NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: MDR-47467
13 July 2009

Mr. Michael Ravnitzky
[redacted]

Dear Mr. Ravnitzky:

This responds to your request and subsequent appeal to the Interagency Security Classification Appeals Panel (ISCAP) to have the following document titled:

"A Brief History of Communications Intelligence in the United States" by Captain Lawrence Safford, USN, dated 21-27 March 1952 reviewed for declassification. The document has been reviewed under the Mandatory Declassification Review (MDR) requirements of Executive Order (E.O.) 12958, as amended.

The ISCAP has determined that the information in the document can be released in full. The document is enclosed.

Sincerely,

Kristina M. Grein

KRISTINA M. GREIN
Chief
Declassification Services

Encls:
a/s

[redacted]

SRH-149

A BRIEF HISTORY OF COMMUNICATIONS INTELLIGENCE IN THE UNITED STATES

by

LAURANCE F. SAFFORD
CAPTAIN, USN (RET.)

~~CLASSIFIED COPY~~

~~TOP SECRET SUEDE~~

PART I

A BRIEF HISTORY OF COMMUNICATIONS INTELLIGENCE IN THE UNITED STATES

CAPTAIN SAFFORD'S VERSION OF PRE-PEARL HARBOR HISTORY

PREPARED 21-27 MARCH 1952

(WITH SPECIAL REFERENCE TO COORDINATION AND COOPERATION)

(N.B. This is a re-typed copy of an original in the files of the office of Archives and History, National Security Agency. The original was a negative copy and unsuitable for reproduction)

Prior to 1917 United States activity in the field of Communications Intelligence* was sporadic, and there is little recorded of it. For all practical purposes the history of American cryptanalysis begins with our entry into World War I. Codes and cyphers at that time,even those used to carry the most sensitive information, were by current standards naive. They were hand-coded and hand-applied cypher systems usually overlying double-entry code books, the attack upon which required skills and patience but not the elaborate electronic and tabulating devices of today. Consequently, the codes which this Government "cracked" from 1917 to 1919 were handled by a small group of lexicographers, mathematicians, and people who had acquired some background in what was then the hobby of cypher construction, usually related to some such cult as the "Baconian Theory."

The War Department set up the first organized cryptanalytic office in June 1917, under Mr. H. O.Yardley, an ex-State Department telegrapher who had taken some interest in cryptography, or cypher construction. The strength of this office, at first three people, grew rapidly, was subdivided into functional sections, and at the conclusion of the War had a table of organization of some 150 persons with an annual budget of $100,000. Its security regulations were primitive. Cyphers were broken and

*The phrase "communications intelligence", abbreviated for the sake of convenience to "COMINT", means intelligence produced by the study of foreign communications, including the breaking, reading and evaluating encyphered communications; "cryptology" is a synthetic which is applied to the combined cypher activity--i.e., constructing cyphers as well as breaking cyphers, to which, in turn, the synthetics "cryptography" and "cryptanalysis" are applied, respectively.

and code values were recovered entirely by hand process. The volume of traffic handled by the group was nevertheless respectable, and the results of their work on the military, diplomatic and economic fronts were important enough to impress both the General Staff and G-2. But its budget for fiscal year 1921 ran into opposition, and during that decade was steadily diminished, falling at length to $25,000. No research was carried on; there were no training activities, no intercept, no direction finding studies. The personnel had fallen to six. The coup-de-grace was given in 1929 a few weeks after Mr. Stimson* became Secretary of State. By default the records and physical possessions of "The American Black Chamber" fell to the Signal Corps of the Army.

(*Note: Include as a footnote a quotation from Mr. Stimson's Book if desired.)

The Navy Department attempted no cryptanalytic work during 1917-1918 but set up a system of medium frequency direction finder stations along the Atlantic Coast for tracking German submarines operating in the Western Atlantic. After the Armistice these Navy coastal D/F stations were diverted to use as aids to navigation but were retained in full operation until "navigational D/F service" was turned over to the Coast Guard in 1941. Although the U. S. led the world in the development and use of the IFDF it lagged badly in development of the HFDF. Finally, in 1937 or 1938, the Naval Research Laboratory developed a HFDF that would work. Production was undertaken at the Naval Gun Factory, installations were made at selected coastal D/F stations in the continental U. S., and overseas "strategic" (HF) D/F stations were established at Manila, Guam, Midway, Oahu, Dutch Harbor, Samoa, Canal Zone, San Juan, and Greenland. By 1939, the "strategic" D/F organization was successfully tracking Japanese

warships and merchant vessels in the Western Pacific; the Japs had been tracking U. S. Naval ships since 1934. By 1940, the East Coast strategic D/F net was successfully locating and tracking German submarines in the Atlantic. About May 1941, the Navy Department and British Admiralty began exchanging D/F bearings on German U-boats: U. S. D/F stations compared favorably with British D/F stations in this respect. These U. S. Navy D/Fs were also supplied to all Naval Air Stations for air navigation and lost plane procedure, and were made available to the FCC and to the Army. In 1940 Monsieur Busignies fled to America from Paris, ahead of the advancing German armies, taking with him complete plans for a new and radically superior fixed-Adcock type of HFDF. The Navy placed a production contract for the Busignies D/F through the Federal Telephone and Telegraph Company. It was necessary to re-engineer the Busignies D/F to take standard American tubes, 60-cycle power supply, and otherwise adapt it to American use and manufacturing processes; as a result the Busignies D/F did not get into service until 1943. The Collins Radio Company submitted to the Navy the plans of a new and radically different type of rotating D/F about the same time as M. Busignies. The Collins D/F was rushed into production and went into service in 1942. On 7 December 1941, the U. S. Navy was using the DT-1 and DT-2 HFDFs of Navy design and construction; and had a continuity of direction finding effort since 1917.

On the Security side, the Navy built up during 1917 and 1918 an integrated organization (the Code and Signal Section of Naval Communications) for the compilation, production, distribution and accounting of Codes and Ciphers. The Registered Publication Section was divorced from the Code and Signal Section in 1923 and its functions

were expanded to include distribution and accounting for all secret and confidential documents prepared by the Navy Department and bearing a register number. During 1917-1918, the U. S. Navy relied heavily on cryptographic advice given by the British Admiralty, whose famous "Room 40" led the world in practical cryptanalysis at that time. The Code and Signal Section, maintained at reduced strength after the Armistice, gradually built up a War-Reserve of Naval Codes and Ciphers and made plans for technical improvements. As early as 1922 the Navy recognized that the future of secret communications lay in machine cipher systems rather than in its current systems of enciphered-codes, and sponsored the development of the Electric Cipher Machine from that time on. By 1931 the Navy had tested and discarded the double-printer model of the Hebern Cipher Machine and had placed an order for 30 single-printer Hebern Cipher Machines for service tests. An early form of "strip cipher" was introduced by the Navy as a step in the transition from codes to ciphers and to serve as an interim system until the Electric Cipher Machine could be perfected. The Army took a dim view of the Electric Cipher Machine at that time and attempted to induce the Navy to abandon it: under the circumstances "collaboration" was impossible.

In 1924 the Navy established a Communication Intelligence Organization under the Code and Signal Section of the Office of Naval Communications with covering title of "Research Desk". The initial allowance was one (1) officer and four (4) civilians, later supplemented by two (2) enlisted radiomen. An immediate start was made on establishing intercept stations in the Pacific Area, getting the Washington Cryptanalytic Unit to function, training personnel, and planning for future expansion. Training was accomplished through

technical manuals (which had to be prepared) and correspondence methods plus temporary duty "under instruction" in Washington. Intercept stations were established as trained personnel became available in approximately the following order: Shanghai, Oahu, Peking, Guam/Manila, Bar Harbor (Maine), Astoria (Oregon), and Washington, D.C. Minor intercept activities were later established at various "strategic" (HF) D/F stations. Advanced CI (decrypting) Units were established in the Manila Area in 1932 and at Pearl Harbor in 1936, serving CINCAF and CINCPAC respectively. Beginning in 1935, selected Naval Reserve officers were ordered to Washington normally for a two-weeks "training cruise" and given advanced cryptanalytical instruction and training. In 1938 the "Communications Security Group" (successor to the "Research Desk") took over the operation of all Naval D/F facilities. The growth of the Navy COMINT Organization was slow, steady, and uninterrupted until the fall of France (June 1940) and the President's proclamation of the Unlimited National Emergency (June 1941) permitted calling to active duty trained (or at least partially trained) Naval Reservists previously earmarked for CI duty. The strength and growth of the Navy COMINT Organization is shown by the following table:

COMPLEMENT OF THE NAVY COMMUNICATION INTELLIGENCE ORGANIZATION

Date	Officers	Enlisted	Civilians	Total
1925	1	2	4	7
1926-1935	Net increase of about 10 men per year, plus "qualified" personnel performing other duties			
1936	11	88	10	109
June 1940	12	121	15	147
	(Does not include 150 operators performing navigational D/F services)			
January 1941	44	489	10	543
7 December 1941	75	645	10	730

Once Intercept Stations had been established at Shanghai and Oahu, and a few radio operators had learned to copy the Japanese Morse Code, the U.S. Navy was off to a flying start in its study of Japanese Naval Messages-due to a fortuitous circumstance. About 1922 a shock-team of FBI, ONI, and New York Police representatives succeeded in "picking-the-lock" of the safe of the Japanese Consul General in New York and discovered a Japanese Naval Code belonging to a Japanese naval inspector. This was photographed, page-by-page, over a period of time, and rephotographed a year or two later to pick up extensive printed changes. The cipher used with this code was not too difficult- and we were literally surfeited with blessings. The one or two available translators could not possibly go through all the intercepted messages so it was necessary to sort out the high priorities, important originators, important addressees, etc., and thus skim off the cream. The Japanese used this code until December 1930, thus giving U.S. Naval Authorities (CNO, War Plans, and Naval Intelligence) a complete picture of the Grand (Japanese Naval) Maneuvers of 1930 including Japanese Naval War Plans, strategic concepts, and the fact that the maneuvers were

a "cover" for a 100% mobilization of the entire Japanese Navy. When the Japanese Army began the invasion of Manchuria a few months later, its rear was guarded by Naval Forces superior in strength to the peace-time U. S. Navy, and CNO knew it.

In the Army, the period 1930 to 1935 was one of energetic revival. In those years the work was under the direction of Mr. William F. Friedman, who has continued to be a leader in the field and who is presently associated with AFSA, the joint Army-Navy-Airforce cryptologic center in Washington. The first job was to reassemble former personnel and enlist new recruits; a training program with instructional literature was organized and it is note worthy that for the first time a total cryptologic activity, (the construction of our own cyphers) was envisaged. There was still no Army intercept service, as we understand it today, but raw material was clandestinely obtained through "backdoor" arrangements, and the secrecy surrounding the work was such as, in the backwash of shock following the Stimson ultimatum, to preclude showing the results of the effort to anybody but the Chief Signal Officer -- even G-2 was proscribed. In these depression years funds were extremely difficult to get, especially in view of the nervous secrecy engendered by the Yardley* disclosures. Perhaps the greatest triumph of the Army cryptanalytic group at this time of stringency and uncertainty was the establishment under the Signal Intelligence Service of a training school for officers, which grew from a student body of one in 1931 to about a dozen ten years later.

When the newly established Navy COMINT Unit began its study of JAP DIP systems in 1924-25, the Army steadfastly refused to give the Navy any assistance or to admit that Yardley's Black Chamber" in New York City

*"The American Black Chamber" by H. O. Yardley; Bobbs Merrill, Indianapolis, 1931.

ever existed. In 1931 the Navy set an example of collaboration by giving the Signal Corps all JAP DIP keys which had been recovered since the abolition of the "Black Chamber" plus full data on new systems which had come into being since that date. The Army more or less took over JAP DIP systems leaving the Navy free to devote its efforts to Jap Naval systems. From that time on there was complete interchange between the Army and Navy regarding all technical features of JAP DIP as well as exchange of important translations. During the winter of 1935-1936 a new Japanese diplomatic system came into effect which the Army correctly estimated to be a machine system. The Navy suspected that it might be similar to a Naval Attache cipher machine, which the U. S. Navy was currently reading, if not the same machine. The Navy gave the Army full technical details of this machine, plus a "reconstructed" equipment, and the techniques of its solution. Shortly thereafter the Army was reading the messages in this diplomatic system, subsequently called the "Red" Machine. Later on the "Red" Machine disappeared from the major embassies and reappeared in less important diplomatic posts. The new machine (subsequently called "Purple") had some similarities to the "Red" Machine but was much more complex. As far as technical difficulties are concerned, the Army's solution of the Purple machine was the masterpiece of cryptanalysis in the pre-war era. It required about two (2) years time plus copious "cribs" and translations, and literally drove some of the participants to the verge of nervous breakdown. The Navy assisted by fabricating "reconstructed" Purple Machines at the Naval Gun Factory. These were distributed to the War Department, Navy Department, CINCAF, and subsequently to the British COMINT organization in London. Solution of the Purple Machine itself was not the whole story by any means because a new key was used each day and had to be recovered each day, as well as the

special keys for special services which were introduced later on. The Navy assisted the Army in the recovery of these daily keys and eventually developed a system of "predicted keys" whereby older keys could be re-used after going through certain manipulations. The all important messages sent from Tokyo to Washington on 6 and 7 December 1941 were in "predicted" keys so the only delay in reading these messages was decoding and editing.

The Navy COMINT Organization always recognized that its proper targets were the major Navies of the world - particularly the Japanese Navy. It began solution of diplomatic systems in 1924 for training of personnel and because the messages were on hand (relayed by U. S. Naval Radio Stations for several years). No Japanese Naval messages were then available and there were no intercept stations or operators capable of copying them. Work on Japanese diplomatic systems was continued, partly for training and partly to be independent of U. S. Army sources, to say nothing of orders of higher authority. During the hiatus between closing of Yardley's "Black Chamber" and the establishment of the "revived" Signal Corps Unit in Washington, the Navy was the only source of JAP DIP COMINT: attempt was therefore made to translate all diplomatic intercept during this period. For the rest of the time, up to 1938 or 1939, Navy interest in JAP DIP centered in solving the ciphers and recovering the keys. The CinC Asiatic Fleet was kept supplied with JAP DIP ciphers and keys from 1931 through 1941, and his Fleet Intelligence Officer made such translations as were required by the CINCAF. In 1938 or 1939 it was discovered that the same safe which yielded the Japanese Naval Code in the early 1920's was a never-failing source of supply for "effective" and "reserve" diplomatic ciphers and keys with the exception of the two machine systems. This enabled the Navy Department to provide

CINCAF and the Army with JAP DIP Ciphers and Keys before they came into use. At that time the U. S. Navy was devoting 100% of its cryptanalytic effort and about 90% of its translating effort to Japanese Naval Codes and Ciphers, leaving JAP DIP to the U. S. Army almost exclusively. Later, during the winter of 1940-41, when the White House and the State Department became seriously interested in JAP DIP messages, the picture changed.

Once the Purple system became readable and the need for current JAP DIP was felt, the War Department COMINT Unit did not have enough Japanese translators to handle the job efficiently. Furthermore it was under pressure to divert some of its cryptanalysts and crypto-clerks to German and Italian crypto-systems. Therefore the Army requested the Navy to assist with JAP DIP on a 50-50 division of effort. After studying and rejecting two earlier proposals it was agreed to divide all JAP DIP "processing" (decrypting or decoding) plus translation on a daily basis, the Navy taking the odd days and the Army the even days, as the simplest way to evenly divide the work load and prevent duplication of effort. A few months later Naval Intelligence and G-2 arranged for the dissemination of JAP DIP to the White House and State Department on a monthly basis, the Navy taking the odd months and the Army the even months.

The collaboration between the Army and the Navy on Japanese Diplomatic crypto-systems did not extend to Jap Military (Army and Navy) crypto-systems. A secret divulged to a third party is no longer a secret. The U. S. Navy witheld all details of its success with Japanese Naval crypto-systems from the Army and in turn made no inquiries about the Army's progress with Japanese Army crypto-systems. The U.S. Army followed a similar policy.

When the Japanese Army invaded Manchuria in 1931 the U. S. Navy intercept station at Peking (manned by Marine Corps operators) went to watch-and-watch condition and obtained a wealth of tactical intercepts. These were all turned over to the War Department for exploitation -- and no embarrassing questions were ever asked. From 1936 on, Navy intercept stations in the Far East copied considerable Jap Army traffic which was turned over to the War Department. For some strange reason the U. S. Army posts at Tientsin (China) and Manila failed to profit from the wealth of Jap Army messages available at slight effort. Not till the spring of 1941 did the War Department attempt to set up an intercept unit in the Philippines and sent a Signal Corps officer to take charge. The Navy collaborated with the three-months loan of an experienced and qualified Chief Radioman to act as instructor, and the supply of all available technical literature on intercept operator training, Japanese radio procedure, Japanese radio organization, Japanese call-and-address system, etc., but left the Army "on their own" so far as Japanese military crypto-systems were concerned.

On 1 December 1930 the old 1918 Japanese Naval Code was replaced by a 1930 Naval Code which remained in effect until 31 October 1938, giving the U. S. Navy COMINT organization a severe, although temporary, set back. The new code was never used without a cipher; the cipher had to be stripped off, before the code could be reconstructed. To make a long story short the Navy cryptanalysts, spear-headed by Mrs. Driscoll, "accomplished the impossible", solved the ciphers and then reconstructed the code. This was the most difficult cryptanalytic task ever performed up to that date and possibly the most brilliant as there were no "cribs" and "translations" to help out as in the subsequent Army solution of the Purple machine. IBM tabluating

machinery was introduced by the Navy incident to the solution of the 1930 Naval Operations Code. This machinery greatly speeded solution and increased the per-capita output of the Decrypting Unit. In 1941 similar IBM equipment was sent to Pearl Harbor and to Corregidor.

The Japanese Navy held Grand Maneuvers every three years. With the 1930 Grand Maneuvers fully digested, comprehensive plans were made for the 1933 Grand Maneuvers. Subsequent events proved that these maneuvers were a dress rehearsal for the Conquest of China - while warding off intervention from the U. S. Fleet. The U. S. Navy tested its theories of Traffic Analysis under simulated war conditions and found them practicable and reliable. The success of the Asiatic CI Unit convinced CINCAF (Admiral Upham) of the necessity of a permanent Navy COMINT installation on Corregidor. The project was begun in 1938 and completed in September 1941. On 7 December 1941 the Asiatic CI Unit consisted of 9 officers and 61 men, located in a bomb-proof tunnel on Corregidor, and functioning with 100% efficiency. This Unit was subsequently evacuated to Australia by submarine and played an important part in the Battle of Coral Sea and in the Battle of Midway.

Extensive arrangements (including a mobile intercept unit aboard a destroyer) were made to cover the 1936 Grand Maneuvers of the Japanese Navy. But these Maneuvers were delayed and finally turned into the real thing, the Invasion of China, as forecast by the 1933 Grand Maneuvers. The Navy COMINT organization gave the CNO and CINCAF advance information on all important moves and this information was later verified without exception. It proved what could be done by COMINT, even without radio direction finders, and HFDF's (we hoped) were "just around the corner". The 1930 Naval Operations

Code was thoroughly reconstructed by that time and the only limits to our detailed knowledge of what was going on inside the Japanese Navy was the acute shortage of translators and the fact that sometimes the Japanese did not entrust important secret matters to radio communications. The "China Incident" high-lighted the need for a secure COMINT post in the Ultimate Defense Area of the Philippines. The Corregidor Project was revived; the CNO finally beat down the objections of the Army Chief of Staff which had delayed the project for two years. The two years additional delay before this project was really commenced were due to cussedness and cowardice on the part of certain high ranking officers* in the Navy Department itself.

The most important and certainly the most dramatic incident connected with the 1930 Naval Code was the message reporting the NAGATO's post-modernization trials in 1936. We were fortunate enough to intercept the message and got a solid translation. The NAGATO's new speed was better than 26 knots - the same as the four KONGO-class battle cruisers. There was no doubt as to the correctness of this information. By inference, this was the prospective speed of the modernized MUTSU and minimum speed for the new Japanese battleships of the YAMATO-class. This information created consternation in the higher echelons of the Navy Department because the MUTSU-class was believed good for only 23 1/2 knots, and our new battleships (then in the blue print stage) were going to have a speed of only 24 knots. The information was referred to the General Board; the maximum speed for battleships NORTH

* When Admiral Moreal was "propositioned" on the Corregidor Project a few days after taking office as Chief of the Bureau of Yards and Docks he exclaimed, "Hell - I don't need Congressional authorization to dig a hole in the ground! But I will need it before I put up any buildings. If the CNO can get me funds for the Tunnel I will start it immediately and I will also get the funds for the Quarters and take care of Congressional approval."

CAROLINA and WASHINGTON was raised to 27 knots, and for later battleships to 28 knots. The twelve (12) battleships of the new building program were thus given a superiority in speed over the Japanese battleships.* It proved impossible to get any COMINT information on the tonnage, speed, or main-battery caliber of the YAMATO-class: the Japs never sent this information by radio.

On 1 June 1939 the Japanese Navy introduced a new type of numerical code referred to by Navy COMINT personnel as AN, JN-25 or the Operations Code. This code used a vast number of "additives" (or subtractor) keys, similar to the British Naval Cypher No. 3** used by the U. S. and British Navies from 1941 through 1943. Mrs. Driscoll and Mr. Currier spear-headed the attack and we were soon stripping off the additives and reconstructing the code. Recovery of the additive keys, however, involved much more labor and required many more crypto-personnel than the earlier transposition keys. Main work of solution was undertaken at Washington. By December 1940 we were working on two systems of keys used with this code book: the "old" keys for code recovery and the "new" keys for current information. In the spring of 1941, the U. S. COMINT Unit at Corregidor pooled its effort with the British COMINT Unit at Singapore. The British had also reconstructed this Japanese Number Code to a partially readable extent and were busy recovering keys and "filling in the blanks" in the code. Upon CINCAF's recommendation, the U.S. Asiatic COMINT Unit was authorized to collaborate with the British on the solution and exploitation of this system, and a set of "code-values", cipher keys, skeleton code-book,

* It is fashionable nowadays to sneer at battleships, but when the war was on and Japanese battleships and heavy cruisers were active our Naval aviators were very glad to include fast battleships in the Carrier Task Forces. A carrier, at night, is an easy victim to any heavy surface craft.

** The Germans read this code, solid translation, and were winning the Battle of the Atlantic so long as Cypher No. 3 remained in use.

cryptanalytical techniques, etc., intended for Pearl Harbor were diverted to Corregidor. A replacement was hastily prepared in Washington and sent to Pearl Harbor, arriving in November 1941. On 10 December 1941 the Pearl Harbor COMINT Unit discontinued attack on the Japanese Flag Officers' Cipher and concentrated all effort on the "Numbers System". [Incidentally, we never solved the Flag Officers' Cipher and the Japanese discontinued its use, probably because of its slowness, complexity, and susceptibility to error. It was the only Japanese Naval Cryptographic system which the U. S. Navy ever failed to solve.]

On 1 December 1941, the numbers system became unreadable, CINCAF promptly advised Washington to this effect. This could have been a tip-off as to coming hostilities, but it also could have been merely a routine change of system. After all, the code had been in use for 2 1/2 years. Two weeks later Corregidor flashed the good news that the same old code was still in use but that new keys were being used with it.* This was the third or fourth set of keys used with this same code-book. By February 1942 the new keys had been solved to a readable extent. This same code was retained in use through the Battle of Coral Sea and the "build-up" for the Battle of Midway. It was finally superseded on 31 May/1 June 1941 by a similar code. If (and it is a big if), if the Japanese Navy had changed the code-book along with the cipher keys on 1 December 1941, there is no telling how badly the War in the Pacific would have gone for Australia and the U. S. or how well for the Japanese in the middle stages. Without detracting in any way from the cryptanalysts who spotted the actual tip-offs, or from the men who did the fighting, due credit

* "COM 16 TO OPNAV INFO CINCAF - TOP SECRET - 151250 - TWO INTERCEPTS IN AFIRM NEGAT PLAIN CODE SIXTH AND THIRTEENTH FOLLOWED WITHIN A FEW HOURS BY ENCIPHERED VERSIONS CONFIRMED INDICATOR SUBTRACTOR ALREADY RECOVERED BY MATHEMATICAL ELIMINATION PM CODE REMAINS UNCHANGED X WILL SEND SUBTRACTOR AND ADDITIVE RECOVERIES THIS SYSTEM IF YOU DESIRE BEGIN WORK ON CURRENT PERIOD"

for Coral Sea and Midway should be given to the Navy's pre-Pearl Harbor COMINT effort.

The decryption of Japanese Diplomatic messages in Washington throughout 1941 is now a matter of public knowledge and some 40 volumes of official record We may summarize by stating that the COMINT organizations of the Army and the Navy worked in perfect coordination during this period and provided the White House, State Department, Army General Staff and Naval Operations with authentic timely and complete information concerning the Diplomatic Crisis and the mobilization and movements of Japanese amphibious forces for the conquest of Southeast Asia. The White House and State Department used this information with consummate skill. The failure of the General Staff and Naval Operations to profit from the same information* is beyond the scope of this "History".

So long as the Navy did all the interception and the Army relied on "back-door methods" for its source of messages there was no problem about "collaboration" or "division of effort" in interception. But troubles arose when the European War broke out and the Signal Corps began to establish intercept units at Army posts. The Signal Corps officers responsible for the Army Intercept Service were strong on theory but weak on performance and unwilling to profit by the greater experience of the Navy. Coordination and consultation were considered by them to be more important than getting on with the job. Weeks were wasted in fruitless conferences while the Signal Corps learned "the hard

* "The Committee has been intrigued throughout the Pearl Harbor proceedings by one enigmatical and paramount question: Why, with some of the finest intelligence available in our history, with the almost certain knowledge that war was at hand, with plans that contemplated the precise type of attack that was executed by Japan on the morning of December 7 - why was it possible for a Pearl Harbor to occur?" Report of the Joint Committee on the Investigation of the Pearl Harbor Attack. (Senate Document No. 244 - 79th Congress) - page 253 (Recommendations).

way" and saw their pretty theories demolished by disagreeable facts. In 1940-41 the Army had no intercept stations which could match the Navy's "big five" /Corregidor (P.I.), Wahiawa (T.H.), Bainbridge Island (Wash.), Winter Harbor (Maine), and Cheltenham (Md.)/ with their directional antennas beamed on the "target" transmitters, diversity receivers to overcome selective fading, syphon recorders for copying high speed automatic transmissions, highly trained operators, and experienced supervisors. Allocation of intercept effort was finally settled on a trial-and-error basis. The Signal Corps covered such of the International Commercial Transmitting Stations as it could; the Navy covered the others as a matter of necessity. Theoretically it was bad to "split" a circuit: practically there was no alternative. Assignments were changed almost weekly as radio propagation suffered seasonal changes, as more operators and more receiving equipment became available, and as the pressure from higher authority required speeding up delivery and "bridging the gaps" in intercept traffic regardless of cost.

Covering international radio circuits is like fishing with a dragnet, anything and everything comes in with the haul.Then it is necessary to sort out the catch and discard what is not wanted. Monitoring for Japanese diplomatic traffic automatically gave naval attache messages, military attache messages, German diplomatic, Italian diplomatic, government messages of neutrals, and of course a volume of unwanted commercial messages. It is needless to review all the arguments and discussions that took place in 1940. Not only did intercept assignments between the services change from time to time during 1940 and 1941, but the assignments to intercept stations within each service changed from time to time. For example, we eventually found we could get the best coverage of the Berlin - Tokyo circuit at Corregidor; messages in

the "Purple" system were therefore re-enciphered in a Navy system and forwarded to Washington by radio. During the last few weeks before the Pearl Harbor attack, while U. S.-Japanese relations were at a crisis, Japanese diplomatic messages intercepted at Bainbridge Island (Wash.), Winter Harbor (Maine), and Cheltenham (Md.) were relayed to Washington by landline teletype. Army intercepts continued to come in by mail after 7 December 1941. The Navy also arranged for "back-door" services on all DIP traffic in and out of Washington and New York - to back up the radio intercept stations.

The squabbles between the Army and the Navy COMINT organizations were confined to the interception, "processing", translation and dissemination of Japanese diplomatic messages. These controversies settled themselves in the course of time, and in retrospect are seen to have been merely petty annoyances. Diplomatic systems of other nations were handled by the Army exclusively and no problems of "collaboration" ever arose. In JAP DIP the Navy found it had a bear by the tail and couldn't let go until after the attack on Pearl Harbor when JAP DIP messages became greatly reduced in volume and importance. Then the Army was able to handle all JAP DIP decryption and translation unaided, leaving the Navy free to undertake a serious attack on German submarine communications.

During November and early December of 1941, JAP DIP was diverting 30% of the Navy's Intercept and D/F effort, 12% of its Decrypting effort and 50% of its Japanese translation effort from their proper military functions. Loss of the translators hurt us the worst as the total number available was inadequate even for Japanese Naval messages. Loss of Decryption personnel was more serious than the numbers indicate because our "first team" in Washington had to be assigned to JAP DIP. Detailed breakdowns are given in tabular form on the page following.

DISTRIBUTION OF NAVY COMINT PERSONNEL - EARLY DECEMBER 1941

CATEGORY	ATLANTIC (Navy Dept.)	PACIFIC (Pearl Harbor)	ASIATIC (Corr-gidor)	IN TRANSIT (Diverted to Australia)	TOTAL
Officers	53	12	9	6	80
Crypto-Clerks	157	18	19	20	214
Subtotal	210	30	28	26	294
Intercept Stations & D/F Control	178	72	42	--	292
Outlying D/F Stations	60	84	8	--	152
TOTAL	448	186	78	26	738

ALLOCATION OF NAVY COMINT EFFORT - EARLY DECEMBER 1941

CATEGORY	JAP DIP	JAP NAVY	GERMAN & ITALIAN NAVIES
Intercept, D/F, & D/F Control	30% (Includes all DIP interception)	50%	20%
Decryption	12%	85%	3%
Translation	50%	50%	None

There were no problems of collaboration for strictly military COMINT matters where each service was working alone in its proper sphere of activity. The Navy COMINT team did a thorough job on the Japanese Navy with no help from the Army and very little help from the British. No assistance was requested from the Army other than permission to establish a Navy COMINT Unit on Corregidor. The Navy gave the Army all its JAP Army intercepts, assisted in training an Intercept Unit at Manila, never denied the Army any legitimate information it requested, and gave the Army all the help it was willing to accept. The Army, in turn, provided the Navy copies of all its technical cryptanalytical manuals and training courses.

Collaboration with the BRITISH COMINT organization got off to a bad start so far as the Navy was concerned, due to an incoherent and weasel-worded message* sent by CNO to SPENAVO, London about November 1940. The U. S. Navy sent the British all the COMINT information it had on the Japanese Navy in early 1941 and got nothing in return. This was rectified by the British a year later, but it set back the U. S. solutions of German submarine messages by this amount. For several months U. S. Navy COMINT personnel thought they had been double-crossed by the British and were reluctant to go ahead with collaboration in direction finding and other matters which were greatly to England's advantage throughout 1941. The U. S. Army got German and Italian diplomatic systems from the British and was very happy with the deal. As a matter of fact, General Strong had practically promised the British everything they wanted, with nothing in return, so anything the U. S. got might be considered as clear profit. The subsequent harmonious collaboration with the British belongs to the post-Pearl Harbor portion of this "History".

---

* Instead of proposing an "exchange of all available German and Italian Naval, Military and Diplomatic crypto-systems for all available Japanese Naval, Military and diplomatic crypto-systems", the message made a vague reference to "exchange of technical information concerning interested third parties." GC&CS interpreted "third parties" as meaning "Foreign Offices".

A summary of the Navy's pre-Pearl Harbor COMINT effort and COMINT concepts may be obtained from a secret letter (Serial 081420) sent by the CNO to the Commanders-in-Chief of the Asiatic and Pacific Fleets and to the Commandants of the 14th and 16th Naval Districts, in October 1940, extracts from which are quoted below:

"Subject: Cryptanlytical Activities, status of.

"1. In view of the present serious international situation, it is desired to acquaint the addressees with the present status and prospects of solution of Orange naval cryptographic systems. ...

"2. During the past ten years, Orange intelligence has been provided by solution of Orange cryptographic systems, and to a lesser extent by direction finding and traffic analysis. Every major movement of the Orange Fleet has been predicted, and a continuous flow of information concerning Orange diplomatic activities has been made available. ...

"3. There are five major Orange naval cryptographic systems in current use, all of the enciphered code type, namely:

A. Administrative Code system.

The cipher used with this code changes every ten days. Code and cipher recovery is in the hands of Commandant, Fourteenth Naval District, and has progressed to the point where intelligible text can be obtained from nearly all intercepted messages. ...

B. Merchant Ship Code system.

The system itself is 99% readable, but an auxiliary system of ship and place names has not yet been recovered. The cipher changes quarterly, and has been predicted through June, 1941. ...

C. Materiel Code System.

This code has its cipher changing at irregular intervals of from ten to thirty days. Current information is not now being obtained from this system, but it is estimated that within six months we will be able to read most of this traffic shortly after receipt. ...

D. Operations Code system.

An additive key cipher is employed with this code, and although the method of recovery is well defined, the process is a laborious one, requiring from an hour to several days for each message. ... Recovery is being pursued by the Department, and details will be promulgated later.

E. Intelligence Code system.

This system, being of least importance, has been neglected in favor of the others. ... Solution is being handled by the Department.

"4. With regard to the immediate dissemination of intelligence, it is incumbent upon the Communications Intelligence Units to provide the proper authorities with information and inferences obtained from Communications Intelligence. Since it is manifestly impracticable for the Commander-in-Chief, U. S. Fleet, to gather such information first hand, and impossible for him even to use recovered cryptographic systems without an Orange language officer on his staff, it is desired that Commandant, Fourteenth Naval District, and Commandant, Sixteenth Naval District, disseminate such intelligence from time to time to both Commanders-in-Chief and to the Department. This will require that all messages in readable Orange navy systems be translated promptly upon receipt, to insure intelligence of as fresh a nature as possible, and all cryptanalytical and cryptographic activity must be subjected to this end. As a general rule, readable Orange navy encrypted communications should be handled in inverse order of interception.

"5. It must be borne in mind that the present Orange cryptographic systems may be replaced by new ones immediately upon the outbreak of war. Therefore, cryptanalytic intelligence, per se, may not be available from that time until after successful attack has been conducted. Meanwhile, enemy information can be obtained from radio intercept and direction finder activities as has been the case during the past year.

(Signed) R. E. INGERSOLL
Acting."

- Finis -