SRH—149

A Brief History of Communications Intelligence in the United States

by
Laurance F. Safford
Captain, United States Navy
(Retired)

REVIEWER'S NOTE:

This document, designated SRH-149 in the records of the National Archives, Washington, D.C., was prepared 21-27 March, 1952, by Captain Laurance F. Safford, United States Navy with special reference to coordination and cooperation and access to various historical records, with the objective of bringing diverse documents into a usable narrative history of a Naval activity. The document does not constitute an official Navy history, and no claims are made regarding its completeness or accuracy. **On 6 March 1982 it was further certified to be declassified by the Director, National Security Agency.**

SRH-149

A Brief History of Communications Intelligence in the United States

Prior to 1917, United States activity in the field of Communications Intelligence[1] was sporadic, and there is little recorded of it. For all practical purposes, the history of American cryptanalysis began with the entry of the United States into World War I. Codes and ciphers at that time, even those used to carry the most sensitive information, were by current standards naive. They were hand-coded and hand-applied cipher systems usually overlying double-entry codebooks, 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 cipher 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 cipher construction. The strength of this office, at first three people, grew rapidly. At the conclusion of the War it was subdivided into functional sections and had a table of organization of some 150 persons with an annual budget of $100,000. Its security regulations were primitive. Ciphers were broken and code values were recovered using hand methods. 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 the decade was steadily reduced each year, falling at length to $25,000. No research was carried on. There was no training activities, no intercept, no direction finding studies. The personnel fell to six. The coup-de-grâce came in 1929, a few weeks after Mr. Stimson became Secretary of State. By default, the records and physical possessions of H. O. Yardley's "American Black Chamber" fell to the Signal Corps of the Army.

---

[1] 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 enciphered communications. "Cryptology" is a synthetic term which is applied to two cipher activities, the construction of ciphers and the breaking of ciphers. In turn, these two activities are termed "cryptography" and "cryptanalysis."

The Navy Department attempted no cryptanalytic work during 1917-18. But it did 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 and were retained in full operation until the "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 medium-frequency direction finding, it lagged badly in development of high-frequency direction finding (HF D/F).

Finally, in 1937-38, the Naval Research Laboratory developed a HF D/F system that would work. Production was undertaken at the Naval Gun Factory. Installations were then 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.[2] By 1940 the East Coast strategic D/F net was likewise 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/F bearings were also supplied to all Naval Air Stations for air navigation and lost plane procedures, and were also 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 HF D/F system. 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 plans of a new and radically different type of rotating D/F system about the same time as Monsieur 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 HF D/Fs of Navy design and construction, and thus 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.

[2] In contrast, the Japanese had been tracking U.S. Naval ships since 1934.

During 1917-18, the U.S. Navy relied heavily on cryptographic advice given by the British Admiralty, who's 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 the then-current systems of enciphered-codes. The Navy, therefore, sponsored the development of the Electric Cipher Machine (ECM) 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 was 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 and attempted to induce the Navy to abandon it. Under the circumstances, "collaboration" with the Army was difficult.

In 1924 the Navy established a Communication Intelligence Organization under the Code and Signal Section of the Office of Naval Communications with the covering title of "Research Desk." The initial allowance was one officer and four civilians, later supplemented by two enlisted radiomen. An immediate start was made on establishing intercept stations in the Pacific Area, which permitted the Navy's 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 Communications Intelligence (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-week "training cruise," where they were 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). The proclamation of the Unlimited National Emergency (June 1941) permitted calling to active duty trained (or at least partially trained) Naval Reservists previously earmarked for communications intelligence 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 DIF services.)			
January 1941	44	489	10	543
7 December 1941	75	645	10	730

Once Intercept Stations had been established at Shanghai and Oahu, with a few radio operators having learned how 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, where they discovered a Japanese Naval Code belonging to a Japanese naval inspector. Over a period of time this code was photographed, page-by-page, and re-photographed 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 Japanese 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 the same 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 hundred percent 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 peacetime U.S. Navy, and the Chief of Naval Operations knew it.

In the Army, meanwhile, the period 1930 to 1935 was one of energetic revival. In these 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-Air Force cryptologic center in Washington. His first job was to assemble personnel and enlist new recruits. A training program with instructional literature was organized, and it is noteworthy that for the first time a total cryptologic activity (the construction of our own ciphers) 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 that, 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 those Depression years funds were extremely difficult to get, especially in view of the nervous secrecy engendered by the Yardley[3] 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 Japanese diplomatic systems in 1924-25, the Army steadfastly refused to give the Navy any assistance or to even admit that Yardley's "Black Chamber" in New York City ever existed. In 1931 the Navy set an example of collaboration by giving the Signal Corps all Japanese diplomatic 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 thereafter more or less took over Japanese diplomatic systems, leaving the Navy free to devote its efforts to Japanese Naval systems.

From that time on there was complete interchange between the Army and Navy regarding all technical features of Japanese diplomatic traffic, as well as the exchange of important translations. During the winter of 1935-36, 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 the Naval Attaché 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 "reconstructed" equipment, and techniques of its solution. Shortly thereafter, the Army was reading the messages in this new diplomatic system, subsequently called the "Red" machine. Later the Red machine disappeared from major Japanese embassies and reappeared in less important diplomatic posts. A new machine (subsequently called "Purple") with similarities to the Red machine but more complex, replaced the Red machines in major embassies.

As far as technical difficulties were concerned, the Army's solution of the Purple machine was a masterpiece of cryptanalysis in the pre-war era. Its solution required about two years plus numerous "cribs" and expected texts, literally driving some of the solution participants to the verge of nervous breakdowns. The Navy assisted by fabricating compatible 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 basic Purple machine itself was not the whole story by any means, because a new key was used each day and had to be recovered daily. Special keys for special services were introduced later on, and these likewise had to be recovered. The Navy assisted the Army in the recovery of the Purple daily keys and eventually developed a system of "predicted keys," whereby older keys could be re-used after going through certain manipulations. All important messages sent from Tokyo to

[3] *The American Black Chamber* by H. 0. Yardley, Indianapolis: Bobbs Merrill, 1931.

Washington on 6 and 7 December 1941 were in "predicted" keys so the only delay in reading these messages was decoding and translating.

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 the training of personnel, because such traffic was on hand, relayed by U.S. Naval Radio Stations. No Japanese Naval messages were then available and there were no intercept stations or operators capable of copying them. Work on Japanese diplomatic systems therefore 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 the closing of Yardley's Black Chamber and the establishment of the "revived" Signal Corps Unit in Washington, the Navy was the only source of Japanese diplomatic COMINT, and attempts were made to translate as much diplomatic intercept as possible during this period. For the rest of the time, up to 1938-39, the Navy's interest in Japanese diplomatic traffic centered on solving their ciphers and recovering keys. The CinC Asiatic Fleet was kept supplied with Japanese diplomatic ciphers and keys from 1931 through 1941, and his Fleet Intelligence Officer made translations from the Japanese texts as were required by the CINCAF.

Even until 1938-39 the same safe which previously yielded the Japanese Naval Code in the early 1920's remained a never-failing source of supply for both "effective" and "reserve" diplomatic ciphers and keys—with the exception of the two Red and Purple machine systems. This enabled the Navy Department to provide CINCAF, as well as the Army, with Japanese diplomatic ciphers and keys before they actually came into use. At that time the U.S. Navy was devoting virtually all of its cryptanalytic effort and about 90% of its translating effort to Japanese Naval Codes and Ciphers, leaving Japanese diplomatic systems to the U.S. Army. Later, during the winter of 1940-41, when the White House and the State Department became seriously interested in Japanese diplomatic messages, the picture changed.

Once the Purple diplomatic system became readable, and the need for current solutions was felt, the War Department's COMINT Unit[4] did not have enough Japanese translators to handle the job efficiently. Furthermore, it was under heavy pressure to divert a number of its cryptanalysts and crypto-clerks to the solution of German cryptographic systems. Therefore, the Army requested the Navy to assist with the reading of Japanese diplomatic traffic on a 50-50 division of effort.

After studying and rejecting two earlier proposals, it was agreed to divide all Japanese diplomatic traffic processing (decrypting or decoding) plus translation on a daily basis, the Navy taking the odd days and the Army the even days. This was the simplest way to evenly divide the workload and prevent duplication of effort. A few months later Naval Intelligence and the Army's G-2 arranged for the dissemination of Japanese diplomatic

[4] The Signal Corps' Signal Intelligence Service (SIS).

traffic to the White House and to the 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 with respect to Japanese diplomatic crypto-systems did not extend to Japanese Military (Army and Navy) systems. A secret divulged to a third party is no longer a secret. The Navy, therefore, withheld all details of its success with Japanese Naval systems from the Army; and in turn no inquiries were made by the Navy to the Army regarding their progress with reading Japanese Army systems. The Army likewise made no inquiries of the Navy.

When the Japanese Army invaded Manchuria in 1931, the U.S. Navy intercept station at Peking (manned by Marine Corps operators) went to a special watch condition and obtained a wealth of tactical intercepts. These were turned over to the War Department for exploitation—and no embarrassing questions were ever asked. Later, beginning in 1936, Navy intercept stations in the Far East copied considerable Japanese Army messages which were likewise turned over to the War Department. However, for some unknown reason the U.S. Army posts at Tientsin and Manila failed to profit from this wealth of Japanese Army messages. Not until the spring of 1941 did the War Department attempt to set up an intercept unit in the Philippines and to this end sent a Signal Corps officer to take charge. The Navy collaborated by making a three-month loan of an experienced and qualified Chief Radioman to act as instructor, and further supplied available technical literature on intercept operator training, Japanese radio procedure including their radio organization, Japanese call-signs, and address systems, etc. The Army was left "on their own," however, insofar as the solution of Japanese military systems were concerned.

On 1 December 1930 the old 1918 Japanese Naval Code was replaced by a 1930 Naval Code. When this latter code was replaced eight years later, on 31 October 1938, the U.S. Navy COMINT organization suffered a severe, though only temporary, setback. Since the new code was an enciphered code, the cipher first had to be stripped off before the basic code could be reconstructed. To make a long story short, the Navy cryptanalysts, spearheaded by Mrs. Driscoll, "accomplished the impossible." They solved the encipherment 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" nor "expected texts" to help out as in the case of the Army's solution of the Purple machine. IBM tabulating machinery was introduced by the Navy incident to the solution of the 1930 Naval Operations Code. This equipment greatly speeded up the solution effort and increased the overall output of the Decrypting Unit. In 1941 similar IBM equipment was sent to Pearl Harbor and to Corregidor.

The Japanese Navy held their Grand Maneuvers every three years. With the Japanese Navy's 1930 Grand Maneuvers fully digested in terms of communications intelligence, comprehensive plans were made for the 1933 Grand Maneuvers. Later events proved that these maneuvers were a dress rehearsal for the Conquest of China—while warding off at

the same time intervention from the U.S. Fleet. The U.S. Navy tested its knowledge and 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 nine officers and 61 men. Located in a bombproof tunnel on Corregidor, they functioned with complete 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 high-frequency D/Fs, which we hoped were "just around the corner." The 1930 Naval Operations Code was thoroughly reconstructed by this time and the only limit to detailed knowledge of what was going on inside the Japanese Navy was the acute shortage of translators plus the fact that sometimes the Japanese did not entrust important secret matters to radio communications. The "China Incident" highlighted the need for a secure COMINT post in the Philippines. The Corregidor Project was thus revived. This was after the CNO finally beat down the objections of the Army Chief of Staff, which delayed the project for two years. The two years additional delay were due principally to obstinance on the part of certain high-ranking officers[5] in the Navy Department.

The most important and certainly the most dramatic incident derived from the solution of the Japanese 1930 Naval Code was a message reporting the *Nagato's* post-modernization trials in 1936. We were fortunate enough to intercept the message and obtain a solid translation. The *Nagato's* speed was better than 26 knots—the same as that of 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 highest echelons of the Navy Department, because the *Mutsu*-class had been believed good for only 23-1/2 knots, and our new battleships (then in blueprint stage) were going to have a speed of only 24 knots. The information was referred to the General Board and as a result the maximum speed for battleships *North Carolina* and *Washington* was raised to 27 knots; for later battleships the maximum

[5] When Admiral Moreal was being briefed on the Corregidor Project a few days after taking office, he exclaimed, "Hell - I don't need Congressional authorization to dig a hole in the ground! But I do need authorization before I put up any buildings. If the Chief of Naval Operations can get me funds for the Tunnel, I will start it immediately; and I will also get the funds for the buildings and take care of the Congressional approval."

speed was raised to 28 knots. The twelve battleships of our new building program were thus given a superiority in speed over the Japanese battleships.[6] Unfortunately, it proved impossible to get COMINT information on the tonnage, speed, or main-battery caliber of the Yamato-class of ships. The Japanese never sent this information by radio.

On 1 June 1939 the Japanese Navy introduced a new type of cryptographic system, a different enciphered code system.

Mrs. Driscoll and Mr. Currier spearheaded the attack against this new code, and we were soon able to reconstruct the basic code. Recovery of the encipherment keys, recovery of additive, however, involved a great deal more labor and more personnel than that required for the recovery of the earlier transposition keys. Main work of solution was undertaken at Washington. By December 1940 we were working on two systems of additives, both used with the same basic codebook. The "old" additives assisted in basic code recovery and the "new" additives were valuable for obtaining current information, i.e., reading current traffic.

In order to permit Japanese traffic to be read as quickly as possible at the scene of potential action, a set of "code-values," cipher keys, skeleton codebook, cryptanalytical techniques, etc., earlier intended for Pearl Harbor, were diverted to Corregidor. A replacement, however, was hastily prepared in Washington and sent to Pearl Harbor, arriving in November 1941. On 10 December 1941, after the Japanese attack at Pearl Harbor, the COMINT Unit there discontinued its cryptanalytic attack on the Japanese Flag Officers' Cipher and concentrated all effort on the enciphered code system introduced by the Japanese in 1939. The Flag Officers' Cipher was never solved, 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 failed to solve.

On 1 December 1941 the Japanese enciphered code of 1939 suddenly 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 basic code was still being used, but that a new set of additives was being used with it.[7] This was the third or fourth set of additives used with this same codebook. By February 1942 the new additives had been solved to a readable extent. This same basic code was retained in use through the Battle of Coral Sea and the

---

[6] It is fashionable today to perhaps sneer at battleships, but when World War II was on and the Japanese battleships and heavy cruisers were active, our Naval aviators were glad indeed to see fast battleships in our Carrier Task Forces. A carrier, at night, is an easy victim to any heavy surface craft.

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

"build-up" for the Battle of Midway. It was finally superseded on 31 May/1 June 1941 by another similar basic code. If (and it is a big if), if the Japanese Navy had changed the codebook along with the cipher additives 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, great plaudits for Coral Sea and Midway successes 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 comprise the 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 the present text. In this connection, the Joint Committee on the Investigation of the Pearl Harbor Attack stated "[We have] been intrigued throughout the Pearl Harbor proceedings by one enigmatic 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?" See Senate Document No. 244—79th Congress, page 253 (Recommendations).

As long as the Navy did all its own interception and the Army relied on "back-door methods" for its source of traffic there was no problem about "collaboration" or "division of effort" in interception. But troubles arose when the European War broke out and the Army's Signal Intelligence Service (SIS)[8] began to establish intercept units at Army posts. The 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 consultations were considered by them to be more important than getting on with the job. Weeks were wasted in fruitless conferences while the Army learned "the hard way" while setting up their own interception system.

In 1940-41 the Army had no intercept stations, which could match the Navy's, which included Corregidor, Bainbridge Island, Washington, and Cheltenham, Maryland. Navy intercept stations contained directional antennas beamed on “target" transmitters, diversity receivers to overcome fading, recorders for copying high speed automatic transmissions, highly trained operators, and experienced supervisors. Allocation of the intercept effort between the Army and Navy was finally settled on a trial-and-error basis.

[8] The Army's Signal Intelligence Service (SIS) later became known as the Army Security Agency (ASA).

The Army covered as many of the international commercial transmitting stations as it could, while the Navy covered the others as a matter of necessity. Theoretically it was bad to "split" the intercept coverage of a circuit, but 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 the delivery and "bridging the gaps" in intercepted 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 produced naval attaché messages, military attaché messages, German diplomatic traffic, etc.

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 intercept stations in the continental U.S. (Bainbridge Island and Cheltenham, for example) were relayed to Washington by landline teletype. Army intercepts, on the other hand, continued to be forwarded to Washington, D.C. by mail even after 7 December 1941. The Navy also arranged for "back-door" services on all diplomatic 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.

In Japanese diplomatic traffic the Navy found it had a bear by the tail and couldn't let go until after the attack on Pearl Harbor. The Japanese diplomatic messages became greatly reduced in volume and importance. By this time the Army was able to handle all Japanese diplomatic decryption and translation, leaving the Navy free to begin an attack on German submarine communications.

During November and early December of 1941, Japanese diplomatic traffic was diverting 30 percent of the Navy's Intercept and direction-finding effort, 12 percent of its Decrypting effort and 50 percent of its Japanese translation effort from other military functions. Loss of the translators hurt the Navy the worst, as the total number of translators available was inadequate even to handle Japanese Naval messages. Loss of

analytic personnel was more serious than the numbers indicate because our "first team" in Washington had to be assigned to the solution of Japanese diplomatic traffic. Detailed breakdowns are given in tabular form below.

There were no problems of collaboration between the Army and Navy for strictly military COMINT matters, as each service was working alone in its proper sphere of activity. The Navy COMINT team did a thorough job with respect to the Japanese Navy with no help from the Army. 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 Japanese Army intercepts, assisted in training an Intercept Unit at Manila, never denied the Army any legitimate information 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.

Distribution of Navy COMINT Personnel - Early Dec. 1941

Category	*Atlantic (Navy Dept.)*	*Pacific (Pearl Harbor)*	*Asiatic (Corregidor)*	*In Transit (Diverted to Australia)*	*Total*
Officers	53	12	9	6	80
Crypto-Clerks	157	18	19	20	214
Sub-total	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 NEW COMINT Effort - Early Dec. 1941

Category	*Japanese Diplomatic*	*Japanese Navy*	*German & Italian Navies*
Intercept, D/F, & D/F Control	30% *(Includes all diplomatic interception)*	50%	20%
Decryption	12%	85%	3%
Translation	50%	50%	None

A summary of the Navy's pre-Pearl Harbor COMINT effort and COMINT concepts may be seen in the secret letter (Serial 081420) sent by the Chief of Naval Operations to the Commanders-in-Chief of the Asiatic and Pacific Fleets and to the Commandants of

the Fourteenth and Sixteenth Naval Districts, in October 1940, extracts from which follow:

Subject: Cryptanalytical 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.
A 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 firsthand, 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 ensure 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