Introduction

Before I treat the main topic of my lecture today, let me delve briefly into the history of cryptanalysis, and we will begin with a cursory background of cryptanalysis in World War I and the subsequent post-war years.

Communication Intelligence in World War I

When we entered the war the United States had at the time no formal cryptologic organization. The British, the French, the Austrians and others had cryptanalytic organizations which had been functioning for quite some time. In order to protect the source of intelligence, the British at first shrewdly attributed their own uncanny success in locating enemy forces and predicting enemy movements to the efficiency of their direction finders. It has since become known, however, that cipher experts of the famous British Room 40 were to a large extent responsible for such important military and political events as the Battles of Jutland and Falkland Islands, and the detection of Zimmermann's attempt to obtain the support of Mexico, which played an important role in stirring

up public opinion in the U. S. against Germany. The Earl of Halifax evaluated the work of this group as follows:

"To Room 40, the country owes an immense debt of gratitude - a debt which at the time, at least, could never be paid. Secrecy was of the very essence of the work, and never was secrecy more successfully observed."

Similar successes were achieved by the French on the Western Front. They repeatedly broke the German ciphers and obtained invaluable information as to German plans and intentions. Likewise the Germans and Austrians had great success with the Russian ciphers in World War I and undoubtedly succeeded in bringing the war on the Eastern Front to an earlier close because of this fact. As for American communication intelligence operations, the successes achieved in this country prior to World War II were not of sufficient importance to impress more than a handful of officers with the great potential value of the work.

Communication Intelligence between Wars

As interesting as the revelations of World War I proved to be, their real significance lay in the profound effect they had upon developments

in the field of cryptography. Nations began to grow increasingly more security conscious. The Japanese in particular, who were profoundly shocked at the revelations of the irresponsible Yardley, embarked upon a program of formidable sophistication of her cryptographic systems, to the great detriment of our national interests in the years prior to World War II. Yardley had been employed by the State Department in communication intelligence activities, and he published a melodramatic book, "The Black Chamber" in which he wrote of our success with Japanese codes during the Washington naval disarmament conference in 1921. The book created a sensation in Japan and was widely circulated. The Japanese felt that they had been tricked, and were extremely resentful. Untold harm was caused by Yardley's violation of security which he himself in his previous official position had counseled others never to reveal anything of the work. A direct and immediate effect of Yardley's unfortunate action was to require the exercise of the greatest caution and secrecy in carrying on communication intelligence work. The result was that it was never possible to present properly the needs of the communication intelligence

organization and to obtain for it the support necessary for its success. The story of what was accomplished under these difficulties prior to Pearl Harbor has been so widely publicized that it needs no reiteration. Let it suffice to say that it took approximately eighteen months of painstaking labor to reconstruct, through cryptanalysis, the complex machine that was used by the Japanese to encipher their highest-level diplomatic communications.

Communication Intelligence in World War II

The importance of communication intelligence in World War II is probably best summarized by the following statement which appears in the Report of the Pearl Harbor Investigating Committee of the 79th Congress:

"All witnesses familiar with communication intelligence material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

When the United States entered the war, it had made a timid beginning in the field of communication intelligence due to lack of funds, personnel

and equipment. In certain phases of the work, notably the solution of the Japanese diplomatic machine, brilliant successes had been scored. But in comparison with the situation at the war's end, exploitation of the field as a whole was in the most elementary stages. Intercept facilities were extremely limited; arrangements for transmitting material from the point of intercept to the cryptanalytic center were hit or miss; cryptanalysis had been carried on successfully only in certain narrow fields, and -- at least in the Army -- methods of getting intelligence from the traffic short of reading it were undeveloped; there was a critical shortage of translators; there were neither sufficient personnel nor adequate procedures for studying and checking the translated product to squeeze out of it all useful intelligence obtainable; the method of presenting the derived intelligence to the responsible authorities in Washington was ineffective; and there was no arrangement for getting such intelligence to commanders in the field promptly and in a manner which

would protect the source and insure security.

On 7 December 1941 there was no overall directive assigning responsibility among the various government departments in the communication intelligence field. Within the armed services, by tacit or express agreement, responsibility for the interception, analysis, solution and translation of encrypted communications had been divided as follows: military traffic - Army; naval traffic - Navy; diplomatic traffic - Army and Navy; clandestine traffic - Coast Guard. Other government agencies were also taking an interest in the field, including the FBI, the FCC and the predecessor of the CIA. In the years to come, there was to be witnessed a fantastic growth in organization of the Army's and Navy's cryptologic organizations, and their combined efforts produced an amount of high-grade intelligence that was beyond the wildest dreams of anyone who knew the size and limitations of the pre-war organizations.

The Battles of Midway and Coral Sea were only two of a multitude of examples of cryptanalytic feats of arms, if I may be permitted to mix a metaphor. According to the official narrative of the Combat Intelligence Center, Pacific Ocean Areas,

"the factors that vitally affected the Battle of Midway were many and complex, but it is undoubtedly true that without radio intelligence it would have been impossible to have achieved the concentration of forces and the tactical surprise that made the victory possible.... In the defensive stages of the war, radio intelligence was not only the most important source of intelligence in the Central Pacific -- it was practically the only source. There were very few captured documents or prisoners of war. There were no photographs of enemy-held positions. In the Central Pacific, excluding the Solomons and New Britain, spies and coast watchers' reports never supplied any important intelligence."

Other important examples of the successes of cryptanalysis may be cited:

1. The movement of four Japanese divisions into Burma in the preparation for the drive into India, which began in March 1944, was discovered far in advance of the beginning of that attack and a number of indications that an attack was pending were obtained.

2. The Japanese plan for an attack on the Torokina perimeter in Bougainville, including the exact scheduled D-Day, was learned in advance, and U. S. forces were so prepared for the attack that it was crushed with serious losses to the Japanese.

3. The movement of two divisions into the Marianas prior to the U. S. attack was discovered.

4. The complete Japanese plan for an attack on the Aitape perimeter in New Guinea was discovered more than a month in advance and the attack was completely smashed.

5. Before the U. S. landing at Hollandia, analysis of traffic and of fragmentary messages showed that no Japanese division had been moved into the area and that it was defended only by service troops.

One of the most dramatic episodes of the war -- the ambush of Admiral Yamamoto -- was a victory of cryptanalysis. U. S. Navy experts decrypted a message which gave information concerning a projected trip by Yamamoto. The sequel may be summarized by an official Japanese Navy Department

communication reading in part as follows:

"The Commander in Chief of the Combined Fleet, Admiral Isoroku Yamamoto, died an heroic death in April of this year in air combat with the enemy while directing operations from a forward position."

The Japanese never found out until the Pearl Harbor Investigation what it was that actually killed Yamamoto -- inadequate cryptography.