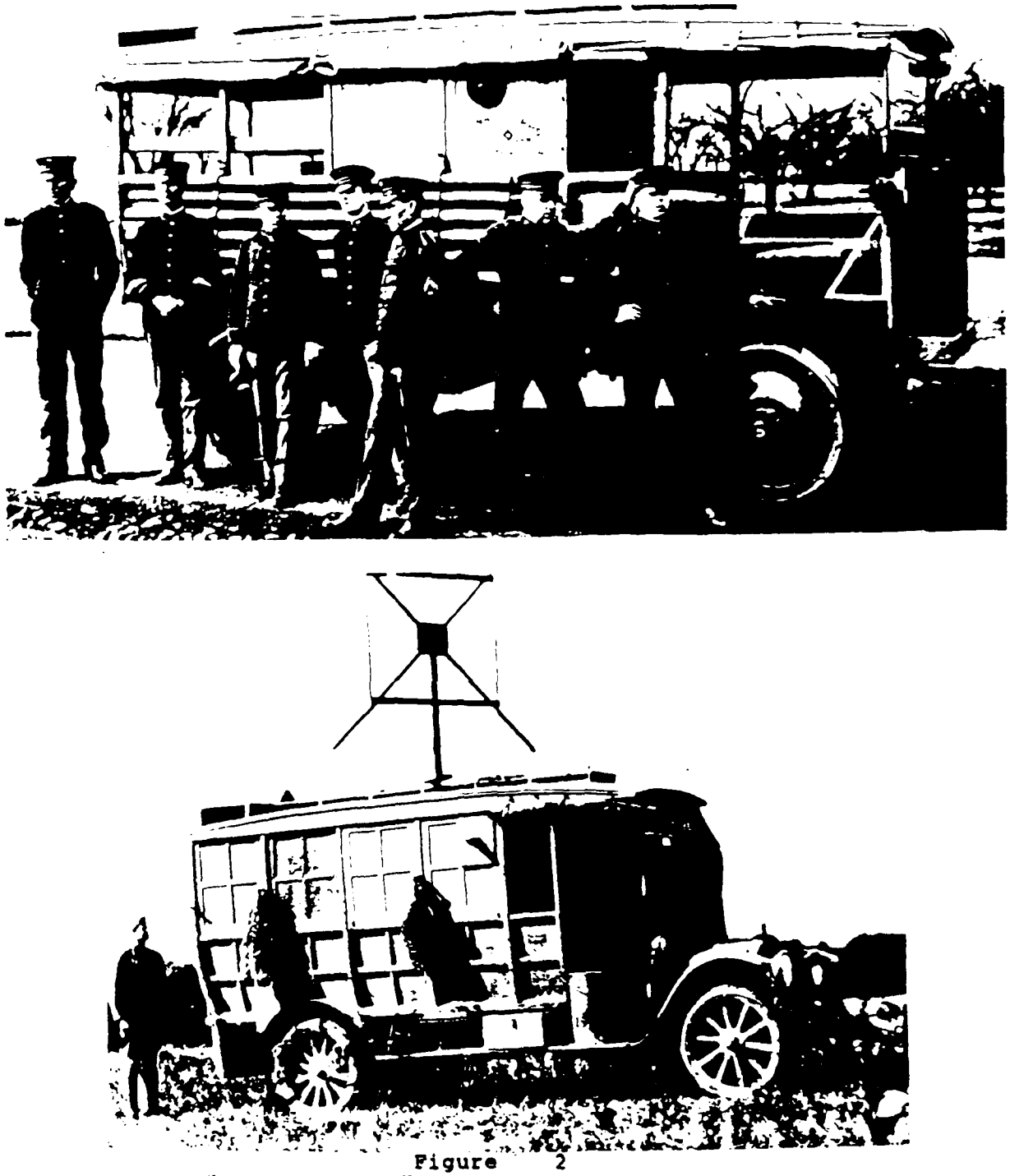


Figure 2
Signal Corps "radio tractor" which accompanied Pershing Expedition to Mexico, 1917 (top)
Radio van used for goniometric radio direction finding Verdun, France, 1918 (bottom)
John P. Finnegan, Military Intelligence: a Picture History, pp. 14 and 34.
Reprinted with the permission of U.S. Army Intelligence and Security Command History Office

on Naval Armament, when Yardley was able to provide U.S. representatives with the negotiating position of the Japanese. Successful decryption of Japanese diplomatic codes enabled the U.S. negotiators to hold steadfast to their positions, having read their counterpart's instructions.[24]

When Henry Stimson became Secretary of State in the Hoover Administration and learned of the "Black Chamber", he withdrew State funding on the principle that "Gentlemen do not read other gentlemen's mail." Moreover, the Army decided to absorb cryptanalytic functions into the Signal Corps, which was already in charge of Army cryptographic activities. In October 1929, William F. Friedman, who had provided tactical intelligence support to the AEF in France, was sent to New York to transfer Yardley's files to Washington, marking the beginning of Friedman's ascendancy as head of the Signals Intelligence Service (SIS).[25] A decade later, as Secretary of War under President Roosevelt, Stimson, ironically, was a principal beneficiary of these earlier cryptanalytic successes.

The Navy's cryptanalytic efforts, following a modest initial effort in World War I, reappeared in 1924 as the "Research Desk" under Commander Laurance Stafford in the Code and Signal Section, OP-20-G, within the Office of Naval Communications. While its emphasis was on communications security, OP-20-G developed radio intercept, RDF, traffic analytic, and cryptanalytic processing capabilities prior to World War II. The primary focus of the Navy's effort was against the Japanese fleet, especially its naval exercises. Some of this information was intercepted by shipborne collectors who shadowed the Japanese fleets. During this time, the Navy provided extensive Japanese language training to some of its enlisted personnel and officer corps as it was concerned about the growing Japanese

naval capability.[26] Prior to the U.S. entry into World War II, the U.S. and the British Royal Navies also cooperated in German naval communications' exploitation.[27]

One of America's premier cryptologists, William F. Friedman, described the 27-year period between the end of World War I and end of World War II as follows:

> "The most significant events during that quarter of a century were directly concerned, firstly, with the advances made in the production of more complex mechanical, electrical, and electronic cryptographic apparatus and, secondly, with the concomitant advances in the production of more sophisticated cryptanalytic apparatus in order to speed up or to make possible the solution of enemy communications produced by these increasingly complex cryptographic machines."[28]

During the period between the wars, Germany started using extensively the ENIGMA machine, a small, compact, battery-powered electromechanical enciphering device. (see Figure 3) Polish cryptanalysts -- working with the French SIGINT service and aided by their purchase of a commercial variant of the ENIGMA machine -- succeeded in decrypting messages encrypted on the German Army ENIGMA device. By the summer of 1939, they could read only some of the ENIGMA traffic because the Germans kept modifying the settings of this enciphering device. Before Poland was overrun later that year, its cryptanalysts turned over their work to the British and French, as well as copies of the German machine, which Polish cryptanalysts had reverse-engineered. Also, the Poles relinquished the plans for a "bombe" -- six ENIGMA machines wired together which, in two hours, could test every possible ENIGMA plug and setting combination. In essence, the bombe was the fore-runner of a modern computer which attempted to parallel the encryption process.[29]

Figure 3

Three-rotor ENIGMA encryption device
Reprinted with permission of the Cryptologic History Office,
National Security Agency

ENIGMA machines were used to some degree by German government officials and extensively by all branches of the Armed Forces, with estimates of the number of the devices ranging from between 30,000 and 100,000.[30] Over ENIGMA, the German High Command issued strategic commands and personal messages to field commanders. The German Air Force encrypted its daily aircraft maintenance and unit status reports. The German Navy used ENIGMA for contacting its forces afloat while the German Army issued orders and filed troop disposition reports. The three-rotored machine used by the German ground forces, for example, permitted 1,560,000 permutations for each encrypted character. Additional security was provided by daily-changing keys and a plugboard which further scrambled each letter which was being encrypted.[31] (see Figure 4)

BLETCHLEY PARK AND ULTRA

The British, building on the Polish work against ENIGMA, centralized their SIGINT activities under the Government Code and Cypher School (GCCS), which moved in 1939 to Bletchley Park, an old manor house in the English countryside, where some of the country's top mathematicians focused on breaking high-grade ciphers and codes. The success against the ENIGMA was dependent upon the invention and manufacture of high-speed prototype computers or bombe's. The bombe enabled analysts to discern the transmitting and receiving ENIGMA rotor settings so that an enciphered message could be converted into plaintext. Material derived from cryptanalytic exploitation of ENIGMA machines was codenamed ULTRA. ULTRA or "special intelligence" messages were disseminated from GCCS to a very limited audience; however, key decision makers were given access. For example, decrypted German naval messages were passed to the Navy's Opera-

Figure 4

German soldiers using ENIGMA machine.
Reprinted with the permission of the Cryptologic History Office,
National Security Agency

tional Intelligence Center (OIC), commanders in the Admiralty, the Royal Air Force (RAF) Coastal Command, and ships at sea. SIGINT related to Air and Army activities were passed to Special Liaison Units (SLU)s attached to field elements of the RAF and the British Army by Bletchley Park.[32]

A critical part of the Bletchley Park success story was the network of intercept stations which ringed the Axis powers, collecting ENIGMA messages. Known as the "Y-Service", these stations in England, North Africa, and the Middle East, sent their high-grade manual Morse ENIGMA intercept to three centers in England -- one for German Army, Navy, and Air Force communications -- for ultimate passage to Bletchley Park for decryption.[33] Bletchley Park, in turn, provided to these stations guidance on codes, callsigns, orders of battle, and signals operating instructions to assist their collection efforts.

Thousands of Y-Service collectors and linguists, working 24 hours a day in 3 shifts in England and worldwide, also intercepted very high frequency, jargon-filled unenciphered or low- and medium-grade enciphered German, Italian, and French communications. These communications yielded tactical intelligence from lower-echelon military commanders; air-to-air and air-to-ground fighter, bomber, and fighter bomber communications; ground-to ground communications; weather reports; reconnaissance information; and calls for air and sea rescue. Moreover, the Y-Service was able to perform RDF and limited traffic and cryptanalysis.[34] By the 1940's then, an intelligence system was in place to provide SIGINT support to British military commanders, not unlike the U.S. system which will be detailed later in this paper. Churchill called this lucrative information "my golden eggs" and the cryptanalysts who provided it "the geese who laid the golden eggs and never cackled."[35]

BATTLE OF BRITAIN AND THE BLITZ

Examples of how British SIGINT "headquarters" and "field" units worked together in support of military commanders was evident in August 1940 during the Battle of Britain. Historians can and have questioned the degree of success which should be accredited to SIGINT during the German bombing campaign. However, one thing is undeniably clear: advance warning of German Air Force intentions enabled Air-Chief Marshal Hugh Dowding to preposition his forces and devise a strategy for his response.

When Air Marshal Goering launched his Luftwaffe against Great Britain on "Eagle Day" (Operation ADLERTAG), 13 August 1940, his British opposite number knew the Luftwaffe's order of battle and Goering's plan. That strategy had been provided in 8 August instructions to Goering's three Air Fleets; this ULTRA message was intercepted, decrypted, and provided to Prime Minister Churchill and Air-Chief-Marshal Dowding.[32] Since this was an entire week before the attack, ULTRA enabled Dowding to distribute his aircraft to defend the seven airfields identified as targets, according to Harold Deutsch.[36] Although air attacks were not new to Britain, the commitment of the Fifth Fleet, stationed in southern Norway and northern Denmark, was supposed to be a complete surprise to the British. Due to ULTRA, it was not. (see Figure 5)

During the Battle of Britain, Y-Service monitored the voluminous amounts of German Air Force air-to-air and air-to-ground unencrypted traffic, passing this information along to higher headquarters. Moreover, intercepting the air-to-air communications of these aircraft during a shoot-down enabled Y-Service operators to alert British air-sea rescue to the

Figure 5

Luftwaffe Fleets and RAF Fighter Command Groups
Map of Battle of Britain and the Blitz
Simon Goodenough, War Maps, p. 23.
Reprinted with permission of St. Martin's Press, New York

last known German location, if it had been passed in the clear, so that the RAF might get to the downed pilot before the Germans did.[37]

The Battle of Britain was at its height between 7 and 15 September 1940. On the 15th, Goering could use only the Second and Third Luftwaffe Fleets during his aerial attacks against Britain; however, he dispatched every available aircraft -- 328 bombers and 769 fighters. Again, forewarned about the attack by Bletchley Park, Dowding sent up about 300 Hurricanes and Spitfires to engage the first wave. Surprised at the large number of enemy fighters, the first wave of Luftwaffe aircraft dropped its bombs and turned back to Germany. The British fighters returned to their airfields, refueled, and launched to meet the second wave. The attack ended with 56 German aircraft lost, as compared to 27 lost British fighters. After 15 September, the momentum of the German air war shifted. By mid-October, Bletchley Park informed the government that Hitler had indefinitely postponed the invasion of England (Operation SEALION) and the daylight bombing of England ceased. The night-time attacks against Britain (the Blitz) continued, however, with Germany making full use of its KNICKEBEIN beam system to guide bombers to their targets.[38]

KNICKEBEIN was a radio beam directed at a target in England along which German bombers flew. When the pilot switched on the KNICKEBEIN receiver in his aircraft, he would hear a continuous signal or "equisignal", produced at the intersection of the two beams. If the pilot deviated from this signal, he would hear "dots" (pulsed by one beam) or "dashes" (pulsed by the other beam). He would then have to change course until he again picked up the equisignal. Another intersecting beam, which would give off a different sound in the pilot's earphones, would cross

the equisignal at the time when the pilot was to release his bombs.[39]

Dr. R.V. Jones of the RAF Air Staff was able to figure out a way to jam these directional signals. The first jammers transmitted a "mush of noise" on the KNICKEBEIN frequencies. A second type of jammer transmitted a dash sounding very much like the KNICKEBEIN dash which it superimposed on the equisignal. This additional signal caused the pilot to take corrective measures because he thought that he had strayed off course.[40] As the air war continued, the pilots became more confused. Between 7 September and 13 November 1940, London was bombed every night (except one) by usually 160 bombers. However, "a substantial proportion of bombs went astray" because of the active jamming operations.[41]

R.V. Jones' initial breakthroughs stemmed from his earlier work with Bletchley Park decrypts. As the air war continued, Jones' jamming techniques worked hand-in-hand with the Y-Service, according to accounts by Jones and Aileen Clayton, a Y-Service operator. For example, the operator would intercept German messages during the day which would lay out the KNICKEBEIN settings for the night. Then, they intercepted the Luftwaffe pilots as they took off on their bombing raids in the evenings and determined their locations through radio direction finding. Fighter Command then correlated the SIGINT information with its radar plots and the RAF jamming operation was underway. Ultimately, the jamming took its toll, undermining the Luftwaffe pilots' confidence. Clayton heard their exasperation as they switched from frequency to frequency, trying to elude the jammers.[42]

If KNICKEBEIN was Phase One of the "Battle of the Beams", another beam system -- X-GERAET -- became Phase Two. In September 1940, a Bletch-

ley Park decrypt described a beam that was no wider than 20 yards at a distance of 200 miles, designed to be used in conjunction with a KGr-100 aircraft. With the X-Beam system, a "director beam" was aimed at the target. This beam was then crossed by a "fore signal" at 20 kilometers from the target and a "main signal" at 5 kilometers from the target. Shortly thereafter, bombs were released.[43]

Working with Bletchley Park cryptanalysts, Jones and his colleagues, by late 1940, were able to provide to the jammers from SIGINT the specifics of the attacks -- place, time, the ground speed of bombers, the line of approach within 100 yards, and the bombers' altitude -- at least one out of every three days. This incredibly specific information was not enough to halt the bombing attacks, however. X-Beam stations had become so proficient at setting and resetting the beams that the bombers could conduct two attacks in one night. Birmingham, Coventry, and Liverpool were bombed during November 1940.[44] This precarious situation lasted for only a few months, however.

By January 1941, Phase Three of the "Battle of the Beams" was initiated because the X-Beam System had been rendered ineffective by jamming. The new beam, designated the Y-Beam system, involved a beam plus a ranging system. In the Y-Beam system, the position of a target was given to only one station whose mission was to direct the KG-26 aircraft to the target. However, Jones and his colleagues learned to thwart this system as well. Although the Blitz did not end until May 1941, by February, the "Battle of the Beams" was as good as won. According to Jones:

> "...all three major German systems, KNICKEBEIN and X and Y, were defeated. Many bombs therefore

> went astray, often attracted by the decoy fires that were now part of the countermeasure programme. Moreover our fore-knowledge of the German targets was at last beginning to result in the destruction of their bombers, as our nightfighters were becoming equipped with good airborne radar and as our ground controlled interception technique improved to the extent where they could now effectively hunt along the beams. With the last major raids of April and May 1941, the Luftwaffe was therefore not only tending to miss its targets, but it was beginning to encounter losses on a potentially prohibitive scale."[45]

BATTLE OF THE ATLANTIC

The British were challenged on the sea as well as in the air. After England declared war on Germany in September 1939, German battleships, battle cruisers, submarines, and bombers relentlessly attacked convoys carrying much-needed war materiel across the Atlantic. At the war's beginning, the Germans introduced two more spare rotors to the ENIGMA, making it impossible for Bletchley Park to break naval messages in spite of captured documentation and a captured machine. Fortunately, German Admiral Doenitz, concerned over the losses incurred during single submarine attacks, concluded that the tactic of using submarines singly must be changed. Consequently, flotilla operations or "wolf pack" movements were instituted, which required greater communication among German U-boats. The increased radio traffic improved the amount of naval communications available for British analysis for direction finding and cryptanalysis.[46]

A major breakthrough occurred in February 1941 when a captured German trawler provided more documentation and the two spare rotors. By March, the first deciphered naval signal was sent through the ULTRA net. Messages dealt with submarines and convoys and great capital ships

such as the BISMARCK. In May 1941, the British captured another trawler and recovered ENIGMA instructions and keys. This was followed by the capture of an intact ENIGMA, the spare rotors, the daily keys, documents explaining the crypto settings, and actual enciphered material. These recoveries, unknown by the Germans, were instrumental in breaking the German navy's ENIGMA M.[47]

By May 1941, ULTRA revealed that the German battleship BISMARCK was leaving Gdynia and moving toward Greenland. However, the flotilla of warships, destroyers, and escort vessels maintained virtual radio silence. Consequently, the Admiralty did not know the whereabouts of the convoy. (see Figure 6) Dispatching the fast cruiser HOOD, the newly-commissioned PRINCE OF WALES, six destroyers, and the cruisers SUFFOLK and NORFOLK, the Admiralty hoped to find the flotilla. An almost chance encounter occurred which resulted in the sinking of the HOOD and the damaging of the BISMARCK and the PRINCE OF WALES on 24 May 1941. Also, the British dispatched an aircraft carrier, a battleship, and a cruiser from Gilbraltar to intercept the BISMARCK before it could get to the Atlantic. Spain's warning message to Germany about the British deployment from Gilbraltar was decrypted by Bletchley Park.[48]

Further, Luftwaffe communications revealed that the BISMARCK's new destination was Brest, France, where the vessel was to undergo repairs. Direction finding, which had had some difficulty in locating the BISMARCK earlier on, became the key to pinpointing and tracking the ship's movements. A torpedo aircraft from the Gilbraltar-based aircraft carrier attacked the BISMARCK, causing her to lose maneuverability. Followup shelling and torpedo fire resulted in the sinking of the BISMARCK, 27 May 1941. According to Admiral Tovey, Commander-in-Chief, Home Fleet:

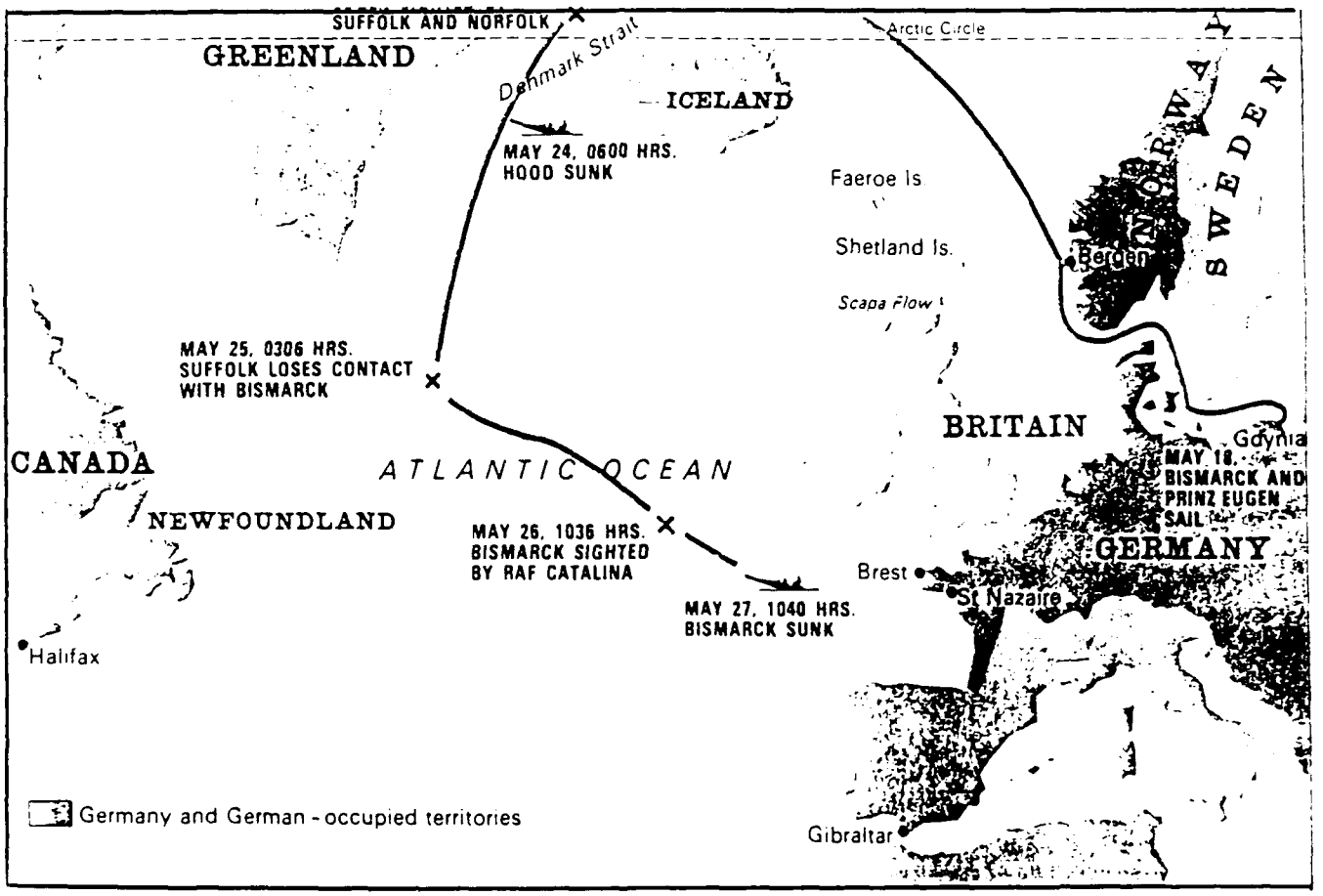


Figure 6

Route of the BISMARCK
Simon Goodenough, War Maps, p. 28.
Reprinted with the permission of St. Martin's Press, New York

> "The accuracy of the information supplied by the Admiralty and the speed with which it was passed were remarkable; and the balance struck between information and instruction passed to the forces out of visual touch with me was ideal."[49]

In the Atlantic, the year 1942 began well for the Allies. According to Beesly, all sources of intelligence were operating with great speed and efficiency. However, on 1 February, the Germans introduced a new crypt system with new keys, TRITON, for submarines on long-range operations. Bletchley Park had great difficulty with these changes and shipping losses in the Atlantic rose alarmingly. Consequently, intelligence from direction finding, aerial photography, and air and ship sightings provided the bulk of support to naval operations during most of 1942.[50]

In December 1942, Bletchley Park broke the secret of the TRITON crypt system. Just when Allied shipping losses started going down, in March 1943, the Germans made still another change to their ENIMGA M, which rendered German naval communications unreadable. This again meant that Allied shipping losses increased. (For example, losses in February 1943 were 360,000 tons; in March, they were 630,000 tons.) Bletchley Park responded to the challenge and, by May 1943, German submarine losses began to increase. On 24 May 1943, Admiral Doenitz ordered the submarines to withdraw from the Atlantic convoy routes. Engagements at sea continued until the end of the war but the "Battle of the Atlantic" was, for all intents and purposes, over. According to Beesly, without Special Intelligence, "the victory might not have been achieved until much later and at far greater cost."[51]

British difficulty in reading German naval communications for 10 months hindered intelligence support to the U.S. Navy as well. Conse-

quently, the Navy's OP-20-G acquired funding to start building its own high-speed bombe to work the difficult naval problem. The Navy's bombes (or bombe deck) were available for production in 1943; they required a large facility with hundreds of operators, usually WAVES.[52] A portion of a U.S. bombe and one operator can be seen in Figure 7.

BRITISH AND U.S. SIGINT COOPERATION

The U.S. Army contingent in Europe, known as a Special Observers Group, was deployed to England six months prior to Pearl Harbor. When the U.S. entered the war in Europe, American and British units began producing SIGINT, either jointly or separately, which they provided to the armed forces of both countries for use either combined or individual military actions. As previously noted, both the British and the Americans had SIGINT organizations with headquarters in their capitals supported by intercept stations throughout their own countries and other nations. The British service was centralized under the Government Codes and Cyphers School near London, with each service maintaining its own service SIGINT organization. The U.S. had no central headquarters. Each service conducted its own, though often times coordinated, SIGINT operations.[53]

Winston Churchill took a personal interest in Anglo-American SIGINT collaboration. He saw to it that ULTRA intelligence was passed to President Roosevelt even before the Japanese attacked Pearl Harbor, personally earmarking specific messages for Roosevelt's attention. After Pearl Harbor, Churchill, himself, provided Eisenhower with a briefing on ULTRA following the general's June 1942 deployment to England as the Commander-in-Chief of U.S. forces. In 1943, the U.S. and Britain formed the BRUSA SIGINT alliance, designed to foster SIGINT collaboration.[54]

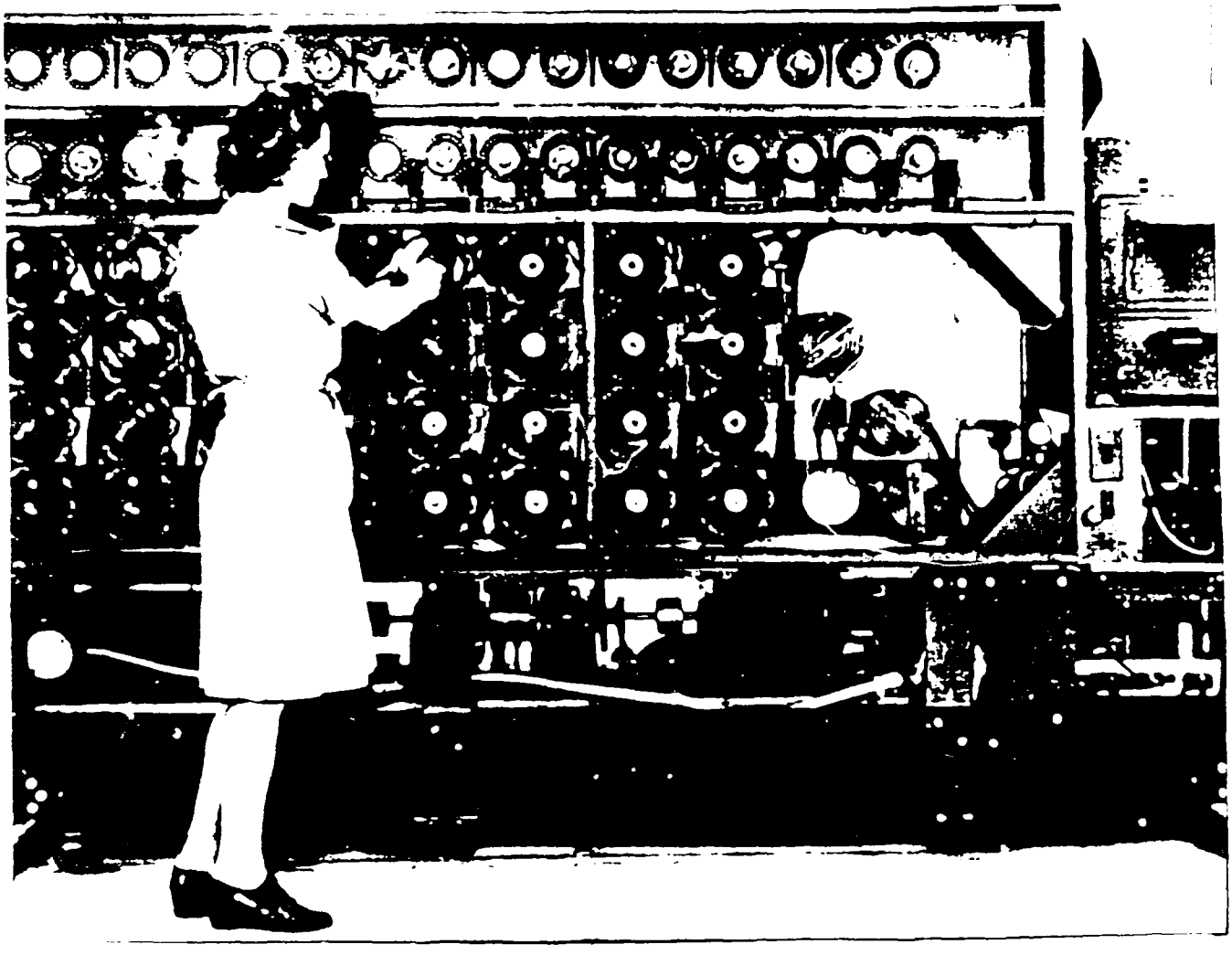


Figure 7

WAVE working a U.S. Navy "bombe" used in message decryption.
Reprinted with the permission of the Cryptologic History Office,
National Security Agency

In June 1942, the U.S. Army Forces in the British Isles (USAFBI) was replaced by Headquarters, European Theater of Operations, U.S. Army (USETOUSA). SIS, ETOUSA, became an operating organization under the theater SIGINT staff element. SIS, ETOUSA was an American counterpart to the British Y-Service, concerned with producing and distributing what the Army then called "radio intelligence".[55]

MEDITERRANEAN AND NORTH AFRICAN CAMPAIGNS

Bletchley Park and Y-Service were able to monitor the progress of the war in North Africa where initial British advances against Italian forces were offset by the arrival of General Erwin Rommel in February 1941. His Afrika Korps began pushing eastward toward Egypt, with the towns of Benghazi, Derna, Bardia, and As-Sollum falling in quick succession.[56]

In the spring of 1941, German forces also overran Yugoslavia and Albania, while pro-Axis forces were causing trouble in Syria and Iraq. The latter caused the diversion of British aircraft from Libya and Greece, forcing the British to evacuate the Greek mainland to Crete in May 1941. ULTRA then revealed that an airborne assault on Crete was imminent. With the movement of many Luftwaffe pilots from northern Europe to the Southern Front, the requirement for Y-Service signals intelligence support (quantity, quality, and timeliness) increased dramatically.[57]

Fuel and supply shortages ultimately took their toll on the German advances in North Africa. Axis convoys were having difficulty getting past the watchful "eyes and ears" of Malta-based aircraft and British naval patrols which were being provided by Bletchley Park with the time of

convoy departures from the continent, their composition, their destination, and probable cargo, making interdiction possible.[58]

Consequently, Malta became a high-priority target for Axis fighters and bombers, two of the targets of Malta's intercept. The heavy bombing of Malta lasted until the end of 1942; it did not fall to Axis control, and its intercept effort remained intact as the Allies prepared for the invasion of North Africa.[59]

The Allies decided in 1942 that a direct attack upon Germany was necessary but would not be possible until that target had been softened up. Therefore, they proposed to tighten the noose around the Third Reich by attacking North Africa, then invading "the soft underbelly" of southern Italy and France. The English Channel crossing was then to follow in 1943 or 1944.

To execute the Mediterranean campaigns, a new North African Theater of Operations, U.S. Army (NATOUSA) was established with Eisenhower as its Commanding General. Moreover, Eisenhower was made the Commander-in-Chief, Allied Force for the North African campaign. The Allied strategy for Operation TORCH called for deployment of three task forces in November 1942. (see Figure 8) The Western Task Force would deploy from the U.S. and launch an assault upon French-occupied Moroccan cities, beginning with Casablanca. The Center Task Force and the Eastern Assault Force, also primarily American forces deploying from England, would simultaneously attack and occupy Oran and Algiers, Algeria, to rout Vichy French forces from this colony. From there, reinforced British troops would deploy toward Bizerte and Tunis since retreating Axis Afrika Korps forces were headed in that direction following their November 1942 defeat

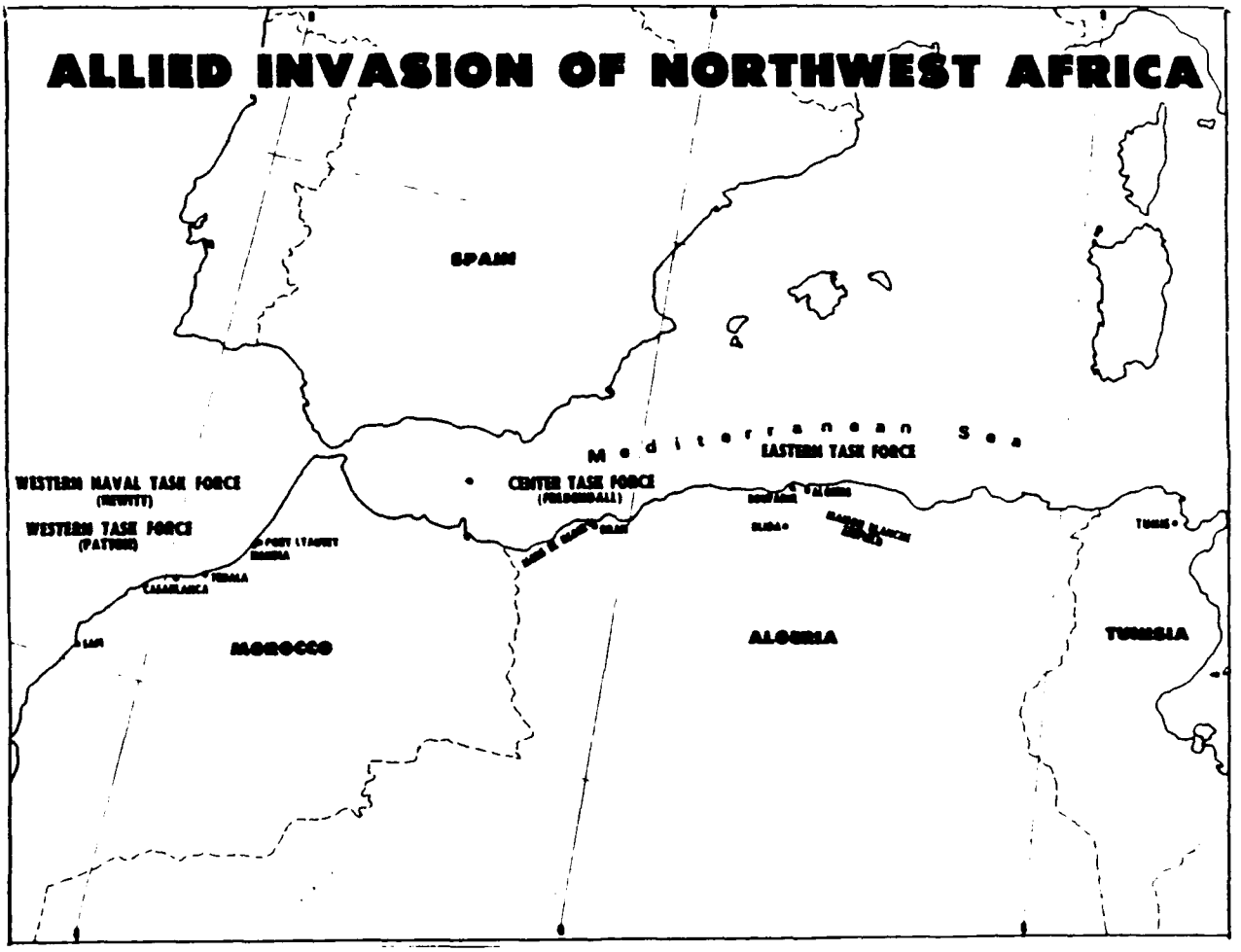


Figure 8

Map of Operation TORCH
George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 16.
Reprinted with the permission of the Cryptologic History Office, National Security Agency

at Al Alamein.[60] To support this campaign plan, the British Y-Service was to provide units for the Eastern Task Force; American radio intelligence companies were to deploy with the Western and the Central Task Forces.[61]

The following vignettes represent some of the more notable SIGINT successes of the North African campaign which began on 8 November 1942:

-- from ULTRA, that Germany was pressuring Vichy to oppose the Allies in North Africa.

-- from ULTRA, that Germany had taken the Tunisian airfields near Bizerte and Tunis and planned to consolidate the two areas into one bridgehead.

-- from ULTRA and Y-Service, that the Axis had consolidated this bridgehead before the Allies got to Tunisia.

-- from ULTRA, that elements of a Panzer regiment had been transported from Italy to Tunisia and that an Afrika Korps General was to take over command of the Tunisia defense.

-- from Y-Service, that the Luftwaffe was planning to attack specific ports, ships, airfields, and troop convoys along the coast from Algiers to Tabarka.

-- from U.S. SIGINT, that a U.S. plan regarding an inflated Allied force size was deceiving the Germans.[62]

ULTRA also contributed to a major intelligence failure in North Africa. The Allies learned that the Germans would be planning a major attack in Tunisia in February 1943. Unfortunately, a number of scenarios could have been deduced from the ULTRA messages. The Allied G-2, British BGEN Mockler-Ferryman, picked the wrong location (Fondouk Pass) for German forces to attack the British 1st Army. Consequently, some troops of the U.S. 1st Armored Division were held back further north, for an attack which never came, as the Germans attacked from the south, through Faid Pass. There, the remainder of the inexperienced U.S. 1st Armored Division, I Corps had to confront overwhelming German forces at Sidi buo

Zid. (see Figure 9) Mockler-Ferryman, who was said to have relied heavi- on ULTRA, was removed from his position and Eisenhower became quite skeptical of SIGINT. In reality, the wrong analysis could have been based on a variety of things. The G-2 may have failed to corroborate his conclusions with other intelligence (such as patrols) and have chosen to ignore aerial reconnaissance reports of a slight build up in the Sidi bou Zid area. Another author has suggested that Rommel may have changed his mind about the axis of advance (from Fondouk to Faid Pass) just prior to the attack.[63]

After the successful Axis attack against Sidi buo Zid, (see Figure 9), Rommel was ordered to take Le Kef. On 19 February 1943, Rommel began his main attack into the Kasserine Pass. For two days, he probed, struck, and almost penetrated hastily-established Allied positions at Thala. During the night of 21-22 February, U.S. SIGINT revealed that Rommel's forces were going to withdraw that night through the Kasserine Pass. Allied SIGINT was able to chart the Axis order of battle as forces withdrew from Feriana, Gafsa, and Sbeitla to Sidi bou Zid, Faid, Maknassy, Sfax, and Gabes.[64]

Throughout March and April, British and U.S. SIGINT services were able to provide timely translations of lower-level German commanders' communications, locations of units through DF and traffic analysis, and constantly-changing SIGINT order of battle. Allied Forces began an attack on 23 April 1943 against significantly weakened German and Italian forces. General Montgomery closed in from the east and Allied Forces from the west. All of Tunisia, including Bizerte and Tunis, was occupied by Allied Forces, who took some 200,000 prisoners because Hitler permitted no substantial German withdrawal until it was too late. Before the collapse of the North African campaign, Field Marshal Rommel returned to Europe

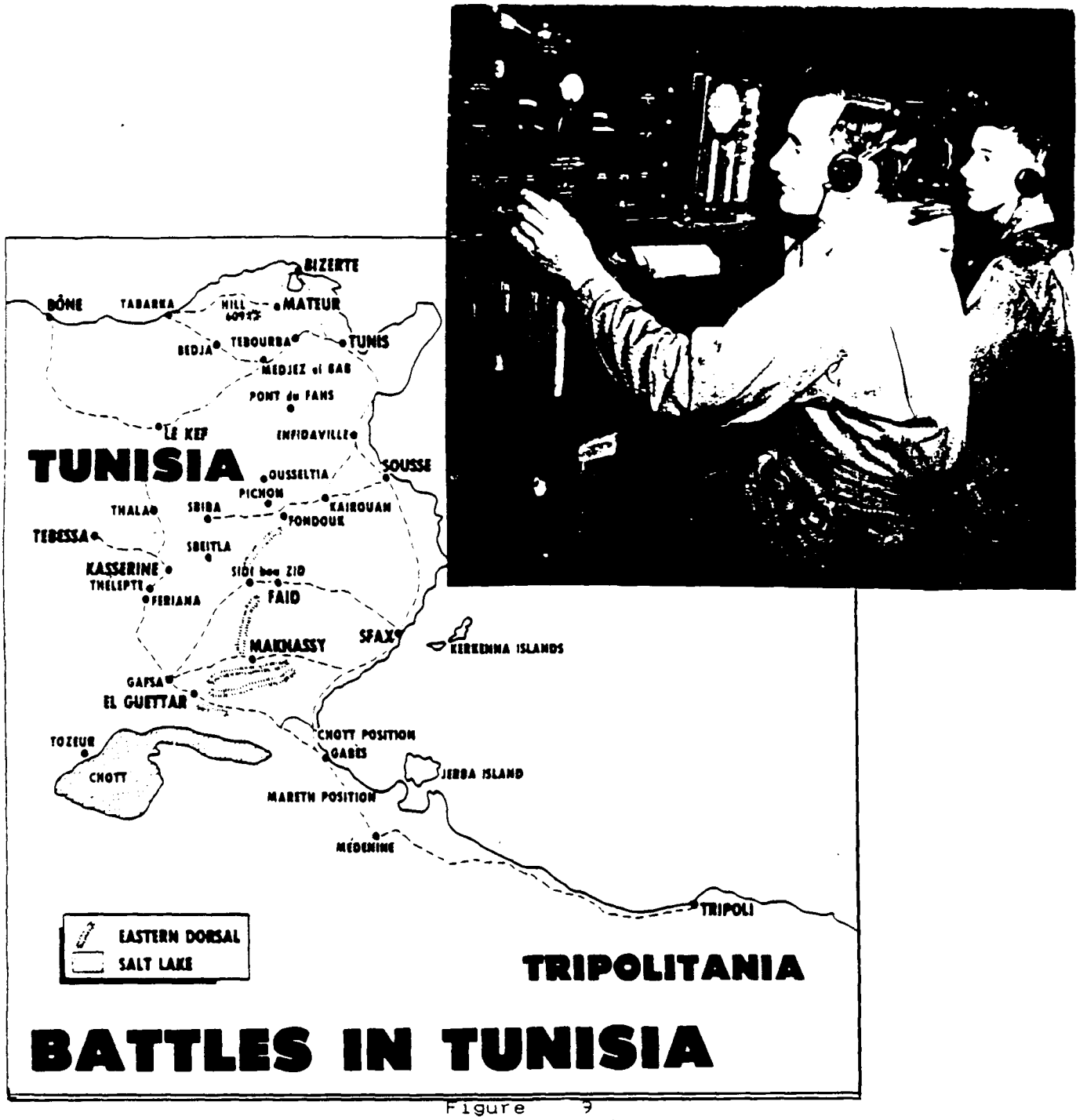


Figure 9
Battles in Tunisia
George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 26.
Reprinted with permission of the Cryptologic History Office, National Security Agency
Intercept operators in Morocco during North African campaign
John P. Finnegan, Military Intelligence: A Picture History, p. 85.
Reprinted with the permission of the U.S. Army Intelligence and Security Command History Office.

without ever knowing that it was the decryption of his ENIGMA messages which had denied him the supplies he so desparately needed to prosecute his campaign.[65]

INVASION OF SICILY

From Tunisia, the Allied plan called for the invasion of Sicily in July 1943. Known as Operation HUSKY, the plan called for LTG George Patton, U.S. 7th Army Commander, to land at the southern part of Sicily, secure Palermo, and push north of Mt. Etna to Messina. Moreover, Patton was to cover the flank of British 8th Army Commander Montgomery, who was to land at the southeastern corner of Sicily, and attack northward, past Mt. Etna, then proceed on to Messina. (see Figure 10) The challenge to U.S. SIGINT efforts was to stretch limited resources in North Africa, while supporting the 7th Army invasion of Sicily as well as an impending attack of the Italian mainland, the 12th Air Force, and the U.S. Navy operating in the Mediterranean.[66]

The Mediterranean Air Command and the Northwest African Air Forces set up a command post at La Marsa, Tunisia to control all air operations in support of Operation HUSKY. An SLU was established and manned 24-hours a day with direct support from Bletchley Park, the Air Ministry, and the Mediterranean Command in Algiers, ensuring that Y-Service and ULTRA material were given every consideration in the planning process. There had been a concern that the Axis defeat in Tunisia would cause this lucrative source of intelligence to disappear. After a temporary cessation of communications, the Germans reinstituted communications links which provided Allied forces detailed information on the transfer of German troops and materiel from North Africa to Sicily. Moreover, SIGINT

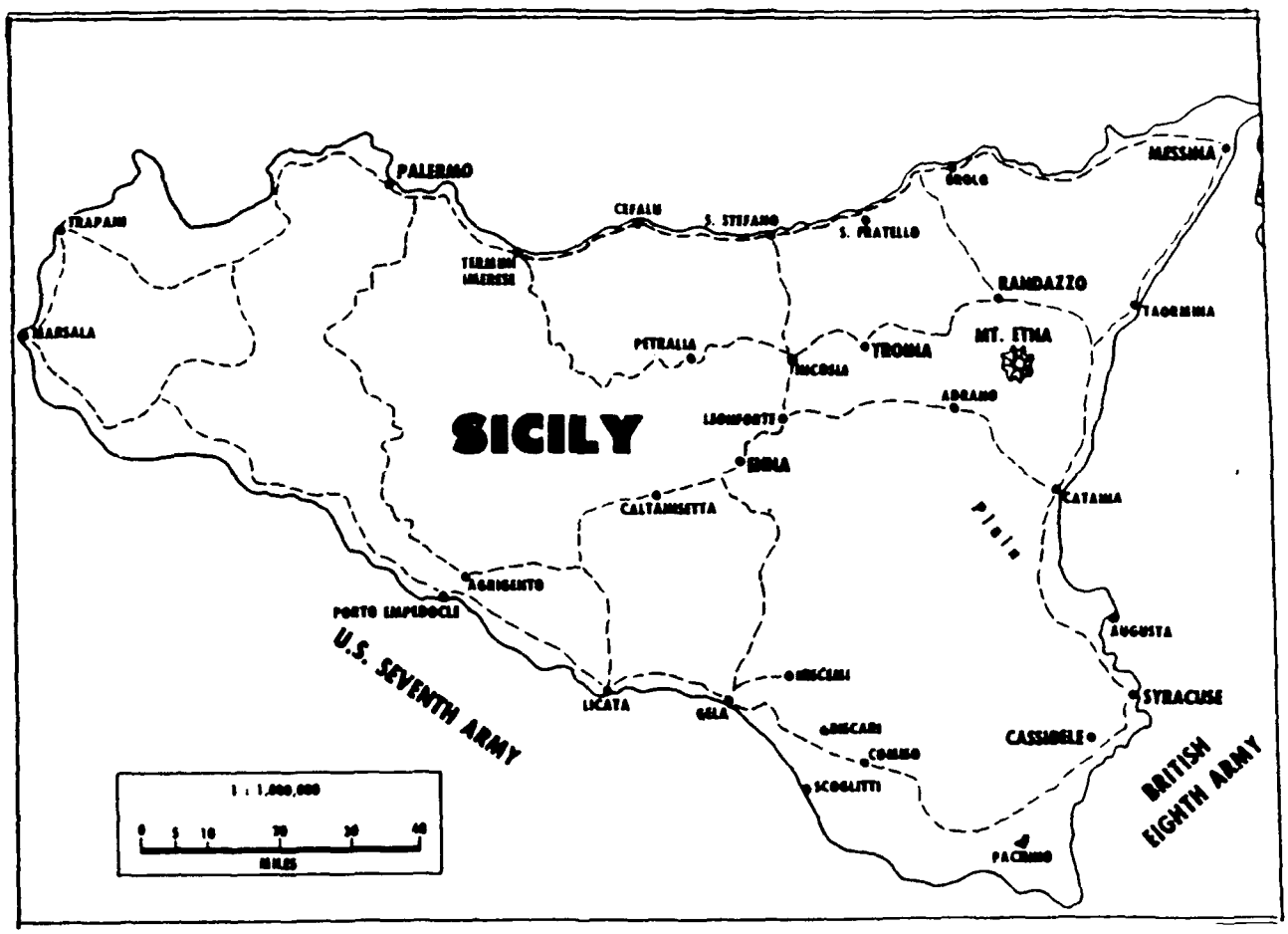


Figure 10

Map of Operation HUSKY
George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 42.
Reprinted with the permission of the Cryptologic History Office, National Security Agency

revealed the positioning of German forces in the center of Sicily, since the Germans expected an attack but did not know from what direction it would come. (During the invasion, airborne units used this information to seal off mountain passes, precluding panzer movements.) Also during the planning stages, Allied SIGINT provided extensive order of battle information on German and Italian forces and tip-offs of impending German air and submarine attacks on Allied convoys and ports in North Africa. Overall, however, the amount of SIGINT available for operational planning was less than that available during the North African campaign.[67]

SIGINT support during the actual invasion was rather limited. Small advance parties embarked with the three American assault forces; however, they never called for the main SIGINT force to join them, so the main body did not arrive in Palermo until 9 August. Y-Service for Allied air controllers arrived in the D+5 follow-up convoy from Tunis. Axis use of radiotelephone communications, however, produced limited yield for Allied Y-Service on Sicily. Conversely, ULTRA was able to confirm the dates and method of Italian and German withdrawal to the mainland in early August.[68]

INVASION OF ITALIAN MAINLAND

Sicily, invaded on 10 July 1943, was conquered in less than six weeks. The Allied strategy then called for an invasion of the Italian mainland. Operation BAYTOWN carried the British 8th Army across the Straits of Messina on 3 September. Operation SLAPSTICK involved an 8th Army attack on Taranto on 9 September. Operation AVALANCHE, the 9 September landing of U.S. General Mark Clark's 5th Army on the beaches of Salerno, marked the beginning of a hard-fought campaign northward. (see

Figure 11

Map of Allied operations in Italy
George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 71.
Reprinted with the permission of the Cryptologic History Office, National Security Agency

Figure 11) SIGINT operators, many of them "seasoned" by the North African and Sicily campaigns, were able to make significant contributions to tactical and operational Allied campaign planning.[69]

The following vignettes represent some of the more notable SIGINT successes during the early Italian campaign:

-- ULTRA provided information that the pre-invasion bombing attacks against Italian infrastructure and military targets had been successful.

-- SIGINT operations were established on board the command ship and other vessels during the amphibious phase of Operation AVALANCHE. Electronic interconnectivity of the commanders, staffs, and message centers enabled the passage of real-time intelligence to military commanders.

-- The U.S. 5th Army commander was provided, over Admiralty channels, ULTRA decrypts concerning German troop strength in Italy, advance notice of enemy reinforcements and their disposition, and their plans for counterattack.

-- Effective use of intercept positions at Malta and La Marsa enabled the RAF to monitor the disposition of German Air Forces units within striking distance in an attempt to call in air strikes to further diminish German air power.

-- Intercept of German air-to-ground communications of German fighters, fighter bombers, bombers, and reconnaissance aircraft gave Allied pilots enough lead time (sometimes 20 minutes) to take the necessary actions to avoid or engage enemy aircraft.[70]

By 1 October, Naples fell and the Allies gained control of Foggia. On 14 October, unloading shifted from Salerno to Naples and the U.S. 5th Army reached the south bank of the Volturno River. As the Allies were about to cross the Volturno, the Badoglio Government formally declared war against Nazi Germany and Italy became a co-belligerent, although not an ally. With Allied forces moving further north, SIGINT provided the following types of information:

-- bomb damage assessments and the disorganization within the German military during Allied advances;

-- German tactics designed to delay the Allied advance;

-- enemy movements, strengths, disposition, and reinforcements.[71]

After their successful landings in southern Italy in September 1943, the Allies had hoped to be in Rome by Christmas. However, by December, they had stalled at the Gustav Line. These German forces, 10 miles wide at some places, ran behind the Sangro River in the East and the Garigliano and Rapido Rivers in the West. The monastery of Monte Cassino dominated the heights along the advance in the West. U.S. commanders prepared for a frontal assault on the Cassino sector and a seaborne hook around the Gustav Line to Anzio.[72]

The invasion of Anzio -- Operation SHINGLE -- was planned to begin on 22 January 1944 with a night landing by the British 1st Division in the north and the U.S. 3rd Division plus Rangers and others to the south of Anzio. A small SIGINT detachment went ashore on D-Day to provide DF and tactical support (especially enemy intentions and locations). Moreover, this unit began to integrate information provided by prisoner of war interrogations to improve the quality of its product. Further, it was able to pass to the Air Warning Service probable early targets of enemy air attacks. At the same time, the two "Task Force" Commanders were provided ULTRA, which enabled them to learn of enemy intentions and capabilities to counteract the Allied invasion of Anzio as well as their surprise over the timing of the attack.[73]

ULTRA also revealed that discord had developed between the German ground and air forces. The Army complained that it had been provided inadequate close air support because, during the Italian campaign, fighters had been diverted north in an attempt to thwart Allied bombings of northern Italy, Austria, and southern Germany.[74]

The U.S. 6th Corps was pinned down on its beachhead for three grim months after a German counterattack in February. After a hard-fought battle at Anzio, Allied forces were able to break out by May, drive north, and finally enter Rome on 4 June 1944.

EUROPEAN THEATER OF OPERATIONS

NORTHERN EUROPE

As the Allies were planning Operation OVERLORD, the long-awaited invasion of northern Europe, they learned from Bletchley Park that two of Hitler's leading generals -- Field Marshal Rommel and General von Rundstedt -- disagreed over possible locations of an Allied invasion. The former believed that the invasion would come at Normandy; the latter, at Pas de Calais. Hitler ultimately supported von Rundstedt, Commander-in-Chief in the West, and agreed that four panzer divisions would remain as reserve forces around Paris. Allied commanders knew of this infighting and did everything to perpetuate the confict and to devise a deception plan to prevent the Germans from forecasting the time and place of the landing. The Normandy-Pas de Calais issue became the linchpin of Operation FORTITUDE, the overall deception program supporting the invasion. To further confuse the Germans, the plan signalled Allied intent to invade Norway, the Bay of Biscay, and the Balkans.[75]

On 6 June 1944, Operation OVERLORD was launched from England against Normandy, France. (see Figure 12) The Normandy landings were accomplished, in part, by commanders, troops, naval forces, and airmen, who had become seasoned in the Mediterranean, receiving "hands-on" experience there. This included SIGINT personnel. Consequently, SIGINT, derived

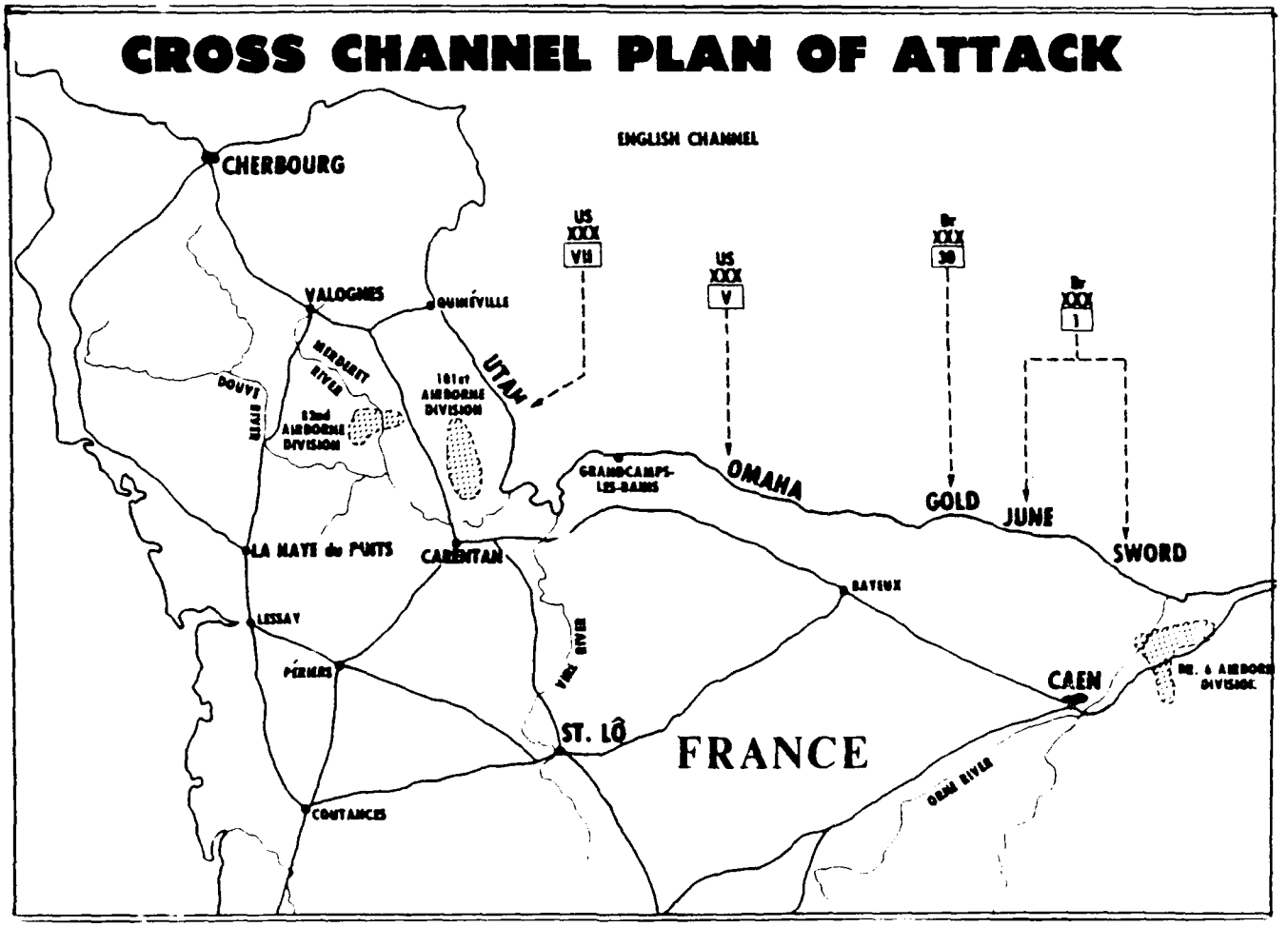


Figure 12

Map of Operation OVERLORD
George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 109.
Reprinted with the permission of the Cryptologic History Office, National Security Agency

from tactical voice and medium and high-grade cryptographic intelligence, was provided in quick order to OVERLORD commanders.

> "Enemy reports showed the locations of command posts, main lines of resistance, outerguard lines of resistance during retreats, boundaries of unit areas, areas, identifications of neighboring units and of the points of contact between them. From rear areas came data on the locations of dumps of fuel, rations and supplies, medical dressing stations, repair shops, replacements and training units, billeting areas, and lines of communications. Large-scale movements of troops for substantial distances could be followed in SIGINT. From enemy divisions in combat zones came standard periodic situation reports and field orders from operations officers, standard situation reports from German intelligence officers, and reconnaissance reports from air ground, and artillery units." [76]

However, there were problems associated with the provision of this material to military commanders. Unless there were communications between a forward intercept unit and a processing center, all medium-grade encrypted messsages had to be couriered back to Army or Army Group for analysis, resulting in a time delay which could depreciate the usefulness of the intelligence. Moreover, the Germans in this area relied heavily on land line communications (not transmitted over the air waves), thereby reducing the amount of SIGINT available for analysis.[77]

From the Normandy Beaches, U.S. forces captured Cherbourg and St. Lo, while the British gained possession of Caen by mid-July. On 28 July, retreating Germans turned eastward, rather than southward, where the U.S. 2nd Armored Division had established blocking positions. This part of Operation COBRA resulted in 1,000 Germans killed and another 4,000 captured, while other Germans escaped. Tactical radio communications of

the disorganized German forces provided abundant information for U.S. SIGINT operators and commanders. Meanwhile, ULTRA revealed details of enemy fuel shortages and Hitler's orders regarding positions that were to be defended "to the last man."[78] (see Figure 13)

As Allied forces continued operations in Normandy and Brittany, German forces counterattacked Mortain, a move which surprised some Allied commanders. Tactical SIGINT, in retrospect, revealed German interest in that town days before the attack; however, no one really pieced together the details. Special intelligence had revealed that Hitler called for an attack on 2 August "to push the Americans back into the sea." Field Marshal von Kulge, who had replaced von Rundstedt, began the attack on 7 August, even though Hitler by then wished that it be postponed. Another ULTRA message revealed that five German armored divisions were being transferred to a location near Mortain for a drive toward Avranches. Patton used this information and diverted some of his forces, thereby halting the German drive. Consequently, German forces started heading eastward toward the Seine and the German "West Wall", a zone of barriers, pill boxes, and obstacles near the German Border. By 15 August 1944, the U.S. invaded southern France and German troops withdrew from much of France. By 25 August 1944, Paris was liberated.[79]

As Allied forces pushed north of the Seine into Belgium and Luxembourg, radio intelligence companies' mobility capabilities were challenged as they tried to provide continuous coverage of German targets. As such, they were able to obtain information on enemy units, especially command posts, supply and ammunition dumps, the enemy's operational status, and warnings of incoming artillery fire. In an effort to press the attack, Eisenhower accepted Field Marshal Montgomery's plan

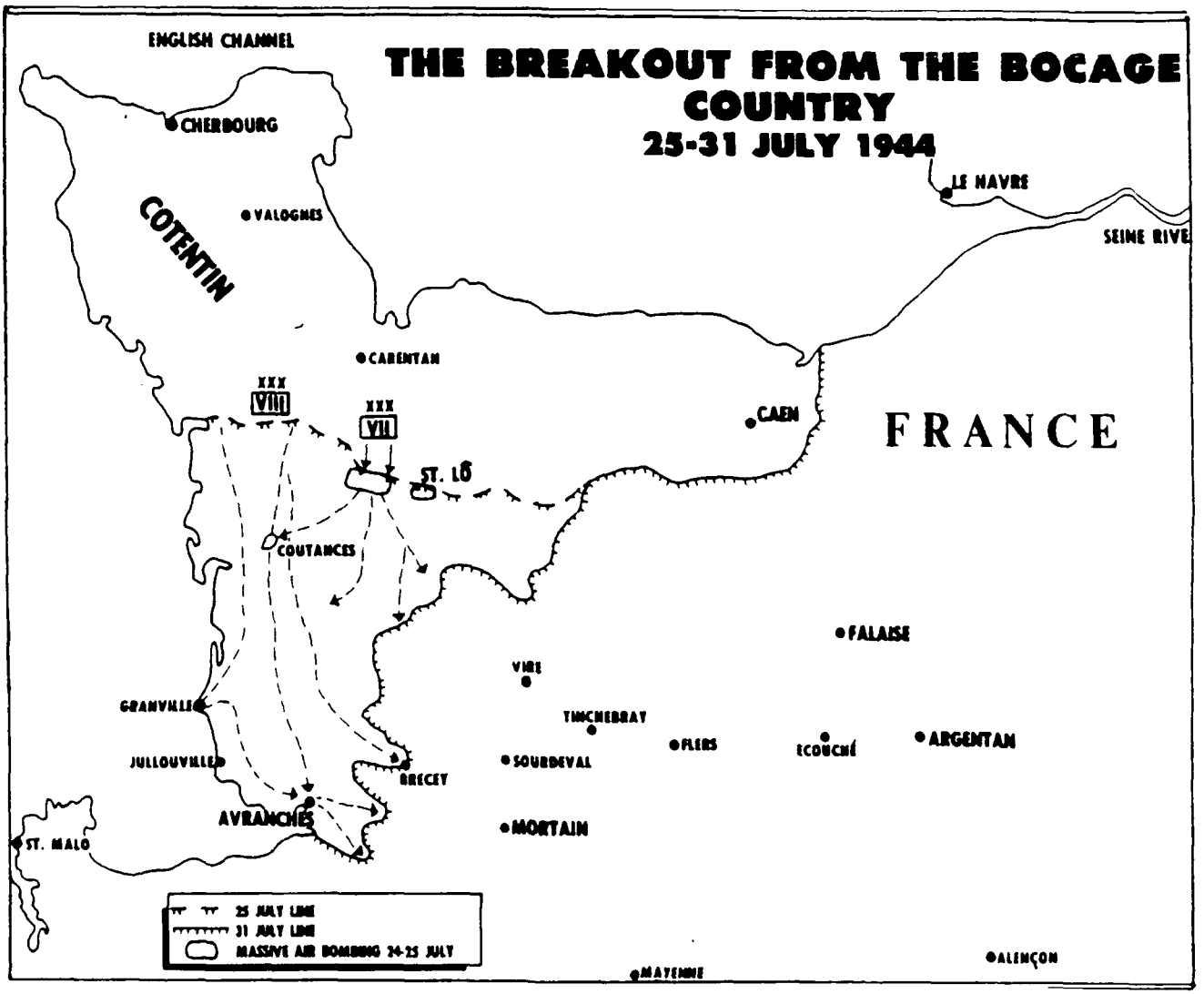


Figure 13

Map of Operation COBRA
George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 137.
Reprinted with the permission of the Cryptologic History Office, National Security Agency

for gaining a bridgehead across the Rhine. Operation MARKET GARDEN called for the insertion of three airborne divisions with which Montgomery hoped to push across the Rhine near Arnhem in the Netherlands before the Germans could organize their defenses.[80]

Days before the operation was to begin (17 September 1944), there were SIGINT indicators of German activity in the Arnhem area. Dutch resistance reported that two Panzer divisions were believed to be refitting in the southern Netherlands. Aerial photography confirmed that tanks were, indeed, near Arnhem; however, the number and their condition could not be determined. ULTRA of 14 and 15 September revealed that the Germans were expecting a large-scale landing on both sides of Eindhoven, as far as Arnhem. Eisenhower refused to call off the operation after having given Montgomery the "green light"; however, several Eisenhower advisors were dispatched to Brussels to discuss the intelligence and possible changes to the operational plan with Montgomery. He dismissed their advice and failed to pass down the SIGINT indicators to subordinate corps commanders. Operation MARKET GARDEN began as planned and German forces were able to overwhelm the paradropped Allied forces that had seized the Arnhem bridge and retake it before Allied reinforcements could consolidate a defense. German forces also struck Allied troops concentrated at the nearby Driel railroad station. A SIGINT unit had learned of that attack about three hours before it was to have begun but was unable to get the forewarning to the Allied forces at Driel.[81]

The failure of MARKET GARDEN marked the end of the Allied pursuit of the German army. In the end, the German's new main line of defense could not be ou'flanked; it would take more time to reach the Rhine. The Front

stabilized and a war of attrition followed. By October, it appeared that Germany would have a panzer reserve strong enough to attack. Bad weather restricted aerial reconnaissance and German Air Force communications revealed in December that the Germans were planning an offensive but no details were provided. SIGINT revealed priority requests for aerial reconnaissance of the Meuse River bridges but no significance was ascribed to these requests. Other SIGINT confirmed German troop movements, such as the 3rd Panzer Grenedier Division, from the Italian Front. However, because of the lack of specificity, no one expected the size and intensity of the German force which, on 16 December 1944, resulted in a large German counterattack in the Belgium-Luxembourg sector of the Ardennes.[82] (see Figure 14)

Hitler had hoped to regain the offensive with this attack, causing the Americans to panic and collapse, enabling the Germans to drive up the middle and take Antwerp. There were many factors which contributed to this "intelligence failure". An investigation of what may have caused this failure revealed that large-scale, undetected rail movements of troops and tanks, limited night-time aerial reconnaissance, strict radio security measures, and dummied radio traffic had enabled the Germans to refit 35 divisions (5 of which were panzer divisions) and create 15 VOLK GRENEDIER divisions. Moreover, the Germans moved 500 medium tanks; large amounts of ammunition, artillery, and rocket launchers; and fuel. As the German attack progressed, the volume of German radio communications increased as well. Special intelligence further revealed Hitler's generals advising him that an advance on Antwerp was impossible and that an attempt should be made to capture Liege and establish a line from there to Aachen. Hitler rejected this advice.[83]

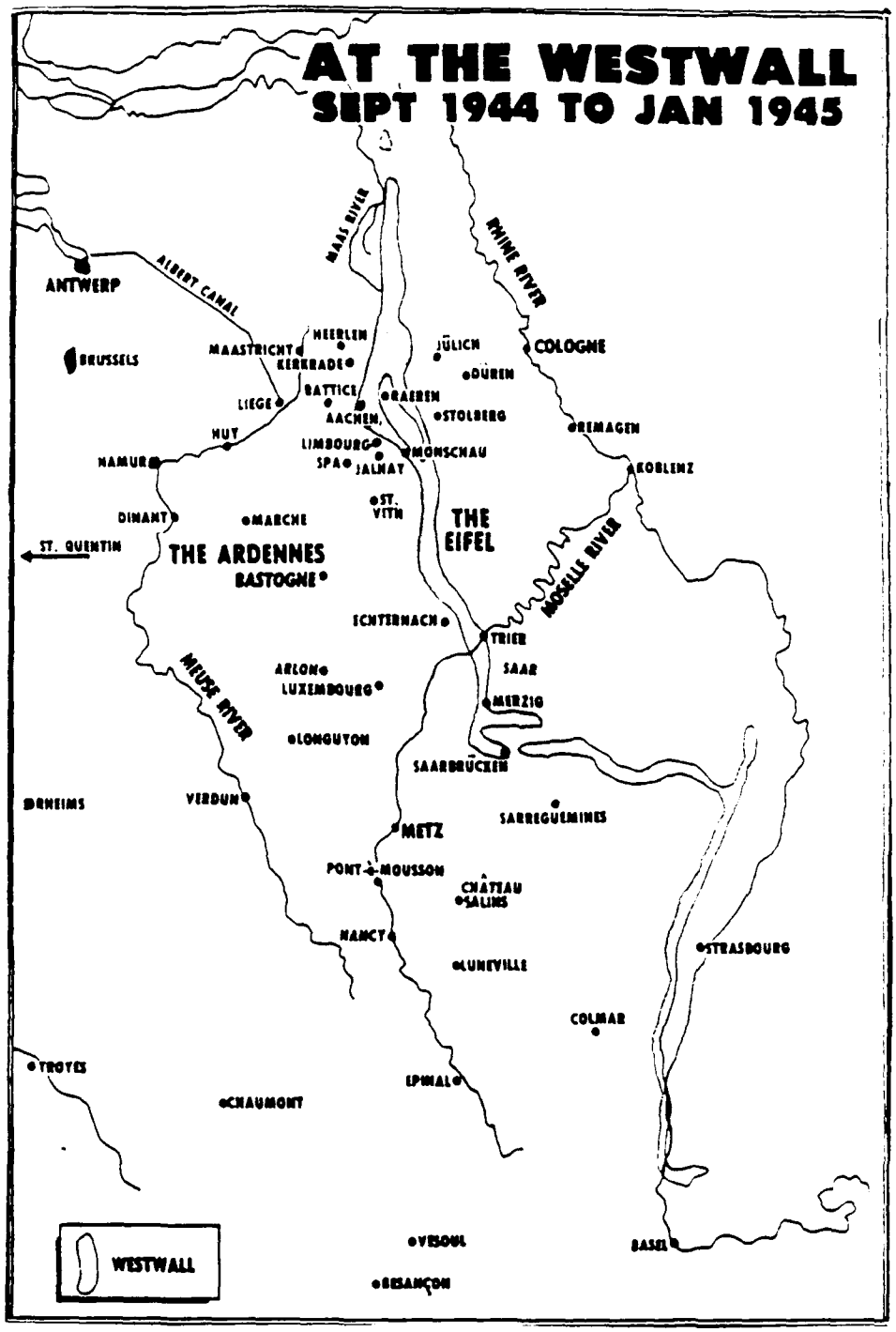


Figure 14

Map of the Battle of the Bulge
George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 147.
Reprinted with the permission of the Cryptologic History Office, National Security Agency

During the Ardennes attack, SIGINT provided important intelligence in both quantity and quality, as American SIGINT units read the traffic of 13 divisional-sized commands.

> "German reconnaissance units reported what they were observing, naming hamlets and villages among which they were moving. Battle groups identified their positions and named adjacent units. The location of command posts, dumps of supplies and ammunition, and even lines of attack were spelled out or were indicated by DF. During periods in which air reconnaissance was restricted by weather conditions, tactical SIGINT was often the only reliable instrument for determining what forces faced an American command."[84]

After initial German gains, the Allies were able to halt the German drive toward Antwerp and reclaim all the ground lost during the December 1944/ January 1945 Ardennes Offensive, popularly known as the Battle of the Bulge.

Allied forces kept pushing eastward toward the Rhine. (see Figure 15) SIGINT was able to provide military commanders with the locations of bridges that German forces would use during this withdrawal. At the same time, Russian forces struck out forcefully against German positions, freeing much of Poland, Hungary, and Czechoslovakia, and pushed into East Prussia. With Eisenhower's forces on the east side of the Rhine, the collapse of German resistance in northern Italy, the execution of Italy's Mussolini, and the suicide of Hitler, Admiral Karl Doenitz, Hitler's successor, notified the Allies that Germany was ready to surrender. On 8 May 1945, the Allies declared Victory in Europe.

By the end of the war, the U.S. operated SIGINT centers in rear areas and mobile units deployed forward in support of tactical operations within their respective theaters of operation. They were organized as teams,

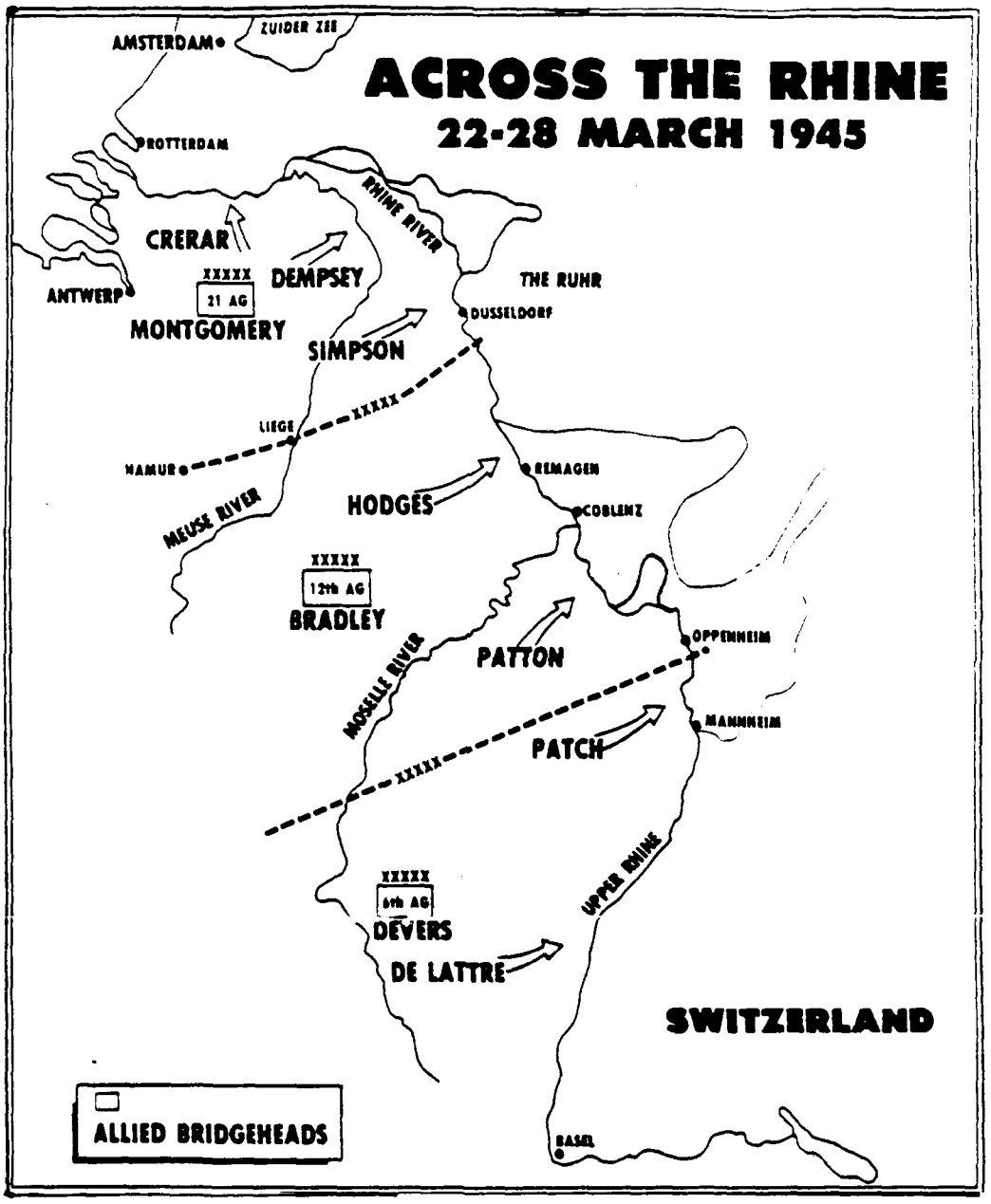


Figure 15
Map of Allied forces moving across the Rhine
George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 164.
Reprinted with the permission of the Cryptologic History Office, National Security Agency

parties, platoons, sections, detachments, companies, and groups. U.S. commanders in the European theater were provided with SIGINT information, intercepted by tactical units under the control of various theater-level signal intelligence services.[85]

These communications emanated from enemy tactical and operational commanders who used low or medium-grade cryptographic systems. By the war's end, each of the 14 corps operating under Supreme Allied Commander Eisenhower was supported by its own signal company which performed SIGINT intercept, DF, and analysis. The cryptologic effort at army group and army field level was accomplished by signal radio intelligence companies which operated with analytical detachments furnished by the signal intelligence services. Of course, applicable ULTRA or "Special Intelligence" was passed from Bletchley Park or the Admiralty to commanders in the theater of operations as required on a very strict "need-to-know" basis.[86]

PACIFIC THEATER OF OPERATIONS

Immediately prior to World War II, the Japanese also began to design their own cipher machines. In 1936, Friedman and his U.S. Army cryptanalysts, building upon the efforts of the Navy's OP-20-G analysis, solved a machine cipher which they called RED and the Japanese termed "A". In 1939, RED was replaced by the PURPLE machine, used to encrypt Japanese Foreign Ministry diplomatic communications, one of the first in a series of Japanese machines which used telephone stepping switches instead of rotors as in the ENIGMA machine.[87] In September 1940, U.S. cryptanalysts succeeded in solving the here-to-fore unbreakable Type No. 97 or "B" machine. MAGIC was chosen as the generic cover name for the PURPLE (B) and RED (A) machine crypt systems for Japanese diplomatic messages. [88]

The ability to read Japanese diplomatic traffic from delegations in the capitals of Washington, Berlin, Rome, Berne, Moscow, Vichy, and Ankara, among many others, and military attache as well as secret agent reporting from Hawaii, Panama, the Philippines, and major U.S. ports gave the U.S. an incredible strategic advantage over the Japanese. Both the U.S. Army and Navy worked together in MAGIC production.[89]

The U.S. also shared its cryptographic breakthroughs with the British. In January 1941, a team of American SIGINT experts brought a PURPLE analog, several RED analogs, and their keys to England. As a result, Prime Minister Churchill was able to learn what the Germans were telling the Japanese about the state of the war by intercepting and decrypting MAGIC messages between the Japanese Embassy in Berlin and Tokyo.[90] The following are examples of those diplomatic exchanges, filed by Baron Oshima in Berlin after speaking with Hitler or his top aides; they were of utmost interest to Allied military commanders and diplomats.

-- Hitler's elation over the heavy Allied losses during the Battle of the Atlantic - March 1942.

-- Hitler's perception that England was going to invade Norway - March 1942.

-- The pace of Germany's industrial mobilization - April 1942.

-- Hitler's belief that the Allies were going to invade the Balkans after the Allied invasion of Italy. Therefore, he held 20 divisions in the Balkans, leaving only 18 divisions to thwart the Allied advance in northern Italy - October 1943.

-- A nine-page text of Oshima's personal inspection of the Atlantic Wall and the German command and control structure for northwestern Europe as the Allies were beginning to plan Operation OVERLORD. It included German defenses, division status and rotation patterns, and an evaluation of Allied bombing effectiveness - December 1943.

-- Germany's ability to increase the production of essential weapons

(tanks and airplanes) in spite of Allied bombings of industrial centers - January 1944.

-- The failure of the assassination plot against Hitler and its ramifications - July 1944.

-- Very detailed technical information about German production of jet-propelled aircraft. Oshima's reports were so detailed, it has been said, that they served as a verbal blueprint - much of 1944.

-- Russia's war intentions. This was very useful information because Moscow communicated very little with the other Allies regarding the status of the war and its plans.[91]

PEARL HARBOR

According to Roberta Wohlstetter's analysis of the U.S. military intelligence structure prior to the 7 December 1941 bombing of Pearl Harbor, there was little duplication of effort between the Army and Navy. The Communications Security Unit handled the interception and decoding of all foreign language communications for the Navy. This 300-man unit in Washington was supplied with intercept from Washington state, Florida, Maine, Maryland, the Philippines, and other locations. These decrypts were then sent to a much smaller unit for translation.[92]

As noted earlier, interception of foreign transmissions within the Army fell to the Signal Intelligence Service (SIS) of the Signal Corps. William Friedman of the SIS had become the principal cryptanalyst among the 180 civilian and military personnel at SIS in Washington. The headquarters was being supplied with intercept from stations in New York, California, Texas, Panama, Hawaii, the Philippines (until that unit was overrun and forces reconstituted in Australia), and Virginia. (see Figure 16) Vint Hill Farms, Virginia was also used to train communicators, intercept operators, and analysts in various types of cryptology.[93] After the U.S. entered the war and MAGIC traffic volumes increased, the division of effort with the Navy regarding MAGIC became unworkable. The

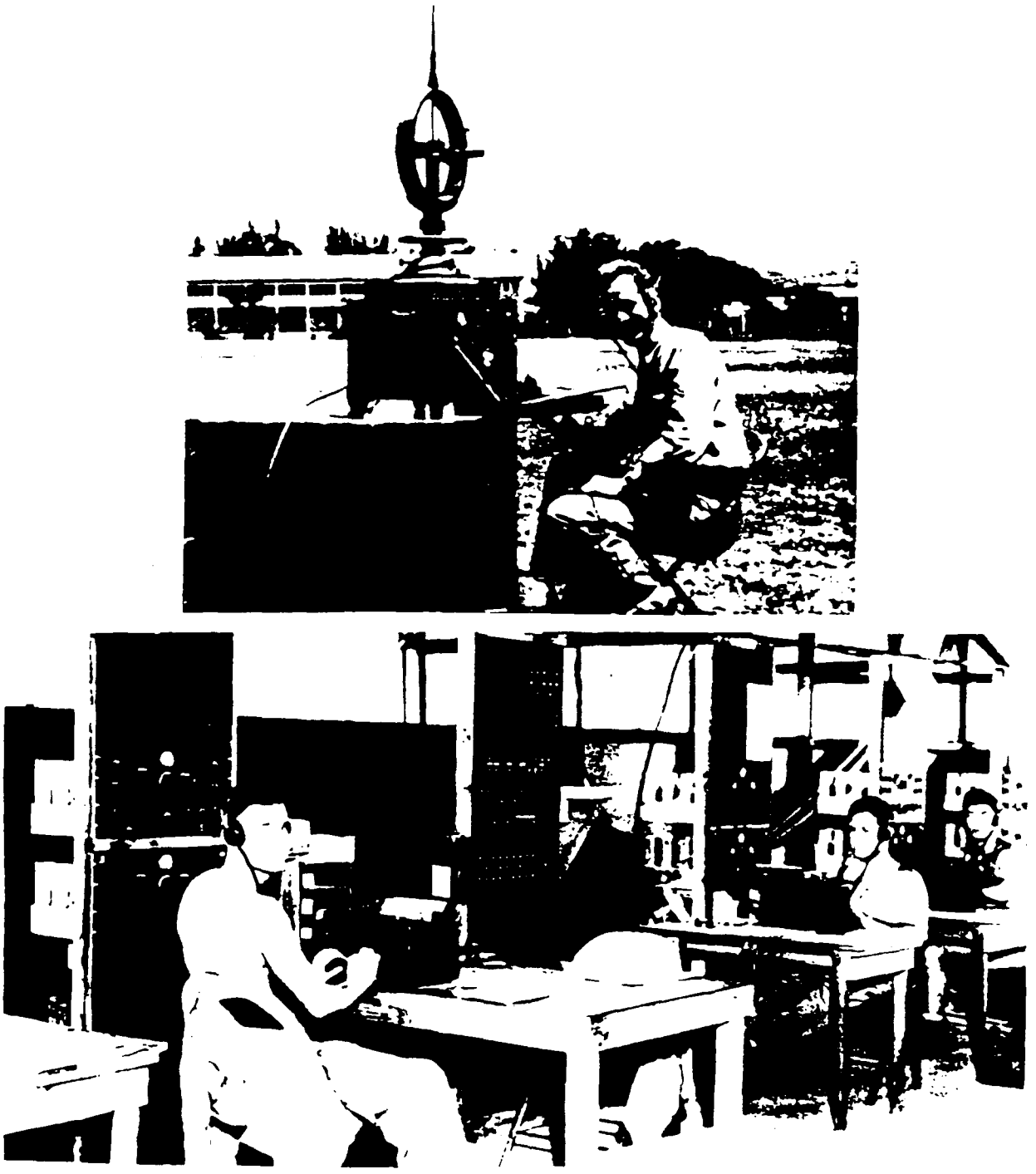


Figure 16

SIS radio direction finding, Hawaii, 1940 (top)
COMINT operators in SWPA, Australia, 1943 (bottom)
John P. Finnegan, Military Intelligence: A Picture History, pp. 56 and 92.
Reprinted with the permission of the U.S. Army Intelligence and Security Command History Office

SIS assumed sole responsibility for producing and handling the diplomatic messages.

MAGIC successes, however, did not prevent the bombing of Pearl Harbor. President Roosevelt was shown 13 of the 14 parts of the MAGIC message to Japan's Washington Embassy before midnight on 6 December 1941, indicating that Japan was formally terminating negotiations with the U.S. because it was impossible to reach an agreement. However, this did not constitute a Japanese execute order. Part 14 was delivered to the President on the morning of 7 December. It instructed the Ambassador to convey Japan's decisions to the U.S. at 1300 hours Washington time (dawn in Hawaii).[94]

Wohlstetter's analysis of the Pearl Harbor attack revealed that MAGIC messages transmitted weeks prior to 7 December 1941 contained a number of indications of worsened U.S.-Japanese relations. Her study revealed problems with late-breaking MAGIC intercepts, message backlogs, the message filing system, the quality of translations, the communication between Washington and Hawaii, the failure to alert proper authorities, and distribution. The case study led her to the conclusion that indicators prior to the event were "fraught with uncertainty"; they only "stand out and scream of impending catastrophe when they are stripped of other meanings." She concluded:

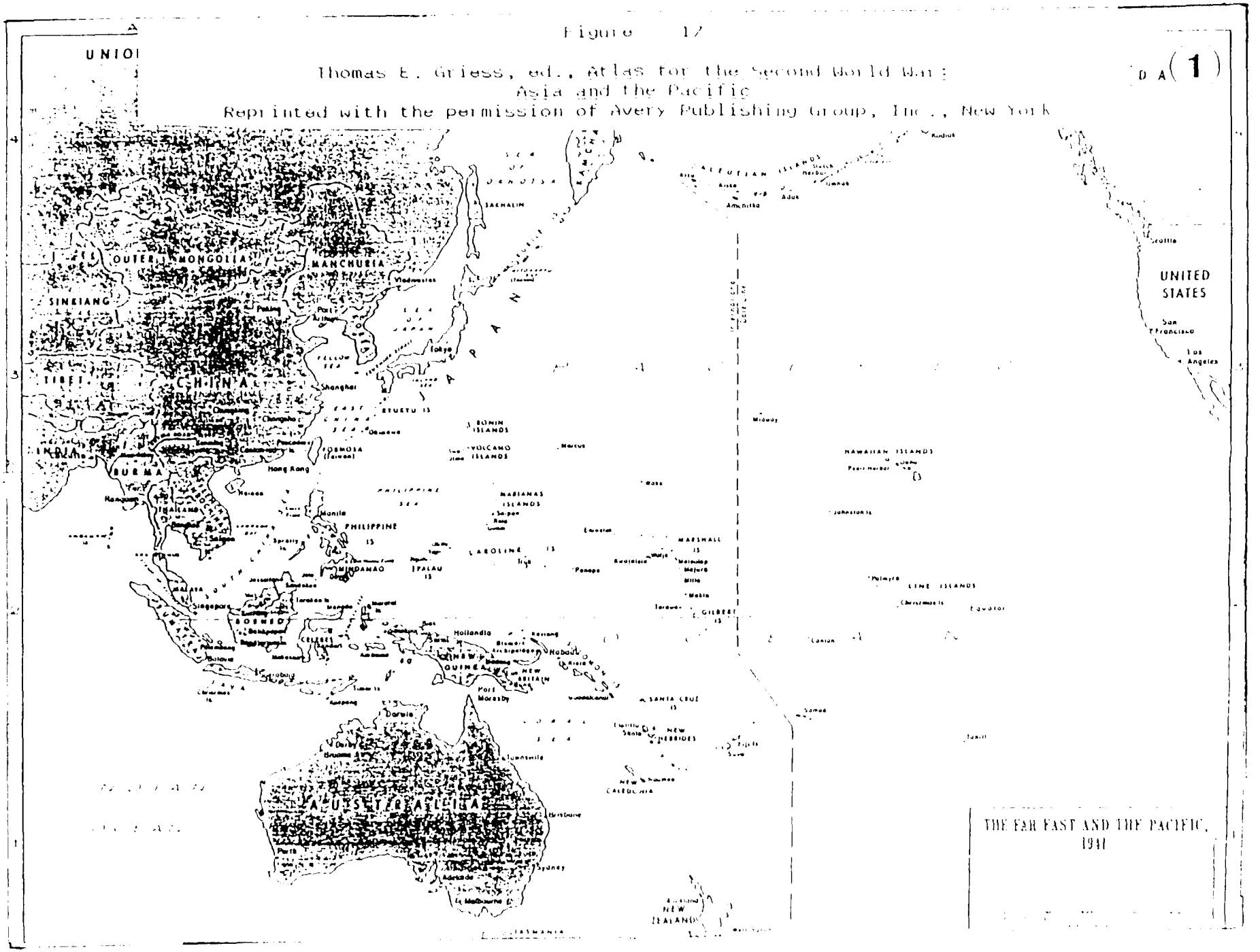
> "In spite of these deliberate and accidental ambiguities, however, intelligence can do a great deal to diminish the uncertainty of military decision. MAGIC did have a lot to say, even if it did not tell all. ... All of the signals were ambiguous. And perhaps one of the important lessons to learn from Pearl Harbor is that intelligence will always have to deal with shifting signals."[95]

In spite of the apparent "intelligence failure" of Pearl Harbor, the U.S. had to regroup quickly to support U.S. military operations in the Pacific. U.S. SIGINT units in the Philippines joined forces with the British in Singapore. The Japanese Navy code (JN-25), a mainstay of the Navy's SIGINT effort, was changed just prior to the Pearl Harbor attack. Naval analytic centers in Washington (OP-20-G) and Hawaii (Fleet Radio Unit, Pacific (FRUPac)) worked continuously with the Naval unit in the Philippines and the British in Singapore to piece together the solution to the modified code (JN-25b). With the U.S. retreats from Bataan (April 1942) and Corregidor (May 1942), the U.S. joined the British and Australians in a Combined Bureau in Brisbane. Since the Corregidor unit had the only MAGIC-decrypting analog in the South West Pacific Area (SWPA), it retained that responsibility in Australia as well. However, Ronald Lewin maintains that the SWPA cryptographic unit lacked the cohesive integration achieved by naval processing centers in Washington and Hawaii.[96] (see Figure 17)

By April 1942, all parties attempting to solve JN-25b had made enough headway that they were beginning to piece together the war strategy of Admiral Yamamoto, the Commander-in-Chief of the Japanese Imperial Navy's Combined Fleet. Interpretation of JN-25b messages suggested Japanese plans to capture Port Moresby in New Guinea. If the Japanese were successful, they could threaten northern Australia. It was from Port Moresby that General MacArthur, Commander-in-Chief, Allied Forces in the Pacific Theater, intended to establish his first base for his return to the Philippines.[97]

Figure 17

Thomas E. Griess, ed., Atlas for the Second World War: Asia and the Pacific



BATTLE OF THE CORAL SEA

To preclude the take-over of Port Moresby, Admiral Halsey sailed for the Coral Sea on 30 April 1942 (see Figure 18) and, the next day, three Japanese carriers -- the ZUIKAKU, SHOKAKU, and SHOHO -- sailed from Truk with the same objective but with only one-third the distance to go. Admiral Nimitz, Commander-in-Chief, Pacific Fleet, was able to position the carriers LEXINGTON and YORKTOWN in the Coral Sea to head off Yamamoto's advance. During the 7-8 May Battle of the Coral Sea, U.S. carrier-based planes sank the SHOHO; the SHOKAKU was temporarily disabled, and the ZUIKAKU was diverted elsewhere. The YORKTOWN was damaged and the LEXINGTON was lost; however, the battle had, indeed, foiled the plan of the Japanese to take Port Moresby as a precursor to overrunning Australia. Moreover, the May 1942 Battle of the Coral Sea, fought by carrier-based aircraft, made Nimitz a SIGINT devotee, a major feat considering that many top commanders perceived intelligence as having failed them at Pearl Harbor.[98]

BATTLE OF MIDWAY

Nimitz's new-found trust in SIGINT was immediately put to the test. From intercepted messages, he learned that an attack against the Aleutian Islands, planned for 3 June 1942, was a feint. Instead, the main thrust would be made by the Japanese against Midway Island on 4 June. Messages revealed the strength of Admiral Yamamoto's fleet -- some 200 ships -- including the fleet aircraft carriers AKAGI, KAGA, HIRYU, and SORYU. Then, one week before the battle, the Japanese changed the JN-25b code. However, Nimitz had the information he needed to preposition the aircraft carriers HORNET, ENTERPRISE, and YORKTOWN. By battle's end on 6 June, Japan had lost 4 aircraft carriers, 1 heavy cruiser, between 275 and

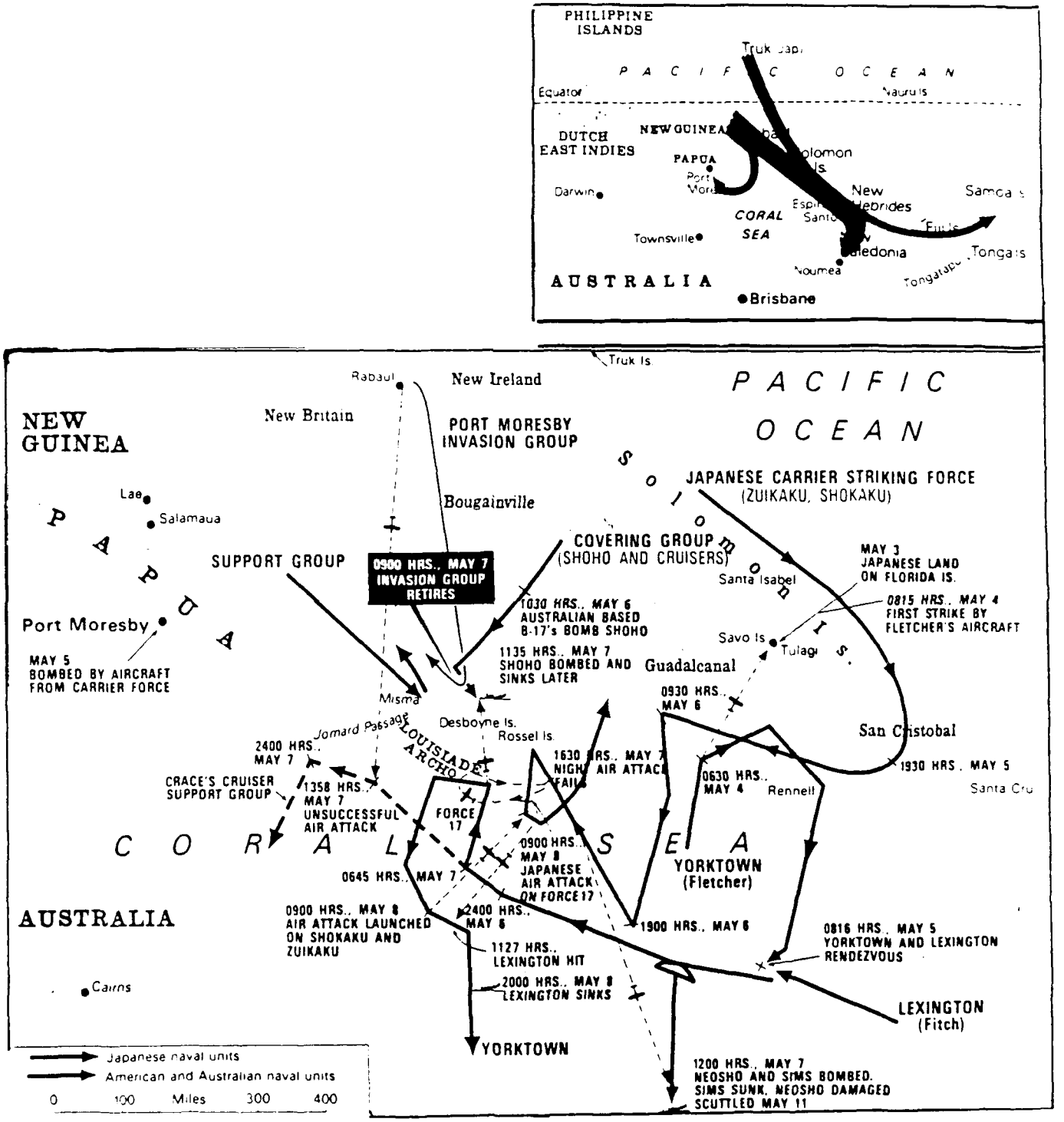


Figure 18

Map of the Battle of the Coral Sea
Simon Goodenough, War Maps, p. 150.
Reprinted with the permission of St. Martin's Press, New York

322 aircraft, 3,500 sailors, and many of its naval aviators, compared to U.S. losses of 1 aircraft carrier (YORKTOWN), 1 destroyer, 150 aircraft, and 307 sailors. The Battle of Midway became a turning-point in the war in the central Pacific, marking the end of the Japanese threat to Hawaii and restoring the balance of power there.[99]

George C. Marshall, Army Chief of Staff, extolled the value of SIGINT in the Japanese defeats at Coral Sea and Midway:

> " ... the battle of Coral Sea was based on deciphered messages and, therefore, our few ships were in the right place at the right time. Further, we were able to concentrate our limited forces to meet their advance on Midway when otherwise we almost certainly would have been 3,000 miles out of place."[100]

That also was the view of Admiral Samuel E. Morison, who called the U.S. Navy's resounding success at Midway "a victory of intelligence bravely and wisely applied."[101] Two Japanese naval officers, Matsuo Fuchida and Matasake Okumiya, agreed with Morison's plaudits, claiming that "it is beyond the slightest possibility of doubt that the advance discovery of the Japanese plan to attack was the foremost single and immediate cause of Japan's defeat."[102]

Following the June 1942 defeat at Midway, the Japanese moved ahead with their plans to attack Port Moresby. In July 1942, Japanese landed troops on the northern coast of New Guinea in the Buna-Gona region, with the intent to move overland to Port Moresby. The Chiefs of Staff in Washington directed Nimitz and MacArthur to begin planning for extensive operations in SWPA: to recapture Tulagi (taken by the Japanese on 1 May) and the neighboring islands; then, through the Solomons to Rabaul; and, finally, the full recovery of New Guinea, opening up the lines between the

U.S., Australia, and New Zealand.

This was not the time to have unreadable Japanese naval codes.[103] However, that was precisely the situation. Cryptologists devoted the bulk of their effort to analyzing message externals through traffic analysis and direction finding in order to reconstruct the Japanese order of battle. (The direction finding was not particularly accurate because only a few intercept stations were involved in trying to pinpoint the locations. Australian coastal watchers became an invaluable corroborating source of information.) Analysis led to the conclusion that the Japanese were consolidating their hold on the Solomon Islands with their 8th and 4th Fleets covering the "Inside" and "Outside" Zones, respectively. By 24 July, three cruiser divisions were known to be in the local order of battle.[104]

GUADACANAL, SOLOMON ISLANDS

On 7 August 1942, a reinforced 1st Marine Division landed at Guadacanal. The Marines gained tactical surprise on the main island of Tenaru but encountered stiff opposition on the neighboring islands of Tulagi and Gavutu. All missions were successfully achieved by 8 August and Henderson Field was abandoned by the Japanese.[105] (see Figure 19)

At the same time that U.S. forces were making their preparations for amphibious assaults, Japanese Admiral Mikawa, 8th Fleet Commander, assembled an impressive strike force east of Bougainville. After coming through "the Slot" of the Solomon Islands, the Japanese, in less than two hours, sank three American heavy cruisers, one Australian cruiser, and seriously damaged another, as well as two destroyers. In addition to these losses, 1,023 Americans were killed and 709 were wounded.[106]

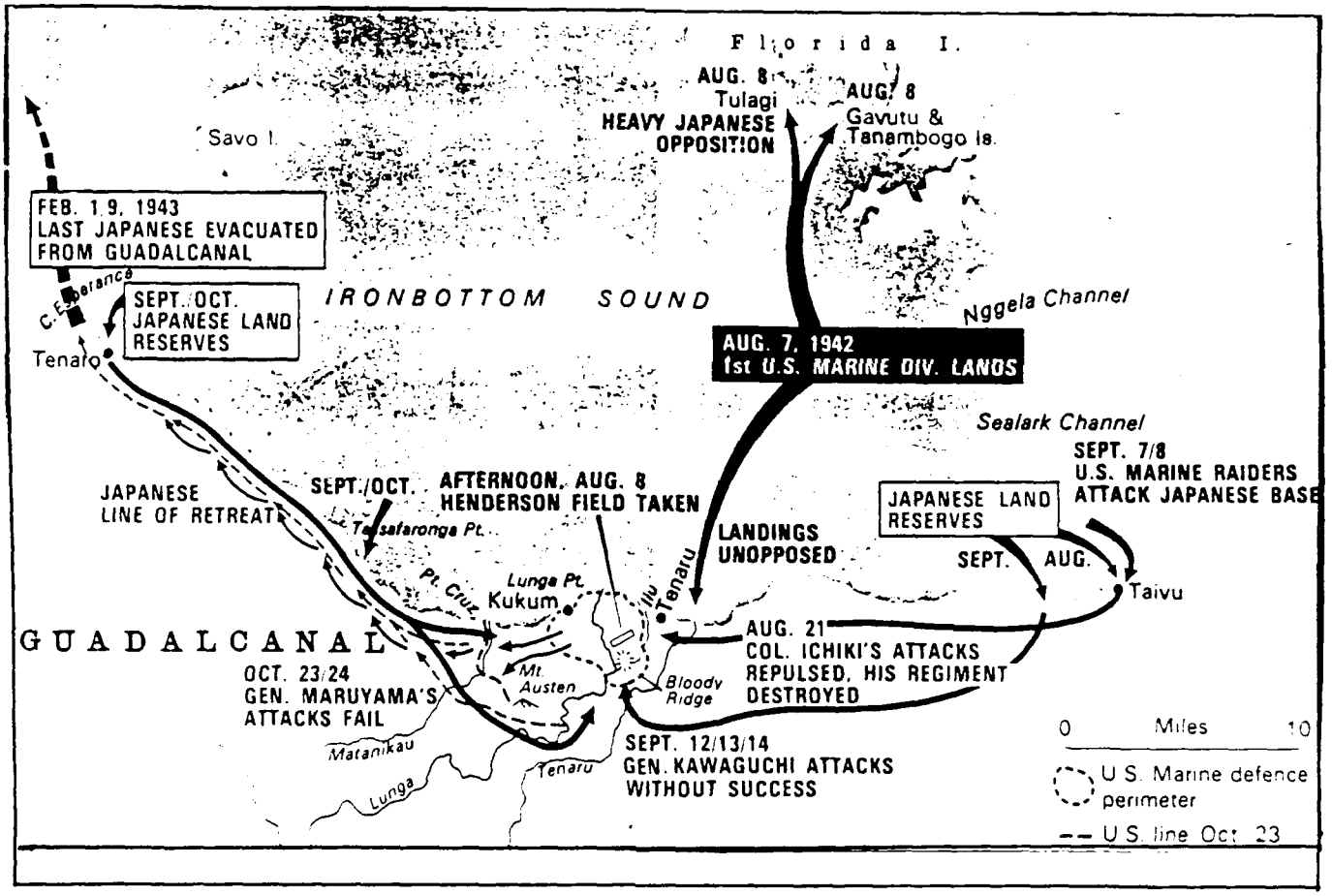


Figure 19

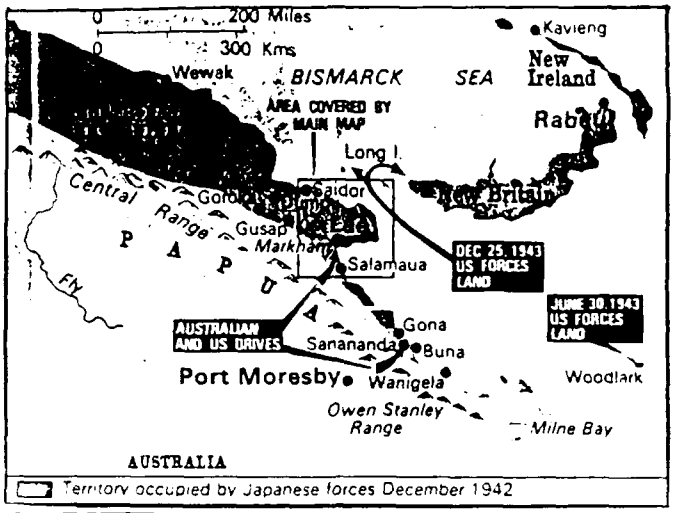
Map of Guadacanal, Solomon Islands
Simon Goodenough, War Maps, p. 156.
Reprinted with permission of St. Martin's Press, New York

Since the JN-25 code was not breaking, commanders did not have the forewarning of the Japanese intentions. However, traffic analysis, low-level codes, direction finding, and the coastal watchers indicated that there was a buildup of Mikawa's forces and suggested a forthcoming attack at Guadacanal. Later, it was learned that Mikawa had sent an execute message at 0800 on 7 August for the Solomon Islands: target Guadacanal.[107]

Ten days into the Guadacanal operation, the Japanese changed their callsigns, depriving military commanders of traffic analysis as well. Costly fighting continued on Guadacanal throughout the summer and the fall of 1942, with both U.S. and Japanese forces receiving large numbers of reinforcements. With the naval Battle of Guadacanal of 12-15 November, the U.S. finally scored a decisive victory. American troops were able to complete their land incursion as well, winning an outstanding psychological and material victory. The Japanese thrust to the south came to an end, they had been denied an important airbase, and, in early 1943, they began their withdrawal.[108]

NEW GUINEA AND BATTLE OF BISMARCK SEA

By February 1943, intelligence warned of a build-up of Japanese troops off the coast of Lae, New Guinea. By 28 February, there were intelligence reports that the Japanese might attempt a landing from Rabaul at Lae on 5 March and at Madang around 12 March. (see Figure 20) The commander of the 5th Air Force, who had developed and had been practicing new methods of aerial attacks against Japanese shipping, was prepared when the Japanese convoy arrived off the coast of northern New Guinea at the beginning of March. The convoy, carrying the 15th Infantry Division, was



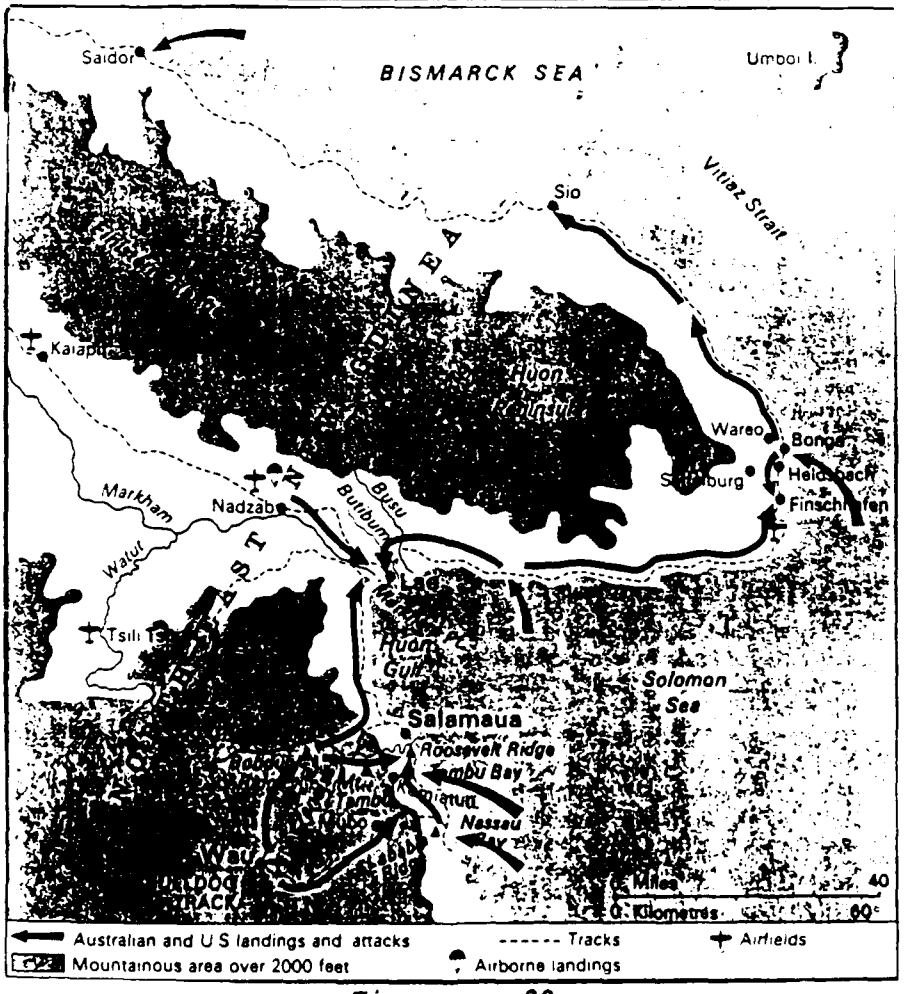


Figure 20

Map of Northeast New Guinea
Simon Goodenough, War Maps, p. 155.
Reprinted with the permission of St. Martin's Press, New York

attacked and 12 transports and 4 destroyers were eliminated. In 400 U.S. sorties, only five aircraft were lost. According to Lewin's assessment of the situation, the Japanese, so discouraged by their heavy losses, did not try again to reinforce the front by large numbers of ships. Further, he called the Battle of Bismarck Sea a "classic example of the effective application of ULTRA" and "a defeat which would prove to be irreversible."[103] Fighting continued in northeast New Guinea, however, for six more months. The Allies captured Salamaua on 12 September and Lae on 15-16 September. From there, they captured the Huon Peninsula and crossed over to New Britain.[109]

YAMAMOTO SHOOT-DOWN

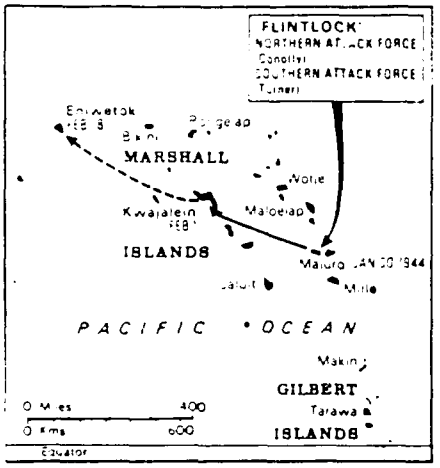
In April 1943, a decrypted ULTRA message revealed that CINC, Combined Forces Yamamoto, precisely at 0945 hours on 18 April, was to visit Ballale Island, just south of Bougainville, in the Solomon Islands, which was just barely within striking distance of American long-range fighters based on Guadacanal. The architect of the Pearl Harbor attack was a very precise person. When his bomber, accompanied by six fighters and another bomber carrying Yamamoto's Chief of Staff, appeared exactly on schedule, P-38's from the Army's 339th Fighter Squadron, Henderson Field, Guadacanal, shot down his plane. The decision to target the p'ane was a very big gamble on the part of decision makers because the Japanese could have suspected a compromise and changed their codes. Consequently, it was the U.S. President who ultimately made that decision. A newspaper claimed that the Yamamoto aircraft downing was a result of a Japanese decrypt. However, U.S. officials attributed their success to a coastal watcher. Other fighter sweeps continued in the area to make it look like the shoot-down had been a fluke encounter. [111]

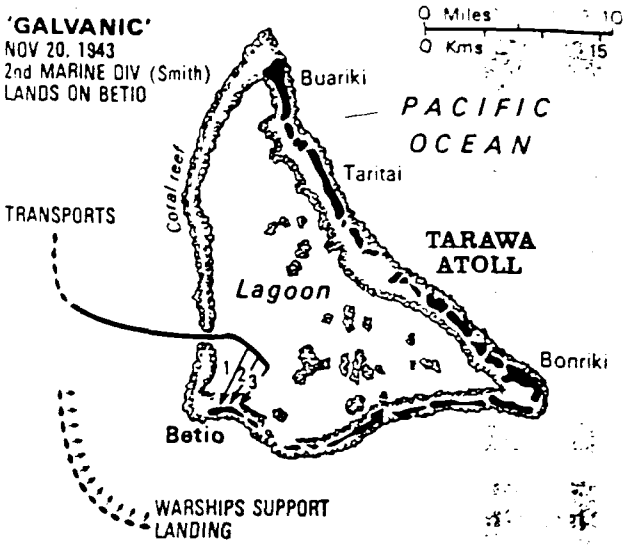
By 1943, the Japanese had sustained enough maritime losses in the Pacific that they, like the Germans, began to travel in convoys. These convoys required communications which contained route assignments, intermediate or final ports of call, and naval and air escort information. The Japanese used the MARU code for passage of this information. It was broken in early 1943 and "U.S. submarine warfare in the Pacific entered a new dimension".[112]

For example, on 9 June 1943, U.S. submarines TRIGGER and SALMON were patrolling the Japanese Inland Sea when they were instructed to intercept the new Japanese aircraft carrier HIYO as it departed Yokosuka. The two submarines went to the location provided in the ULTRA message and fired torpedos. The TRIGGER thought she had become the first submarine to sink an aircraft carrier! In reality, the HIRO was towed to port for repairs and later sank in the June 1944 Battle of the Philippine Sea.[113]

GILBERT AND MARSHALL ISLANDS

Fighting on many of the Solomon Islands continued throughout the summer and the fall of 1943. Meanwhile, further north, Marine and Army elements successfully invaded several atolls in the Gilbert Islands in November. (see Figure 21). SIGINT had provided the theater commanders with outstanding order of bat'le information: unit name; location; strength; available ammunition and rations; commanding officers, etc. However, as Marines waded ashore at Tarawa on 20 November 1943, SIGINT had not been able to provide commanders with topographical information such as unknown or concealed, defensive positions, which caused tremendous casualties to the landing parties. This example points out both the strength and limitation of SIGINT information.[114]





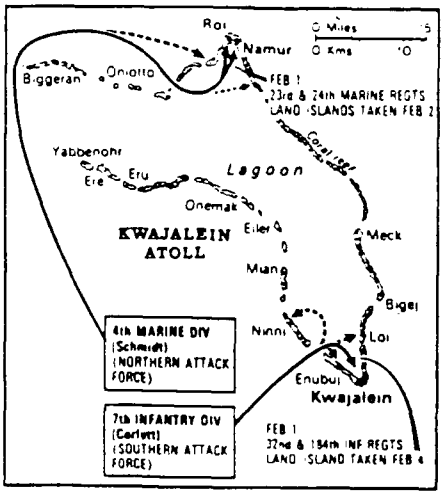


Figure 21

Maps of landings on the Gilbert and Marshall Islands
Simon Goodenough, War Maps, p. 162.
Reprinted with the permission of St. Martin's Press, New York

The landings on the Marshall Islands on 1 February 1944 (Operation FLINTLOCK) were less difficult. (see Figure 21) Kwajalein was taken in four days and the other islands fell within the month. However, the decision to attack Kwajalein was made by Admiral Nimitz over the advice of his commanders because Nimitiz was privy to SIGINT. Whereas his commanders had argued for a naval attack against the secondary/outer islands of Wotje and Maloelap, Nimitz decided to attack Kwajalein. From daily Japanese status reports, Nimitz had learned of a Japanese buildup of naval, army, air, and construction units on the outer islands, a shift outward from Kwajalein. Nimitz' commanders were shocked by his decision.[115]

SUCCESS AGAINST JAPANESE SHIPPING

The war against Japan's maritime shipping, both personnel and logistics, intensified in 1944. ULTRA revealed lists of supplies, cargo, personnel reinforcements, convoy size, escort force, and arrival times of convoys destined for Wewak, New Guinea. Of these, 12 freighters were sunk between 29 February and 24 March 1944 by Allied air or naval forces. Also, ULTRA identified that a convoy was to ferry from Shanghai to New Guinea the 32nd and 35th Divisions (approximately 21,000 men) as reinforcements against MacArthur's advances. Throughout April and May 1944, ULTRA and traffic analysis identified the route and positions of the nine-vessel TAKE convoy as well as her dozen escorts. At several locations, U.S. submarines were able to destroy parts of the convoy. The remaining personnel were rescued and Tokyo decided to abandon the convoy operation. The broken remnants of the two divisions were ferried to New Guinea by landing barges. According to Lewin, this was a "supreme example of how immaculate SIGINT immaculately applied in action could produce a decisive

result." Drea concluded that ULTRA played a critical role in anti-convoy operations during 1944.[116]

The same was true for Allied efforts against Japanese submarines. The U.S adopted the German-introduced "wolf pack" submarine warfare doctrine in the Pacific. With ULTRA providing the tip-offs in 1944, submarines got to the right places at the right time and moved in for the kill. According to Lewin, improved tactics and increasing U.S. strength resulted in the following Japanese losses:

> "Between January and April 1944, U.S. submarines sank 179 ships of some 799,000 gross tons: between May and the end of August a further 219 ships had gone to the bottom, and their ton reckoning had passed the million mark. By the end of 1944, imports of oil, the vital essence of war, had almost entirely ceased and domestic stocks in Japan, as high as 43,000,000 barrels at the end of 1941, sank to less than 4,000,000 by March 1945."[117]

Japanese naval and maritime communications as well as MAGIC provided the bulk of support to military commanders through 1943. However, in early 1944, an entry was made into a primary Japanese administrative code which provided extensive details on Japanese order of battle and the Japanese logistics network. In February 1944, a copy of the code was captured as well as some encoding devices. In the spring of 1944, cryptanalysts broke the code used by the Japanese Army Air Force; it provided timely intelligence on air units' strengths, movements, and states of readiness. So, as MacArthur was receiving instructions to establish a base at Hollandia, New Guinea (by-passing Rabaul) in preparation for an invesion of the Philippines, SIGINT was providing thousands of backlogged messages, offering SWPA commanders an "unparalleled insight into the

thinking of their Japanese adversaries."[118]

HOLLANDIA, NEW GUINEA

Using ULTRA-produced order of battle information, U.S. B-24's and P-38's performed aerial attacks against Hollandia in late March and early April 1944, destroying nearly 131 aircraft at Hollandia and smashing any Japanese ambitions about regaining aerial superiority over New Guinea. ULTRA revealed that Japanese troops around Hollandia during the spring were beginning to thin out as the Japanese were expecting a U.S. attack further south at Wewak. (see Figure 2?) Therefore, under Operation RECKLESS, MacArthur staged an elaborate deception feint at Wewak/the Hansa Bay area, but then landed at Hollandia with a secondary landing at Aitape on 22 April.

An ULTRA message then revealed that the Japanese were planning an all-out attack at Aitape on 10 July in spite of serious logistical problems. This message included the order of battle for the four divisions (20,000 men) involved in the counterattack and the locations to which the rear echelons and army command posts would move just prior to the attack. According to the Combined Bureau, "never has a commander gone into battle knowing so much about the enemy as did the Allied commander at Aitape on 10-11 July 1944."[119] The attack did come on the 10th and the Japanese 18th Army commander lost 9,000 men. Even with his spent force, Adachi Hatazao continued fighting in some capacity, primarily against Australian forces, for nearly a year until Wewak finally fell.

THE MARIANAS: SAIPAN, TINIAN, GUAM, AND PALAU

A new Japanese Naval CINC, the second since Yamamoto, sought a decisive victory at sea. He formed a naval Mobile Force with which he

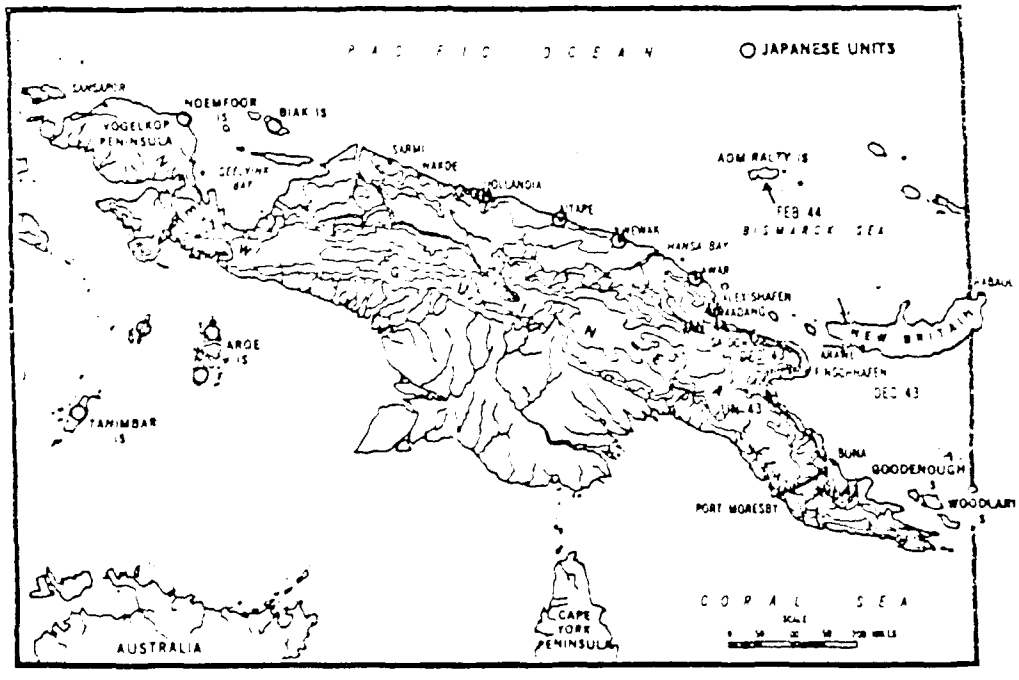


Figure 22

Map of the Allied Advance in New Guinea

Edward Drea, Intelligence and Military Operations in New Guinea, 1942-1944, Fort Leavenworth, Kansas: U.S. Army Command and General Staff College Press, 1984, p. 2.

Reprinted with the permission of Edward Drea and the U.S. Army Command and General Staff College Press.

hoped to lure U.S. naval forces into a battle to which land-based aircraft could lend support. Thinking that MacArthur's forces represented the major axis of advance, Admiral Toyoda deployed many of his aircraft to New Guinea while the Mobile Force was stationed at Tawitawi, off North Borneo. This strategic error wasted between one-third to one-half of his strike force. Much to Toyoda's surprise, by mid-June, Admiral Halsey's fighters and bombers commanded the skies over Saipan, Tinian, and Guam in the Mariana Islands. On 15 June 1944, U.S. Marines landed on Saipan.[120] (see Figure 23)

Meanwhile, the Japanese sent out a message that "the fate of the Empire rests on this one battle. Every man is expected to do his utmost."[121] With part of the Mobile Force in the New Guinea/Borneo area Admiral Ozawa rendezvoused with a Southern Force off the Philippines and prepared to attack. He led his fleet of 9 carriers, 5 battleships, 13 cruisers, and 28 destroyers toward the Marianas through the San Bernadino Strait, in the heart of the Philippines. The U.S. had amassed a great force of 15 carriers, 7 battleships, 21 cruisers, and 69 destroyers, covering hundreds of square miles. Ozawa's scouting planes spotted U.S. forces on the morning of 19 June. The Battle of the Philippine Sea became known as the "Great Marianas Turkey Shoot" as the U.S. carrier-based aircraft wreaked havoc on the Japanese opposition. At the end of the battle, between 300 and 400 Japanese aircraft had been destroyed and 3 carriers sunk. Only 30 U.S. aircraft had been downed.[122]

One of the contributing factors to the U.S. victory was the ex-

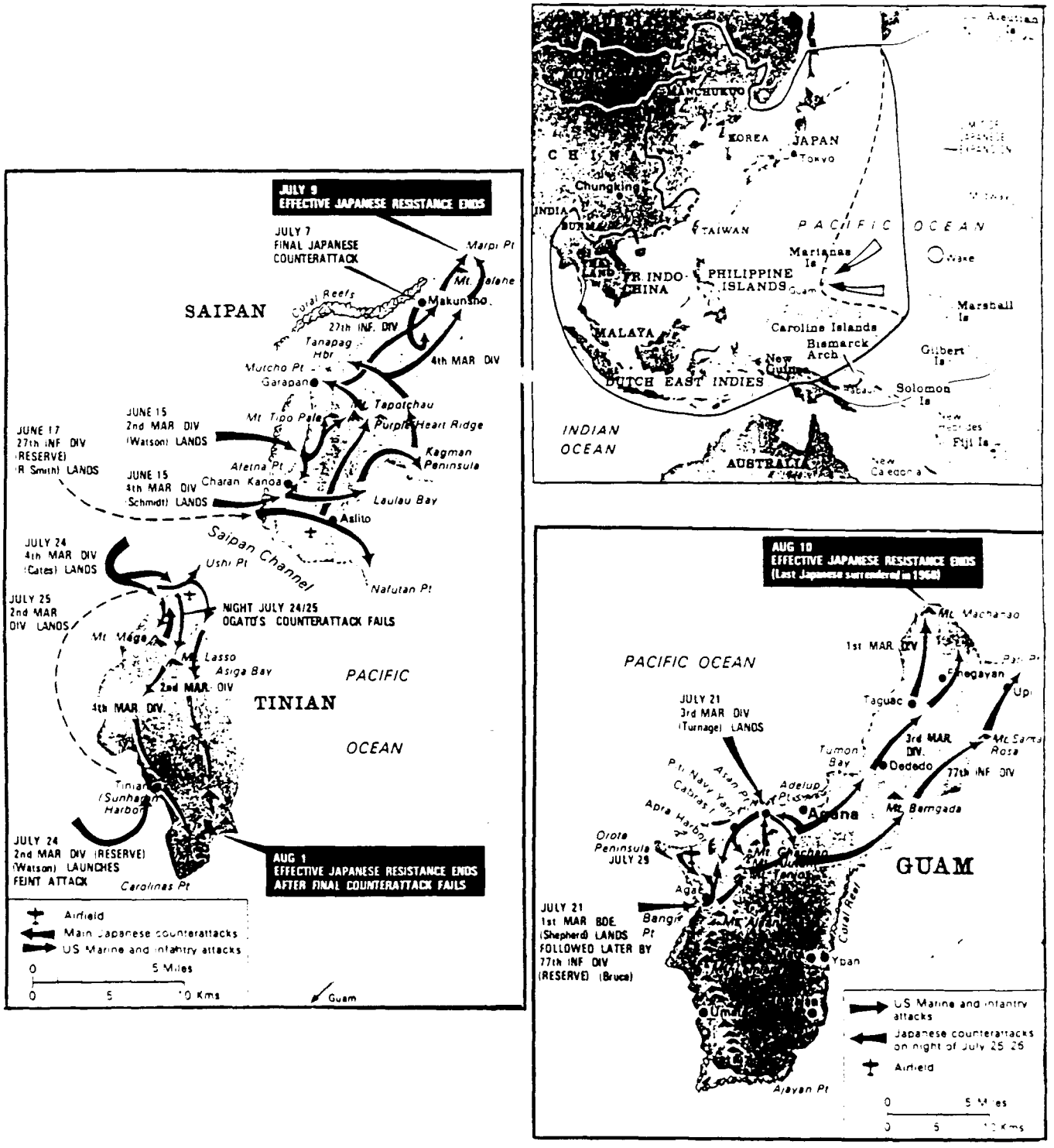


Figure 23

Map of the Battle of the Marianas
Simon Goodenough, War Maps, p. 164.
Reprinted with permission of St. Martin's Press, New York

ploitation of the communications of the Japanese master pilot. From the the flagship, a U.S. SIGINT linguist, well-trained in spoken Japanese, listened to the exchanges of the attacking aircraft and provided real-time tactical support to the U.S. fighter-direction staff. "It was like running an air battle from the bridge."[123]

On 24 and 25 July 1944, Marines launched their attack on Tinian and, on Guam, Marine and Army units staged a joint assault on 25 and 26 July. These incursions on the Marianas chain represented the first penetration of the final Japanese defensive perimeter. The decision was then made to attack the Palau Islands, further west and closer to Japan. Supplemented by a cache of captured documents from Saipan, SIGINT was able to provide, by late July 1944, an extensive unit disposition of all Japanese forces stationed in the Palau Islands. Following the U.S. attack, which began on 15 September, all units on Palau and the surrounding islands, except one, had been just where they were identified in a 28 July ULTRA message entitled "Disposition of Forces". [124]

This is not to minimize the intensity of the fighting for Palau, however. Even with all the forewarning, SIGINT did not reveal the tremendous defenses of off-shore mines, beach obstacles covered by machine guns and artillery, and hidden bunkers and pill boxes. The Marines expected to capture the island in four days; it took two months, claiming nearly 1,800 killed and 8,000 wounded. Because of the Japanese defenses, Admiral Halsey convinced the Chiefs of Staff that the U.S. should proceed with an attack on the Philippines through Leyte Gulf, by-passing Mindinao.[125]

LEYTE, THE PHILIPPINES

In preparation for the Leyte invasion, 1,000 aircraft from Task Force 38 bombed Luzon, Okinawa, and Formosa, destroying about 500 Japanese aircraft. Over Tokyo Radio, the Japanese claimed great victories over U.S battleships and carriers. Through SIGINT, U.S. commanders could monitor the more accurate account of losses as well as the state of Japanese morale. [126]

The SIGINT available to the planners of Operation KING II, derived from Army and Navy ULTRA, was "incessant", according to Lewin. Through intercepted messages, the Americans were able to lay out the structure, organization, location, strength, and movement of Japanese stationed in the Philippines. This information was compared with other SIGINT derived from traffic analysis and direction finding as well as other intelligence media -- captured documents, prisoner of war interrogations, and photography.[127] When the large invasion force landed at Leyte on 20 October 1944, it had been primed with good intelligence. (see Figure 24)

The U.S. 10th and 24th Corps landed and established a beachhead, encountering only slight opposition from Japan's XXXV Army. Meanwhile, the Mobile Fleet and the I Striking Force were approaching the Philippines from the north and west. Vice Admiral Ozawa commanded a Mobile Fleet, steaming south toward the Philippines, which was nearly stripped of naval aircraft after the Marianas and Formosa. Vice Admiral Kurita led the I Striking Force coming from Singapore which was to head east, sail through San Bernadino Strait, and rally in Leyte Gulf with forces of Admiral Nishimura who was headed to Leyte through the Surigao Strait. Nishimura was to be followed by the II Striking Force of Vice Admiral Shima, steam-

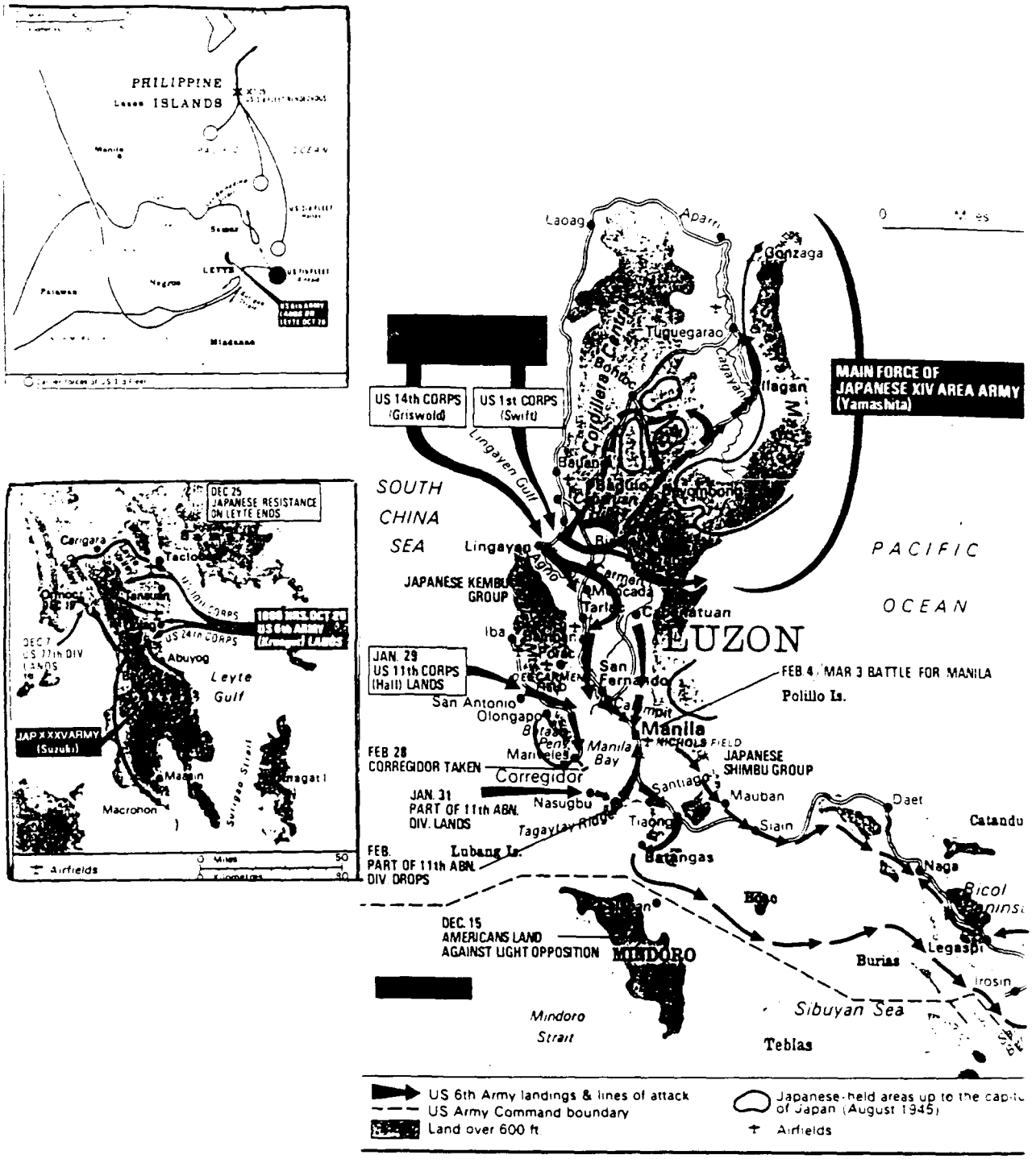


Figure 24

Maps of the Phillipine Campaign
Simon Goodenough, War Maps, p. 168.
Reprinted with the permission of St. Martin's Press, New York

ing from the South China Sea through the Straits.[128]

Facing such overwhelming opposition, Vice Admiral Ozawa decided that he would attempt to lure away some of the U.S. forces supporting the 6th Army's landing. With only 116 aircraft, Ozawa thought that he could make better use of his four carriers and semicarriers if he could draw Halsey's 3rd Fleet further north, away from Leyte Gulf, enabling Kurita to slip safely through the San Bernadino Strait. Ozawa allowed himself to be "detected" by American reconnaissance planes and the chase was on, with Halsey falling to the deceptive defensive plan. However, air attacks against Kurita's forces hindered his steaming time, precluding the Japanese from taking full advantage of Ozawa's daring plan. In the end, Toland concluded, Ozawa's sarifice had been in vain. [129].

For three days, Halsey and Mitscher's forces battled with Ozawa, Nishimura, and Kurita, enabling Kinkaid to protect the landing of 200,000 ground forces at Leyte. By the 25th, the Japanese had lost 4 carriers, 3 battleships, 6 heavy and 3 light cruisers, and 10 destroyers. Approximately 300,000 tons of combat shipping were sunk, more than a quarter of Japanese losses since Pearl Harbor, thereby shattering Japanese sea power.[130]

On Leyte, between October and December 1944, the 10th Corps slowly moved north and the 24th Corps turned south and west, attacking the Japanese stronghold of Ormoc which fell on 10 December. The two corps linked up and staged a number of overland and amphibious operations which culminated in the capture of Leyte by 25 December 1944.[131]

After securing Leyte, the U.S. 1st and 14th Corps, on 9 January

1945, landed without opposition in Lingayen Gulf of Luzon Island. The 1st Corps took on the majority of Yamashita's forces in the north and the 14th Corps turned south toward Manila. Both Task Forces were around Manila by January 1945; but fierce fighting, including street-to-street fighting in the old city, ensued until early March. Meanwhile, on 16 February 1945, airborne troops took Corregidor and, by 13 April, Fort Drum, guarding Manila Bay, was secured. The bulk of the U.S. 6th Army then turned toward the mountain encampments of Yamashita's Army. When the General sued for peace on 15 August 1945, more than 190,000 Japanese had been killed during the fight for Luzon as well as nearly 8,000 Americans.[132]

Lewin makes a good observation about intelligence support to military commanders in the Pacific as the war was reaching its final days:

> "However good the intelligence, however massive the superiority in numbers and equipment, any invader who is drawing close to the heartland of a fanatic, warrior nation must expect battles at least as bloody as those he has so far experienced -- if not bloodier. This was a bitter truth which Ultra could alleviate but not dispel."[133]

This was precisely the case on Iwo Jima and Okinawa as well.

IWO JIMA AND OKINAWA

On 19 February 1945, the U.S. 4th and 5th Marine Divisions, after a prolonged aerial and naval bombardment, landed on Iwo Jima, an eight-mile square island of firmly-entrenched defensive positions and caves. Withstanding fierce coordinated fire, 30,000 Marines landed on the first day and, within four days, raised their flag at Mt. Suribachi in the south. The fight in the north raged on until 26 March; by then, 7,000 Americans and 22,000 Japanese had died.[134]

The attack on Okinawa came on 1 April 1945 with the U.S. 10th Army

tackling the Japanese XXXII Army. U.S. forces cleared the northern part of the island but the heavy defenses of the south pinned down the U.S. 24th Corps. Between 3 and 4 May, the Japanese conducted a suicidal counterattack and resistance continued until 22 June. Again, the casualties were staggering -- 7,500 for the Americans and perhaps as many as 100,000 Japanese died (many trapped in underground caves).[135]

One of the more graphic revelations of signals intelligence during World War II is evident in the following MAGIC decrypt read by U.S. military commanders and political leaders in early August 1945.

> Hiroshima, 6 August 1945:
> "Two or three B-29's penetrated Hiroshima City at high altitude, about 0825, dropping several bombs vicinity Hiroshima City. A terrific explosion accompanied by flame and smoke occurred at an altitude of from 500 to 600 meters. The concussion was beyond imagination, demolishing practically every house in the city. Present estimate of damage: about 80% of the city was wiped out (destroyed or burned). Only a portion of the western section of the town escaped the disaster."[136]

Warfare had entered the nuclear age.

LESSONS LEARNED WITH REGARD TO SIGINT SUPPORT TO MILITARY COMMANDERS DURING WORLD WAR II

These historical vignettes were obviously selected because they exemplified the burgeoning use of modern communications and cryptography to exploit enemy communication weaknesses during World War II. There are those who would claim SIGINT to be the "unsung hero" of that conflict. After examining the ULTRA and MAGIC intelligence support provided to top political and military leaders, Ronald Lewin has suggested that:

> "it has become clear that the whole struggle against Hitler would have to be reconsidered, for never in the history of warfare has it become so rapidly necessary to revise, in a radical fashion, the pre-existing ideas about how battles were fought and strategies devised."[137]

It is not the intent of this paper to overrate SIGINT successes in World War II. It would be instructive, however, to examine some of the shortcomings of SIGINT support to military commanders during that conflict to derive some constructive lessons learned for the 1990's.

MACRO-LEVEL PROBLEMS

LIMITED DISTRIBUTION OF SIGINT PRODUCT: The difficulties associated with breaking German and Japanese codes and ciphers invariably led to the need to protect sensitive sources and methods. SIGINT information was, consequently, provided to only some military commanders. ULTRA usually was not distributed below Army/Tactical Air Command level. There were presumptions that certain people were on distribution for much-needed information, when they were not. Others, it has been said, were put on distribution because of the status SIGINT access afforded, not because the information was needed for operational purposes.

LACK OF TIMELINESS: The tactical exploitation of clear language and lower grade ciphers enjoyed a fairly rapid turn around to supported G-2's. That which required expensive mechanical processing in Washington, Hawaii, or Bletchley Park could be delayed. Also, frequent changes to crypto-variables required time for initial break-through and delayed processing until all settings were recovered. Undoubtedly, field cryptologists could not always meet the needs of a commander on a fluid battlefield. Moreover, inadequate communications linkages between tactical intercept units and Army-level processors and limited SLU's caused time delays as well.

DIMINISHED UTILITY: The need for secrecy regarding cryptographic breakthroughs was imperative. Germany and Japan, throughout the war, did "sanity checks" of their communications, each time concluding that their codes and ciphers were so secure that they continued to pass voluminous information with impunity. There were commanders in World War II who refused to read Special Intelligence and one who chose to go down with the ship rather than risk possible disclosure of this secret, if captured. These extraordinary fears diminished the utility of this information. Other commanders would not use the Special Intelligence unless there was plausible cover and denial by some other intelligence source and, then, only in a sanitized, imprecise form. Although this helped to protect the sensitive source, these restrictions limited SIGINT usage and utility.

FAILURE TO BELIEVE SIGINT MATERIAL: There were many reasons for commanders to doubt SIGINT. Firstly, they thought it had let them down with the failure to predict the Pearl Harbor attack. Secondly, they did not understand signals intelligence, as it had not been part of their military education. There was no doctrine or standard operating procedures governing SIGINT use. Lewin claimed that there was "an almost universal fear

distrust, or misunderstanding of this strange phenomena called SIGINT." Thirdly, even when they "understood" it, commanders did not always know how to integrate it with other intelligence and/or operational plans. Further, as a new art, it was not always precise and correct. Differing interpretations of transcriptions and translations, particularly as they related to jargon and unfamiliar acronyms, sometimes led to inaccurate reporting.

Lastly, some commanders simply refused to believe SIGINT information unless it confirmed their own assessments of a situation. Montgomery and MacArthur were frequently cited among the non-believers. Bradley was not particularly fond of SIGINT but it was said that he had a poor intelligence staff. A student of military history and military art, Patton liked SIGINT and used it. Eisenhower and his G-2, BGen Kenneth Strong, made great use of SIGINT, in spite of some intelligence failures attributed to SIGINT. In all cases, these leaders clearly demonstrated that intelligence is only one tool in decision-making. It is then the military commander who, ultimately, must choose how or if he will use this tool.

OVER-RELIANCE ON SIGINT: A seeming contradiction of the above, some commanders relied almost exclusively on SIGINT, neglecting other intelligence forms. This reliance on ULTRA material, for example, probably caused Eisenhower's G-2 in Tunisia to overlook human intelligence and misidentify the German axis of advance which resulted in heavy losses of U.S. Ist Division during the Battle of Kasserine Pass.

FAILURE TO PROVIDE ALL THE ANSWERS: Even when highly accurate, timely, and detailed, SIGINT still didn't hold all the answers. As described earlier, SIGINT during the war was fairly specific about hard facts (troop strength, disposition, location, casualties, logistics, armament, etc.)

and less likely to provide good information about fighting capabiiities, morale, etc. Moreover, in World War II, SIGINT did not always reflect measurements of a nation's political will or resolve and the decisions of the innermost workings, feelings, and intentions of a nation's leaders and generals. The wartime use of SIGINT clearly demonstrated the need for combining SIGINT with other intelligence (human intelligence or imagery) for the most complete picture/assessment of any situation.

TOO MUCH INFORMATION: Sometimes, there were many smaller bits of SIGINT information available; however, the "big" intelligence picture was not. In her study of the Pearl Harbor intelligence failure, Wohlstetter called this the inability to discern the "signals" from the "noise". In the absence of the enemy's stated overall plan, it became the responsibility of the G-2 to piece together all the SIGINT information and then convince his commander that he was correct. The relationship between the commander and the G-2 often defined the success of those efforts.

LACK OF SIGINT AVAILABILITY: Good target operational and communications security could and did deprive Allied intercept of precious signals intelligence. Extensive use of land line in northern Europe further exacerbated the above.

LACK OF COORDINATED INTELLIGENCE SUPPORT: During World War II, there was no governing body (until late in the war) to pull together all the U.S. service intelligence elements. Consequently, their cryptologic attacks were often made in isolation of one another. Recognition of the need for a joint doctrine toward signals intelligence will be discussed later in this paper. The United States also discovered, in World War II, the need to combine SIGINT operations with its Allies. The British, for example,

provided much of the technical training to U.S. forces during the early years of the war. It goes without saying that combined operations were more difficult. However, by war's end, many of these problems had been overcome and the groundwork laid for future Allied SIGINT collaborative division of effort agreements.

MICRO-LEVEL PROBLEMS

-- Inadequate numbers (sometimes critical shortages) of personnel trained in all aspects of signals intelligence (linguistics, cryptanalysis, traffic analysis, signals analysis, intelligence analysis, signals interception, signal processing, etc.).
-- Inadequate numbers of intercept stations to handle the high volume of message traffic in several theaters simultaneously.
-- Inadequate data storage facilities, requiring immediate SIGINT destruction after reading.
-- Inadequate communications lines to forward collected intercept.

Many of these same concerns have been raised in conjunction with signals intelligence in the post-war period. Needless to say, these have also been concerns of those within the SIGINT community who believe that information must be provided to those who need it in the format, periodicity, and time in which they require this information. The breakthroughs in faster processing and turn-around times, secure communications, improved product timeliness to theater and/or deployed U.S. fighting forces, and sanitized, usable products are representative of the types of changes which have occurred in the SIGINT world, particularly within the last ten years.

Most of that information cannot be provided in an unclassified document. However, a description of the SIGINT process and how that is now designed to support the military commander, throughout the conflict continuum, is the focus of the second half of this paper.

SIGINT RESPONSIBILITY

In the latter stages of the war, the services created a coordinating body to facilitate COMINT cooperation. In 1945, President Truman authorized the Secretaries of War and Navy to bring other U.S. governmental departments and agencies into COMINT association in an organization called the State-Army-Navy Communications Intelligence Board (STANCIB). Following the passage of the 1947 National Security Act, the Defense Department was formed with the Army, Navy, and the newly-created Air Force subordinated to the Secretary of Defense. STANCIB evolved into the United States Communications Intelligence Board (USCIB). The Federal Bureau of Investigation (FBI) and the newly-created Central Intelligence Agency (CIA) were then added as members in 1948.[138]

Improved efficiency through centralization, demobilization, economization in the immediate post-war period were driving factors for consolidating service cryptologic assets into one national agency. In 1949, the Armed Forces Security Agency (AFSA) was formed, with the naval component at Nebraska Avenue in Washington, D.C. and the army component at Arlington Hall, Virginia. AFSA had great difficulty in overcoming a sense of "separateness", eliminating interservice rivalry, and building upon the technological breakthroughs of World War II cryptology. By the 1950's:

> "the quality of strategic intelligence derived from COMINT fell below that which had been provided in World War II. Consumers were disappointed and increasingly critical. By late 1951, AFSA had clashed with the service cryptologic agencies, with consumers, with the CIA, and with the State Department, although not all at one time nor with all on one issue. Despite the

intentions, AFSA had, in fact, become a fourth military cryptologic agency."[139]

On 13 December 1951, President Truman ordered that a special committee, under the chairmanship of lawyer George Brownell, analyze the cryptologic community and make recommendations regarding economization and greater efficiency. In June 1952, the Brownell Commission recommended the formation of a unified COMINT agency with greater powers in conjunction with clearly-defined responsibilities. Moreover, the Commission recommended that this agency be made directly subordinate to the Secretary of Defense, acting with the Secretary of State on behalf of the National Security Council. Brownell further proposed that the unified agency be controlled by a reconstituted USCIB, under the Chairmanship of the Director of Central Intelligence, so that military and non-military intelligence concerns would be more evenly balanced. In October 1952, President Truman adopted much of the Brownell Commission report and issued a revised version of National Security Council Intelligence Directive (NSCID) 9.[140]

The production of COMINT for both military and nonmilitary consumers was considered to be a national mission; therefore, the new unified cryptologic agency was named the National Security Agency (NSA). The Joint Chiefs of Staff were no longer in the chain of command, since the Director of NSA reported directly to the Secretary of Defense through an office which dealt with sensitive operations. The Secretary of Defense was designated the Executive Agent for COMINT but was instructed to delegate COMINT responsibilities to NSA's Director who, in turn, was to most effectively apply all U.S. cryptologic resources to fulfill the national requirements levied on NSA by USCIB. On 4 November 1952, Army MGen Ralph

Canine became the first Director of NSA. In 1957, NSA consolidated its headquarters operations at Fort George G. Meade, Maryland.[141]

After two decades of growth and experimentation with problems of inter-service cooperation, President Nixon was persuaded that further centralization was required. He issued a memorandum in November 1971, calling for a unified cryptologic command under the Director, NSA. That was implemented by DoD through the creation in 1972 of the Central Security Service (CSS), producing an economical and effective cryptologic structure within DoD, in accordance with the 1971 DoD Directive S-5100.20, "The National Security Agency and the Central Security Service". Since that time, the Agency has been known as the National Security Agency/ Central Security Service (NSA/CSS) with a three-star flag officer serving as both Director, NSA and Chief, CSS.[142] In this capacity, he supervises and directs the Service Cryptologic Elements (SCEs) -- the Army Intelligence and Security Command (INSCOM), the Naval Security Group (NSG), and the Air Force Electronic Security Command (ESC); their subordinate elements; and integral cryptologic elements of military tactical or combat commands, including those of the U.S. Marine Corps.[143] (see Figure 25)

Other documents defining SIGINT responsibilities and relationships include: National Security Council Intelligence Directive (NSCID) No. 6, "Signals Intelligence", dated 17 February 1972; DoD Directive S-3115.7, "Signals Intelligence (SIGINT)", dated 25 January 1973; and Executive Order 12333 signed by President Ronald Reagan on 4 December 1981. Executive Order 12333 charged NSA with the following SIGINT responsibilities:

-- establishment and operation of an effective and unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through

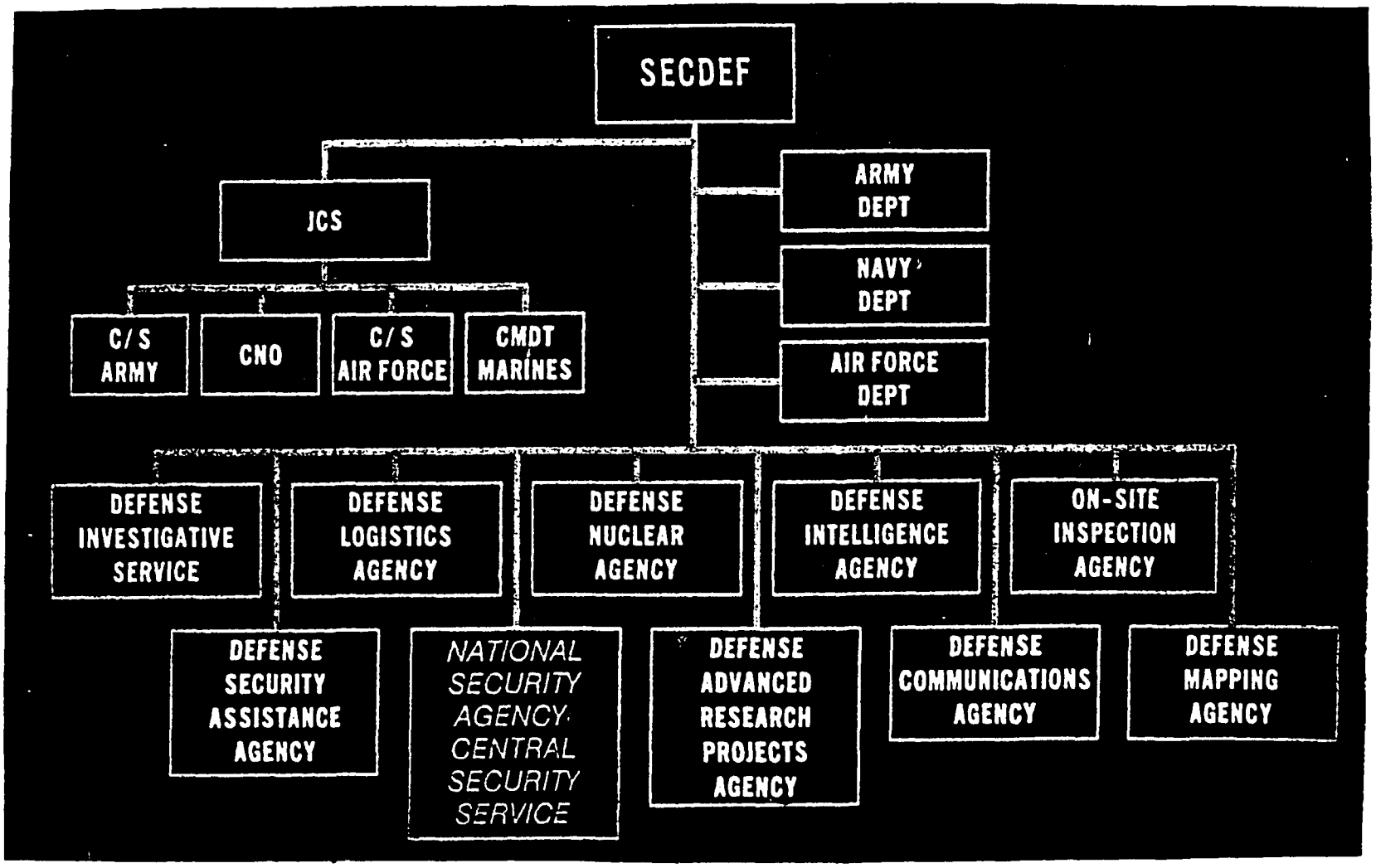

SECDEF
JCS
ARMY DEPT
NAVY DEPT
AIR FORCE DEPT
C/S ARMY
CNO
C/S AIR FORCE
CMDT MARINES
DEFENSE INVESTIGATIVE SERVICE
DEFENSE LOGISTICS AGENCY
DEFENSE NUCLEAR AGENCY
DEFENSE INTELLIGENCE AGENCY
ON-SITE INSPECTION AGENCY
DEFENSE SECURITY ASSISTANCE AGENCY
NATIONAL SECURITY AGENCY· CENTRAL SECURITY SERVICE
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
DEFENSE COMMUNICATIONS AGENCY
DEFENSE MAPPING AGENCY

Figure 25

other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense.

-- control of signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders.

-- collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence.

-- processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence.

-- dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military services, in accordance with guidance of the Director of Central Intelligence. (NSA produces SIGINT information; other intelligence agencies combine the SIGINT with other material to produce finished intelligence.)

-- collection, processing, and dissemination of signals intelligence information for counterintelligence purposes.

-- provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provision of such support requires use of national collection systems, these systems will be tasked within existing guidance from the Director of Central Intelligence.

-- conduct of research and development to meet the needs of the United States for signals intelligence and communications security.[144]

The Secretary of Defense is the Executive Agent of the U.S. Government for the conduct of SIGINT activities in accordance with Executive Order 12333 and NSCID 6 and is responsible for the direction, operation, control, and fiscal management of the National Security Agency. National Security Decision Directive 204, dated 24 December 1985 and implemented through DoD Directive S-3325.2, dated 18 June 1987, addresses the transfer of National Collection Tasking Authority between the Secretary of Defense and the Director of Central Intelligence.[145]

As a result of the above authorization, the Director, NSA/Chief, CSS

is charged to provide for the SIGINT mission of the United States; to produce SIGINT reports in accordance with objectives, requirements, and priorities established by the Director of Central Intelligence; and to serve as the principal SIGINT advisor to the Secretary of Defense, the Director of Central Intelligence, and the Joint Chiefs of Staff. The Director, NSA/Chief, CSS exercises these responsibilities and authorities across the entire conflict continuum -- peace through combat (to include exercises) and, as such, works in close coordination with the Office of the Secretary of Defense and the Joint Chiefs of Staff to provide SIGINT support to the National Command Authorities, military commanders, and other agencies and organizations, as appropriate.[146]

As a result of the Goldwater-Nichols Department of Defense Reorganization Act of 1986, NSA/CSS was designated a DoD Combat Support Agency (CSA) by the Secretary of Defense on 21 June 1988.[147] MJCS-111-88, "Concept of SIGINT Support to Military Commanders" (10 August 1988), together with the SECDEF-approved criteria developed jointly by JCS and NSA, provide the agreed-upon basis for NSA/CSS participation in joint evaluations, joint exercises, and combat readiness in support of military commands worldwide.[148] NSA's CSA role will be discussed more thoroughly below.

In summary, the above-outlined documentation makes NSA responsible for the overall management of U.S. SIGINT efforts which are responsive to the intelligence policies, needs, and priorities of the Director of Central Intelligence, while functioning within the framework of the Department of Defense. Although that may appear as a disjointed chain-of-command, an explanation of the Intelligence Community and NSA's role within it, and the means by which the Executive Department levies its requirements on NSA should eliminate that seeming hierarchical inconsistency.

INTELLIGENCE AND THE EXECUTIVE AND LEGISLATIVE BRANCHES

Executive Order 12333, entitled "United States Intelligence Activities", charges the Intelligence Commmunity to undertake intelligence activities necessary for the conduct of foreign relations and the protection of national security of the United States including:

-- collection of information needed by the President, the National Security Council, the Secretaries of State and Defense and other Executive Branch officials in support of their decisions concerning the conduct and development of foreign, defense, and economic policy and the protection of U.S. national interests from foreign security concerns. This collection is to maintain a balance between technical collection efforts and other means.

-- production and dissemination of intelligence. Moreover, intelligence agencies are encouraged to develop a free and fair exchange of information in order to derive maximum benefit from each other's efforts.

-- collection of information concerning the conduct of activities to protect against intelligence activities directed against the U.S. as well as international terrorist and narcotics activity directed against the U.S. by foreign powers, organizations, persons, and their agents.[149]

In order to execute the responsibilities outlined above, the Director of Central Intelligence (DCI) is directly responsible to the President and the National Security Council (NSC) and is to:

-- act as the primary advisor on national foreign intelligence and to provide the President and other Executive Department officials with national foreign intelligence.

-- develop objectives and guidance needed to enhance capabilities for anticipated national foreign intelligence needs.

-- establish uniform criteria for the determination of relative priorities for the transmission of critical national foreign intelligence and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such intelligence.

-- have full responsibility for production and dissemination of national foreign intelligence and authority to levy analytic tasks on departmental intelligence production organizations, in consultation with those

organizations, ensuring that appropriate mechanisms for competitive analysis is developed so that diverse points of view are considered fully and differences of judgment are brought to the attention of national policy makers.

-- ensure the timely exploitation and dissemination of data gathered by national foreign intelligence collection means and ensure that the resulting intelligence is disseminated immediately to appropriate government entities and military commands.

-- establish mechanisms which translate national foreign intelligence objectives and priorities approved by the NSC into specific guidance for the Intelligence Community, resolve conflicts in tasking priorities, and provide for the development of plans and arrangements for transfer of desired collection tasking authority to the Secretary of Defense when directed by the President.

-- together with the Secretary of Defense, ensure that there is no unnecessary overlap between national foreign intelligence programs and Department of Defense intelligence programs, consistent with the requirements to develop competitive analysis.[150]

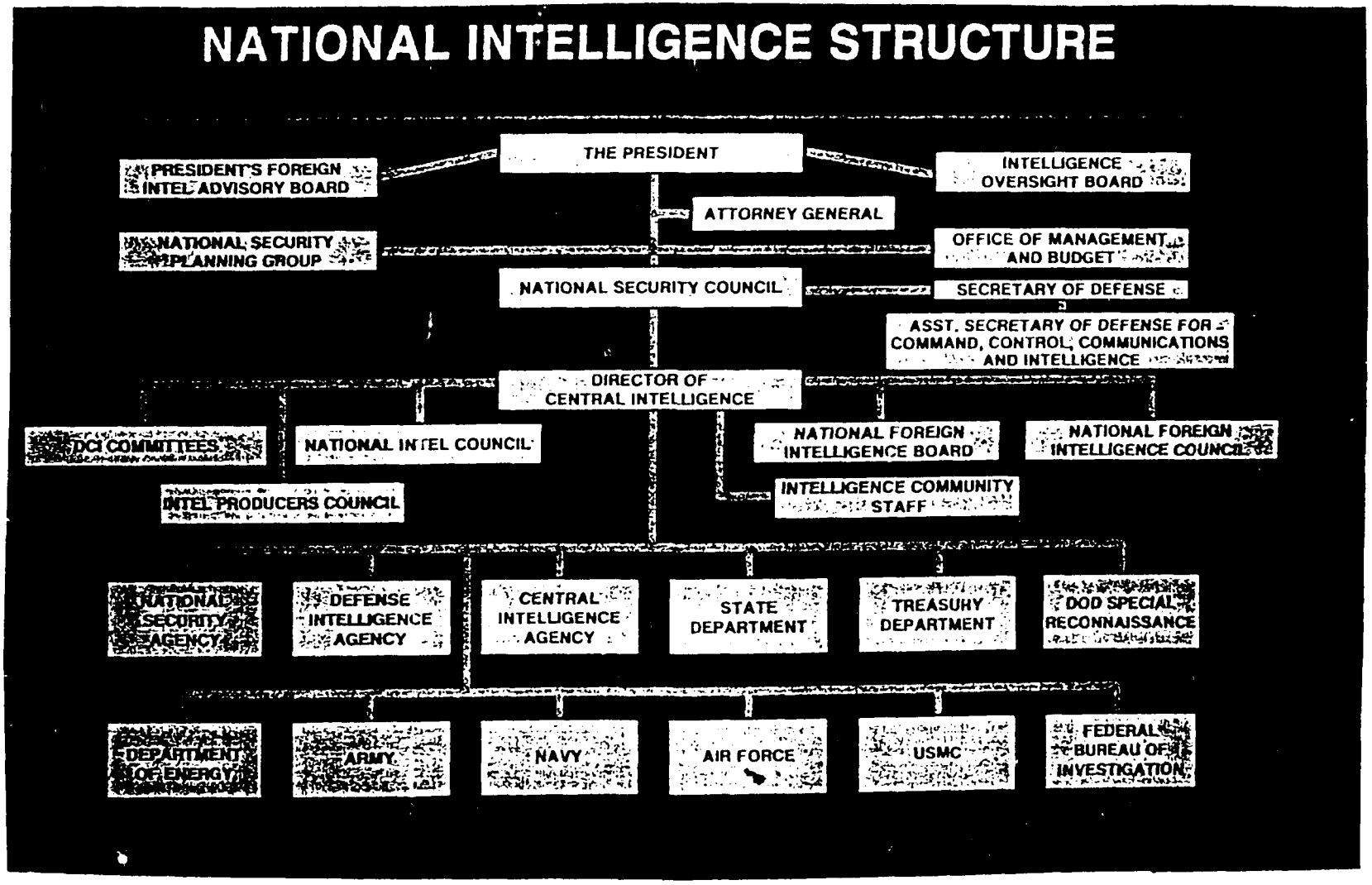
INTELLIGENCE COMMUNITY MEMBERSHIP

NSA's role within the Intelligence Community has already been defined. The other members of the Intelligence Community are listed below. Their differing mission statements are also codified in Executive Order 12333. A schematic of the Intelligence Community structure is found in Figure 26.

THE CENTRAL INTELLIGENCE AGENCY (CIA) - collects, produces, and disseminates foreign intelligence, counterintelligence, and intelligence related to the foreign aspects of narcotics production and trafficking. Moreover, CIA conducts counterintelligence activities outside the U.S. or within the U.S. in conjunction with the Federal Bureau of Investigation (FBI). Executive Order 12333 also empowers the CIA to conduct special activities approved by the President.[151]

THE DEPARTMENT OF STATE (BUREAU OF INTELLIGENCE AND RESEARCH) - overtly collects, produces, and disseminates foreign intelligence relating to

NATIONAL INTELLIGENCE STRUCTURE



U.S. foreign policy. Moreover, the Department of State tasks Chiefs of Mission with the reporting requirements of the *Intelligence Community* and disseminates reports received from U.S. diplomatic and consular posts.[152]

DEPARTMENT OF THE TREASURY - overtly collects foreign financial and monetary information and participates with the State Department in the overt collection, production, and dissemination of general foreign economic intelligence information.[153]

DEPARTMENT OF DEFENSE - collects, produces, and disseminates military and military-related foreign intelligence and conducts programs and missions necessary to fulfill national, departmental, and tactical foreign intelligence requirements. Moreover, DoD conducts counterintelligence activities in support of DoD components outside the U.S. in coordination with the CIA and within the U.S. in coordination with the FBI. Additionally, DoD establishes and maintains military intelligence relationships and military exchange programs with selective foreign defense establishments and international organizations. Lastly, as outlined above, DoD conducts signals intelligence and communications monitoring as the executive agent of these activities.[154] Intelligence agencies other than NSA which fall under the Department of Defense are:

-- DEFENSE INTELLIGENCE AGENCY (DIA) - collects, produces, and provides military and military-related information for the Secretary of Defense, the Joint Chiefs of Staff, other Defense components, and, as appropriate, non-Defense agencies and collects and provides military intelligence for for national foreign intelligence and counterintelligence products. DIA is the DoD HUMINT mamager and manages the Defense Attache system and serves as the *J-2 (Intelligence Staff) for the JCS.*[155]

-- SPECIAL RECONNAISSANCE PROGRAMS - carry out consolidated recon-

naissance programs for specialized intelligence and respond to tasking in accordance with procedures established by the DCI.[156]

-- SERVICE INTELLIGENCE COMPONENTS - consisting of the foreign intelligence and counterintelligence elements of the Army, Navy, Air Force, and the Marine Corps, which collect, produce, and disseminate military and military-related foreign intelligence, counterintelligence, and the foreign aspects of narcotics production and trafficking in coordination with CIA and the FBI. Moreover, they conduct counterintelligence activities outside the U.S. in coordination with the CIA and the FBI.[157]

DEPARTMENT OF ENERGY - participates with the State Department in overtly collecting, producing, and disseminating information related to foreign energy matters while lending their expert technical, analytical, and research capabilities to other Intelligence Community members. Moreover, they levy requirements on other Intelligence Community members, as required.[158]

FEDERAL BUREAU OF INVESTIGATION (FBI) - conducts counterintelligence and coordinates counterintelligence activities within the U.S. with other agencies within the Intelligence Community and, with the CIA, outside the U.S. Moreover, the FBI conducts within the U.S., when requested by officials of the Intelligence Community and directed by the President, foreign intelligence collection for the purpose of producing and disseminating foreign intelligence.[159]

SIGINT differs from the intelligence produced by CIA, DIA, State, Treasury, FBI, Energy, DoD Special Reconnaissance, and the Service component intelligence agencies because of the manner of collection of target communications. From the above mission statements, it should be apparent that NSA is the only intelligence agency which is tasked to col-

lect intelligence signals derived from foreign communications -- whether they be COMINT, ELINT, or FISINT -- by targeting foreign communicants or emitters, regardless of their mode of transmission. As revealed in the historical section of this paper, these signals are used for indications and warning of upcoming events or military actions, insight into an opposing commander's intent, or the specifics of his battlefield plans and troop disposition. Moreover, SIGINT can provide insight into a nation's political intentions and diplomatic maneuvering as well as its economic plans and status.

The Executive Order allows for different collection methods employed by various intelligence agencies. In fact, a similar requirement for information may be levied against the entire Intelligence Community, with each member employing its own unique resources and capabilities for requirement satisfaction and, perhaps, reporting intelligence information as seen through the prism of its own sources. Not only does Executive Order 12333 acknowledge the differences in mission, but it directs that maximum emphasis be given to fostering analytical competition among Intelligence Community members. Although intelligence consumers have frequently criticized the diversity of intelligence information, producers generally have favored the freedom to express divergent views. According to Thomas Hughes:

> "Consistency, after all, is not a goal of intelligence. ... As a vehicle for ventilating a variety of viewpoints, the intelligence process should be highly suspicious of consensus. ... The freedom to be inconsistent is a major argument bolstering the independence of the Intelligence Community."[160]

In several of his books on intelligence and the military commander,

Michael Handel has spoken of the commander's need for multiple intelligence inputs and some of the advantages and disadvantages of multiple advocacy. It is Handel's contention that the military commander really would like to do his own intelligence analysis. However, his own busy schedule, the growth of the Intelligence Community, the distinctive agency/department missions (as outlined above), and their publication of their own specialized intelligence products (all of which may be on the same subject but contain different sources of information) have made it impossible for the military commander to act as his own intelligence analyst.

Consequently, the commander has come to rely on his intelligence staff to sort through this information, culling out and providing him with a range of intelligence estimates/options which best satisfy his requirements. The military commander should foster an atmosphere in which conflicting information can be surfaced and analyzed; competitive analysis should lead to higher-quality decisions. In this manner, the intelligence staff and the commander have used the multiple advocacy system in a constructive fashion.[161]

However, the military commander and his intelligence staff can also use multiple advocacy in an adversarial fashion, playing off one intelligence agency against another and invariably causing some friction among all concerned. In the end, Handel concluded, the military commander may then pick the information from the agency which he most respects or which most clearly reflects his own mind set (paradigm). On the other hand, if he has no previous policies or preconceived ideas, he may formulate a compromise position from among the inputs and pursue a less effective policy.[162]

In his discussion of the make-up of the Intelligence Commmunity and its ability to accomplish its diverse missions, LTG William E. Odom, the Director of the NSA between 1985 and 1988, stated:

> "The Intelligence Community is institutionally fragmented. It is spread out through several executive departments and agencies. Its biggest customer is the military services. Getting this fragmented community to operate effectively with the military is not easy. When it does act as a whole, and when it does accept its intimate relationship with the operational staffs of the services and the unified commands, the results are truly impressive. Making progress in this regard brings turf conflicts, concerns with security, concerns with who gets the credit. Sometimes, ignorance about our capabilities, both within the Intelligence Community and within the services, causes a less than desired result. New technologies, delicate operational details, and lack of experience in coordination also add to the difficulties in achieving all that is possible in providing intelligence support. We should not be surprised, therefore, at some of our failures, but we also should not be parochial in overcoming them. The symbiosis that we gain through cooperation is remarkable, too remarkable to let cooperation go unattended. The trend in this regard is good."[163]

INTELLIGENCE COMMUNITY OVERSIGHT

The intelligence collection, analysis, and reporting functions of these agencies of the intelligence community have caused them to be scrutinized closely, especially after sensationalized charges of abuses surfaced following the mid-1970's House and Senate investigations of the Intelligence Community. Consequently, Presidents Ford and Carter instituted specific "watch dog" committees designed to preclude unauthorized activities while also clarifying intelligence supervisory responsibilities. During the same period, House and Senate intelligence oversight committees also were formed.

PRESIDENTIAL FOREIGN INTELLIGENCE ADVISORY BOARD (PFIAB) - is the successor to the President's Board of Consultants, appointed by President Eisenhower in 1956. After an on-again, off-again history, PFIAB was reconstituted by President Reagan in 1981 through Executive Order 12331. The number of members was reduced by President Bush from 14 to 4 members, appointed from outside the government because of achievement, experience, and independence. The PFIAB has no authority over the Intelligence Community; instead, it makes recommendations to improve operational efficiency relating to collection, evaluation, and production of intelligence or to the execution of intelligence policy. Moreover, it reviews Intelligence Community administrative matters such as management, personnel, and organizational policies at a "macro" level. Like the Presidential Intelligence Oversight Board (PIOB), there has been some criticism about its objectivity, because some members have held previous high-level government positions.[164]

THE PRESIDENT'S INTELLIGENCE OVERSIGHT BOARD (PIOB) - was created by President Ford in 1976 to monitor potentially illegal or improper intelligence activities and to clarify, at the national level, intelligence supervisory responsibilities. President Reagan reconfirmed PIOB's role through his 4 December 1981 Executive Order 12334, making it a part of the Executive Office of the President. Functioning within the White House, its three members, appointed from outside the government, are to examine intelligence activities and to inform the President and the Attorney General if there are any questions regarding potential illegality or impropriety when compared to the U.S. Constitution, U.S. law, or Presidential Executive Orders. Additionally, the PIOB is responsible for reviewing internal intelligence agency guidelines, inspector general and

general counsel procedures, and reporting to the Attorney General. The Attorney General, in addition to acting upon the reports forwarded by the PIOB, is charged with establishing and approving operational procedures to ensure that Intelligence Community activities are conducted in accordance with law. Additionally, he is to ensure that such procedures protect individual rights. Criticism has surfaced regarding PIOB's utility and objectivity, given that it is a part of the Executive Branch.[165]

SENATE SELECT COMMITTEE ON INTELLIGENCE (SSCI) - was created by Senate Resolution 400 in 1976. It has legislative and oversight jurisdiction over the DCI and CIA, including budget authorization. The SSCI stated in 1977 that it intended to: obtain information relevant to foreign policy decisions; use the budget process as a control mechanism; investigate improprieties as a means of Intelligence Community control; and review covert action proposals. The SSCI also considers nominations of the DCI and the D/DCI. The SSCI has four subcommittees: Analysis and Production; Legislation and Rights of Americans; Collection and Foreign Operations; and Budget.[166]

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE (HPSCI) - was created by House Resolution 658 in 1977. It, too, has legislative and oversight jurisdiction over the DCI and CIA and must be informed of covert actions. Its three subcommittees are: Legislation; Program and Budget Authority; and Oversight and Evaluation.[167]

Although both committees have similar jurisdictions, they do not work wholly in tandem, often pursuing different areas of interest and different political agendas. The two committees have, thus far, resisted any moves for merger.

In 1978, the Foreign Intelligence Surveillance Act (FISA) was passed, mandating judicial warrants for all electronic surveillances for foreign or counterintelligence purposes in the United States when communications of U.S. persons might be intercepted. "Not only did the president thereby submit to congressional rule-making in a field long held to be his protected national security sanctuary, but he also submitted to a system of judicial review, to be conducted by the Foreign Intelligence Surveillance Act court, of specific operational proposals."[168]

There are differences between Executive and Legislative Branch oversight. Executive Branch oversight deals primarily with possible abuses of authority or inappropriate activities. Further, Executive Branch boards evaluate operational effectiveness and possible need for systemic change at a "macro" level. Legislative Branch oversight can focus on the same concerns, but its primary areas of interest are covert intelligence operations oversight and the intelligence community budget.

BUDGETING FOR INTELLIGENCE

Resource management of the Intelligence Community is through the National Foreign Intelligence Program (NFIP) which includes the programs of the CIA, the intelligence programs within DoD, and other programs of agencies designated by the DCI or the President. The DCI has budgetary approval authority for the NFIP and must justify his requirements when the budget goes before Congress. There are 13 programs within the NFIP.[169]

Two of the larger intelligence programs under the NFIP are the General Defense Intelligence Program (GDIP) and the Consolidated Cryptologic Program (CCP). The program manager for the CCP is the

Director, NSA as the CCP includes resources for SIGINT projects and activities. Program management for the GDIP is provided by the Director, DIA as it includes funding for the Defense Intelligence Agency, Service human intelligence programs, intelligence data handling systems, intelligence production activities of the Services, technical reconnaissance, and some intelligence activities of unified and specified commands.[170]

In addition to the NFIP budget and of special interest to military officers, many intelligence resources are included under the Tactical Intelligence and Related Activities (TIARA) program. TIARA includes most intelligence resources which directly support operational commanders, as will be discussed below, including military intelligence (MI) Combat Electronic Warfare Intelligence (CEWI).[171]

As a result of Goldwater-Nichols, unified and specified (U&S) commanders now formally participate in the Planning, Programming, Budgeting and Evaluation System (PPBES), including budgeting for intelligence resources. U&S Commands identify their intelligence collection, analysis, and dissemination resource requirements through the Theater Intelligence Architecture Program (TIAP).[172]

By the early 1980's, there was an Intelligence Community structure in place, the activities of which were being monitored by both the Executive and Legislative Branches of government. We will turn now to the process which drives intelligence production and the specific mechanism by which the SIGINT process is tasked in both peacetime and during crisis and war and the capability of the USSS to respond to those requirements.

THE INTELLIGENCE CYCLE

At the national level, the intelligence cycle is a logical but interactive process whereby intelligence consumers express their requirements and the Intelligence Community accepts, validates, and attempts to satisfy those requests for information. Although different analysts and authors view this process somewhat differently, the intelligence cycle generally contains the following interrelated steps.

REQUIREMENT REFINEMENT, PLANNING, AND DIRECTION: This initial step is both the beginning and end of the cycle -- the beginning because it involves the generation of collection requirements and the end because the resultant product can generate new requirements. It very simply begins with a statement of need, either generated top down from the President, National Security Council, or an Executive Department (including the U.S. military) or bottom up from an analyst who requires information to fulfill a levied requirement for intelligence production. At some location within an organization (probably within a staff element), a review of current intelligence collection is conducted in order to determine the priority of this new requirement and whether this intelligence task warrants the development of a collection requirement as well.

COLLECTION ANALYSIS AND OPERATIONS: This step involves the analysis of the requirement to determine if it can be satisfied by a particular discipline -- signals intelligence; agent or human intelligence; imagery or photographic intelligence; or open sources (newspapers, books, periodicals, etc.). The task is then levied against the appropriate collection discipline at the priority determined by the Director of Central Intelligence.

PROCESSING: This step involves the conversion of vast amounts of information into a more usable form which can be manipulated by an analyst. Data reduction also occurs at this step within the cycle.

SUBSTANTIVE ANALYSIS: During this step, a further reduction of applicable data occurs as an analyst integrates, evaluates, and studies possibly fragmentary and contradictory information. In this manner, the analyst weighs the information in terms of its reliability, validity, and relevance while integrating the data, placing it in its proper context, and arriving at a valid conclusion.

PRODUCTION AND DISSEMINATION: The analyses are then published in either hard-copy or electrical format to those same people who initially requested the information, as well as others who might have similar intelligence needs. The receipt of this information answers the question which then terminates the requirement, causes new requirements to be generated, or results in the formulation of a standing intelligence requirement.

The intelligence cycle may appear as a sequentially, cyclical process; however, it is dynamically interactive. At any one point in the process, something may occur which will impact on another part of the cycle. For example, an increase for collection on subject A may cause a drawdown of the effort on subject B. A discovery during the processing step may cause the generation of new collection requirements. A need for increased timeliness in production may force changes in all preceding steps.

Signals intelligence is just one of the disciplines involved in the intelligence cycle. The receipt of requirements for which SIGINT production is required initiates a similar interactive cycle at NSA. (see

Figure 27).

THE SIGINT INTELLIGENCE CYCLE

CONSUMER STATEMENT OF THE REQUIREMENT: the identification by consumers of their new or modified intelligence needs (which they surface through their agency/organization's requirements tasking authority) in order to fill informational gaps, usually in response to changes in the international political, economic, or military situation. These latter requirements tend to be more critical in nature and may require an immediate change to most of the other steps defined below. Some requirements may be a one-time request for information, while others may become standing requirements for intelligence support. New intelligence requirements received by NSA are numbered and placed in the National SIGINT Requirements List. Consumers are so notified.

TASKING SELECTION: the identification of the SIGINT resources which will be used to collect the information needed to satisfy new or changed requirements. Tasking will be levied on SIGINT resources after the new or changed requirement is evaluated by the IC Staff, which determines its relative priority. (Requirements often have to compete for the same SIGINT collection assets.)

COLLECTION: the application of national, theater, and/or tactical SIGINT collection assets to satisfy prioritized consumer requirements in conjunction with SIGINT collection strategies devised by the appropriate NSA office of primary interest.

PROCESSING AND ANALYSIS: the application of analytic methods (cryptanalysis, traffic analysis, signals analysis, language analysis, in-

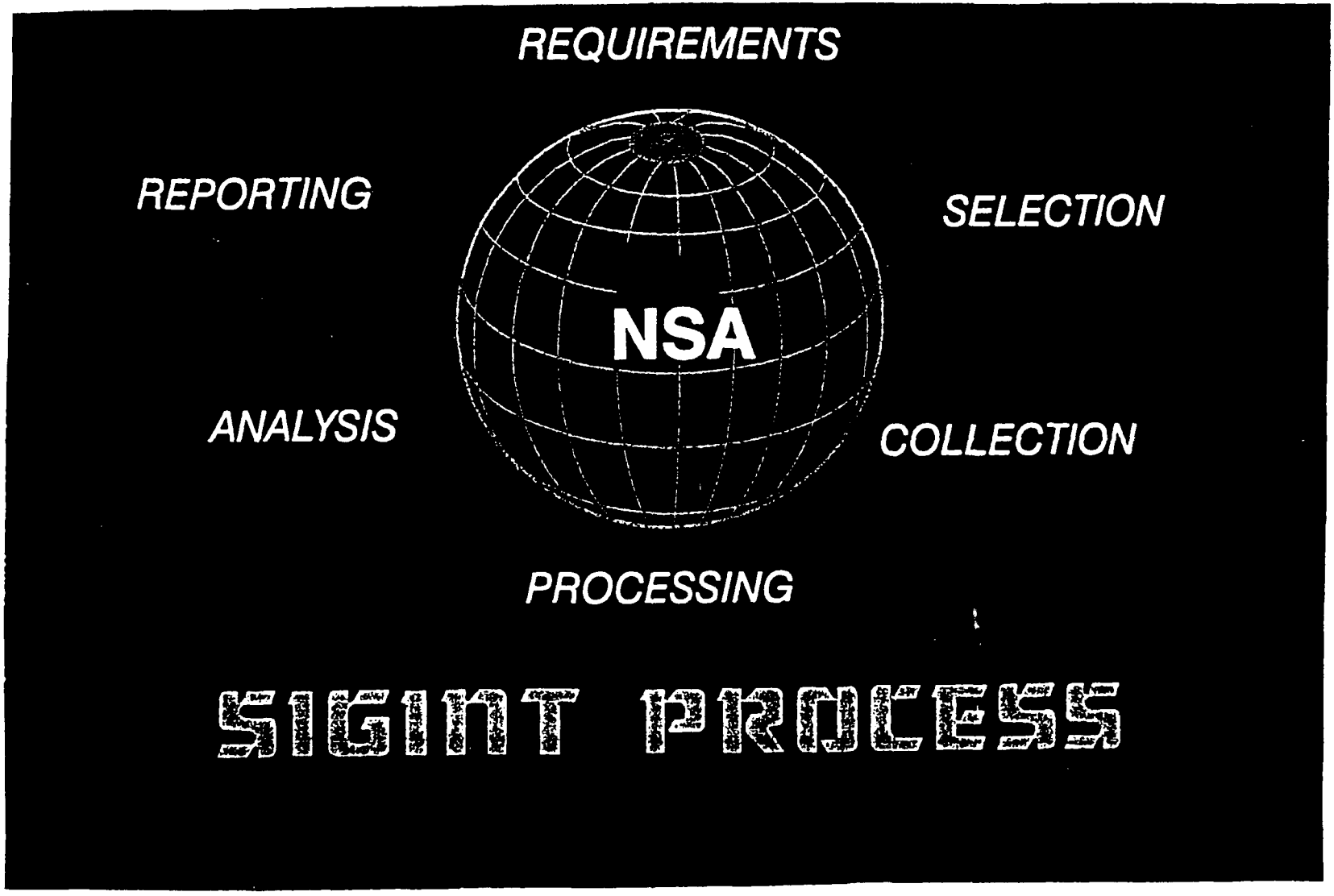

REQUIREMENTS
REPORTING
SELECTION
NSA
ANALYSIS
COLLECTION
PROCESSING
SIGINT PROCESS

Figure 27

telligence analysis, etc.) to produce SIGINT "facts". An analyst compares the new data with existing data to determine its meaning.

REPORTING: the publication of the requested information in conjunction with the consumer's requirement. Unlike some national-level intelligence producers, NSA publishes intelligence information, not finished intelligence. Depending on its content, this intelligence information will be published in hardcopy or electrical form, provided verbally, or as a data base transfer, depending upon the urgency of the requirement and the expressed needs of the consumer. The information can be released in a stand alone report or combined with other information in either a narrative or tabular summary, again depending upon the requirement. Regardless of its format, however, all SIGINT product carries the requirement number and priority so that consumers can monitor requirement satisfaction. Moreover, the resultant product should meet the intelligence quality standards found in JCS Pub 2-0:

Timeliness: intelligence must be available and accessible in time to effectively use it.

Objectivity: intelligence must be objective, unbiased, and free from political influence and constraint.

Usability: intelligence must be suitable for application.

Readiness: intelligence systems must be responsive to the existing and contingent operational intelligence requirements of commanders, staffs, and forces.

Completeness: intelligence must satisfy the needs of commanders, staffs, and forces so that they will be able to accomplish their missions.

Accuracy: intelligence must be factually correct and convey the situation as it actually exists.

Relevance: intelligence must contribute to an understanding of the situation and to the planning, conduct of, and evaluation of operations.[173]

The provision of SIGINT products is in accordance with consumers' established requirements. Primary SIGINT consumers supported by NSA worldwide include: the White House and the National Security Council, the Secretary of Defense, the Secretary of State and embassies abroad, the Secretary of the Treasury, the Secretary of Energy and various Energy laboratories, the Secretary of Commerce, the Federal Bureau of Investigation, the DCI and CIA, the DIA and military attaches, the Joint Chiefs of Staff, Service intelligence agencies, unified and specified commands and their Commanders in Chief, operational and tactical commanders (as required), and allied nations.[174]

The USSS produces SIGINT information in accordance with the classification standards required to protect sensitive sources and methods, while trying to ensure the widest possible dissemination and use of SIGINT product. Intelligence should be "sanitized" when personnel who need a particular category of intelligence cannot be cleared for it or when the physical security requirements for that category of intelligence material cannot be met. Security can be attained by separating the intelligence from its sources and methods. The policy and guidelines for sanitization of intelligence must be sufficient and flexible to ensure timely access and application of intelligence for operations.

The responsibility of the consumer, especially the military commander or his staff, is to frame precisely his requirements, enabling him to get the output -- the format, the periodicity, and the classification -- that he needs for strategic, operational, and tactical planning and execution. According to Lowenthal, consumers bear some respon-

sibility for the quality of the product which they receive:

> "A glaring omission in most analyses of U.S. intelligence is the tremendous importance played by intelligence consumers. Not only do the consumers establish the milieu in which intelligence operates, but they also bear a responsibility for making clear their needs and requirements and for establishing useful feedback channels to allow necessary modifications by the producers. Although this responsibility should be obvious, it has been overlooked."[175]

If the consumer is not getting what he requires from SIGINT, then NSA should be provided with that feedback so that corrective modifications can be made. This can be accomplished through formal or informal messages to NSA, face-to-face or conference analytic discussions, and/or discussions with the NSA/CSS representative (NCR) or Cryptologic Support Group (CSG), located within the J-2 staff at unified and specified commands. Concerns with NSA reporting should <u>not</u> wait until the SIGINT Requirements Validation and Evaluation Sub-committee (SIRVES) of the DCI's SIGINT Committee conducts a formal evaluation of that reporting. Although problems could be raised at that time, it would be much more prudent and timely to raise those concerns earlier in the process to ensure more immediate corrective action.

MILITARY INTELLIGENCE REQUIREMENTS

The USSS initiates action in response to consumer requirements. The USSS is managed and organized to support peacetime, crisis, and wartime needs of military commanders at all echelons, depending on need. A thorough understanding of the commander's plans, operational concepts, and intelligence needs under various conditions is crucial for providing such

support. The dynamic nature of military operations calls for close and timely dialogue and cooperation between commanders and supporting SIGINT elements.

> "Doctrine should be used in providing and applying intelligence. It points the way for intelligence support in formulating objectives and strategy, in determining, planning, and conduc ting operations, and in evaluating the effects of operations with respect to their objectives. Commanders and senior members of their staffs should recognize how the employment of the principles of intelligence stated herein can enhance effectiveness of their decision making and prioritization processes. The application of intelligence doctrine must, however, be adapted to particular situations and the commander's intent, and his determination of how intelligence is to support the conduct of joint operations."[176]

Military requirements for signals intelligence information -- especially timeliness, degree of detail, and format -- vary depending upon the echelon which perceives a need for SIGINT support. The following descriptions provide basic Army structures and composition and generic intelligence requirements at the tactical, operational, and strategic levels of command in linear warfare. (see Figure 28)

INTELLIGENCE FOR THE TACTICAL LEVEL OF WAR

The purpose of tactical intelligence is to provide commanders with information about the enemy, terrain, and weather as quickly as possible so that he may assess enemy capabilities, and possible courses of action and intentions while planning his own operations. Tactical intelligence services maneuver companies, battalions, brigades, and divisions.[177]

MANEUVER COMPANY: The company commander almost exclusively needs combat information which requires little processing and analysis. His intel-

USE OF TACTICAL, OPERATIONAL, AND STRATEGIC

INTELLIGENCE

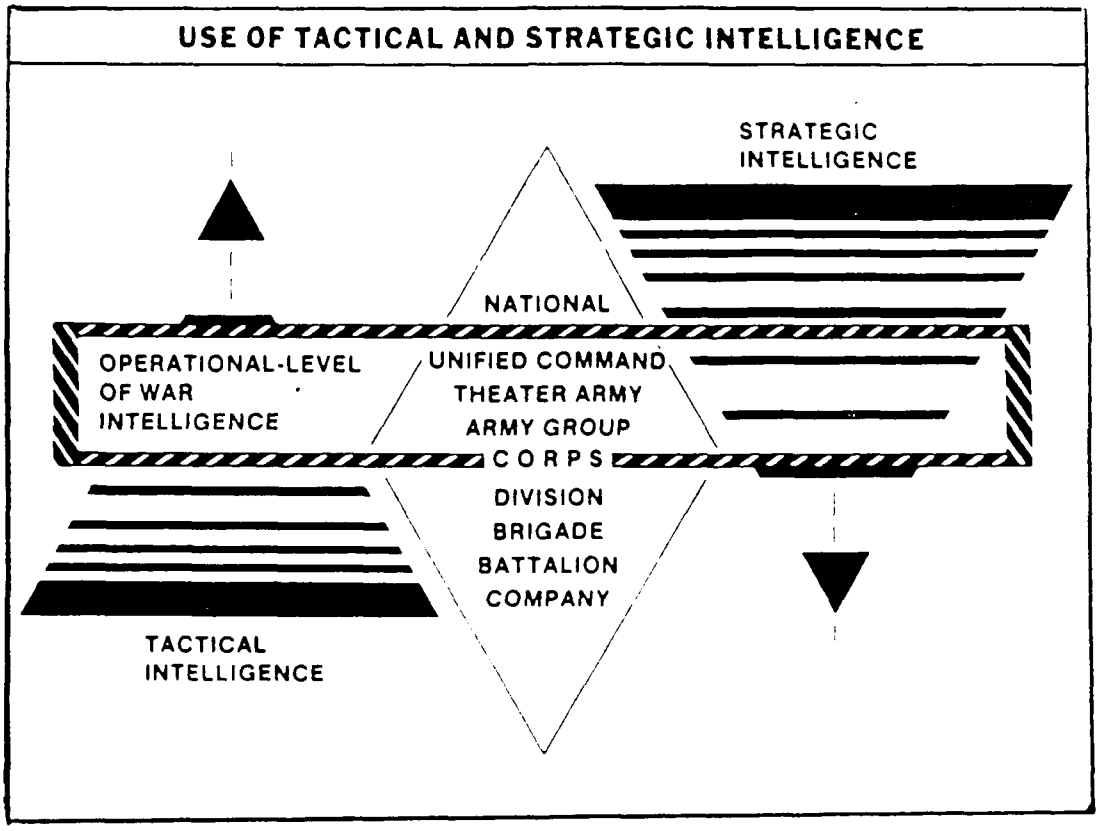


Figure 28

U.S. Army Field Manual 34-1, July 1987, p. 2.9.

ligence requirements include the status of the enemy (morale, location, training, combat effectiveness, weapons, changes in tactics), weather, and terrain. Company commanders direct the operations of company elements -- such as fire support teams (FIST) -- to satisfy intelligence requirements. Moreover, companies collect significant quantities of valuable, timely information through overt HUMINT collection -- patrols, reconnaissance, and listening and observation posts. Also, intelligence is derived from contact resulting from engaging, capturing, and destroying the enemy.[178]

BATTALION: The battalion task force maneuvers against and fights enemy battalions within its area of operations of 5 KM from the Forward Line of Troops (FLOT) and, therefore, relies primarily on combat information for the execution of the battle. The battalion commander needs information on the number, size, location, and capabilities of enemy units and weapons systems within his area of operations and the number and types of enemy units in his area of interest (15 KM from the FLOT) within a 12-hour timeframe. Tasking for reconnaissance patrols, ground surveillance radars, or remotely-employed sensors (REMs), as well as observation missions, are passed to the companies, scout platoon, or FIST. Military intelligence (MI) resources attached to or supporting the battalion may be allocated to the companies or held under battalion control. The Battlefield Information Coordination Center (BICC), with its limited analytic capability, is the first processing element to receive front-line information about the enemy, thereby serving as a key link in the intelligence system.[179]

BRIGADE: The brigade commander directs, coordinates, and supports operations of battalions against assaulting enemy brigades and regiments. He usually plans for operations up to 12 hours in advance; his area of opera-

tions extends to 15 KM while his area of interest is 70 KM. Brigades must be provided information on follow-on forces that can affect brigade operations. To meet requirements, the brigade commander relies on subordinate battalions and support provided by elements attached from the division MI battalion. MI support will normally include intelligence and electronic warfare (IEW) support elements which liaise between the brigade and the MI battalion. MI support will also include IEW assets deemed appropriate such as counter-intelligence (CI) or interrogation teams, or collection and jamming assets. Mission, enemy, terrain, troops, and time available (METT-T) drive the stated command or support relationship. The IEW requirements of the brigade still emphasize combat information; however, the need for intelligence, EW, and CI support is of nearly equal importance. The brigade BICC coordinates closely with the IEW support element to ensure the intelligence effort between organic collection assets and supporting MI assets are coordinated effectively. Brigades rely on divisions for Intelligence Preparation of the Battlefield products and detailed all-source analysis.[180]

DIVISION: The division commander usually controls the operations of three combat brigades with an area of operations extending 70 KM and an area of interest of 150 KM. The nature of combat operations and target development requires that targeting information be processed rapidly. Similarly, situation assessments of enemy disposition and capability must be current. Generally, the division commander must receive information about locations, strengths, and direction of movement of regimental and division command posts, artillery, rocket, air defense, radio electronic combat, and service support forces located in or moving to the division's area of influence. The division's generic intelligence information

requirements should be satisfied by information derived from inputs from Corps and Echelon Above Corps (EAC), Army and Air Force tactical air reconnaissance, organic, and subordinate battalions' collection resources. His organic capabilities include an MI battalion with a Technical Control and Analysis Element of SIGINT and EW assets and companies for communications and jamming, intelligence and surveillance, electronic warfare, and long-range surveillance units. The MI battalion has three airborne COMINT and EW systems to provide aerial communications intercept, locating, and jamming support.[181] Moreover, the division commander also has numerous non-MI intelligence collectors at his disposal: the AN/TPQ-36 radar and non-MI aviation assets, military police, and scouts.

INTELLIGENCE FOR THE OPERATIONAL LEVEL OF WAR

Intelligence requirements of the theater or unified commander-in-chief (CINC) reflect the peacetime to wartime responsibilities assigned to that theater under the Joint Strategic Capabilities Plan. The military strategy, force structure, and intelligence requirements for each theater of war vary considerably because of the different countries involved; the scope of U.S. commitments; varied foreign friendly, Allied, and threat military capabilities; and U.S. political, military, and economic interests in the area.[182]

Intelligence at the operational level of war is defined as that information which is required for planning and conducting campaigns within a theater of war, especially identifying and isolating enemy centers of gravity. Operational level of war intelligence focuses on theater, army group, field army, or corps commanders.

CORPS: The corps directs, coordinates, and supports the operations of

divisions against enemy first-echelon divisions and simultaneously directs the corps' battle against enemy second-echelon divisions and armies. His area of operations extends up to 300 KM and his area of influence up to 150 KM. The corps commander's planning time is up to 72 hours. He is continually engaged in target development, employing corps' weapons and electronic countermeasures supported by Air Force air interdiction and close air support missions. To ensure efficient application of available weapons systems, the corps must receive timely and accurate locations of enemy targets. The corps' intelligence requirements can be fulfilled from information recovered from subordinate divisions; from organic intelligence resources at EAC; and from tactical air reconnaissance (e.g., side-looking airborne radar, imagery, infra-red assets, and COMINT and ELINT collection). The aerial assets comprise the source of most of the intelligence, target development, and post-strike assessment data generated at corps level. The corps relies heavily on Echelons Above Corps (EAC), other services, and national agencies to supplement its collection capabilities. The TCAE interfaces with division TCAEs and EAC TCAEs, as well as with NSA, to complete the vertical integration of tactical and national-level SIGINT. Moreover, at the corps level, the commander is provided with SIGINT "direct service", a tailored SIGINT product in which non-organic SIGINT producers provide support to the corps in response to its requirements. The product may vary from recurring, serialized reports produced by NSA to instantaneous aperiodic reports provided to the command, usually by a fixed SIGINT activity engaged in collection and processing.[183]

ECHELON ABOVE CORPS (EAC): EAC organizations vary in size, depending upon the theater; however, they generally control the operations of between two

to five corps deployed over a large geographic area. The EAC area of operations extends to 150 KM and its area of interest extends to 1000 KM beyond the FLOT. Commands at EAC may include allied army groups with operational command of U.S. Army forces, allied regional commands, a U.S. unified command, and separate Army units assigned to NATO. EAC also may be a joint task force headquarters formed for contingency operations. Planning for operations 72+ hours in advance, the EAC military commander must be provided intelligence information about second echelon armies and fronts that may affect the central battle (force generation and deep interdiction planning) within 96+ hours. Intelligence support can be provided by national-level SIGINT direct service, derived from intelligence assets of subordinate units, or EAC organic assets. An MI brigade or similar unit provides IEW support to EAC. These MI commands are regionally and functionally tailored to provide multi-disciplined IEW support to each theater or contingency force.[184]

INTELLIGENCE FOR THE STRATEGIC LEVEL OF WAR

Strategic intelligence is defined as that intelligence required by national decision makers for the formulation of national foreign and defense policy in conjunction with the national security strategy provided by the President of the United States. The intelligence needs of the National Command Authority are global in dimension, covering all elements of national power -- political, military, economic, and informational. Intelligence needs vary and constantly change because of the volatile, uncertain, complex, and ambiguous environment in which strategic leaders operate. Timeliness, degree of detail, and reporting will change, depending on leaders' needs. For example, critical situations may demand

immediate, short reports whereas long-term policy planning may require longer, in-depth studies such as National Intelligence Estimates. Strategic political and military leaders expect strategic intelligence to keep pace with their ever-changing intelligence needs.[185]

MILITARY INTELLIGENCE REQUIREMENTS LEVIED UPON THE USSS DURING PEACETIME

Authorized SIGINT recipients may originate a new requirement or propose a change to an existing SIGINT requirement. SIGINT requirements from military commanders usually are forwarded to the unified or specified command by lower-level collection requirements managers (CRMs). CRMs receive, validate, analyze, integrate, and process requests for intelligence information (RII). They task and levy intelligence collection requirements (CR) on organic, theater, and national collection systems. When an analyst alerts the CRM to an intelligence gap, the CRM translates these RIIs and CRs into essential elements of information (EEI), known in the Army as priority intelligence requirements (PIR).[186] JCS Pub 1 defines PIRs as the "critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision."[187]

Usually, the EEI are drafted for the commander's approval by the intelligence staff (S-2/G-2) in coordination with the operations staff (S-3/G-3). However, they can be stated partially or entirely by the commander. In any case, the intelligence staff must then manage the satisfaction of the EEI by devising a SIGINT requirement which includes information desired, required timeliness and periodicity, and desired recipients. When completed, this requirement forms the basis for re-

questing action by tactical, theater, and national SIGINT managers as completely and quickly as possible. On occasion, the requirement may become dynamic, providing for continuous collection because of fluid changes in the collection and target environment.[188] Further, the CRM should be looking to disciplines other than SIGINT to ensure only minimal essential duplication and maximum operational effectiveness.

The following guidelines should be applied by the CRM when selecting national SIGINT systems:

AREAS OF INTEREST: national systems are best employed against high-priority targets outside the range of organic or theater sensors or beyond standoff collection range and/or in high threat or denied areas.

TIMELINESS: targets should be chosen such that, under presently applicable timeliness constraints, exploitation reports will reach the commander while he still has time to react.

JUSTIFICATIONS: justifications must fully explain the need for the information and support the priority assigned by the requester.

SENSOR CAPABILITIES: target descriptions should place minimum restrictions on system use while still allowing for satisfaction of the commander's information needs.

EXPLOITATION/ANALYSIS REQUIREMENT CLARITY: exploitation/analysis requirements should be concise, explicit statements of the actual information needed. Requirements should be prepared considering the time required for exploitation/analysis.

EXPLOITATION/ANALYSIS REQUIREMENT PURPOSE: exploitation/analysis should state the purpose of the information desired when it will benefit the interpreter/analyst in preparing a useful product.

PREPLANNED COLLECTION: preplanned target sets, submitted in advance of an operation, can do much to relieve the workload of everyone concerned and should be considered where the tactical situation permits.[189]

When the CRM determines that national-level SIGINT assets are required to satisfy the commander's EEI, a SIGINT requirement will be forwarded to the theater J-2 staff. If it is determined that national systems must be tasked, the requirement is forwarded to DIA. DIA then

assesses the new or changed requirement, determines its priority vis-a-vis all DoD SIGINT requirements, and presents the requirement and its supporting justification statement and other appropriate documentation to the DCI's Signals Intelligence Requirements Validation and Evaluation Sub-Committee (SIRVES). This justification must include: the importance of the information, the intended use of the product, and the timeliness of the response required; the identification of the intended recipients of the information; the anticipated contribution of the requested information to the overall body of knowledge on the subject; and a comparison of the anticipated SIGINT contribution to that which is available from other collection resources. DIA also is responsible for ensuring any tie-in between the SIGINT requirement and the Joint Strategic Planning System.

Coordination of proposed changes to existing requirements is normally accomplished by message or telephone, with SIRVES members (representatives from various intelligence agencies and the services) providing their comments and/or concurrences to the SIRVES' staff. If a SIRVES member takes issue with a proposed change, the Chairman of the appropriate SIRVES working group is contacted and an attempt is made to resolve the matter. If no agreement can be reached, the proposed change is placed on the next SIRVES' agenda.[190]

SIRVES votes on new requirements to assess their priority in conjunction with the expressed DCI standing list of military, political, economic, science and technology, and other requirements found in the U.S. Foreign Intelligence Requirements Categories and Priorities. The proposed SIGINT requirement and the proposed priority are then provided to NSA to satisfy.

USSS' RESPONSE TO MILITARY COMMANDERS' REQUIREMENTS DURING PEACETIME

NSA will assess the proposed narrative and the required timeliness, priority, and reporting mode -- electrical message, data base/video display/tape, hard copy, or magnetic tape. It will then provide a written capability statement to SIRVES, detailing the USSS' ability to satisfy this new requirement, as well as any actions which might be under way to enhance the SIGINT response. The extent to which SIGINT assets can be used to satisfy requirements depends on the target's communications environment; the availability of collection, exploitation, and analytic assets; other competing requirements; the target's technical communications characteristics; and technical collection problems. The range of response capabilities for COMINT requirements encompasses the following:

CAN RESPOND WITHOUT ADDITIONAL RESOURCES: the USSS can routinely and meaningfully respond to a requirement specification with existing resources.

CAN RESPOND WITH LIMITED INFORMATION: the USSS can respond to a requirement specification but is able to provide only limited information.

CANNOT RESPOND WITHOUT ADDITIONAL RESOURCES: the USSS cannot provide any information, or so little as to be inconsequential, in response to a requirement specification without the application of additional resources.

RESEARCH AND DEVELOPMENT AND THE SUBSEQUENT APPLICATION OF ADDITIONAL RESOURCES NEEDED: the information is believed to exist. However, specialized (not currently available) equipment or techniques would be necessary in order to provide the information.

RESOURCES NOT A FACTOR; NO COMINT INFORMATION CURRENTLY AVAILABLE: the information being requested is not currently available. In this case, the application of additional resources would not enable the USSS to produce the information requested.[191]

USSS' responses to operational ELINT (OPELINT), technical ELINT (TECHELINT), and foreign instrumentation signals (FISINT) requirements are

somewhat different than COMINT requirements. OPELINT data forwarding requirements are expressed in terms of signals of interest, geographic areas of interest, geolocation accuracy, report timeliness, and collection frequency.[192] TECHELINT requirements give the known history of the emitter; its intended use, deployment, and technology; and the state of existing intelligence on the emitter. It will include country of origin, current locations, first observed date, dates that any changes were first observed, and the operational status of the system. A narrative statement includes instructions for: recognition, recording, analysis, or processing of the emitter signal; data to support in-depth technical analysis; an emitter's performance with associated weapons systems capabilities/vulnerabilities; and current production tasks.[193]

FISINT requirements are structured very much like COMINT requirements to include linking the requirement to the JCS Joint Strategic Planning System. In addition to the SIGINT FIS priority, a Foreign Instrumentation Signals Working Group provides an intradisciplinary collection and processing priority for each FIS requirement to assist the national-level collection manager in allocating resources.[194]

It is important to note that the capability statement of an existing requirement will be changed when the USSS' capability to satisfy that requirement changes. Therefore, it is wise to aperiodically review NSA's capability statement of any SIGINT requirement found within the SIGINT Requirements Data Base to ensure that expectations and capabilities are commensurate with one another.

The national SIGINT system, during peacetime, operates primarily against long-term standing requirements. This entire process may seem

rather protracted and time consuming, thereby making it less dynamic in time-critical and evolving situations. However, the requirements system is both flexible and responsive during times of heightened consumer interest. It is activated through the following types of ad hoc requirements.

AMPLIFICATIONS OF REQUIREMENTS (AMPs): are generated when a requirement currently exists but something about the requirement's parameters (perhaps the timeliness, degree of detail, periodicity) requires changing, usually because of some change in the international environment. An AMP usually covers a defined time period.

REQUESTS FOR INFORMATION (RFIs): usually a one-time query for information in answer to specific consumer-generated questions.

TIME-SENSITIVE REQUIREMENTS (TSRs): a high-interest, usually unforeseen, informational need prompts a TSR. A USSS capability statement is generated within 8 hours. A TSR usually covers a limited time period. Care should be taken to ensure that only time-critical intelligence requests become TSRs.[195] Time-sensitive requirements are forwarded directly to NSA from users.

All the above ad hoc requirement modifications can be requested for COMINT, OPELINT, TECHELINT, and FISINT information.

The CRM and the J-2 staff should constantly review standing and ad hoc requirements and evaluate the reporting. They can consolidate, modify, or develop new requirements. Most importantly, all standing and ad hoc requirements should be terminated by the consumers once the need for that information is no longer required.

OTHER PEACETIME SIGINT USES IN SUPPORT OF MILITARY COMMANDERS AND JCS

As mentioned previously, the Director, NSA/Chief, CSS (DIRNSA/CHCSS) is responsible to the Secretary of Defense to ensure that U.S. SIGINT planning is coherent and provides for effective use of SIGINT resources.

Consequently, all unified and specified commands and military services coordinate all SIGINT plans with DIRNSA/CHCSS. In a military support context, SIGINT planning includes, but is not limited to: SIGINT sub-architectures to the Theater Intelligence Architecture Program; SIGINT support plans to command operations plans (OPLANS) and concept plans (CONPLANS) under the deliberate planning provisions of JOPES; Wartime Intercept Coverage Plans; Technical Support Plans; new or revised policies, concepts, or procedures for enhancing SIGINT support to unified, specified, or combined military plans; and planning with allied nations.[196]

The USSS also provides support to JCS and joint exercises, either as a player or as a supporting organization, to the extent that resources permit. Consistent with current priorities and capabilities, the USSS will authorize SIGINT collection programs to participate in and support joint exercises, even at some expense to collection of real-world targets. The intent of this joint training is to develop and to test new or revised operational support concepts and procedures, new equipment, and joint command support capabilities. Specifically, the goal of joint exercising is to make national collection systems more responsive to tactical commanders' intelligence needs.[197]

DESIGNATION OF NSA AS A COMBAT SUPPORT AGENCY

On 21 June 1988, Secretary of Defense Carlucci designated NSA as a Combat Support Agency (CSA) with respect to those combat support activities it performs for the Department of Defense. Over the next several months, NSA and the JCS further refined that relationship in keeping with the Goldwater-Nichols Department of Defense Reorganization Act of 1986. Although DIRNSA's 10 October 1988 memorandum to the Chairman of the Joint

Chiefs of Staff delineated all of NSA's CSA responsibilities, only NSA's SIGINT *functions* (and not the information systems security functions) have been outlined here, delineating the basis for NSA SIGINT participation in JCS-conducted evaluations and readiness reporting of CSA efforts in support of military commands worldwide. The following list also includes modifications to the 1988 memorandum; these principles will be included in the SIGINT Annex to JCS Pub 2-0 when it is published later in 1991:

-- exercise SIGINT operational control over all SIGINT activities of the U.S.

-- respond in a comprehensive, direct, and timely way to the validated and prioritized peacetime information requirements of military commanders.

-- respond <u>immediately</u> to the changing and time-sensitive needs of military commands in crisis or war in response to SIGINT requirements forwarded directly, or via other means, to NSA.

-- provide SIGINT support to Command, Control, and Communications countermeasures and electronic warfare.

-- function as SIGINT advisor to the Secretary of Defense, Joint Chiefs of Staff, and the commanders of the unified and specified commands and provide advice and assistance to military commands through NSA's representational activities (NCRs/CSGs) attached to the commands.

-- develop SIGINT support plans to command operational and contingency plans.

-- develop, test, and implement new concepts, plans, and procedures to improve SIGINT support to military commands.

-- provide SIGINT support to U.S., combined, and allied military commands in coordination with U.S. and allied SIGINT activities.

-- support U.S. contingency operations with procedures defined in JCS Joint Operations manuals for support to conventional and special operations missions and consistent with the functions herein.

-- provide support to special technical operations of military commanders.

-- ensure that the capabilities of SIGINT activities, designed for warfare or contingency deployment, are productively used during peacetime in support of appropriate readiness requirements.

-- provide systems development, engineering, and programmatic support to Joint/Service tactical SIGINT initiatives.

-- conduct, participate in, and support both U.S. and allied exercises to facilitate the use of SIGINT in military operations.

-- provide direct and dedicated SIGINT communications support to facilitate the delivery of perishable SIGINT to military commands and provide for continued SIGINT support to emergency or rapid recovery and reconstruction teams.

-- ensure that personnel of the NSA and the SCE, through the military commanders and in conjunction with the services, are adequately trained to fulfill peacetime, crisis, and wartime cryptologic tasks.

-- determine, in conjunction with commanders of unified or specified commands and general/flag commanders of task forces designated by the JCS or the commanders of unified and specified commands, when SIGINT operational tasking authority (SOTA) should be delegated by NSA to an appropriate commander. SOTA is a military commander's authority to direct operationally and to levy SIGINT requirements directly on designated SIGINT resources. These requirements are directive, irrespective of other priorities, and are conditioned only by the capability of the resources used to produce such information. Operational tasking includes the authority to deploy and re-deploy all or part of the SIGINT resources for which SOTA has been delegated by NSA and JCS.[198]

-- in the case of mobile (airborne and seaborne) military SIGINT platforms, provide SIGINT support and state movement requirements through appropriate channels to the military commanders who shall retain responsibility for military command of the platforms.[199]

As a limited CSA, NSA had prepared, by December 1990, two biennial JCS status reports, providing SECDEF with a "Combat Support Agency Responsiveness and Readiness Report". In addition, the unified and specified commands assess CSA support to their commands as part of their annual CINC's Preparedness Assessment Report input to the JCS Preparedness Report, which is written for the Chairman, JCS. NSA also participates in JCS exercise and operations evaluations.[200]

USSS' RESPONSE TO MILITARY COMMANDERS' REQUIREMENTS DURING CONTINGENCIES AND WARTIME

During military contingencies and wartime, SIGINT information must be moved -- in varying degrees of timeliness, accuracy, and detail -- to different decision makers, based on a variety of consumer requirements. Therefore, an accurate identification of consumers and event-keyed statements of requirements must be received by NSA. The only process described in this chapter is that support which is provided to military commands and commanders. During contingencies and wartime, however, a vast array of Executive Department consumers also will levy their requirements for event-specific reporting.

During contingencies and wartime, the requirements system must be dynamic, enabling interaction between consumers and collectors. This will serve as a collection management tool, keyed to the immediate mission of the command/commander, thereby permitting the rapid changing and processing of requirements as the tactical situation dictates. (see Figure 29)

From the outset, the conflict will be analyzed at multiple centers. JCS and the supported commander will immediately determine whether a JOPES deliberate action plan (operations plan) and its companion SIGINT Support Plan already exists which applies to the unfolding situation. Assuming that this is not the case, crisis action centers among military, political, and intelligence organizations begin working on a plan. In theater and at supporting U&S commands, the NSA/CSS representatives (NCR) will ascertain command intelligence requirements and will immediately forward the crisis-related requirements without waiting for higher headquarters or

Figure 29

SIGINT RESPONSE TO A CRISIS

REQUIREMENTS PROCESS ACTIONS

PEACETIME

- LOOK FOR CRISIS INDICATIONS
  - POLITICAL INSTABILITY
  - MILITARY UNREST
  - ECONOMIC PROBLEMS
  - INTERNAL UNREST
  - POPULAR MOVEMENTS
- ORDER OF BATTLE
- LEADERSHIP PROFILES

PRE-EXECUTION

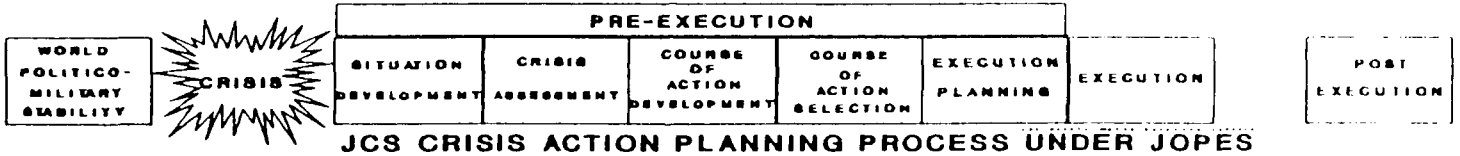
- I&W
- DISPOSITION OF FORCES
- READINESS
- CAPABILITIES
- INTENTIONS
- AWARENESS OF U.S. INTENTIONS

EXECUTION

- COMBAT INFO
- REALTIME THREATS
- HOSTILE REACTIONS
- WEATHER

POST-EXECUTION

- IDENTIFY RESIDUAL/ NEW THREATS
- BDA
- BAR
- REACTION OF OTHER GOVERNMENTS



JCS CRISIS ACTION PLANNING PROCESS UNDER JOPES

PRE-EXECUTION AND EXECUTION

- IDENTIFY SIGINT SHORTFALLS
- DEVELOP SIGINT STRATEGY IN SUPPORT OF CONTINGENCY PLANNING
- ACTIVATE TAILORED SIGINT SUPPORT PLANS
- ESTABLISH CRISIS ACTION TEAM
- OPTIMIZE COMMUNICATIONS CONNECTIVITY AMONG ALL PARTIES
- WORK WITH COMMAND TO REFINE REQUIREMENTS
- IMPLEMENT TIMELY REPORTING PROCEDURES
- WORK WITH COMMAND IN DEVELOPING WARFARE STRATEGIES
- IMPLEMENT CRISIS MANAGEMENT, COLLECTION, ANALYSIS, AND TIMELY REPORTING PROCEDURES IN CONJUNCTION WITH COMMAND REQUIREMENTS AND DEVELOPED SIGINT STRATEGY

PEACETIME

- ROUTINE MONITORING

POST-EXECUTION

- DRAW DOWN OF EFFORTS

SIGINT SUPPORT IS EXPANDED, EVALUATED, AND REFINED

DURING THE PRE-EXECUTION AND EXECUTION PHASES OF A CRISIS IN ACCORDANCE WITH CHANGING HOSTILE AND FRIENDLY ACTIONS AS EXPRESSED THROUGH COMMANDER'S REQUIREMENTS

DIA validation and prioritization, as described previously.[201]

With the receipt of initial SIGINT intelligence requirements, the SIGINT system will identify the intelligence information shortfalls and develop a contingency collection strategy designed to fill those information gaps. This probably will require the reprioritization of existing SIGINT requirements, which means that some collection assets probably will be diverted to higher-priority missions. Consequently, some other tasks will probably receive lower collection priorities and some others may not be addressed at all, depending upon the scope and duration of the crisis and competition for collection resources.

At NSA, crisis action teams will be established during the conflict. Some persons will be involved with SIGINT analysis and reporting; others with managing collection assets; and others with liaison among various Executive Department planners, decision makers, and consumers of intelligence. (All but the last of these functions will be executed at Service Cryptologic Elements (SCEs) as well.) As described previously, SIGINT reporting will be tailored at NSA and the SCEs to meet the commander's needs: it will be reported in the required format, at the required periodicity, and sanitized to the lowest possible level for rapid dissemination and use at the commander's level. SIGINT Direct Service, as this reporting procedure is called, is dedicated primarily to the fulfillment of national, not tactical, requirements.[202]

As in peacetime, a fundamental tenet of providing SIGINT support to military commanders is that the national and tactical SIGINT program will continue to operate as a unitary system during a crisis. However, should a unified or specified command be given SIGINT operational tasking author-

ity (SOTA), as described previously, the military commander will operationally direct and levy SIGINT requirements on designated resources. At the time that the commander receives SOTA, he may also receive SIGINT Direct Support by units organic to that command as well as by the units over which he now has SOTA.[203] Despite this bifurcated management arrangement, NSA will continue to optimize collection efforts to minimize duplication between national and tactical collectors.

In addition to increased collection and reporting (see Figure 30), NSA ensures that dedicated communications are activated to optimize the connectivity among all parties. Moreover, additional personnel will be provided to assist with additional requirements and analysis required of the additional reporting which the command will receive.

SIGINT SUPPORT TO MILITARY OPERATIONS

SIGINT ON ENEMY CHARACTERISTICS	→ SUPPORTS →	FRIENDLY MILITARY OPERATIONS
. DISPOSITION OF FORCES . ORDER OF BATTLE . INDICATIONS & WARNING . STRATEGY . TACTICS . C3CM/EW . INTENTIONS . READINESS . CAPABILITIES	SUPPORTS SUPPORTS	. CLOSE COMBAT . INDIRECT FIRE . BATTLEFIELD ENGINEERING . AIRBORNE/AIRMOBILE OPNS . INTERDICTION . AIR DEFENSE . OFFENSIVE COUNTER AIR . OFFENSIVE AIR SUPPORT . TACTICAL AIR SUPPORT/ NEAR-TIME REPORTING . SURFACE WARFARE . ANTI-SUBMARINE WARFARE . MINE WARFARE . AMPHIBIOUS WARFARE . ELECTRONIC WARFARE . UNCONVENTIONAL WARFARE . REAR AREA SECURITY . STRATEGIC AIR . SPACE

DURING

CONDITIONS OF	→ FOR →	PURPOSES OF
. PEACETIME . EXERCISES . CRISIS . CONTINGENCIES/SOLIC . WAR	FOR FOR	. TARGETING . PLANNING . DECEPTION . C3CM/EWC . WEAPONEERING . SPECIAL OPERATIONS

Figure 30

FRAGILITY OF SIGINT SOURCES

In the process described above, it is the intent of NSA to provide as much information as required to those who need it, especially to military commanders who use SIGINT to plan and prosecute a war at the tactical, operational, and strategic levels. The desire to provide critical intelligence while still maintaining protection of sensitive intelligence sources and methods has been a tremendous paradox for the USSS throughout the years. The increased provision of SIGINT to national decision makers and military commanders also increases its vulnerability to exposure. Espionage, deliberate leaks of information by the Executive and Legislative Branches, and speculative media revelations have, historically, been damaging to intelligence sources and methods. Understandably, a secret is only a secret until it falls into the hands of someone who no longer keeps the secret. Even George Washington understood that; hence, his creation of secret committees.

With regard to SIGINT, the revelation of sensitive sources and methods usually results in others taking protective measures, which ultimately deprives the United States of that information in the future. Consider this admonition from Prime Minister Winston Churchill regarding secrecy and the naval battles in the Pacific:

> The American Intelligence system succeeded in penetrating the enemy's most closely guarded secrets well in advance of events. Thus Admiral Nimitz, albeit the weaker, was twice able to concentrate all the forces he had in sufficient strength at the right time and place. When the hour struck, this proved decisive. The importance of secrecy and the consequences of leakage of information are here proclaimed."[204]

Unlike the military commander who plans, trains, and equips his

forces for possible combat, intelligence agencies are always "at war". Clearly, those nations with different ideologies and visions of world order do not want their plans and intentions, military strategies, weaknesses, strengths, and capabilities known by their adversaries. Consequently, they take every precaution to secure their communications, not only in the cryptography which they employ but by their transmission as well. Our ability to exploit their communications errors or weaknesses has enabled the USSS to provide the highest quality of intelligence to national political leadership and military commanders over the past 45 years. Therefore, when assessing the success of the foreign and military policy of deterrence during the Cold War, one should also factor in the successful role of intelligence.

LTG William E. Odom, former NSA Director, appropriately focused on the "wartime" function of intelligence even during times of peace:

> "It is not easy to justify intelligence activities as purely 'military operations' because we were officially at peace. In fact, we were engaged with building a postwar international security order in the face of opposition from the Soviet Union that perhaps legally was at peace but certainly not politically at peace with the West.
>
> "In fact, American intelligence remains at war today, even in peacetime. While our forces train and develop new weapons and doctrine, intelligence must strive to know the potential adversary's intelligence war against us. Here lies, in my view, the basic tension we as intelligence officers have with the law and the society. Legally, our nation is at peace. In fact, our front is at war."[205]

Espionage is the act of spying or the use of spies to obtain information. Today's "spies" appear to be motivated by greed and the financial gain derived from their espionage or by self/ego-gratification. Political

and ideological differences appear to be less of a driving force than in the earlier days of the Cold War.[206] Regardless of the motivation, however, the second and third order effects are usually significant because the activity probably lasted for a protracted time and probably involved more persons than the one or two who might ultimately have been caught and prosecuted.

A more common revelation of sensitive SIGINT sources and methods occurs through leaks, whether unintentional or intentional. Examine the case of H.O. Yardley who published his book, The American Black Chamber, in 1931 after his orgainzation was abolished and the Signals Intelligence Service was established. Yardley's book revealed U.S. communications intelligence activities, including examples of Spanish, German, Russian, and Japanese cryptosystems and their solutions. The Japanese, realizing that they had been duped at the Washington Naval Conference, immediately changed their codes and ciphers.[207]

"Official" leaks also occur when the Executive or the Legislative Branch intentionally provides information that might unintentionally expose the SIGINT sources of intelligence information. Disclosure of this type of classified information is prohibited by Executive Order and U.S. Code.

Executive Order 12356 provides for a system for classifying, declassifying, and safeguarding national security information. This Executive Order, signed by President Ronald Reagan on 2 April 1982, recognizes that it is essential that the public be informed of government activities. However, "the interests of the United States and its citizens require that certain information concerning the national defense and

foreign relations be protected against unauthorized disclosure". Cryptology, intelligence activities, and intelligence sources and methods are among those categories which the Executive Order specifies.[208]

Section 798 of Title 18, U.S. Code is much more specific regarding the disclosure of classified communications intelligence information.

> "Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person or publishes, or uses in any manner unprejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information ... shall be fined not more than ten years, or both."[209]

This document is very specific about the type of information covered by this code and the ramifications of its disclosure. It rightly categorizes U.S. or foreign government codes, ciphers, or other cryptographic devices among that information regarding the communications activities of the United States or any foreign government as well as any information which is derived from SIGINT collection and analysis of the communications of foreign governments.[210]

Reasons for leaking classified information have been offered by analysts of the political process. Morton Halperin, for example, has suggested that information is leaked to undermine rivals, particularly to discredit or expose them, to attract attention to the leaked information, to build support against a particular policy, to alert or send messages to foreign governments, to get information into the public domain, to publicly announce a policy, or to float a trial balloon to test domestic reaction.[211]

Robert Gates, at the time that he was Deputy Director of Central

Intelligence (before becoming Deputy National Security Advisor), suggested that some ground rules must exist so that sanitized intelligence can be released to the public. Although he didn't really suggest the proper mechanism to do so, he concluded that the long-standing absence of such a systematic approach contributes to leaks and the politicization of intelligence by the White House and other decision-makers who release previously classified information for their own purposes.[212]

In the case of SIGINT source disclosures, however, information frequently gets leaked to give credence to the source and validity of the information. The leaked information then can be used by the U.S. Government as incontrovertible technical support in its dealings with other nations. These claims of technical confirmation also are useful in persuading the public of the veracity of the U.S. Government information. In any event, leaks are usually picked up by the media, (as, indeed, intended), ensuring further dissemination of the information. Such media coverage frequently includes analytic commentary regarding NSA's role in producing that information.

The relationship between the media and the Intelligence Community is frought with contradictions. Both are interested in discerning the actions and the plans of foreign governments and militaries (which may not want their plans revealed) and in reporting their findings in an accurate, timely fashion. One could maintain that the media and the Intelligence Community, therefore, have similar interests. However, it is the similarity of interests which makes them, at best, rivals and competitors and, at worst, natural enemies, inevitably trying to frustrate the other's activities.[213]

Journalists could and have argued that the people's "right to know" is implicit in the First Amendment right of free speech and was among the basic reasons for the adoption of the amendment. One can rationally argue that the "right to protect" outweighs the "right to know" in matters of national security.

The simple fact is that no law or Executive Order will preclude a decision maker from leaking classified information if he perceives it's in his best interest to do so. Hopefully, leaders will weigh the potential compromise of current and perhaps future exploitability against the political or diplomatic gains provided by the leaked information. Intelligence agencies may advise against the disclosure of information derived from sensitive sources and methods. Realistically, however, leaders will make those trade-offs, depending upon their interpretation of the risk versus the gain in the larger political context in which they operate.

CONCLUSIONS

Advanced technology will improve intelligence acquisition, quality, quantity, timeliness, and accuracy. However, intelligence will always remain an art, not a science, because it is a discipline which relies, at some point in the process, on human interpretation of fact. As such, there will always be intelligence "failures" -- failure to recognize indications of potential world "hot spots" or failure to see the "forest" through the vastness of smaller "trees". Military commanders should not, however, focus on this potential for failure and dismiss intelligence as imprecise, unreliable, and unnecessary, as did Clausewitz.

Such an attitude would be both incorrect and dangerous. The first part of this paper detailed the unclassified examples of intelligence support provided during SIGINT's infancy, highlighting its strengths and weaknesses. Part Two of this paper focused on the Intelligence Community structure which was developed after World War II to deal with the complex problems of intelligence acquisition, production, and dissemination in support of political and military leaders living under a Cold War threat. Then, and even more so now, the Intelligence Community is prepared to maximize its efforts to support military commanders. Improved communications with consumers, faster national processing turn-around times, improved product timeliness to theater and/or deployed fighting forces, and tailored products in requested formats and at appropriate classification levels are representative of the types of changes in support provided by the Intelligence Community to the military within the last ten years.

In the 1990's, as the United States works with traditional Allies and former adversaries toward the accomplishment of a "new international

world order" in a multi-polar world, the Intelligence Community will need to be flexible in order to handle what will, undoubtedly, be less clear-cut requirements for information. Moreover, as the role of the U.S. military in a democratic society evolves during this transitional period, so must intelligence. To make a successful transition, all intelligence consumers, but especially the military, must work with the Intelligence Community to define new "threats" to national security, based on assessments of all elements of national power -- military, political, econmic, and informational. Accurate, timely, and usable intelligence will be the mainstay of the evolving threat assessment.

Together, the military and the Intelligence Community should be re-looking intelligence requirements to determine their relevance in the 1990's post-Cold War world. We may have to focus collection assets and analytic efforts on areas of the world where far less is known than about conventional strategic adversaries. Without a crystal ball to craft this new world, we must look more closely at potential threats and strengthen our understanding and perceptions of possible risk.

As the drivers of the intelligence process, intelligence consumers, especially the military, must articulate their perceived needs for intelligence which may include more diverse types of information than normally would be provided commanders. Frequent dialogue between consumers and producers could facilitate an exchange of needs and assessments and feedback on the desired format, type, and periodicity of intelligence product.

Just as intelligence officers of the 1990's must become truly "renaissance" analysts with a multitude of skills, so must military officers become more cognizant of the vast intelligence network available to sup-

port their mission and fulfill their informational needs. Military education must reflect, not only the changing threat, but the military's responsibility in formulating its intelligence requirements of the future. At the same time, military officers must be more cognizant of the types of intelligence information which will help them in defining the threat; developing a fighting doctrine; and raising, equipping, training, and modernizing the forces required to meet that threat.

Intelligence is a combat service function. Enlightened military leadership will use that service to maximize the mission. Apreciation of intelligence shouldn't be left to chance or exceptional military commanders, such as we just witnessed in DESERT STORM. Michael Handel has suggested that:

> "The potential contribution of intelligence to the success of wartime operations must be taught at all levels of military education in peacetime. Officers, particularly those in senior positions, must become familiar with all aspects of intelligence work: How to respect professional advice while recognizing the limitations of intelligence. All this must take place in peacetime. To begin learning these lessons once war has broken out is too expensive, too wasteful, and too late."[214]

ENDNOTES

1. Samuel B. Griffith, Sun Tzu: The Art of War, p. 144.

2. Ibid., p. 145.

3. Carl von Clausewitz, On War, p. 117.

4. Ibid., p. 140. For another interpretation of Clausewitz and intelligence, see Victor M. Rosello, "Clausewtiz's Contempt for Intelligence", Parameters, Spring 1991, pp. 103-114.

5. R.V. Jones, "Intelligence and Command," in Leaders and Intelligence, ed. by Michael I. Handel, p. 288.

6. Sherman Kent, Strategic Intelligence for American Policy. p. 3.

7. Michael I. Handel, "Leaders and Intelligence," in Leaders and Intelligence, ed. by Michael I. Handel, p. 3.

8. Ernest Volkman and Blaine Baggett, Secret Intelligence: The Inside Story of America's Espionage Empire, pp. xvii-xviii.; The Nathan Hale Institute, Intelligence in the War of Independence, pamphlet.

9. David Kahn, "Cryptology," The Encyclopedia Americana, 1987, Vol. 8, p. 276. Despite this seeming enthusiasm for SIGINT, Dulles, nevertheless, focused most of his attention as DCI upon HUMINT, espionage, and covert political action.

10. DoD Directive S-3115.7, "Signals Intelligence (SIGINT)". The term "plaintext" is SIGINT professional jargon for communications which either originally were or have been converted into clear language communications (no codes or ciphers).

11. The New Encyclopedia Britannica, 1987, Vol. 3, p. 768.; Lambros D. Callimahos, "Codes and Ciphers", The World Book, 1989, Vol. 4, p. 749.; William F. Friedman, The Friedman Lectures on Cryptology, (hereafter referred to as Lectures), p. 5.

12. The New Encyclopedia Britannica, p. 768.; Friedman, Lectures, p. 5.

13. Callimahos, p. 749. A syllabary is a matrix within a code used for spelling terms for which designated code groups are not given. For example, a code used by a ground army may not have terminology for aviation. Should a commander need to report something about his or the enemy's aviation assets, he could go to the syllabary and spell out the words for which there are no code groups.

14. Gerald W. Hopple and Bruce W. Watson, The Military Intelligence Community, p. 43.

15. DoD Directive, S-3115.7; U.S. Department of the Army, Field Manual 34-1, p. 2-13. (hereafter referred to as FM 34-1).

16. Handbook of the National SIGINT Requirements System, (hereafter referred to as NSRL Handbook), 1988, p. IV-1.

17. Ibid., p. III-1.

18. Ibid., p. V-1.

19. Hopple and Watson, p. 47.

20. William F. Friedman and Charles J. Mendelsohn, The Zimmermann Telegram of January 16, 1917, p. 1.; Patrick Beesly, Very Special Intelligence, p. 1. The analysts of Room 40 O.B. in World War I formed the nucleus of the British SIGINT effort at Bletchley Park in World War II.

21. National Security Agency, Origins of NSA: 1945-1952. p. 1.; George F. Howe, American Signal Intelligence in Northwest Africa and Western Europe, p. 5.

22. John P. Finnegan, Military Intelligence: A Picture History, p. 34.

23. Ibid., p. 24.

24. Chancel French, Deadly Advantage: Signals Intelligence in Combat, p. 39.; Howe, p. 5.

25. French, p. 41.

26. Ronald Lewin, The American Magic, pp. 28-29.

27. Howe, p. 5.; Origins of NSA: 1945-1952, p. 1.

28. William F. Friedman, Lectures, p. 131.

29. Cipher A. Deavours, "Cryptography," Collier's Encyclopedia, Vol. 7, p. 526.; Jozef Garlinski, The Enigma War, pp. 19-45.; Beesly, pp. 62-63; Foster McLeod, "Full Offensive Restricted," World War II, January 1988, p. 38.

30. Garlinski, p. 33.; French, p. 68.; McLeod, p. 37. The Luftwaffe relied almost exclusively on ULTRA for passing operational orders and logistical reports as well as for guidance from Air Marshal Goering. Consequently, it was a lucrative source of intelligence regarding Luftwaffe intentions and capabilities throughout the war. McLeod, p. 39.

31. Finnegan, p. 80.; Garlinski, p. 23. "The final number of encoding positions of any ordinary ENIGMA with only three rotors, a reflector, and six plug connectors is represented by the following number:

5 172 165 503 971 832 752 302 775 832
450 732 675 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000"

32. Patrick Beesly, p. 22-23.; French, pp. 70-71.; Garlinski, pp. 35-37.; Howe, p. 117.; You will note the term SIGINT used extensively throughout the World War II portion of this text. For the most part, the activities described in these passages are really derived from communications intelligence (COMINT) intercept, not "SIGINT" as used in current lexicon: SIGINT=COMINT + ELINT + FISINT. Signal intelligence (SIGINT) was the British term for what the U.S. termed COMINT. For consistency, the U.S. adopted the same term. It was not until after World War II that the U.S. officially split the overall generic term "SIGINT" into its two, and later three, integral parts. Howe, p. 1. For additional details of the production and dissemination of ULTRA, see G. Dickson Gribble, Jr., ULTRA: Its Operational Use in the European Theater of Operations, 1943-1945.

33. Garlinski, p. 52.; Howe, p. 7.

34. Garlinski, p. 52.; Howe, p. 7.; Aileen Clayton, The Enemy is Listening, pp. 41-59. Although German fighter pilots conversed extensively, bomber pilots restricted their comunications to mission-oriented information. Usually, they asked only for instructions home.

35. Christopher Andrew, "Churchill and Intelligence," Leadership and Intelligence, ed. by Michael I. Handel, p. 181.

36. Garlinski, p. 85; French, p. 96 and Deutsch quote from p. 72. According to Hough and Richards' analysis of the Battle of Britain, it had been the German intention to crush all RAF opposition and clear the way for SEALION. "It was, instead, to be a day of anti-climax and gaunt tragi-comedy." Richard Hough and Denis Richards, The Battle of Britain, p. 154.

37. Clayton, pp. 36-58. During the Battle of Britain, initially, communications between intercept units and Fighter Command Groups were so inadequate that the operational value of messages was limited or wasted. Sometimes, overloaded circuits precluded the passage of tactical information, even when Y-Service operators heard German sightings and commands to fire on unsuspecting RAF planes. Ultimately, a greater number of telephone lines were installed between headquarters and Y-Service units, thereby reducing the lag to about one minute. This exemplifies the challenge to, and response by, intelligence in support to military commanders during wartime. Clayton, p. 48.

38. Garlinski, pp. 82-89.; Clayton, p. 58.; R.V. Jones, The Wizard War: British Scientific Intelligence 1939-1945, p. 129.; Simon Goodenough, War Maps: World War II From September 1939 to August 1945, p. 22. Churchill's praise of Dowdy's defense during the Battle of Britain can be read as a testiment to the skill of the Commanding Officer, the pilots, and the SIGINTers alike:

> "On August 15, about a hundred bombers, with an escort of forty Me.110's, were launched against Tyneside. At the time a raid of more than eight hundred planes was sent to pin down our forces in

the South, where it was thought they were already all gathered. But now the disposition which Dowding had made of the Fighter Command was signally vindicated. The danger had been foreseen. Seven Hurricane and Spitfire squadrons had been withdrawn from the intense struggle in the South to rest in and at the same time to guard the North. They had suffered severely, but were nevertheless deeply grieved to leave the battle. The pilots respectfully represented that they were not at all tired. Now came an unexpected consolation. These squadrons were able to welcome the assailants as they crossed the coast. Thirty German planes were shot down, most of them heavy bombers (Heinkel 111's, with four trained men in each crew), for a British loss of only two pilots injured."

August 15 was the largest air battle of this period of the war; five major actions were fought, on a front of five hundred miles. It was indeed a crucial day. In the South all our twenty-two squadrons were engaged, many twice, some three times, and the German losses, added to those in the North, were seventy-six to our thirty-four. This was a recognisable disaster to the German Air Force." Winston S. Churchill, Memoirs of The Second World War, p. 359.

39. Clayton, p. 67.; Jones, pp. 98-99.

40. Clayton, pp. 68-69.

41. Jones, pp. 127-129.; Hough and Richards, p. 269.

42. Clayton, pp. 71-74.

43. Clayton, pp. 79-81.

44. Jones, pp. 135-156. Some authors have suggested that Coventry was not evacuated because this foreknowledge of the impending raid would compromise the readable ULTRA source. R.V. Jones contends that the foreknowledge of the Coventry raid was not available to Churchill. Jones, p. 147.

45. Ibid., p. 179.

46. Garlinski, pp. 89-93.; Beesly, 52. The German ENIGMA M machine was very versatile, capable of processing many different ciphers. By the end of World War II, the following different ciphers had, in turn, been analyzed and processed by Bletchley Park:

HYDRA - used for all surface ships in the Baltic and North Sea and then for ships operating from or off the occupied territories. It was also used by minesweepers and anti-submarine and patrol craft in Norway and France.

TRITON - used for all operational U-boats in the Atlantic, under the operational control of Befehlshaber der U-boote from his headquarters in Lorient.

TETIS - used for training U-boats in the Baltic.

MEDUSA - used for all U-boats in the Mediterranean.

AEGIR - used for all surface warships likely to remain for any length of time outside the Baltic or North Sea.

NEPTUN - used by the heavy ships of the main fleet when they were on specific operations, such as the transit of the BISMARCK in May 1941.

SUD - used for surface ships in the Mediterranean and Black Sea.

SPECIAL CIPHER - used for disguised merchant raiders and supply ships in overseas waters.

TIBET - used by supply ships overseas which had taken refuge in a neutral port at the outbreak of war and had only been supplied with the earliest type of ENIGMA.

POTSDAM - cipher used for operations against the Russians in the Baltic.

FREYA - used for communications between the German Admiralty and naval shore units when the use of land line was impossible or undesirable.

SLEIPNER - used by vessels engaged in torpedo-firing practice in the Baltic.

BERTOK - used for communications between the naval attache in Tokyo and the German Admiralty.

Beesly, pp. 64-65.

47. Garlinski, pp. 93.; Beesly, pp. 70-72.

48. Garlinski, pp. 94-97.; Goodenough, pp. 28-29.; Beesly, pp. 74-82.

49. Garlinski, pp. 97-98; quote from Beesly, p. 86. The BISMARCK's destination was also compromised by a high-ranking Luftwaffe officer in Athens. When learning of the BISMARCK's damage, he inquired of Berlin the ship's ultimate destination, because his son was on board. The location of Brest was compromised in diplomatic communications as well, pointing out the need for operational need-to-know. Beesly, pp. 84-85.

50. Garlinski, p. 137; Beesly, pp. 102-116.

51. Garlinski, p. 136-139; Jack E. Ingram, History of COMINT and COMSEC, p. 4.; quote from Beesly, p. 255.; McLeod, p. 40.

52. Howe, pp. 117-119.; Ingram, p. 2.

53. Howe, p. 1.

54. Andrew, p. 192. The British had achieved the ULTRA success at great expense; therefore, American participation in the production or receipt of ULTRA was always negotiated with British Allies. The enormous amount of work and long hours took its toll on cryptanalysts at Bletchley Park. In 1943, the British brought in Americans to assist in the ULTRA effort, including a future Supreme Court Justice, a future national security advisor, and a future prosecutor at Nuremberg. McLeod, p. 39. Americans also served in London and at some SLU's. Gribble, pp. 16-26.

55. Howe, pp. 11-12, 88.

56. Clayton, p. 142-143.

57. Ibid., pp. 143-146.

58. Ibid., pp. 162-164.; McLeod, p. 40.

59. Clayton, pp. 162-184. It was reported that, during the siege of Malta: 14,000 tons of bombs had fallen on Malta and Gozo; 24,000 buildings were damaged or destroyed; 1 in every 200 people was killed or died of injuries. The RAF lost 568 aircraft, while the Axis lost 1,120 aircraft. Clayton, p. 184.

60. Ingram, p. 7.; Garlinski, pp. 129-130. From ULTRA, Montgomery knew that Rommel was complaining about every kind of shortage, most especially, equipment, aircraft, and fuel. Clayton, p. 216. Nevertheless, it has been said that Montgomery did not place much value in the ULTRA material he received, even though it was providing him with information on the movements of Rommel's Afrika Korps and the sea routes of resupply which the British were interdicting. By August 1942, Montgomery was using ULTRA in planning his strategy against the Afrika Korps. Learning that Rommel was trying to outflank him, Montgomery was then able to counter this maneuver, preventing the Germans from breaking through to the Suez Canal. By November 1943, Montgomery was pushing the Afrika Korps westward as Operation TORCH was unfolding in Northwest Africa. Garlinski, pp. 129-130.; McLeod, p. 40.

61. Howe, p. 15.; Goodenough, p. 56.

62. Howe, pp. 21-33.

63. Michael E. Bigelow, "Eisenhower and Intelligence," Military Intelligence. March 1991, p. 20.; Ralph Bennett, "Intelligence and Strategy: Some Observations on the War in the Mediterranean, 1941-45," Intelligence and Military Operations, ed. by Michael I. Handel, p. 452.

64. Howe, pp. 29-30.; Goodenough, p. 58.

65. Howe, pp. 34-41.; Goodenough, pp. 60-63. In June 1943, Bletchley Park learned of the precise location of the forward HQ of Field Marshal Albert Kesselring, the German Commander-in-Chief in Italy. The RAF bombed that facility, killing many officers. However, Kesselring survived because he was in Rome that day. Garlinski, p. 140.

66. Howe, p. 43. The Allies ran a deception plan -- Operation MINCEMEAT -- as part of the planning for HUSKY. They hoped to deceive Hitler into thinking that the attack would be coming somewhere else, thereby diffusing German forces. A phony plan for the Allied invasion of Sardinia and Greece, codenamed HUSKY, was packed into a suitcase which was handcuffed to a corpse. "The Man Who Never Was" was put afloat off the coast of Spain and Bletchley Park provided the ULTRA message that the Germans believed in the phony plans. McLeod, p. 41.; Bennett, pp. 454-455.

67. Garlinski, pp. 129, 140.

68. Howe, pp. 51-53.; Clayton, pp. 262-264.; Bigelow, p. 20.; Bennett, p. 454.

69. Goodenough, pp. 64-65.

70. Howe, pp. 57-62.; Clayton, pp. 268-279.

71. Howe, pp. 62-70.; Clayton, p. 295. The SS evacuated Mussolini and reestablished him in northern Italy as head of a provisional Fascist republic where he remained, with German help, until the spring of 1945.

72. Goodenough, pp. 66-71.

73. Howe, pp. 70-77.

74. Clayton, p. 329.

75. Garlinski, p. 157.; Bigelow, p. 21.; McLeod, p. 41. The deception plan -- codenamed Operation FORTITUDE -- involved the establishment of a fictitious 1st Army Group (FUSAG), under the command of George Patton. Information was fed to Berlin through a network of compromised Nazi spies in England and a phony communications net supporting FUSAG was established in Scotland. ULTRA again revealed that the deception plan was working.

76. Howe, p. 134.

77. Ibid., p. 135.; Bigelow, p. 21.

78. Howe, pp. 134-138.; Garlinski, p. 165.

79. Howe, pp. 136-143.; Garlinski, pp. 164-165.; Harold Deutsch, "Generals and the Use of Intelligence," in Leaders and Intelligence, ed. by Michael I. Handel, pp. 230-235. Deutsch contends that this 2 August ULTRA message was not sent. The order by Hitler was sent telephonically on 9 August. Deutsch, p. 235.

80. Howe, pp. 134-144; Bigelow, p. 21.

81. Deutsch, pp. 244-247; Bigelow, pp. 21-22; Howe, p. 144.

82. Howe, pp. 142-150.; Garlinski, pp. 179-180.; Kevin A. Austra, "The Battle of the Bulge: The Secret Offensive," Military Intelligence, January-March 1991, p. 27.; Deutsch, p. 242.

83. Garlinski, p. 180.; Austra, p. 29.

84. Howe, p. 155.

85. Howe, p. 1, 6-7.

86. Howe, p. 1 and 7; Finnegan, p. 85.

87. Collier's Encyclopedia, p. 526.; Ladislas Farago, The Broken Seal, pp. 94-95.

88. Garlinski, pp. 123-135.

89. Lewin, p. 57.

90. French, p. 95.; Garlinski, p. 126.; Lewin, p. 46 and 232-233. The "analog" was a U.S.-produced prototype. No PURPLE machine fell into Allied hands during the war. Also, a small American mission arrived at the Combined Bureau in Singapore to exchange information on British and U.S. cryptanalytic successes against Japanese communications. A back-channel network between Americans in the Philippines and the British in Singapore was then established. Lewin, pp. 46-47.

91. Lewin, pp. 232-238.

92. Roberta Wohlstetter, Pearl Harbor: Warning and Decision, p. 171.

93. Ibid., pp. 172-173.; Howe, p. 6.; Lewin, pp. 39, 132-133. SIS served the Special Branch, MID, which was attached to, but not a part of, the War Department General Staff. It was controlled by the Assistant Chief of Staff, G-2, and provided intelligence to the General Staff, the Army Ground Forces, the Army Air Forces, Army Service Forces, overseas Theaters of Operations, and certain federal agencies. In 1942, SIS moved to Arlington Hall, Virginia. On the grounds of this former junior college, the Army established the headquarters of its cryptologic organization. In 1943, SIS was redesignated the Signal Security Agency (SSA). Howe, p. 10. and Finnegan, p. 62.

94. Lewin, p. 76.

95. Wohlstetter, pp. 219-227. The quote is from p. 227. In this study, Wohlstetter advanced the notion, borrowed from communications theory, of "signals" (truth, fact, relevant information) and "noise" (untruth, clutter, irrelevance).

96. Lewin, p. 148.

97. Ibid., pp. 92-95. Yamamoto's plan to eliminate the U.S. naval threat in the Pacific hinged on the following three plans which were to be executed "as soon as the war situations permits." The targets contained in Combined Fleet Operation Order No. 1, issued on 1 November 1941, were:

--bases of Tulagi in the Solomons and Port Moresby on the southern flank of New Guinea were to be occupied to secure domination of the Coral Sea and northern Australia.

--Midway was to undergo an amphibious assault. Yamamoto hoped to lure the U.S. Pacific Fleet into a fight and destroy it. At the same time, a diversionary strike would be made on the Aleutian Islands.

--the Fiji-Samao-New Caledonia line would be secured, thus severing a direct channel of communication between the U.S. and Australia.

--Pearl Harbor became the catalyst for this plan. Lewin, p. 84.

98. French, pp. 46-49; Lewin, pp. 92-95. Admiral Nimitz's interest in SIGINT was heightened over the precise location of an upcoming attack in an unknown location. The Japanese used special code values for place locations in their naval messages; therefore, U.S. cryptanalysts were not always able to provide the exact identifications. U.S. cryptanalysts knew that an upcoming attack was planned for location "AF"; there fore, they passed a phony plaintext report about a water shortage on Midway, hoping the Japanese would intercept the report. This is precisely wnat happened and the U.S. was able to intercept the Japanese forwarding of the American message in which the Japanese spoke of a water shotage on "AF". In this fashion, it was clear that Midway was the target of the upcoming Japanese attack.

99. French, pp. 49-51.; Lewin, pp. 104-106.; Ingram, p. 6.; Goodenough, pp. 152-153.; Garlinski, p. 177. This victory was almost bought at the price of a great defeat in the world of secrets, for an American journalist somehow discovered the cryptanalysts' achievement and disclosed it in the press. There was an immediate reaction from Churchill and no such compromise occurred again.

100. Wohlstetter, p. 177.

101. William F. Friedman, Lectures, p. 134.

102. Ibid.

103. Lewin, p. 157.; Edward J. Drea, "ULTRA Intelligence and General Douglas MacArthur's Leap to Hollandia, January-April 1944," Intelligence and Military Operations," ed. by Michael I. Handel, p. 324.

104. Lewin, pp. 157-162.

105. Goodenough, p. 156.

106. Lewin, pp. 163-166.; Goodenough, p. 158.

107. Lewin, pp. 162-166; French, pp. 53-54.

108. Ibid., pp. 169-175.

109. Ibid., pp. 185-186.

110. Goodenough, pp. 154-155.

111. French, pp. 54-60.; Friedman, Lectures, p. 137.; Lewin, pp. 187-188.; Ingram, pp. 6-7.; Dennis Beck, "Yamamoto - Reach and Destroy," World War II, November 1986, pp. 8, 56, 58.

112. Lewin, p. 223.

113. Ibid., pp. 226-227.

114. Ibid., pp. 193-194.

115. Ibid., pp. 194-196.; Goodenough, p. 162.

116. Lewin, p. 228, 253-254.; Drea, p. 331.

117. Lewin, p. 229.

118. Ibid., p. 197.; Drea, pp. 239-240.

119. Lewin, p. 250-253; quote is from p. 253. Edward Drea, in his analysis of Hollandia, also concluded that the SIGINT-derived knowledge of MacArthur's opponent, Adachi Hatazao, Commander of the 18th Army, significantly influenced MacArthur's strategic and operational planning. Drea, pp. 328-343.

120. Lewin, pp. 254-255.

121. Ibid., p. 255.

122. Ibid., pp. 255-256.; Goodenough, pp. 166-167; French, pp. 59-60.

123. Lewin, pp. 255-256.

124. Ibid., p. 257.

125. Ibid., pp. 258-259.

126. Ibid., pp. 260-261.

127. Ibid.

128. Goodenough, pp. 170.; John Toland, The Rising Sun: The Decline and Fall of the Japanese Empire, 1936-1945, pp. 617-633.

129. Toland, p. 618.

130. Goodenough, pp. 168-171.

131. Ibid., p. 168.

132. Ibid.

133. Lewin, p. 261.

134. Goodenough, p. 169.

135. Ibid.

136. Ingram, p. 10.

137. Lewin, p. 17.

138. Origins of NSA, p. 3.

139. Ibid., p. 4.

140. Jeffrey Richelson, The U.S. Intelligence Community, p. 15. Tyrus G. Fain, Katherine C. Plant, and Ross Milloy, The Intelligence Community: History, Organization, and Issues, p. 351.

141. Origins of NSA, p. 5.

142. Richelson, pp. 19-20.

143. Ibid.

144. "Executive Order 12333", in United States Code Congressional and Administrative News, 1981, Vol. 3, pp. B109. The missions listed in this paper represent only the SIGINT functions of NSA. NSA's information and operational security missions have not been outlined here.

145. SIGINT Annex to JCS Pub 2.0 (Draft)

146. Ibid.

147. Frank Carlucci, SECDEF Memorandum: Policy and Procedures Relating to NSA's Role as a Combat Support Agency, p. 1.

148. MJCS-111-88, "Concept of SIGINT Support to Military Commanders", 10 August 1988.

149. "Executive Order 12333", p. B104.

150. Ibid., pp. B104-105.

151. Ibid., p. B107.

152. Ibid., pp. B107-B108.

153. Ibid., p. B108.

154. Ibid.

155. Ibid., p. B109.

156. Ibid., p. B110.

157. Ibid.

158. Ibid., p. B111.

159. Ibid.

160. Thomas L. Hughes, The Fate of Facts in a World of Men: Foreign Policy and Intelligence-Making, pp. 49-50.

161. Michael T. Handel, Leaders and Intelligence, pp. 3-4. Alexander George made similar conclusions about the multiple advocacy system in his study of Presidential decisionmaking: "The solution it strives for is to ensure that there will be multiple advocates within the policymaking system who, among themselves, will cover a range of interesting viewpoints and policy options on any given issue. The premise of the model is that multiple advocacy will improve the quality of information search and appraisal and, thereby, illuminate better the problem the executive must decide and his options for doing so." Alexander L. George, Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice, p. 193. While, Kam agrees that there are advantages to be gained from pluralism, he also notes several disadvantages. Ephraim Kam, Surprise Attack, p. 226.

162. Handel, p. 5.

183. William E. Odom, American Intelligence: Current Problems in Historical Perspective, pp. 1-11. Cited with special permission of LTG Odom.

164. Sam C. Sarkesian, U.S. National Policy, p. 96.; Amos A. Jordan, William J. Taylor, Jr., and Lawrence J. Korb, American National Security, p. 141.; Mark M. Lowenthal, U.S. Intelligence: Evolutions and Anatomy, pp. 111-113.; CIA Factbook on Intelligence, p. 19.

165. Sarkesian, p. 96.; Jordan, Taylor, and Korb, p. 141.; Oseth, p. 94.; Lowenthal, pp. 110-111.

166. Jordan, pp. 144-146.; Lowenthal, p. 107.

167. Lowenthal, pp. 107-109.

168. Jordan, p. 147.

169. Army Command Management: Theory and Practice, p. 23-10.

170. Ibid.

171. Ibid.

172. Ibid.; U.S. Special Operations Command (USSOCOM) may also apply major force Program 11 funds to intelligence activities if they are solely for special operations support purposes.

173. JCS Pub 2-0, p. II-10.

174. JCS Pub 2-0, p. II-25.

175. Lowenthal, p. 71.

176. JCS Pub 2-0, p. I-3.

177. FM 34-1, p. 2-11.

178. FM 34-1, p. 2-22.

179. Ibid., p. 2-24.; USSS Concept for Support to Military Operations, (hereafter referred to as Concept), p. A-4.

180. FM 34-1, pp. 2-26-2-28; Concept, p. A-4.

181. FM 34-1, pp. 2-30-2-36; Concept, pp. A-3-4.

182. FM 34-1, pp. 2-9 - 2-10.

183. FM 34-1, pp. 2-41 - 2-43.; Concept, A-3.; SIGINT Annex to JCS Pub 2-0. (draft)

184. FM 34-1, 2-45 - 2-47.; Concept, A-3.

185. FM 34-1, p. 2-9.

186. Joint Service Tactical Exploitation of National Systems (JTENS) Manual, p. 2-11.

187. Ibid.

188. Ibid., pp. 2-5 - 2-10.

189. Ibid., p. 2-11.

190. NSRL Handbook, p. I-2.

191. Ibid., p. II-4.

192. Ibid., pp. IV-1 - IV-3.

193. Ibid., pp. III-1 - III-7.

194. Ibid., pp. V-1 - V-6.

195. Ibid.

196. SIGINT Annex to JCS Pub 2-0. (draft)

197. Ibid.

198. Ibid.; Other DoD CSAs include: the Defense Communications Agency, DIA, the Defense Logistics Agency, and the Defense Mapping Agency.

199. Ibid.

200. Ibid.

201. Ibid.

202. Ibid.

203. Ibid.

204. Friedman, Lectures, p. 197.

205. Odom, p. 7.

206. George A. Carver, "Intelligence in the Age of Glasnost", Foreign Affairs, March/April 1990, p. 160.

207. French, pp. 41-42.

208. "Executive Order 12356", in United States Code Congressional and Adminstrative News, 1982, Vol. 4, pp. B52-B54.

209. "Disclosure of Classified Information", U.S. Code, 1988, Vol. 7, pp. 266-267.

210. Ibid.

211. Morton H. Halperin, Bureaucratic Politics and Foreign Policy, pp. 176-189.

212. Robert Gates, "An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House," The Washington Quarterly, Winter, 1989, p. 44.

213. Hopple and Watson, p. 122.

214. Michael I. Handel, "Leaders ar telligence," in Leaders and Intelligence, ed. by Michael I. Handel, p. ..

BIBLIOGRAPHY

BOOKS

Aspin, Les; Bork, Robert H.; Colby, William; and Shattuck, John. Foreign Intelligence: Legal and Domestic Controls. Washington D.C.: American Enterprise Institute for Public Policy Research, 1979.

Beesly, Patrick. Very Special Intelligence: The Story of the Admiralty's Operational Centre 1939-1945. London: Hamish Hamilton, 1977.

Berkowitz, Bruce D. and Goodman, Allan E. Strategic Intelligence for American National Security. Princeton: Princeton University Press, 1989.

Bradley, Omar N. A General's Life. New York: Simon and Schuster, 1983.

Churchill, Winston S. Memoirs of The Second World War. Boston: Houghton Mifflin Company, 1959.

Cimbala, Stephen J., ed. Intelligence and Intelligence Policy in a Democratic Society. New York: Transnational Publishers, Inc., 1987.

Clausewitz, Carl von. On War. Princeton: Princeton University Press, 1984.

Clayton, Aileen. The Enemy is Listening: The Story of the Wire Service. London: Hutchinson and Co. LTD, 1980.

Fain, Tyrus G., Plant, Katherine C., and Milloy, Ross. The Intelligence Community: History, Organization, and Issues. New York: R. R. Bowker Company, 1977, pp. 347-369: "Testimony of Lt. Gen Lew Allen, Jr. Before the Pike Committee" and "Testimony of Lt. Gen Lew Allen, Jr. Before the Church Committee".

Farago, Ladislas. The Broken Seal: "Operation MAGIC" and the Secret Road to Pearl Harbor. New York: Bantam Books, 1968.

Finnegan, John P. Military Intelligence: A Picture History. Arlington: U.S. Army Intelligence and Security Command History Office, 1984.

French, Chancel T. Deadly Advantage; Signals Intelligence in Combat. San Antonio: USAF Electronic Security Command, 1990.

Friedman, William F. and Mendelsohn, Charles J. The Zimmermann Telegram of January 16, 1917 and Its Cryptographic Background. Laguna Hills: Aegean Park Press, 1976.

Garlinski, Jozef. The Enigma War. New York: Scribner and Sons, 1979.

George, Alexander L. Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice. Boulder: Westview Press, 1980.

Godson, Roy. Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence, and Covert Action. Lexington: Lexington Books, 1989.

Goodenough, Simon. War Maps: World War II From September 1939 to August 1945, Air, Sea, and Land, Battle by Battle. New York: St. Martin's Press, 1982.

Gribble, Jr., G. Dickson. ULTRA: Its Operational Use in the European Theater of Operations, 1943-1945. Carlisle Barracks: U.S. Army War College, 1991.

Griffith, Samuel B., trans. Sun Tzu: The Art of War. London: Oxford University Press, 1963.

Halperin, Morton H. Bureaucratic Politics and Foreign Policy. Washington D.C.: The Brookings Institute, 1974.

Handel, Michael I., ed. Intelligence and Military Operations. London: Frank Cass and Company, LTD., 1990.

Handel, Michael I., ed. Leaders and Intelligence. Totowa: Frank Cass and Company, LTD, 1988,

Handel, Michael I. War, Strategy, and Intelligence. London: Frank Cass and Co. Ltd., 1989.

Hopple, Gerald W. and Watson, Bruce W., ed. The Military Intelligence Community. Boulder: Westview Press, 1986.

Hough, Richard and Richards, Denis. The Battle of Britain. New York: W.W. Norton and Co., 1989.

Howe, George F. American Signal Intelligence in Northwest Africa and Western Europe. Fort George G. Meade: National Security Agency, 1980.

Hughes, Thomas L. The Fate of Facts in a World of Men: Foreign Policy and Intelligence-Making. New York: Foreign Policy Association, 1976.

Jones, R.V. The Wizard War: British Scientific Intelligence 1939-1945. New York: Coward, McCann, and Geoghegan, Inc., 1978.

Jordan, Amos A.; Taylor, Jr., William J.; and Korb, Lawrence J. American National Security: Policy and Process. Baltimore: John Hopkins University Press, 1989.

Kam, Ephraim. Surprise Attack. Boston: Harvard, 1988.

Kent, Sherman. Strategic Intelligence for American World Policy. Connecticut: Archon Books, 1965.

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

Lowenthal, Mark M. U.S. Intelligence: Evolution and Anatomy. Washington D.C.: The Center for Strategic and International Studies, 1984.

Oseth, John M. Regulating U.S. Intelligence Operations: A Study in Definition of National Interest. Lexington: The University Press of Kentucky, 1985.

Richelson, Jeffrey. The U.S. Intelligence Community. Cambridge: Ballinger Publishing Company, 1985.

Sarkesian, Sam C. U.S. National Security: Policymakers, Processes, and Politics. London: Lynne Rienner Publishers, Inc., 1989.

Shaver, David E. Justifying the Army. Carlisle Barracks: U.S. Army War College, 1990.

Thomas, Stafford T. The U.S. Intelligence Community. Lanham: University Press of America, Inc. 1983.

Tinsman, Robert T., ed. Army Command and Management: Theory and Practice. Carlisle Barracks: U.S. Army War College, 1990.

Toland, John. The Rising Sun: The Decline and Fall of the Japanese Empire, 1936-1945. New York: Random House, 1970.

Volkman, Ernest, and Baggett, Blaine. Secret Intelligence: The Story of America's Espionage Empire. New York: Doubleday, 1989.

Wohlstetter, Roberta. Pearl Harbor: Warning and Decision. Stanford: Stanford University Press, 1962.

Wilson, George, ed. The Role Of American Intelligence Organizations. New York: The H.W. Wilson Company, 1976.

JOURNALS/MAGAZINES

Austra, Kevin R. "The Battle of the Bulge: The Secret Offensive", Military Intelligence, January-March 1991, pp. 26-33.

Beck, Dennis. "Yamamoto -- Reach and Destroy", World War II. November 1986, pp. 8, 56-58.

Bialer, Seweryn. "The Passing of the Soviet Order?", Survival. Vol. 32, No. 2, March/April 1990, pp. 107-120.

Bigelow, Michael E. "Eisenhower and Intelligence", Military Intelligence, January-March 1991, pp. 19-25.

Carver, Jr., George A. "Intelligence in the Age of Glasnost." Foreign Affairs, Vol. 69, Summer 1990, pp. 147-166.

Gates, Robert M. "An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House." The Washington Quarterly. Winter 1989, Vol 12, No 1, pp. 35-44.

McLeod, Foster, "Full Offensive Restricted", World War II. November 1988, pp. 34-41.

Rosello, Victor M. "Clausewitz's Contempt for Intelligence", Parameters, Spring 1991, Vol. XXI No. 1, pp. 103-114.

ORGANIZATIONAL REPORT

Department of Defense (DoD) Security Review Commission. Keeping the Nation's Secrets. Washington: 1985.

ENCYCLOPEDIAS

Callimahos, Lambros D. "Codes and Ciphers". The World Book Encyclopedia. Chicago: World Book, Inc., 1989, Vol. 4, pp. 749-752.

Deavours, Cipher A. "Cryptography". Collier's Encyclopedia. New York: Macmillan Educational Company, 1989, Vol. 7, pp. 519-527.

Kahn, David. "Cryptology." The Encyclopedia Americana, International Edition, 1987, Vol. 8, p. 276.

The New Encyclopedia Britannica. Chicago: Encyclopedia Britannica, Inc., 1987, Vol. 3, p. 768.

PUBLIC DOCUMENTS

Carlucci, Frank. SECDEF Memorandum: "Combat Support Functions of the NSA/CSS". Washington D.C.: November 1988.

Carlucci, Frank. SECDEF Memorandum: "Policies and Procedures Relating to NSA's Role as a Combat Support Agency". Washington D.C.: June 1988.

Central Intelligence Agency. Central Intelligence Agency: Fact Book on Intelligence. Washington D.C.: 1985.

Intelligence Community SIGINT Committee. Handbook of the National SIGINT Requirements System. Washington D.C.: October 1988.

Joint Chiefs of Staff. JCS Pub 2-0: "Doctrine for Intelligence Support to Joint Operations". Washington D.C.: May 1990.

Joint Chiefs of Staff. JCS Pub 3-0: "Doctrine for Unified and Joint Operations". Washington D.C.: January 1990.

Joint Chiefs of Staff. JCS Memorandum MJCS-111-88: "Concept of SIGINT Support to Military Commanders". Washington D.C.: August 1988.

Joint Chiefs of Staff. SECDEF CM-1573-88: "Combat Support Functions of the NSA/CSS". Washington D.C.: October 1988.

Laird, Melvin. DoD Directive S-3115.7, "Signals Intelligence (SIGINT)". Washington D.C.: January 1973.

The Nathan Hale Institute. Intelligence in the War of Independence. Washington D.C.: The Nathan Hale Institute, 1980. (This is a reprint of a CIA publication of the same name.)

National Security Agency. USSS Concept for Support to Military Operations. Fort George G. Meade: June 1982

National Security Agency. Joint Service Tactical Exploitation of National Systems (JTENS) Manual. Fort George G. Meade: 1987.

National Security Agency. Origins of NSA: 1945-1952. Fort George G. Meade: 1990.

National Security Agency. SIGINT Annex to JCS Pub 2-0 (Draft). Fort George G. Meade: publication anticipated in 1991.

U.S. Code. Washington: Government Printing Office, 1988. Vol 7, pp. 266-267: "Title 18 - 798: Disclosure of Classified Information."

U.S. Code Congressional and Administrative News, 97th Cong., 1st Sess. St. Paul: West Publishing Co., 1981. Vol 3, pp. B102-116: "Executive Order 12333: United States Intelligence Activities".

U.S. Code Congressional and Administrative News, 97th Cong., 2nd Sess. St. Paul: West Publishing Co., 1982. Vol 4, pp. B51-63.: "Executive Order 12356: National Security Information".

ARMY REGULATIONS

U.S. Department of the Army. Field Manual 34-1: Intelligence and Electronic Warfare Operations. Washington D.C.: July 1987.

U.S. Department of the Army. Field Manual 34-130: Intelligence Preparation of the Battlefield. Washington D.C.: May 1989.

LECTURES

Friedman, William F. The Friedman Lectures on Cryptology. Lecture. Fort George G. Meade: National Security Agency, 1963.

Ingram, Jack E. History of COMINT and COMSEC. Presentation. National Security Agency: National War College, Spring, 1990.

Odom, William E. American Intelligence: Current Problems in Historical Perspective. Lecture. Washington D.C.: Association of Former Intelligence Officers, 10 October 1987 (Cited with special permission of LTG William E. Odom.)

VIDEO RECORDINGS

U.S. Army War College Videotape, Theater Intelligence and Deception, Carlisle Barracks: U.S. Army War College, 1990.