In inviting me to address the staff and students of the Senior School of the Marine Corps on the subject of "Communications Intelligence and Communication Security" I assume that the objective is to make you aware of the roles that these two branches of the science of cryptology have played as vital military weapons in the past and may in the future again play.

Soon after the close of World War II, service schools began to ask for lecturers to tell their student officers something about our cryptologic activities during the war. There was at first serious question as to the advisability of lifting the security veil sufficiently to permit discussion of the subject, but in time an affirmative decision was made. The official views of the Naval War College on the matter were stated in a letter dated 5 February 1946, and because the letter admirably states those views I shall read two paragraphs of it.[1] In commenting upon the fine presentation made by a certain

[1] From the then President of the College, Admiral R. A. Spruance, to the Chief of Naval Communications, Admiral E. E. Stone.

speaker, the letter said:

"His treatment of the subject matter emphasized the value of communication intelligence to naval commanders, the vital importance of maintaining the security of our own communication intelligence activities, and the necessity for observing the principles of communication security in defense against enemy communication intelligence. I consider that the value to be derived from the indoctrination of senior officers of the Navy in these principles far outweighs any possible loss of security resulting from a partial revelation of our activities in the past war, particularly in view of the disclosures which have been made in the press.

The latter continues:

"It appears axiomatic that the full benefit of communication intelligence can be obtained only when all senior officers realize its potentialities for winning and losing battles and wars, and when their actions are tempered by complete knowledge of the elements of communication intelligence, rather than by incomplete and inaccurate information obtained through the channels of gossip."

My talk being divided into three periods, I will give you first some of the historical background of cryptology. Next will come a presentation of the basic manner and the apparatus whereby Communication Security, or for short, COMSEC, is established and maintained; principles, procedures, machinery, and organization whereby Communications Intelligence, or, for short, COMINT or SIGINT, in British terminology, is obtained, how it may be properly used and safeguarded, and its unrivalled utility as an intelligence weapon in the conduct of modern warfare; and finally will come a presentation of the

This being a TOP SECRET lecture, I will begin by reading from a LOW SECRET source which you'll all recognize--TIME magazine, issue of 17 December 1945. I will preface the reading by reminding you that by that date the war was all over--or at least V-E and V-J days had been celebrated some months before. Many of you no doubt remember the loud clamor on the part of certain vociferous members of Congress who had for years been insisting upon learning the reasons why we had been caught by surprise in such a disastrous defeat as the Japanese inflicted upon us at Pearl. This clamor had to be met, for these Congressman

contended that the truth could no longer be hushed up or held back because of an alleged continuing need for military secrecy, because the war was over. There had been investigations--a half dozen or more of them--and now there was to be a grand finale Joint Congressional Investigation which not only would itself bring into the open every detail and exhibit uncovered by its own lengthy hearings but would also disclose to America and to the whole world everything that had been said and shown at all the previous Army and Navy investigations.

There came a day in the Congressional Hearings when the Chief of Staff of the U.S. Army at the time of the Pearl Harbor Attach, 5-star General George C. Marshall, was called to the witness stand. He testified for several long, long days. Toward the end of his ordeal he was questioned about a letter it had been rumored he'd written to Governor Dewey in the Autumn of 1944, during the Presidential Campaign. General Marshall balked. He pleaded long and most earnestly with the Committee not to force him to disclose the letter or its contents, because of necessity for continued secrecy about code matters, but to no avail. He had to bow to the will of the majority of the Committee. I now read:

> "U.S. citizens discovered last week that perhaps their most potent secret weapon of World War II was not radar, not the VT fuse, not the atom bomb, but a harmless little machine which cryptographers painstakingly constructed in a hidden room at Fort Washington. With this machine, built after years of trial and error, of inference and deduction, cryptographers had duplicated the decoding devices used in Tokyo. Testimony

before the Pearl Harbor Committee had already shown that the machine known as 'Magic' was in use long before December 7, 1941, had given ample warning of the Japs' sneak attack if only U.S. brass hats had been smart enough to realize it (TIME - Dec. 1Ø). Now General Marshall continued the story of 'Magic's' magic. It had:

1. "Enabled a relatively small U.S. force to intercept a Jap invasion fleet, win a decisive victory in the Battle of the Coral Sea, thus saving Australia and New Zealand.

2. "Given the U.S. full advance information on the size of the Jap forces advancing on Midway, enabled the Navy to concentrate ships which otherwise might have been 3,ØØØ miles away, thus set up an ambush which proved to be the turning-point victory of the Pacific war.

3. "Directed U.S. submarines unerringly to the sea lanes where Japanese convoys would be passing.

4. "By decoding messages from Japan's Ambassador Oshima in Berlin, often reporting interviews with Hitler, it had given our forces invaluable information on German war plans."

TIME goes on to give more details of that story, to which we shall return.

It is hardly necessary to tell you how carefully Magic was guarded before, during, and after the war. It is still very carefully guarded. Even the fact of its existence was known to only a very few persons at the time of Pearl Harbor--that is an important element in any attempt to explain why we were caught by surprise.

TIME says, in connection with this phase of the story of Magic during World War II:

"So priceless a possession was Magic that the U.S. high command lived in constant fear that the Japs would discover the secret, change their code machinery, (and) force U.S. cryptographers to start all over again."

Now I don't want to seem to over-emphasize the importance of COMINT in the Pearl Harbor affair but I must not fail to tell you that General Chamberlin, who was MacArthur's G-3 throughout the war in the Pacific, has written: "The information G-2 gave G-3 in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." We can't put a dollar-and-cents value on what our possession of COMINT meant in the way of saving lives; but we can make a dollar-and-cents estimate of what COMINT meant by shortening the war by two years. I made a calculation and found that $1.00 spent for COMINT is worth $1,000 spent for other military activities and materials.

In short, when our commanders had COMINT in World War II they were able to put what small forces they had at the right place, at the right time. But when they didn't have it--and this happened, too,--their forces often took a beating.

I hope I've not tried your patience by such a lengthy preface to the real substance of my talk, so let's get down to brass tacks, and since a bit of history is always useful in introducing a subject belonging to a special and not-to-well-known field, I'll begin by giving you some historical information about cryptology, which comprises two related science, namely cryptography, and cryptanalysis. They are but opposite faces of the same very valuable coin; for progress in one inevitably leads to progress in the other.

If time permitted we could go far back into history to see the earliest beginnings of secret communications and this might take us to the very dawn of the art of writing because there is room to wonder which came first, ordinary,

intelligible writing or unintelligible, secret writing. Instances of cipher are found in the Bible, for example, but we must pass over the history of the early days of cryptology with the foregoing single mention. There is, however, one item in that history which is worthy of special notice, the scytale, which is the earliest cipher device history records and which was used by the ancient
(2) Lacedamonians or Greeks for military secrecy. They had a wooden cylinder of specific dimensions, around which they wrapped spirally a piece of parchment; they then wrote the message across the edges of the parchment, unwound it, and sent it to its destination by courier, where the recipient would wind the parchment around an identically-dimensioned cylinder, and thus bring together properly the bits of letters representing the message. And, by the way, the baton which the European field marshal still carries as one of the insignia of his high office derives from this very instrument.

It is well known that Julius Caesar used cryptography--a very simple method--because all he did was to replace each letter by the one that was fourth from it in the alphabet.

The beginnings of modern cryptology can be traced back to the days of the princes and chanceries of the Papal states, beginning even before the year
(4.10) 1300. I show next an alphabet of that period; it is interesting because it shows that even in those early days they already had a recognition of the basic weakness of what we call single or monoalphabetic substitution. Solution of this type of cipher, as you all know, is accomplished by taking advantage of the fact

that the letters of the alphabet in languages are used with greatly differing
4.10 frequencies. This slide shows that the early Italian cryptographers understood this fact and introduced stumbling blocks to solution by having the high-frequency letters represented by more than a single character. I will add that the earliest tract that the world possesses on the subject of cryptography, or for that matter, cryptanalysis, is that which was written in 1474 by a Neapolitan, whose name was Sicco Simonetta. He sets forth the principles and methods of solving ciphers in a very clear and concise form. The first book or extensive treatise
(245.2) on cryptography is that by a German abbot named Trithemius, who wrote his monumental work in 1531. He planned to write four volumes, but he quit with the third because he wrote so obscurely and made such fantastic claims that he got charged with being in league with the Devil. They burned his books, as a
(151) (242) matter of fact. This may be a good place to present a slide which shows that the necessity for secrecy in this business was recognized from the very earliest days of cryptology.

(5) The next slide I show is a picture of what cryptographers usually call the Vigenère Square or Vigenère Table; a set of twenty-six alphabets successively displaced one letter per row, with the plain-text letters at the tops of the square, the key-letters at the side, and the cipher letters inside. The method of using the table is to agree upon a key word, which causes the equivalents of the plain-text letters to change according to the row designated by the key letter. Now, Vigenère also has an interest to the professional cryptologist because although he is commonly credited with having invented that square, he

really didn't and, what's more, never said he did.

The next cryptographer I wish to mention is a Frenchman, Francois Vieta, an eminent mathematician, founder of modern algebra. In 1589 he became Councelor of Parliament at Tours and then Privy Counselor. While in that job he solved a Spanish cipher system using more than 500 characters, so that all the Spanish dispatches falling into French hands were easily read. Phillip II of Spain was so convinced of the safety of his cipher that when he learned that the French were aware of the contents of his letters to the Netherlands, he complained to (5.2) the Pople that the French were using sorcery against him. Here's a slide that shows one of the hundreds of ciphers the Court of Spain was then using. Vieta was called on the carpet and made to explain how he'd solved the ciphers.

I want to jump now to the period of the American Revolution, in U.S. history. The cipher systems used by the Americans and by the British, as well as the code systems, were almost identical! In one case, in fact, they used the same dictionary as a code book!

For additional security conventional words were used to represent the names of persons and places. The British used the following code names:

American Generals - Names of the Apostles: Washington - James
Sullivan - Matthew
etc.

Names of Cities - Philadelphia - Jerusalem
Detroit - Alexandria

Names of Bays & Rivers - Delaware - Red Sea
Susquehanna - Jordan

Indians - Pharisees
Congress - Synagogue

There was an American who seems to have been the Revolution's one-man NSA, for he was the cipher expert to Congress, and, it is claimed, he managed to decipher nearly all, if not all, of the British code messages intercepted by the Americans. Of course, the only way in which enemy messages could be obtained in those days was to seize couriers, knock them out or off, and take the messages from them. Rough stuff compared to getting the material by radio intercept.

(6.2/1) The next chart shows a picture of a code or "syllabary", as we call it, used by Thomas Jefferson. This syllabary is constructed on the so-called two-part principle. This is a portion of the decoding section. You will note that the numerical groups are in consecutive order but their meanings are in no alphabetical order at all, which means that you have to have another section, the encoding section, in which the words are in alphabetical order, and their equivalents are in random order. This sort of system even today is in extensive use. Jefferson was an all-round genius, and I shall have something to say about him and cryptography a little bit later.

I'm sure you've learned as school children all about Benedict Arnold when he was the Commanding General of the American Forces at West Point; but you probably don't know that practically all his exchanges of communications with Sir Henry Clinton, Commander of the British Forces in America, were in cipher, or in invisible inks. Here's an interesting slide showing one of Arnold's cipher

6.4 messages, in which he offers to give up West

6.5 Point for 120,000. Here's another one in which he gave the British information

6.6 which might have led to the capture of his commander-in-chief, General Washington--but Washington was too smart to be ambushed--he went by a route other than the one he said he'd take.

I think you'll be interested to hear a bit more about that one-man NSA I mentioned a couple of moments ago. His name was James Lovell and besides being a self-trained cryptologist he was also a member of the Continental Congress. There's on record a very interesting letter which he wrote to General Nathaniel Greene, with a copy to General Washington. Here it is.

Philadelphia, Sept. 21, 1780

Sir:

You once sent some papers to Congress which no one about you could decipher. Should such be the case with some you have lately forwarded I presume that the result of my pains, herewith sent, will be useful to you. I took the papers out of Congress, and I do not think it necessary to let it be known here what my success has been in the attempt. For it appears to me that the Enemy make only such changes in their Cypher when they meet with misfortune, [illegible] and therefore if no talk of Discovery is made by me here or by your Family you may be in chance to draw Benefit this campaign from my last Night's watching.

I am Sir with much respect,

Your Friend,

JAMES LOVELL

In telling you about Lovell I should add to my account of that interesting era in cryptologic history an episode I learned about only recently. When a certain message of the revolutionists came into Clinton's possession he sent

it off post haste to London for solution. But, of course, Clinton knew it was going to take a lot of time for the message to get to London, be solved and returned to America--and he couldn't afford to wait that long. Now it happened that in his command there were a couple of officers who fancied themselves cryptologists and they undertook to solve the message, a copy of which had been made before sending the original off to London. Well, they gave Sir Henry their solution and he acted upon it. The operation turned out to be a dismal failure, because the solution Clinton acted upon was all wrong! The record doesn't say what Clinton did to the two amateur cryptologists when the correct solution arrived from London weeks later. By the way, you may be interested in learning that the British have operated a cryptanalytic bureau ever since the year 1540, save for a few years about 1850 to 1914.

There's also an episode I learned about only very recently, which is so amusing I ought to share it with you. It seems that a certain British secret agent in America was sent a message in plain English giving him instructions. But the poor fellow was illiterate and had to call upon the good offices of a friend to read it to him. What he didn't know, however, was that his friend was one of General Washington's secret agents!

If interest in cryptology in America wasn't very great, if it existed at all after the Revolution, this was not the case in Europe. Books on the subject were written and studied. Here's a picture of the frontispiece to a book in French published in 1796, dealing with espionage and counter-espionage; it has a section dealing with cryptology.

I had intended to say a few words about the decipherment of Egyptian hieroglyphic writing because it is supposed to represent the next and a great landmark in the history of cryptology. Professor Norbert Wiener, of M.I.T., in his famous book entitled Cybernetics calls that decipherment the greatest feat in the history of cryptology, but the good professor is wrong. The cryptanalysis was rather simple; the difficult part was the reconstruction of the language and its grammar. I'm sorry we can't go into that now, but I do want to add that it was very fortunate that the early students of Egyptology didn't even suspect that the Egyptians also used cryptography: there were cryptographic hieroglyphics, if you can imagine such things.

There is one person I should mention before coming to the period of our Civil War. Edgar Allan Poe, in 1842 or thereabouts, kindled an interest in cryptography by his famous story of "The Gold Bug", and by some articles on cryptography in newspapers and journals of the period. For his day he was perhaps the best informed person in the U.S. on cryptologic matters.

The period of the Civil War or the "War Between the States", in U.S. history was, as a result of the invention and development of telegraphy, a period that saw the use of cryptology in a large way. Here is a picture of a Confederate cipher device, captured at Vicksburg. The device is a cylinder of wood, covered with a sheet of paper bearing alphabets, the alphabets of the Vigenère table, in other words. Here is a pointer that you could slide, and a knob with which you could turn the cylinder according to the key letters. You might like to know two of the keys

they used with this system and device: COMPLETE VICTORY was the first; and COME RETRIBUTION the second.

8 Here is a picture of a message, authentic without question, which was sent by President Lincoln to General Burnside. It's very simple. It reads this way, of course, and makes no sense; but if you read it backwards it makes excellent sense: "If I should be in a boat off Aquia Creek at dark tomorrow, Wednesday evening, could you without inconvenience meet me and pass an hour or two with me? (Signed) A. Lincoln." I think the President was kidding a bit, but he may have lacked confidence in the official cryptosystems in the same way that President Wilson lacked confidence in the codes of the State Department, as can be seen in the slides which I now show.

152, 152.1 152.2

9 This is a photograph of a page or two from the code book and cipher system used by the Federal Army. They had what we call "route ciphers", that is, they used a matrix with indications of the route to be followed in inscribing and transcribing the words of the message. Here's how you write the message in: the first word, second, third, fourth, fifth, sixth and so forth; then you take them out according to another route. And here the thing is complicated by the use of arbitrary equivalents for the names of important people.

"President of the U.S." is represented by "Adam" or "Asia". It had two equivalents, you see. Here are some of the names of famous or well-known officers of that period. I have with me today the complete set of cipher books used by the Federal Army during that period. The next slide is a picture of a message sent to General Grant in one of those route ciphers. I shall not take time to read it.

After the Civil War, or War Between the States, the use of cryptography in United States military affairs went into a decline, because there was a long period of peace, broken only briefly by the Spanish-American War. In 1885 the War Department published a code called "Code to Insure Secrecy of Telegrams". It is a cryptographic curiosity and no tribute to the imagination of the officer who was responsible for its production, because he copied almost word for word the title page, the instructions for use, and the arrangement of contents from

a commercial code a picture of which I show in this slide in which pages of

215 both codes are placed side by side for your inspection. But good old Lieut.

Colonel Gregory did have a little spark of imagination. See what he changed

(here point out the minor differences). But believe it or not this was the

code that the Army used during the Spanish-American War and in the copy in

my collection, on the inside of the front cover, there appears the additive

that was used: 777. I have that copy among my exhibits here. ~~[illegible]~~

There was little use for sound cryptosystems then because radio was just in

its infancy during that war and there wasn't much danger from interception of

messages.

(The Navy Code in the Spanish American war--if there's time.)

In 1899 the Chief Signal Officer undertook the preparation of a suitable

code. Economy was stressed--the Chief Signal Officer personally did all the

work--and in 1902 the "Cipher of the War Department" was published by the

Adjutant General. In 1906 a revision of that book was published, and in 1915

a completely new code, the War Department Telegraph Code, was published. But,

believe it or not, that code was printed by a commercial printer ~~house~~ in Cleveland!

At least that is what my predecessor in the Office of the Chief Signal Officer

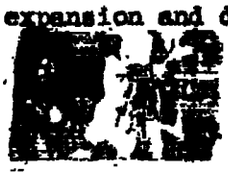
told me when I took over from him in January 1921, after my World War I service

in France.

When World War I came in August 1914 cryptology entered upon a new and

rapid expansion in invention and development, and we must now turn our attention

to the principal events in that expansion and development. With Hertz's



discovery of the so-called Hertzian waves, and Marconi's practical demonstration of signalling by wireless, a new era in military communications was ushered in, and this, of course, was what brought about renewed interest and a new era in cryptology. The first military usage of wireless, or radio, as it soon came to be called in American terminology, was made in Europe before 1915 but wide usage of it was in World War I. Developments in cryptography lagged a bit, as we shall see.

Before coming to these developments a few words should be said about the U.S. position vis a vis the Allies and the Central Powers. Some of you well remember how President Wilson strove and promised to keep the U.S. out of the war, how at one time during a period of strained relations with both sides he'd declared that he'd never send our boys to war and that there was such a thing as being too proud to fight. U.S. sympathies for the most part were with the Allies, especially the British, but there were in the U.S. hundreds of thousands of German-Americans and German sympathizers, and all of them exercised an important role in helping to prevent our entry into the war on either side, least of all on the side of the Allies. The British tried their best not to provoke or irritate the U.S. but even so there were times when British high-handed action almost precipitated us into the war against them. There were some activities toward preparedness and national defense in case circumstances made our entry into the war unavoidable, but these activities weren't of much account. In the cryptologic field, for example, nothing was being done by either the Army or the Navy. Two Army officers became interested in the subject and I show you the title page of the first U.S. manual on military ciphers, by the

212

then Captain Parker Hitt, ~~and the title page of a small brochure by the then~~ ~~Lieut. J. O. Mauborgne.~~ But ~~these were~~ THIS WAS almost A private ventures; officially, as regards cryptographic preparations, no new codes were in preparation in either Service; no new ciphers were being dreamed up; no cipher devices or cipher machines were being investigated or invented. As for cryptanalytic operations--well, there just were none whatever in either Service, and, for that matter, in the whole government. A private research institution near Chicago, the Riverbank Laboratories, of which I happened to be a member, working in a totally different field of science, began studying cryptology and soon certain members of the staff were working on messages which were furnished us by various government departments and agencies in Washington. Most of these were solved and returned to Washington, and the staff became more and more adept. But, mind you, this was not even a quasi-governmental agency; it was operated as a patriotic gesture and at his own expense by the man who, in 1915-16, as an astute and wealthy business-man, Colonel George Fabyan, foresaw the inevitable entry of the U.S. into the war, wholly unprepared for any cryptologic work. The Colonel was right, for on 6 April 1917 the U.S., almost suddenly it seemed, declared war on Germany. How did this come about? It came about when it did as a result of a nice piece of cryptanalytic work by British cryptanalytic experts in London on a message now world-famous as the Zimmermann Telegram. The message first came from the German Foreign Minister in Berlin, Arthur Zimmermann, to the German Ambassador in Washington, Count von Bernstorff; it was 28 then sent on to the German Minister in Mexico City. Here's the message in the

form in which it was transmitted to Mexico. I won't go into the story about how the British solved it, for this was dramatic and complex, because it involved the reconstruction of two rather large codes. The solution represented a
28.1 Here's a picture of the young British Naval Reservist who gets most credit--Ensign DeGrey.
first-class piece of work. / But I do want to add a few words about the political effects of the solution, and about British cleverness in the handling of the case because it gives a good illustration of how astute, diplomatically, they are. As I have already said, it resulted in bringing us into the war on their side.

29 Here is the translation of the Z. T. It was important because the message said the Germans were going to resume unrestricted submarine warfare and this part, here, dealing with a proposal to be made to Mexico, was the straw that broke the camel's back. People in the Middle West had been very lukewarm toward the idea of our getting into the War---on either side--but when the Germans began talking about returning Texas, New Mexico and Arizona to Mexico, that was something else again. So, we got into the war within a couple of weeks after the British gave us and we had established the authenticity of the translation of the Zimmermann Telegram. A year or so ago the telegram and episode was the subject of one of the series of Walter Cronkhite's "You Are There" television programs. And a book of almost 25# pages, dealing only with that telegram and episode, was published just about six weeks ago. I brought a copy with me.

Well, as I said a few minutes ago, on 6 April 1917 we were in the war as belligerents and things began popping, especially in my own little world at Riverbank Laboratories. We began training more people and doing more solution work--all paid for by Colonel Fabyan. We had messages to solve that dealt with

our neighbor on our southern border as well as messages that dealt with the activities of enemy agents.

There was one rather interesting case, in which I happened to play a minor role. In 1916-17 the Germans financed a large number of Hindus in their attempts to stir up a rebellion in India, the idea being to cause so much trouble in India that the British would be forced to withdraw troops from the Western Front to quell disturbances in India. These Hindus were negotiating for the purchase of arms and ammunition in the United States, with the idea of sending them over to India. Since the U.S. was neutral, it was against our own laws to permit such undertakings against a friendly nation. So the business had to be conducted secretly and that is how cryptograms entered into the picture.

33 Here is one page of a long, seven or eight-page letter that was intercepted between the top Hindu agent in the United States and his chief in Switzerland. The letter consisted of groups of figures, in which were interspersed some plain-text words. We recognized pretty quickly that the letters of the secret text had been replaced by numbers which indicated specific letters in some ordinary book which could be carried by an agent without arousing suspicion. Each group of numbers represented the page number, the line number, and the position number in the line of that key book. All we needed was the book, but unfortunately the Hindu failed to tell in his letter was the book was, so we had to go ahead and try to solve the message without it. It was solved, but there isn't time to tell you how it was done except to say that by working back and forth between the message and the hypothetical keybook, building up the various words on various

pages of the book, then building up the words of the message--one helped the other--I finally got certain clues as to the sort of book involved--that it was a book dealing with the history of German political philosophy, economy, or history. I hunted and hunted for that book, and finally found it, all right. It was Price Collier's Germany and the Germans. This message figured in a long-drawn out trial in San Francisco, where there were about a hundred Hindus on trial simultaneously. They were searched every day before they came into court, but one day, the day after I testified, one Hindu managed to secrete a gun in his clothes and in the midst of the court proceedings shot a Hindu who had turned State's evidence, whereupon the United States marshall, a great big fellow, six feet four, standing in the back of the court, drew his weapon and shot the first Hindu dead. They were both dead right there, within two or three seconds. That's the way that trial ended up, rather dramatically, I'd say

To go back to the work at the Riverbank Laboratories, the Adjutant General began sending us officers for training.

82 Here's a picture of one class, the biggest and the last one I directed before being commissioned and going directly to France, for service at GHQ, working

That picture spells out a message in cipher: KNOWLEDGE IS POWER.
on German codes and ciphers. /And now for a quick-look at the sort of things I found at GHQ when I got there and was assigned to work.

Let's first take a look at and discuss the use of cipher systems by the

various belligerents, because these were used for tactical purposes in preference
11 to codes and code systems, which came as a later development. Here's a picture of the cipher system used and misused by the Russians. You will note that it is based upon the old Vigenere principle, using numbers instead of letters. It represents a case involving only a set of 7 or 8 alphabets used repetitively, by a key number, for substitution. This was the deciphering table. Russian ineptitude in communications, and especially in cryptography, cost them dearly; because of it they lost the Battle of Tannenberg, which greatly contributed to their being
12 knocked out of the war. The next slide is a picture of a tactical cipher system used by the French. It was a transposition system, the columns being here transcribed according to the columnar key; in addition, certain disturbing elements came into the method by taking off the letters in diagonals. And here
13 is a picture of the system used by the Italian Army in World War I. Again, it is only a variation of the old Vigenere system. Here is a system used by the Germans beginning in the latter part of 1917. It was invented by them, or, I should say, they invented a clever combination of two methods. We called it the
14 ADFGVX cipher because the cipher text consisted exclusively of those letters. An alphabet in here, arranged according to some pre-arranged plan, with the coordinates AHFGVX; the letters of the message were replaced by pairs of coordinates; for example, the letter R is represented by AG, and so forth. The whole message is written out in the letters ADFGVX in a transposition diagram at the top of which is a key, developed from a key word; the letters are then taken out of the diagram

in columnar fashion, according to the key order. That system was a brand new thing in military cryptography and caused no end of headaches for the Allied cryptanalysts until it was discovered just how a solution could be achieved. The solution was not a general one but depended upon special cases; however, these happened so often that we could bank on them occurring practically every day. The ADFGVX system was used by the German high command and it wasn't long before it was discovered that if you made a study of just the number and direction of ADFGVX messages you could infer certain things about the tactical situation and, more important, you could, with some degree of assurance, predict what might happen
15 in three or four days at a certain sector of the front. Here is an example of a chart based upon the ADFGVX intercepts. This, gentlemen, is the first illustration that I know of in history of one of the basic principles of what we call traffic
14.1 analysis and traffic intelligence. (Explain chart.) The next slide gives a picture of the sort of "Bulletins", as we called them, that we put out when the ADFGVX messages were read.

For tactical messages the British and Americans in World War I used a method known as the Playfair Cipher, allegedly invented by Lord Playfair, but he didn't invent it--Sir Charles Wheatstone invented it.

THE
23 A method of Playfair encipherment is to have a square 5 x 5, or 25 cells in all, in which you start in with a key word, then follow with the rest of the unused letters of the alphabet. (I and J are treated as the same letter). If you want to encipher "AT" the equivalent is "VR", by diagonals, and so on. Here is an example of how a message is enciphered. In those days, 1914, that was regarded as pretty hot stuff. In fact, an officer of the American Army / Lieut. Mauborgne, whom I've already mentioned and who later became Chief Signal Officer, wrote a little
213 treatise, published in 1914, in which he dealt with this Playfair cipher system. The title of his work is "An Advanced Problem in Cryptography". Today, our most elementary students are given things of that sort to solve after a few lessons.

The British Army developed a cipher device in World War I. They had manufactured a great many of them, thousands in fact, and they proposed to the French and the Americans that all the Allies should use it for tactical communications; but to the chagrin of the British it was never put to use, for reasons that I may tell you later.

So much for the ciphers and cipher systems used in World War I. Now, I'd like to say a few words about the codes and code systems. A code is simply a sort of dictionary in which the words, phrases and sentences are
Ko representable by arbitrary groups of letters or figures. Here is a page from a commercial communication company's codebook, which they offer to their customers for economy. You'll notice that each of these code groups differs from every other code group by at least two letters. We call that "the

two-letter differential." The reason for having such a differential is that errors are sometimes made in transmission, but the likelihood of making two errors in the same group is not nearly as great as making a single error. The 2-letter differential affords methods of readily correcting a group if it has a single error in it; with a bit more trouble 2-letter errors can also be corrected. Now, code books and codes are compiled to be suited to general or to specific kinds of business. If generalized, as in a general trade or shipping code, or a code for the automotive industry, and so on, they get wide distribution by purchase. But codes may also be highly specialized in character, as in the case of the one I show in the next slide.

18 You know, there are certain people who believe firmly and implicitly in the power of healing by suggestion, and here is a picture of a code book put out by a practioner in that field, a code that is in English and French. It's clear that the purpose of it is to be able to receive treatment by your practitioner no matter where you are or he is. Thus, if you should go away on a trip and want to consult your practitioner, you can send him a message and tell him what you are suffering from, or, rather, what you think you are suffering from. You would simply represent your illness, or alleged illness, by the code group corresponding to your malaise. Now, note that the professional who got up this code was pretty well versed in the intricacies of code and communication difficulties, because these code groups differ by at least <u>three</u> letters. The reason for this extra precaution is, of course, clear: It would be a

pretty serious thing if you sent a message telling him that you think you are suffering from coma, but/the code group/ having been garbled in transmission, because is wrong, he unfortunately gives you the treatment for convulsions. That would be pretty tough!

Prior to World War I the use of code books for tactical purposes was thought to be impracticable, largely because of the difficulties of compiling, reproducing, distributing and protecting the books. I don't think they thought too much about the possibilities of solving code. Early in 1916 the Germans began to use small field codes, and the Allies soon followed suit. I had some slides to show you pictures of pages of the code books of the various belligerents, but I will omit them and say that I also have brought exhibits of such books as were actually used for the purpose. Those who would like to see what they were like are welcome to come up after this talk and examine them. The only slide that I will show is one that will give you a picture of the American Army's unpreparedness in World War I for code communication. This is authentic--I didn't make it up--because I found it in the records when I closed our office in the AEF in April 1919. It's a code gotten out by the 52nd Infantry Brigade, dated 17 April 1918, and it is what we may call "the baseball code". If you wanted to say "killed", you said "struck out";"wounded" was represented by "hit by pitched ball", and so forth--very elementary.

21

[redacted]

[redacted]

In all I've said thus far about our World War I crypto-communications there's been little or nothing said about our high-command ones, messages between General Pershing and Washington, for instance. I did mention the War Department Telegraph Code of 1915, which we had when we entered the war as a belligerent. It is with some sadness but also some amusement that I tell you that soon after we joined the British they told us, with as much delicacy as you may imagine the situation required, that that code wasn't at all safe. You don't have to wonder very much what the implications of such a notice meant, and I'm sure our authorities manifested no great astonishment at the time. You'll remember what I said about the British success in solving the Zimmermann Telegram which brought us into the war on their side.

Well, steps were taken right quickly to produce a new and much safer code for the War Department and high command use; also a new one for military intelligence and secret agent communications. It was also about this time that our Navy began to improve its communication secrecy by adopting a cipher which went under the curious and almost movie-like title of the NCB--the Navy Cipher Box. It was a sort of strip cipher system and I have a picture of it.

219

I don't know what our State Department communication security was like in those days but I have my suspicions. The long tradition of secrecy and secret diplomacy wasn't our tradition--this was distinctly a European piece of skullduggery and we had and wanted to have no part in it. Maybe we were

taken for a cryptologic ride--I don't know. That would be something for some cryptologically-minded historian to look into--[redacted]

[redacted]

And here is a good point at which to bring to a close this first period. We'll continue with a bit more history in the next period but it will be devoted to watching the developments in a direction opened up by inventions made about the time of World War I.

SLIDES FOR SECOND PERIOD

PAGE	SLIDE NO.	TITLE
6	229	Marshall-Dewey
8	255	RFP
	254	Morse Op.
11	234	Chart showing bulletin production, average daily volume of daily messages 1 Dec 1941-31 Aug 1945
	235	Chart showing progress of a message.
12	245	Trithemius
13	6.1#	Dlandol
16	139	Analog deciphering machine
	145	Another deciphering machine
	137	Brute Force
17	138	Slide Run Unit
	141	Section of Wing of IBM, Arlington Hall, 1945
	15#	Purple
	15#.5	Purple dudbuster
17-A	I-1	Antenna field at Hof, Germany
	I-2	Intercept position
	I-3	Intercept position
18	X-1	ABNER
	X-2	ALWAC
	X-3	ATLAS
	X-4	ATLAS & BOGART
	X-5	BOGART
	X-6	DUCHESS
	X-9	SOLO
	X-1#	IBM 7#4

The title of this period of my talk, might well be "The Influence of C-Power on History", and lest some of you jump to the conclusion that I've suddenly gone psychotic and am suffering from a delusion that I'm a reincarnation of the great Admiral Mahan, I hasten to explain that the "C" in such a title for my talk is not the word "SEA" but the letter "C" and it stands for the word CRYPTOLOGIC. The full title of the talk would therefore be: "The Influence of Cryptologic Power on History." As a sub-title I would offer this: "Or how to win battles and campaigns and go down in history as a great tactician, strategist and leader of men; or, on the other hand, how to lose battles and campaigns and go down in history as an incompetent commander, a military 'no-good-nik'."

At this point let me hasten to deny that I'm casting any reflections upon certain successful--spectacularly successful commanders; names will occur to you without my calling them to your attention--and there will be names of men in each of the two categories--"how to win" and "how to lose" battles and campaigns--and entire wars, for that matter.

In his recent book Eisenhower: Captive Hero (Harcourt, Brace & Co., New York, 1958, p. 55) Marquis Childs says:

> "Any examination of the relationship between Eisenhower and Marshall is handicapped by the fact that Marshall has never told his own story. Repeated efforts have been made to persuade him to write his account of the great events in which he played such a decisive part. He has replied

more often than not that no honest history of any war has ever been written, and since he would not write unless he could tell the truth he meant to keep silent."

Could it be that among other reasons why General Marshall held the belief that "no honest history of any war has ever been written" he felt that if the COMINT facts were included in the history the laurels of commanders of the winning side mightn't look so shiny as they generally appear? I am here reminded of a story that came to me from a pretty reliable source a couple of years ago about a military figure much in the current news. I think the story quite apropos in connection with what I've just said.

(Story about General Montgomery if there's time.)

Sometimes the course of history is materially changed by the amount and quality of the COMINT and COMSEC available to field commanders and also how well they use these offensive and defensive weapons. Sometimes it is materially changed by the absence of COMINT and COMSEC where it had previously been in existence and used. We have already noted incidents of the first type, those in which lots of first-class COMINT was available, including the COMINT available before the attack on Pearl Harbor. We may now take note of an incident of the second type, one in which the consequences of a lack of COMINT plays the most prominent role.

I have reference here to the Battle of the Bulge, wherein a serious catastrophe was barely averted because our G-2's had come to rely too heavily

on COMINT, so that when it was unavailable they seemed to lack all information or at least they felt that way. I said that a serious catastrophe was barely averted but even so the losses were quite severe, as can be seen from the following:

"According to Eisenhower's personnel officer, American losses in the Battle of the Bulge totalled 75,890 men, of whom 8,607 were killed, 47,139 wounded, and 21,144 missing. Over 8,000 of these casualties were in the 106th Division. Because of heavy German attacks, 733 tanks and tank destroyers were lost. Two divisions, the 28th and 106th, were nearly completely annihilated, although the 28th Division did subsequently enter combat after being rebuilt."[1]

---

[1]Robert E. Merriam, Dark December, 1947, p. 211.

What happened? Why?

In an article which is entitled "Battlefield Intelligence: The Battle of the Bulge as a Case History", and which was published in the February 1953 issue of Combat Forces Journal, Hanson Baldwin said:

"Intelligence deficiencies and an astigmatic concentration upon our own plans with an almost contemptuous indifference for the enemy's, set the stage in December, 1944 for the German successes in the Battle of the Bulge--a case history in the 'dos and don'ts' of intelligence."

Further on Baldwin notes that:

"In General Sibert's words, 'we may have put too much reliance on certain technical types of intelligence, such as signal intelligence ... and we had too little faith in the benefits of aggressive and unremitting patrolling by combat troops ... . Dependence upon 'Magic', or signal intercepts, was major, particularly at higher echelons; when the Germans maintained radio silence, our sources of information were about halved."

In what I read from TIME in the first period, the word "MAGIC" seemed to refer only to the machine that we reconstructed for solving Japanese Foreign Office communications. In reality the word MAGIC was used as a sort of code name among the initiated and indoctrinated persons who were entitled to receive the highly secret information that came from the solution of German, Italian, and Japanese secret communications. The term was introduced to us by the British when we began to play together in the cryptologic gardens; we found it useful and adopted it, too. Later on we came to use other secret words to designate this sort of intelligence and to change the words from time to time, for security reasons. Currently, COMINT is composed of three types or categories of intelligence, and by far the greatest part of it comes from intercepting, recording, and studying enemy radio traffic. The three types or categories are:
(1) Special intelligence, which comes from the solution and processing of the encrypted messages themselves and the result is information of highest reliability because it comes, so to speak, "right out of the horse's mouth". (2) Traffic intelligence, which comes from the study of what are called "the externals" of

those messages, data applicable to such things as their callsigns, the frequencies employed, the direction or routings, and so on and from this comes information from which inferences can be drawn; and (3) Weather intelligence, which comes from the study of the enemy's weather messages, which in wartime and even in peacetime to a certain degree, are encrypted. In this audience it's hardly necessary to mention how important a role the weather plays in the conduct of war. Recently NSA has also been assigned over-all responsibility for ELINT, or electronic intelligence, but I won't go into that in this talk.

There is hardly need for me to give you a definition of COMINT, but perhaps I should cite its three principal objectives. First, to provide authentic information for policy makers, to apprise them of the realities of the international situation, of the war making capabilities and vulnerabilities of foreign countries, and of the intentions of those countries with respect to war. Second, to eliminate the element of surprise from an act of aggression by another country. Third, to provide unique information essential to the successful prosecution, and vital to a shortening of, the period of hostilities.

It was in response to this third and last objective of COMINT that World War II gave a brilliant answer. I'm sure you would find the detailed story of the successes of Navy, Army, and Army Air Corps cryptanalysts, and of their opposite numbers in the British Services on German, Italian and Japanese messages in World War II highly interesting but there just isn't time. I think the contents of the Marshall-Dewey letter, from which I read a bit in the

first period, will have to suffice. However, it in itself is sufficient to give you a pretty good idea of the contributions COMINT made toward our winning World War II. It is unfortunate that General Marshall's letter was disclosed during the Congressional Hearings for it's now in the public domain and its contents are undoubtedly now known in all the important chanceries and war offices of the world. General Marshall, you'll remember, in his letter to Governor Dewey, sent during the hot political campaign of 1944, was asking the Governor not to use certain information Dewey got by surreptitious channels. Here are some excellent illustrations of the manner of employment of COMINT:

229

"Now the point to the present dilemma is that we have gone ahead with this business of deciphering their codes until we possess other codes, German as well as Japanese, but our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government. These are still in the codes involved in the Pearl Harbor events.

"To explain further the critical nature of this set-up which would be wiped out almost in an instant if the least suspicion were aroused regarding it, the Battle of the 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 on our limited forces to meet their advances on Midway when otherwise we almost certainly

would have been some 3,000 miles out of place.

"We had full information of the strength of their forces in that advance and also of the smaller force directed against the Aleutians which finally landed troops on Attu and Kiska.

"Operations in the Pacific are largely guided by the information we obtain of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them, and what is of vast importance, we check their fleet movements and the movements of their convoys.

"The heavy losses reported from time to time which they sustain by reason of our submarine action largely results from the fact that we know the sailing dates and the routes of their convoys and can notify our submarines to lie in wait at the proper point.

"The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based in timing on the known movements of Japanese convoys, two of which were caught, as anticipated, in his destructive attacks.

* * * * * * * * * * *

"The conduct of General Eisenhower's campaign and of all operations in the Pacific are closely related in conception and timing to the information we secretly obtain through these intercepted codes. They contribute greatly to the victory and tremendously to the savings of

American lives, both in the conduct of current operations and in looking toward the early termination of the war."

It will be helpful to list in sequence the steps involved in the production of COMINT. First, of course, there comes the intercept--you've got to have the traffic and getting it is no small trick. Modern electrical high-speed communication systems used by all large governments require high-speed intercept operations, and together with the intercept there must be direction finding, when you are working on the mobile communications of enemy or foreign armed forces. The Russians, for example, have complex callsign systems, complicated by shifting of frequencies, so that it is important to be able to identify transmissions either by direction finding or by one of two other
255 types of operations. One is called radio fingerprinting, which takes advantage of the fact that every transmitter emits electro-magnetic radiations characteristic of that transmitter and it is possible therefore to identify a transmitter by studying the characteristics of its emanations. When the headquarters served by this transmitter and the transmitting station moves, the move can be followed by means of the transmitter's "fingerprint", so to speak. It is also
254 possible to identify operators of Morse telegraph communications. That is, every operator has characteristics of his own, and you can by studying their transmissions identify them wherever or whenever they move. This is very useful. Much work remains to be done in direction finding, in radio fingerprinting and in Morse operator identification.

The interception of the traffic is not only a complicated but also a very expensive enterprise, costly in numbers of personnel and equipment. If there were time I'd show a few slides of typical intercept stations and intercept positions. You surely must realize that the business of intercepting a message while similar to is hardly identical with that of receiving a message when the receiver is a legitimate member of the radio net. The intercept operator can hardly break in and say: "Hey, bud, I didn't get that last group. Repeat it, please". The detection and copying or recording the intercepted enemy traffic passed over modern high-speed communications systems is a very complicated but important step--and getting the intercept copy back to where it can be worked on, that is, getting it there in good time, is also complicated and highly important. Much of the traffic has to be forwarded electrically to be of anything more than historical interest, and this requires the Armed Forces to allocate to NSA special communication channels and facilities solely for NSA's own and sole use. NSA is the largest user of electrical communications in the world; its communications center at Fort Meade handles two million groups a day; it is the largest center in the world. It is fairly obvious that it's our communications peoples' job to get the traffic to the desks of the traffic analysts and the cryptanalysts as fast as possible and as accurately as possible.

Looked at from a purely philosophical or logical point of view, COMINT operations and activities should be, and in the U.S. Navy they are, conducted within Naval Communication commands and by Naval Communications personnel. I think this is logical because they are certainly the same generically as those

as those conducted by any large organization for providing communications systems, that is, systems and means for getting messages from certain people to certain other people--we call them originators and addressees. The only and the principal difference between this ordinary type of communications and what goes on in the production of COMINT is that we interpose ourselves between the actual originators and intended addressees of the messages, that is, without their permission and often without even their knowledge we put ourselves on their distribution list. Of course, we're not furnished the keys and crypto-materiel that the intended addressees are provided with to make unbuttoning the messages a direct and easy process; we have to find or work out the keys, and this is often very difficult but it has been done in the past and will probably be done again in future wars. Lastly, there's the job of translating the messages--this usually involves making the necessary corrections and explanatory notes, sometimes. There is an important corollary to what I'm saying here and it is that the real key to success in the production of COMINT is excellence in our own communication systems. Unless we can get the traffic quickly and accurately back to where it can be worked on by the analysts and unless we have rapid and secure communications among the various analytical stations and also to those authorized to receive the final COMINT, you're conducting a mere exercise, not a real operation.

The next step after interception is traffic analysis, that is, the reconstruction of the radio nets of the enemy and the location of their transmitter stations. This gives very important information on two counts. First of all, establishing or reconstructing the nets gives you order of

battle, which is very important. The reconstruction of the radio networks is not an easy thing when the callsigns and frequencies are changed rapidly. It is a curious thing that all through World War II the Germans seemed to be able to change their callsigns and frequencies without too much trouble--it gave us and the British a good deal of trouble and we had to keep a good many people working at it all the time.

The second good reason for engaging in traffic analysis is that every once in a while your cryptanalysis meets a roadblock and you don't have any COMINT, in which case the only thing you have to fall back upon are non-COMINT sources of information, but you still can get good information from traffic analysis from simply watching the ebb and flow of traffic, changes in routings, etc., from which you can make inferences of what is happening or going to happen. Now these, mind you, are inferences--they are not right out of the horses mouth as decrypts are.

The next step, of course, is cryptanalysis, to which I'll return in a few moments, after I've outlined briefly the succeeding steps in COMINT production. It is obvious that the decrypts, if they are in foreign language, have to be translated into good English and with the translation there is always a certain amount of emendation, because of errors in transmission or in reception, and errors by cipher clerks and so on. You must bear in mind that all this business is conducted as a very large-scale production or exploitation operation. You are not dealing with single or just a few messages a day--there are thousands of them. I'll show you by a

734
735

graph [redacted] what this means.

The next step is the evaluation of the information and mind you, I've been talking about the COMINT product as information. This is something which the intelligence people are most insistent about, saying that it's their job to evaluate the COMINT and to collate and check it with information from other sources. And I suppose that this is a very necessary thing. It is conceivable that an astute enemy might actually mislead you by sending out a phoney or two, in which case the intelligence people should be able to detect the spurious message by collating what it says with what there is from other sources.

And then there comes finally the dissemination of the COMINT product and this has to be very, very carefully controlled. For this purpose there are special crypto-systems and special security officers, and the decrypts are kept out of the normal communication or message centers, so as to keep the number of persons seeing them to an absolute minimum. All of them have to have a special clearance; they take special baths on signing on and off.

Now I will go back to COMINT processing and give you some information about cryptanalytic techniques and gadgetry. I venture to say that you all know the mental picture the average citizen has of a cryptanalyst, for the picture is a very old one, like the one I now show you, of Trithemius, whom I mentioned before. He's a long-haired egg-head; he wears thick spectacles, has long whiskers, with crumbs in them, he has grimy fingers and finger nails, and so on. This chap goes into a huddle all by and with himself and the cryptogram and sooner or later

245

he comes up with the answer, shouting Eureka! Or, as a development the smart
6.1Ø cryptanalyst gets himself an assistant, or clerk, or a secretary, as shown in this slide. Well, that picture or the preceding one is far from the truth these days, for cryptanalysis and COMINT is "big business" now--very big business indeed, because we're spending well over half a billion dollars on it every year now.

Cryptanalysis of modern crypto-systems has been facilitated, if not made possible, by the use and application of special cryptanalytic aids, including the use of high speed electronic machinery and digital computers, some of which I'll show in slides to come. Some are standard machines, but mostly we devise and use modifications of them. More importantly, we have recently gone into the invention, development, and production of highly specialized electronic cryptanalytic gadgetry. At this point I must take a few moments to clarify the picture and in simple language tell you what gadgets do for us. As I said before, the mere number of permutations and combinations afforded by a cryptosystem per se isn't too significant; it's what they amount to or involve in terms of cryptographic meaningfulness and complexity. In modern cryptanalytic attacks on the crypto-communications of knowledgeable governments what you are up against are usually quite complex cryptosystems which generally involve, for their solution, the making of a great multiplicity of hypotheses each of which must be tested out, one after the other, until you find the correct one. The job of the cryptanalyst is to devise short cuts for testing the hypotheses, short cuts often based upon the use of statistics and statistical theories having to do with the relative

frequency of letters, pairs or sets of letters, words, sets of words, and so on. Once having devised the proper test or tests for each hypothesis, or for several concurrent hypotheses, human labor could be set to work making the millions of tests in order to find the correct hypothesis or to cast out the vast majority of incorrect ones. When each test is complicated, or lengthy, it is obvious that you'd have to have, as we used to say, factorial n Chinamen to do the job, or else the job would take eons of time. But it is our experience that every test which can be made by hand can be mechanized, and it is further our experience that in most cases it is practicable to build machines which will make the tests. I don't have to tell you that machines don't tire as rapidly as humans, they don't need much sleep, or time out for meals, or for recreation or for such things as shopping, love-making, etc.-- in short, the "care and feeding of machines" is a relatively much more simple matter than the "care and feeding of human beings." So, we have cryptanalysts who devise the tests; then we have cryptanalytic engineers who mechanize the tests, then devise, invent, develop, and produce the machines to perform the tests at high speed. We have to have maintenance engineers to keep the machines in good working order; and the cryptanalytic assistants who examine the output of the machines and who are usually able to take the correct hypothesis or few correct ones and go on with them to the final stage where a key is recovered. Next we may have to have other machines which apply the recovered keys to specific messages and produce the plain texts from them. But in all

these steps, let me emphasize, the machines can do only one thing: they can only perform, at a high rate of speed, processes which the human brain and hand can perform but only at a much slower rate. Let me emphasize that these machines don't, they can't, replace the thinking processes involved in cryptanalysis.

This may be a good place to read a paragraph or two from a very recently published book by retired 4-star General Albert C. Wedemeyer to show you what misconceptions about cryptology can be entertained even on the highest levels, when the information comes, as the Navy letter I read you at the beginning of the first period states, via channels of gossip.
General Wedemeyer states, in connection with his discussion of U.S. culpability in the Japanese attack on Pearl Harbor,[1] that President Roosevelt had ample time to broadcast a warning, and he goes on to say:

[1] Wedemeyer Reports, Henry Holt & Co., New York, p. 43$.

> "The argument has been made that we could not afford to let the Japanese know we had broken their code. But this argument against a Presidential warning does not hold water. It was not a mere matter of having broken a specific code; what we had done was to devise a machine which could break any code provided it was fed the right combinations by our extremely able and gifted cryptographers. The Japanese kept changing their codes throughout the war anyway. And we kept breaking them almost as a matter of routine."

Would that we had had such a machine then--or that we had it now, for it would do what no machine can yet do, so far as I am aware, namely, think, even

simple thoughts. It is to be hoped that the rest of General Wedemeyer's book is more accurate in other respects than it is in regard to cryptologic ones.

Now, I want to show you what some of these machines look like. Here is a 139 highly-specialized World War II machine for deciphering messages; we call it an "analog" because although it does what the enemy's cryptosystem does, any resemblance between it and the enemy's machine is purely coincidental. To explain, I'll say this: In a cryptanalytic processing center, we try to duplicate with a few people what thousands of people on the enemy side are doing, for it takes thousands of soldiers to encipher and decipher the messages of the many headquarters involved in intercommunication. All these messages, or most of them are intercepted, they all flow into one place, and you can only have a certain number of people to process them. If you have the key or keys, then it becomes a problem of production-line deciphering; so we devise special machines to decipher the messages. As I said before, the machines may not have any resemblance whatsoever to the enemy's cryptographic machines, but they duplicate what their machines do, and do so at a high rate of speed. Here's a picture of another such device.

145 In this next slide you see a tabulator, a standard tabulator with a special attachment devised by our own engineers susceptible of doing what 137 we call "brute force" operations, where you are trying to solve a thing on the basis of repetitions which are few and scattered over a large volume of messages. Well, if you've got millions and millions of letters, or code groups, the location of those repetitions is a pretty laborious thing if you have to do it

by hand, so we speed the search up A machine of this kind will locate these repetitions in, say, one-ten-thousandths of the time that it would take to do
138 it by hand. Here is a specialized machine, again a tabulator, with an attachment, here, that is used for passing the text of one message against the text of another message in order to find certain similiarities, or perhaps differences, or maybe homologies, and it does it automatically. These relays are set up according to certain circuitry; you start the machine, and low and behold, it produces a printed record of the message repetitions or what not.

Here is a machine which I personally call "Rodin", after the piece of work by the great French sculptor Rodin, who sculpted a piece of engineering known as "The Thinker." This machine <u>almost</u> thinks. What it does is this: you feed into it a certain number of hypotheses and you tell it, "Now, you examine these hypotheses and come up with one which will answer all the following conditions." The machine takes the first hypothesis, let's say, examines that, and as soon as it comes to a contradiction it says, "Hell, that's no good; I'll go back and take up the next one." And so on. It tests the hypotheses, one after the other, at a high rate of speed, at electronic speed. That's only one small section of the machine.

141 To give an idea of size of machine installation at Arlington Hall, 1945--one wing. We now have more modern and much faster machines, and I'll ~~now~~ show you
150 a few of them, just after this next slide--the Purple machine--reconstructed
150 5 entirely by cryptanalysis. We also built machines to take faulty Purple messages and decipher them.

Before showing you a few of our newer machines I want to switch to another projector and this gives me a chance to show a few slides related to intercept

I-1 work. Here's an antenna field at Hof, Germany showing two types of masts and

I-2 mobile intercept vans. Next, an intercept operating position at a Navy station

I-3 on Skaggs Island and one at Bremerhaven. Practically all the equipment is specially designed and developed by or for NSA, and a great deal of the intercept is taken in record form, on magnetic tape as a rule.

I'll now show a few of our newer machines, which for the most part are

X-1 specially designed high-speed electronic digital computers. Here's one called

X-2 ABNER II, which uses a mercury tank for storage or memory. Next is ALWAC III which is one of a set of four machines remotely controlled so that four analytic units can call the machine into action to solve the same or different but already programmed-for problems. This is a machine which can be used when a job is too big for hand work and too small for one of our large machines built to handle

X-3 really big and complex jobs, such as ATLAS 2, Serial 1, which has a magnetic-drum and also an electrostatic-tube storage system, the former for high-speed memory operations. A newer ATLAS using magnetic cores for memory is now under con-

X-4 struction. In this next slide you'll see how the substitution of solid state diodes such as magnetic cores permits miniaturization. The slide shows ATLAS and alongside it BOGART, which does everything that ATLAS does but is much smaller and faster. ATLAS will be the last of the old style machines using

X-5 X-6 electronic tubes. Here's a large view of BOGART; and next I show you DUCHESS which does certain quite complex matching and cryptanalytic operations with 5-digit

X-9 code groups at the rate of 50,000 groups per second. Next I show you SOLO, a transistorized machine which has the general capability of ATLAS and can operate at megacycle speed--a million pulses a second. I may add that NSA has, of course,

X-10 a number of other types of computers, including IBM's 704; in fact, NSA has the largest collection of electronic computers and data processing machines in the world. It must have them in order to handle the very large and complex analytical problems which it is expected to handle.

Because of the complexity of modern high-grade crypto-systems, the great majority of them cannot be solved in the field, either at the intercept site or at a rear headquarters. Certain low-grade systems and a certain amount of traffic analysis can be performed by field units. As I've already said some COMINT processing can be done in the field to meet certain immediate needs of field or base commands, or forces afloat; but as the crypto-systems get more complicated I am beginning to be doubtful how far this can be pushed.

Each Service provides for its own special needs in this category but COMINT processing is essentially a complex activity and much of it can be done well only at major processing centers where the limited numbers of highly skilled personnel can be concentrated and very specialized analytic machinery can be installed and maintained. It is not enough to install them--you know they have to be maintained and that's not easy. There is no pool in civil occupations for cryptanalytic engineering and maintenance personnel--this is an important fact to remember. We've got to train our own in pretty nearly all cases.

I want to say a few words about the great importance of coordinating COMINT activities with other intelligence operations and with the tactical situation. Although COMINT is the most reliable, the most timely and, in the long run, the most inexpensive kind of intelligence, it must, as I've said before, still be evaluated, collated, correlated and coordinated with

intelligence coming from other sources, if for only this reason: to provide data for cover and protection of COMINT sources. When a decision has been made to take action based on COMINT, careful efforts must be made to insure that the action cannot be attributed to COMINT alone. This is very, very important. When possible, action must always be preceded by suitable reconnaissance and other deceptive measures, otherwise the goose that lays the golden eggs will be killed. I am going to give one example of what is meant by COMINT cover.

On a certain day in November 1944, an enciphered code message was sent by a certain Japanese staff section to a certain Japanese Air Force unit, requesting air escort for two convoys carrying troops to reenforce the Philippines. The message gave the number of ships, tankers, escort vessels, date of departure, port and route, and noon positions for the next seven days. The message was solved in Washington. Two days after the convoy left, one convoy commander reported in a message which was also intercepted and solved, that his had been sighted by a B-29, with strong indications that the other convoy had also been sighted. A few hours later, messages from these convoys reported losses as follows: six ships definitely sunk, one disabled, one on fire. Later we learned from another source that one aircraft carrier was also sunk. But did you notice that message about the B-29? That B-29 just didn't happen to be cruising around there; it was sent there to be observed.

Of course knowledge and experience point to the necessity of exploiting every possible advantage a tactical situation affords, and the temptation is naturally very great, in the heat of battle, to use COMINT whenever and wherever

it is available. This may lead to carelessness which quickly jeopardizes COMINT sources. Of course, the full value of COMINT cannot be realized unless operational use is made of it; however, when action based on it is contemplated, possible compromise of source must always be borne in mind and the danger of compromise weighed against the military advantages to be gained. A minor military advantage is never alone sufficient grounds for risking the loss of the source--this is a cardinal principle.

Also we must bear in mind that cryptosystems are usually world-wide or area-wide in distribution and changes made as a result of suspicion of compromise may therefore have a far-reaching consequence on the ability to produce COMINT elsewhere. The Commander seeking a minor advantage by using COMINT in one locality may thus deprive another Commander of much greater advantage or even deny it to a Commander of a major operation

Finally, another aspect of coordination is that between the operations officers and the COMINT officers The COMINT authorities should be carefully oriented to give the optimum coverage for operations in progress. There are just so many facilities and personnel available, and only a part of the enormous amount of traffic can be obtained and processed. Therefore it is essential that the COMINT producers be constantly informed of current and planned operations so as to direct attention where most needed. This was a very, very important point to get across. It was a difficult one to get across because commanders in charge of large-scale operations are naturally leery of

telling any outsiders what they were planning to do, and the how, when, and where of the impending operation. Mutual confidence must be established, so that the COMINT producers learn what the operations staff is planning; they support each other.

This isn't the only or the most important kind of cooperation that is absolutely vital for success in COMINT production, which nowadays is done on a really world-wide scale and requires a great deal of cooperation of all sorts, among many thousands of skilled personnel scattered practically over much of the earth's surface and separated by hundreds or thousands of miles. The integration and direction of the COMINT effort is a truly huge military enterprise and requires a high order of managerial ability and intelligence. Let me close this part by saying that not only does NSA have a large number of workers in COMINT endowed with great intellectual capacity but it also has available to it and uses the brains of some of the greatest scientists of this country. They come as consultants and advisers; they work on NSA contracts, and they help NSA in other ways, for instance, by moral support when it comes to reaching into high places in government for money and people.

This ends the COMINT portion of my presentation. In the next and final period we'll devote our attention to COMSEC.