SECOND PERIOD

COMMUNICATIONS SECURITY

Gentlemen, this period will be devoted to the subject of communications security, how it can be established and maintained.

Three or four years ago I gave a talk before the student officers of another Service School on this subject. About that time there was being hammered into our ears over the radio in Washington a slogan concerned with automobile traffic safety. The slogan was: "Don't learn your traffic laws by accident." I thought the slogan useful as a title for my talk but I modified it a little--"Don't learn your COMSEC laws by accident." I began my talk on that occasion, as on this one, by reading the Webster Dictionary definition of the word "accident". I know, of course, that this group here today is not directly concerned with COMSEC duties, but as potential future commanders of fighting units the definition of the word "accident" should be of interest in connection with what will be said in a moment or two, so I will read Webster's definition if you will bear with me.

> "Accident: Literally a befalling; an event which takes place without one's foresight or expectation; an undesigned, sudden and unexpected event, hence, often an undesigned or unforeseen occurrence of an afflictive or unfortunate character; a mishap resulting in injury to a person or damage to a thing; a casualty, as to die by accident."

Having defined the word, I will not proceed to make the definition relevant to this talk by reminding you of a minor but nevertheless quite

important episode of the war of the Pacific during World War II, and I will introduce the account of that episode by saying that: During the war the President of the United States, Commander-in-Chief of the Army and Navy, the Chief of Staff of the United States Army, the Commander-in-Chief of the United States Fleets, and certain other high officers of the Armed Forces and the U.S. Government journeyed several times half-way around the world to attend special meetings and conferences. They apparently could go with safety almost anywhere except directly over or across enemy or enemy occupied territory. They met with no accident. On the other hand, the Japanese Commander-in-Chief of the Combined Fleet, Admiral Isoroku Yamamoto went on an inspection trip in April 1943, the sequel to which may be summarized by an official Japanese Navy communique 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."

As is often the case, the communique did not tell the whole truth. Yamamoto didn't die in air combat with the enemy while directing operations--he met with an accident. I don't know who first used the following terse statement, but it is decidedly applicable in this case: "Accidents don't happen, they are brought about". U.S. Navy communications intelligence experts were regularly reading practically all of the Japanese Navy's messages because its cryptosystems were not secure. In the case of Yamamoto's inspection trip our Navy had his schedule pat down to the day, hour and very minute. They knew when he would leave Truk, and the time he would arrive at Buka, his scheduled stop-overs,

when he was to leave, etc.
would leave Buka for Balalae. They also knew what his air escort would be, and so on. You can see, therefore, that It was relatively easy to bring about the "accident" Yamamoto was to suffer. Our top Commander-in-Chief and his party, on the other hand, journeyed with safety because the communications connected with his various trips were secure. The Japanese Commander-in-Chief journeyed in peril because his communications were insecure. ~~His~~ and the circumstances that his death was no accident in the dictionary sense of that word--it was brought about. The Yamamoto incident later gave rise to a somewhat amusing exchange of TOP SECRET telegrams between Tokyo and Washington, and after the war was all over certain of them turned up in the Forrestal Diaries, from which I will now read (Page 86):

> The formal surrender took place on the deck of the U.S.S. Missouri off Tokyo Bay on September 2nd. The mood of sudden relief from long and breaking tension is exemplified by an amusing exchange a few days later of urgent TOP SECRET telegrams which Forrestal put into his diary. In the enthusiasm of victory someone let out the story of how in 1943 Admiral Yamamoto, the Japanese Naval Commander-in-Chief and architect to the Pearl Harbor attack had been intercepted and shot down in flames as a result of the American ability to read the Japanese codes. It was the first public revelation of the work of the cryptanalytic division and it brought an anguished cable from the intelligence unit already engaged at Yokohama in the interrogation of Japanese Naval officers.

"Yamamoto story in this morning's paper has placed our activities in very difficult position. Have meticulously concealed our special knowledge, we now become ridiculous." They were even then questioning the Japanese officer who had been responsible for these codes and he was hinting that in the face of this disclosure he would have to commit suicide. The cable continued: "This officer is giving us valuable information on Japanese cryptosystems and channels and we do not want him or any of our other promising prospects to commit suicide until after next week when we expect to have milked them dry...."

Washington answered with an operational priority TOP SECRET dispatch. "Your lineal position on the list of those who are embarrassed by the Yamamoto story is 5,692. All the people over whose dead bodies the story was going to be published have been buried. All possible schemes to localize the damage have been considered but none appears workable. Suggest that only course for you is to deny knowledge of the story and say you do not understand how such a fantastic tale could have been invented. This might keep your friend happy until suicide time next week which is about all that can be expected."

But not many years passed before the Japanese began to realize what had happened to them in the cryptologic campaigns of World War II. For example, Rear Admiral Nomura, the last Commander-in-Chief of the Japanese Navy said (this was on an interrogation):

"Not only have we been beaten in the decisive battles of this war, but also we lost the communications war. We felt foolishly secure and failed to take adequate measures to protect our own communications on one hand, while on the other hand, we failed to succeed in breaking into the enemy's traffic. This is undoubtedly one of the major reasons for our losing battles and in turn one of the major contributing factors to our losing the war. We failed in communications."

Here is another comment from a Japanese Naval Officer:

"Our Navy was being defeated in the battle of the radio waves. Our cards were bad and the enemy could read our hand. No wonder we could not win in this poker game." (Toshiyuki Yokoi. The Story of the Japanese Black Chamber.)

Books recently published in Japan by former Japanese military naval officers come out quite openly with statements attributing their defeat to poor COMSEC on their part and excellent American COMINT and COMSEC. For example, there is Captain Fuchida's book entitled Midway: The Battle that Doomed Japan, Chapter VIII, p. 131:

"If Admiral Yamamoto and his staff were vaguely disturbed by persistent bad weather and by lack of information concerning the doings of the enemy, they would have been truly dismayed had they known the actual enemy situation. Post-war American accounts make it clear that the United States Pacific Fleet knew of the Japanese plan to invade Midway even before our forces had started from home waters. As a result of some

amazing achievements of American intelligence, the enemy had succeeded in breaking the principal code then in use by the Japanese Navy. In this way the enemy was able to learn of our intentions almost as quickly as we had determined them ourselves."

(Here ad an aside what Wenger told as to disbelief in decrypts.)

And then in the last chapter, entitled "Analysis of the Defeat", Captain Fuchida says:

"The distinguished American Naval historian, Professor Samuel E. Morison, characterizes the victory of the United States forces at Midway as 'a victory of intelligence'. In this judgment, this author fully concurs for it is beyond the slightest possibility of doubt that the advance discovery of the Japanese plan to attack was the foremost single and immediate cause of Japanese defeat. Viewed from the Japanese side, this success of the enemy's intelligence translates itself into a failure on our part--a failure to take adequate precautions regarding the secrecy of our plan. Had the secret of our intent to invade Midway been concealed with the same thoroughness as the plan to attack Pearl Harbor, the outcome of this battle might well have been different."

Lest you infer that our side didn't meet with any COMSEC accidents, let me say that we had plenty of them. These were not attributable, however, to serious weaknesses in our COMSEC devices, machines and procedures, but principally to human failure to follow the rules implicitly or to weaknesses in the COMSEC devices, machines and procedures of some of our Allies. Take for instance the heavy losses that the United States Army Air Corps sustained in

their air strikes on the Ploesti oil fields in southeastern Europe. We lost several hundred big bombers within a relatively short time because of weaknesses

which let the German fighter commands know

in Russian communications, ~~weaknesses we didn't suspect. Those big raids~~ con- stituted field days for the German fighter commands, ~~because merely by traffic~~

our bombers left

~~analysis, and simple~~ traffic analysis at that, ~~they knew~~ exactly when and where

they were going. When out

~~our bombers were headed~~. We found what the trouble was, ~~but sad to say,~~ it was

when you fight a war with allies their

too late. This incident leads me to say that ~~the~~ COMSEC weaknesses ~~of Allies~~

are bound to affect the security of your own forces; and some-

~~even today lead to a rather serious illness which afflicts our high level~~

thing must be done to eliminate those weaknesses, even at the

~~authorities from time to time. I've given the disease a name--cryptologic~~

risk of jeopardizing other important things. For instance, you

~~schizophrenia. It develops when one is torn between an overwhelming desire to~~

~~may have to tell them about their weaknesses, which is always a~~

~~continue to read friendly traffic by cryptanalytic operations and the almost~~

~~delicate matter, or you~~ may have to provide them with

~~certain knowledge that the same traffic is also being read by others and should~~

some of your own cryptomaterial, in which case you

~~be made secure against the common enemy. What to do? Thus far, no real~~

lose control of the continued secrecy of that material.

~~psychiatric or psychoanalytic cure has been found for the illness. The powers~~

~~that be have decreed that the illness will be avoided by the very simple ruling~~

other

~~that~~ COMSEC interests will always over-ride ~~COMINT~~ wishes.

It is hardly necessary to tell you that with the advances made in the

means, instruments and weapons

invention and development of ~~all~~ the many ~~instrumentalities~~ of warfare, including communication systems, the so-called "pencil-and-paper ciphers", the hand-operated small cipher devices, the codes and code systems of former days, even

as early as

~~during and throughout~~ the period of World War I, appeared to be and were indeed completely inadequate. Military, naval, air, and diplomatic cryptographic

communications had to be speeded up; and obviously the road along which crypto-engineering and development had to travel was that which by mechanical or electro-mechanical apparatus speed in crypto-communications would at least begin to approach the ever-increasing speed of electrical communications, ~~in general, including both wire and radio systems~~. The need to invent, develop and learn how to use practical crypto-apparatus became obvious even before World War I had ended. ~~It is a truism that as mechanization and automation progresses in our civilization, parallel progress has to follow in communications systems and instrumentalities.~~ And let me remind you that the impetus for devising and developing better and faster means for crypto-communication came not only from the need for speedier crypto-apparatus ~~to match the ever-increasing speed of electrical communications~~, but also--and perhaps more importantly--from the need for much greater security in those communications, which were now largely by radio and were therefore susceptible of interception and study by the enemy. And, I will add, greater security was needed because the weapon of cryptanalysis had been made much more effective by advances ~~that started~~ made by new cryptanalytic tools

A brief history of the invention and development of crypto-devices, crypto-machinery, and crypto-apparatus will therefore be of some interest. We will proceed now with some slides.

Aside from the much earlier Scytale used by the ancient Greeks, ~~First, I show you~~ the earliest cipher device known to history ~~is this slide is a picture of~~ the cipher disk, first described by an Italian cryptographer named ~~taken from~~ Alberti, who wrote a treatise on ciphers in Rome about 1479. His ~~It~~ is the oldest tract on cryptography that the world possesses.

The next slide shows a similar sort of wheel which appeared many years later in a book by another Italian cryptographer, Porta, who ~~Porta's a book, which I showed you after the first period,~~ recommends the use of the cipher disk with keywords. ~~a similar device, if you call it a device.~~

The next disk is that, patented in November 1885 by the first Chief Signal Officer of the United States Army, and the next slide pictures the U.S. Army Cipher Disk, which was used in the period of World War I. It follows exactly the same principle that Alberti recommended. It seems to have taken a long time for the Signal Corps to get caught up with Alberti!

Now I know it takes a long time to nurse a patent through the United States Patent Office, but Alberti's device was finally patented in 1924. Here it is.

Next is a picture of the Wheatstone Cryptograph, the first real improvement on Alberti's device. I have the only copy in the United States, maybe in the world, and I've brought it with me. Sir Charles Wheatstone interested himself in cryptography and invented his device in the latter part of the decade 1870. It is not just a simple cipher disk. Of course, as you see, it consists of the ordinary alphabet on the outside and an alphabet on the inside, the latter being a mixed sequence; but there is one additional important feature--the alphabet on the outside contains 27 places, the one on the inside, 26. There is a differential gear in the device so that as you encipher a message and turn the big or "minute" hand to the letters to the plain text, the small or "hour" hand advances one step for each complete revolution of the "minute" hand, just as in a clock. At the close of this period those of you who would like to examine the device may do so.

Now in 1917, in casting about for a field cipher device for use on the Western front, our British allies resuscitated Wheatstone's principle,

embodied it in a little different mechanical form, and made thousands of them. Here is one of them and here is an American copy of the British model. It has a 27-unit alphabet on the outside and a 26-unit one on the inside; but there is now one additional and very important feature. You will notice that both alphabets ~~are now arranged for~~ can now be made variable mixed sequences, whereas before, in the original Wheatstone, only the inner alphabet ~~was mixed~~ could be varied. Insert here Now I suppose you would be interested in a story about this thing. It was decided to adopt the device for use on the Western front after it was approved by the cryptologic authorities at the GHQ's of each of the principal allies, British, French and American. A copy of the device was then sent to Washington and the head of the American cryptologic agency in Washington approved it. At that time I was teaching school--remember that photograph I showed you of the school for instruction in cryptography and cryptanalysis? Somebody said why not send it out to Riverbank and see what they have to say. So they sent out a set of test messages and one day Colonel Fabyan came walking into my office, handed me a piece of paper, and said: "These are in Wheatstone, I think. Solve them". I took one look and saw there were five messages, just five, and they were all very short--each had about 35 letters. I said, "Oh! It's ~~silly~~ futile to try this. I have other ~~fish to fry~~ things to be of greater importance and priority." The Colonel said, looking hard at me, "Young man, on the last day of each month, you get a little green piece of paper with my name in the lower right-hand corner, ~~of~~ If you would like to continue receiving those bits of paper, you'll start working on these messages right away." I said: "Yes, Sir!" Well, I started in and by means too involved at

Rewrite REF ID:A63406 insert

top p. 48

In fact, a good many were just about to be issued to field units, not only British but also French and American. All forces were to use it. But even before they could be put into use it was shown that the security of the device was inadequate ~~too [illegible]~~ and they were withdrawn. Reliance continued to be placed in codes.

I had something to do with demonstrating the weakness of the device and when I reached GHQ in France about three months later I found I wasn't a bit popular with certain British, French + Am crypt.

the moment to tell you, I felt that ~~the other~~ one of the alphabets, ~~in this case the mixed sequence~~, had been derived from a rectangle based on a keyword, and it appeared to me, from the distribution of the sequence of about half-dozen letters I'd reconstructed, that the keyword ~~for mixing the sequence~~ might have been the word "cipher". At that time I'd not discovered what later turned out to be an important new principle in cryptanalysis whereby having the one alphabetic sequence the other could readily be found by a process of conversion. So not having this principle I was at a loss as to what to do, except try to guess what the other alphabetic sequence might have been based upon. I sat back and thought: Now, if a chap is simple-minded enough to use as a keyword a word connected with the subject ~~for mixing up the letters in the one alphabet~~ of cryptography, he would probably use a word associated in his mind with that word as the keyword ~~for~~ for disarranging the other alphabet. So I tried every word that was associated in my mind with the word "cipher" -- "cipher alphabet", "cipher device", "cipher polyalphabet", and so on, one after the other. This took a little time, because with each guess I had to derive the mixed sequence and try it out on the messages. Finally, I came to the end of my rope and said to the then new Mrs. Friedman: "Elizebeth, I want you to stop what you are doing and do something for me. Now make yourself comfortable," --whereupon she took out her lipstick, and made a few passes with it, and said: "I'm ready." I said: "Now I'm going to say a word to you and I want you to come back with the very first word that comes to your mind. ~~Are you ready?~~ Here goes: cipher!" Quick as a flash she ~~said: "Yes" I said:~~

Captain Lowe said: "Machine". Machine was the word. You see my male mind didn't regard this thing as a machine at all; but the female mind is, as you know, a thing apart. Well, the messages were deciphered in a hurry by me. The first message, by the way, read: "This cipher is absolutely indecipherable." We sent the solution to Washington, where on arrival there was a to-do; there was also a to-do in Europe. I wrote up the solution and Colonel Fabyan sent it to Washington so that when I got to American GHQ in France, about three or four months later, I wasn't very popular with our British friends, because a mere amateur had found something their experts had overlooked. Moreover, what was worse, they had to withdraw the device from users, and thousands of them had been issued.

Now I show you a poor picture of a very similar device, bearing on its face the engraved date 1817. It was invented by a Decius Wadsworth, at that time the Chief Ordnance Officer of the United States Army. The device itself is still in operative condition and is housed in the museum of a little hamlet in Connecticut. I borrowed it for a short time from the curator and unfortunately didn't have a good picture made. Decius Wadsworth anticipated Sir Charles Wheatstone's invention by a good many years.

Next comes the cipher cylinder. A French Army reserve officer, Commandant Bazeries, tried to interest the French Army in a device which he called the "Cryptographe Cylindrique", or cylindrical cipher. His device consisted of a series of disks with a central hole so that they can be mounted upon the shaft; each disk bears an alphabet (of 25 letters in this case) in disarranged

sequence, and the mixed alphabets are all different, each bearing an identifying letter or number for assembling them upon the shaft in some key order, so that the correspondents have the same sequence of disks on their cylinders. You put your message into cipher 25 letters at a time (because there are 25 rings), by rotating the rings to align the letters of your plain text horizontally, whereupon for the cipher text you can choose any other one of the other 24-rows of cipher text. (Bazeries used a 25-letter alphabet.) This principle seemed to be a very good one and messages in it appeared to be quite safe. But Bazeries Here is a picture of the gentleman--he was quite a controversialist--and he was always exchanging letters with the French War Department but he never got anywhere in his attempts to get the Army to adopt any of his ciphers.

In 1915, an American Army officer, Captain Parker Hitt, about whom I have told you, conceived the crypto-principle of the cipher cylinder independently. He knew nothing about Bazeries. His device, however, took the form of strips, you see. This was Hitt's very, very crude first shot at it, and, as a gift from him, it is among my treasured the interesting items in collection. Here is a better model, one he made in 1915, with the paper strips mounted on wood--wooden sliders. That device was brought to the attention of the then Signal Corps Major Marbourgne in Washington, who thought he'd thought up something new when he made a cylindrical form of the thing, going back, unknowingly to Bazeries' model. Here is Mauborgne's model; it is made of brass and is very heavy. And here's the final form of the device, as adopted in 1922 by the U.S. Army. It became

What we call Cipher Device, type M-94. Now, when Major Marbourgne decided to go ahead with this device, Mrs. Friedman and I were back at Riverbank, after I had returned from the AEF. We didn't think the device was very secure and said so, whereupon Maubourgne issued a challenge, which was accepted. He sent 25 messages. We started in with our crew to try to solve the messages by lining them all up and trying to guess words in them. It was no-go. We spent a lot of time trying to solve those messages--and so did the crew of cryptanalysts in G-2. Ten years later I found the plain text of the set of 25 challenge messages amongst some old papers in the Office of the Chief Signal Officer and then I knew why neither we nor G-2 solved them--look at them! And we were expecting military text! In defense of Mauborgne I'll say that it was not he who cooked those test messages up for the challenge--it was one of his assistants who thought he'd put one over on us, which he did. ~~Mauborgne told me he'd said to an aide, "Put up some messages in this thing," and the aide thought the best thing to do was to make up messages of this sort.~~ When after some days or so months nobody had solved his challenge messages Mauborgne went ahead and got the thing out, and ~~this is the history of the development of the M-94.~~ We had thousands of them made, and they were used by the Army, the Navy, the Coast Guard, and the Treasury. Here's a picture of the thing. A couple of years after the M-94 was put into service a friend showed me a ~~description of the cipher~~ write up of something he'd come across more or less accidentally in the Library of Congress, among ~~cylinder in~~ the papers of Thomas Jefferson. ~~He Thomas~~ Jefferson was the first to invent the cipher cylinder principle, and he anticipated the Frenchman, Bazeries, by a century. Here is the first page of his description of his

which he called "The Wheel Cypher".

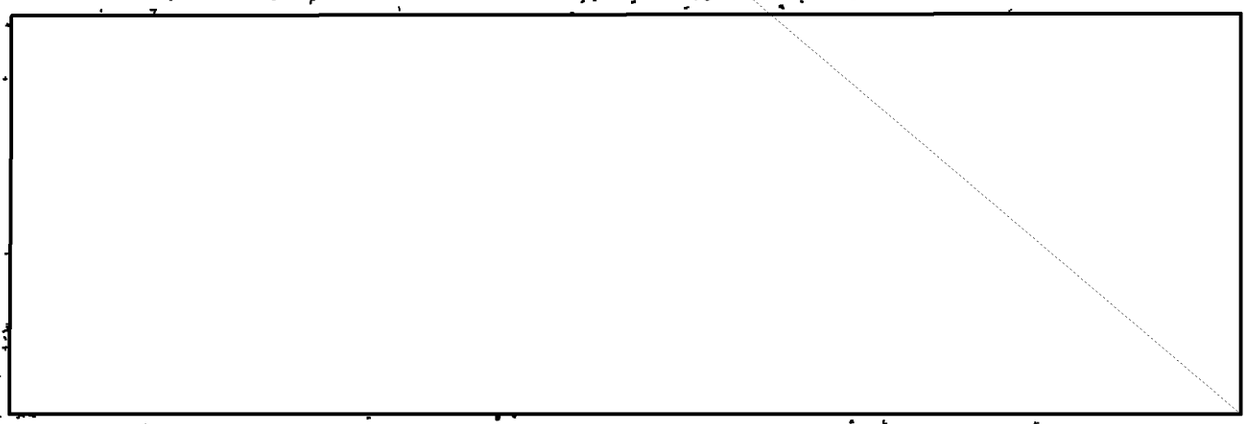
device. Here is the second page. You see his calculations, giving you at the bottom the number of permutations that his particular device affords--a whale of a large number because Jefferson proposed a set of 36 disks.

In studying the degree of security provided by the M-94 both Army and Navy cryptologist soon came to the conclusion that security would be much increased by the use of variable or changeable alphabets. Army other versions I had one which used metal pegs so I had a gadget built on which we could mount slips of paper and fasten them; and then change the alphabet as often as was felt thus we could necessary. That was the beginning of Navy tried other versions. the various variant forms of the strip cipher devices used by the Armed Forces, and later by the State Department and the Treasury Department. Here's the original version of the strip cipher device that used changeable alphabets. Both the Army and the Navy cryptographic divisions proceeded to improve on the system, both as to the form of the device itself as well as the ways of making the strips in quantity. Here is a picture of the final Army type of strip cipher device. You see the channels in which the alphabet strips were inserted according to the daily key, and according to the particular crypto-net to which your command belonged. I mean by this that not all the traffic would be in the same set-up of strips or even used the same strips. The idea was to cut down the amount of interceptible traffic in the same key. The strip ciphers carried an enormous amount of traffic.

Next we come to a machine called the Kryha, invented by a German, in about the year 1925. The Kryha was the last word in the way of mechanical cryptographs at the time, and Mr. Kryha tried to interest various governments in his machine. I think I should explain it for those who have never seen it.

Here is an outer alphabet and here an inner alphabet. The inner alphabet is mounted on a disk which is rotated angularly according to the toothed wheel which is in here. The alphabets can be rearranged if you wish, by sliding the metal pieces on which they are printed into the slots. From a given starting point and with a given mixed alphabet you start with the first letter to be enciphered, see what letter stands opposite it, and write it down. Then you push this button and the moveable disk will skip a certain number of spaces, one to seven, something like that, and you encrypt the next letter, write down its equivalent, and give the button a push. Now here is a dissertation on the number of permutations and combinations the Kryha machine affords, written by a German mathematician. All I have to say about it is that in this case, as in many others, merely the number of permutations and combinations which a given machine affords, like the birds that sing in the Spring, often have little to do with the case. Much depends upon just what kinds of alphabets are employed and exactly how they are employed. Large numbers of permutations and combinations don't frighten the cryptanalyst at all. For example, to give you a simple illustration, take a simple monoalphabetic substitution cipher. The number of alphabets that can be produced is factorial 26--that's a large, large number--403 quadrillions, 291,451 trillions, 126,605 billions, 635,584 millions and a few more but you know as well as I that you don't solve the monoalphabetic substitution cipher by an exhaustion method. There are very much simpler ways of doing it. Take another example: Suppose you have a machine that provides hundreds of millions

of mixed alphabets for use in encipherment, that is, the alphabets are presented successively in a fixed sequence. Such a machine would give poor security because in heavy traffic many messages would be enciphered by the



To return now to our general survey of crypto-machines it became clear that there was a pressing need in the military and naval services for two types of automatic machines, that is, machines which would get out of the realm of hand-operated gadgets. First we needed a small machine for low echelon or field use and all mechanical; second, we needed a larger and perhaps electrically-operated machine for rear echelon, high-command use. Let us take up the first of these two types and see what happened.

I show you next a development model of a machine constructed by the Signal Corps Laboratories, developed without guidance from Washington. The Director of the Laboratories at that time was a great believer in autonomy and he wasn't going to have Washington tell him anything about how things were to be done. When it came to developing a cipher machine, he decided that he and his staff could produce a really good machine without the help of the cryptanalysts. So he proceeded on this basis to use up the tiny bit of money that was available--$2,000. We in Washington were not permitted even to know what

was being built until the final model was completed and ready to be delivered to us. ~~After a quick look I asked the Chief of the Division to put up some messages for us himself, so that there would be no question as to whether I or some of my assistants had gotten any illegitimate help. Well, he enciphered a few messages and I brought him back the answer to the first one in 25 minutes, and the answer to the rest of them in 35 minutes.~~ The whole development represented a loss of time and energy and moreover, it wasted what little money we had for such business. ~~I almost forgot to tell you. This was very amusing.~~ When we finally went to pick up the machine, I talked to Colonel So and So, who told me with some pride that his machine was all mechanical and that there was nothing in the way of an electrical machine or operation that you couldn't do mechanically. I asked: "Colonel, can you light a room mechanically?" To which he replied: "You've said enough--get out. ~~That's~~ There's the machine, take it with you." The power source, which in the model was laughable, he planned to motorize, but he never was given the opportunity to carry out that plan, because ~~But I do not regret to say that~~ the crypto-principle was very faulty--it didn't take very much time ~~as I indicated~~ to read ~~the~~ test messages ~~sent~~ put up by my chief himself, and the laboratories development came to an ignominious end. But I'm glad to say that was an unusual Colonel; those who came later were much more inclined to take advice from persons experienced in the field of cryptology. that chief of the laboratories

Now we come to a development which is of ~~deep~~ considerable interest to us. Here's a picture of a gentleman named Boris C. W. Hagelin, a Swedish engineer, who was responsible for the invention and development of one of the machines that we used all the services

in World War II in great quantities. Mr. Hagelin and I became very good friends after the war. I was opposed to taking on Hagelin's device in 1940-41 for reasons that will presently become clear, It wasn't a case of NIH--"not invented here"; but the decision to have them made for and used by the United States Army was a decision on a level higher than my own, and I simply accepted it. It turned out, I think, that my superiors were right, for our troops had for low-echelon crypto-communications, whereas if I'd had my way they'd have had nothing but pencil-and-paper ciphers, or the M-94 device.

Now just a bit about Mr. Hagelin. He did what I best describe as a hysteron-proteron. That's a four-bit word, ~~not four-bit in the sense that you use it for digital computers~~ but in the everyday sense; it's a four-bit word from the Greek meaning to do a thing "ass-backwards". I mean that usually you go into cryptographic work and then you have a nervous breakdown. He did it the other way. He had a nervous breakdown and while he was recovering he invented this machine--and he made several million U.S. dollars from his invention. That's ~~why I say he did~~ not at all a poor sort of a hysteron-proteron if you're going to do one.

Here's a picture of Hagelin's very first machine. I've brought one of his very first models, in fact, number one, for your inspection. It was a present from Mr. Hagelin, for my museum, ~~and when I've passed on, for the museum of the United States on Constitution Avenue in Washington~~. It's a very interesting device. From that prototype we built in America, for World War II, this six-wheel Hagelin machine, ~~with American inch specifications~~, and with American tools, rather than European ~~millimeter~~ specifications and tools, the astonishing number of over one hundred and ten thousand of these machines. ~~They were manufactured by the~~

He built better models and interested the Signal Corps in them. As a consequence we built the M-209 according to American inch-measurements and metric measurements and we built them—

Smith-Corona Typewriter Company, in Groton, New York, and are undoubtedly known

¶ Many of you may know that
to many of you as Converter M-209. But the M-209 had a serious, a very serious

security about which I'll say a few words later.
weakness, you know, among other things it had no printing mechanism, but I'm

not really concerned with that. I'm concerned with its cryptographic

deficiences, about which I'll tell you presently. This is a picture of one

The M-209 has no printing mechanism, and
of the Hagelin machines as modified by some of our GI's in Italy. You know

A couple of them
how resourceful GI's can be, they scrounged parts here and there and they'll

improved their machine to make it a printing model. See, here's is the

keyboard, and here's the printing mechanism. Inside the cover is a cartoon

of a couple of GI's getting ready to test a home-made still for the production

of you-know-what. The caption at the bottom of the cartoon says: "Yes, but

PL 86-36/50 USC 3605
EO 3.3(h)(2)

will the God damned thing work?"

Now, Mr. Hagelin proceeded to improve his machine and this is a side view

of one of his latest models--the CX-52. It prints not only the plain text but

and it incorporated a much improved
also the cipher text, It has a ciphering mechanism that represents a very great

because
advance. Now the wheels, instead of being permanently fixed upon the shaft,

are demountable and can be rearranged in 720 different ways. The stepping

We've studied this improved model for some time
motion for these wheels is complicated and as of this moment we do not know

ciphers produced by
how to solve this machine. But it has certain weaknesses, as did the M-209.

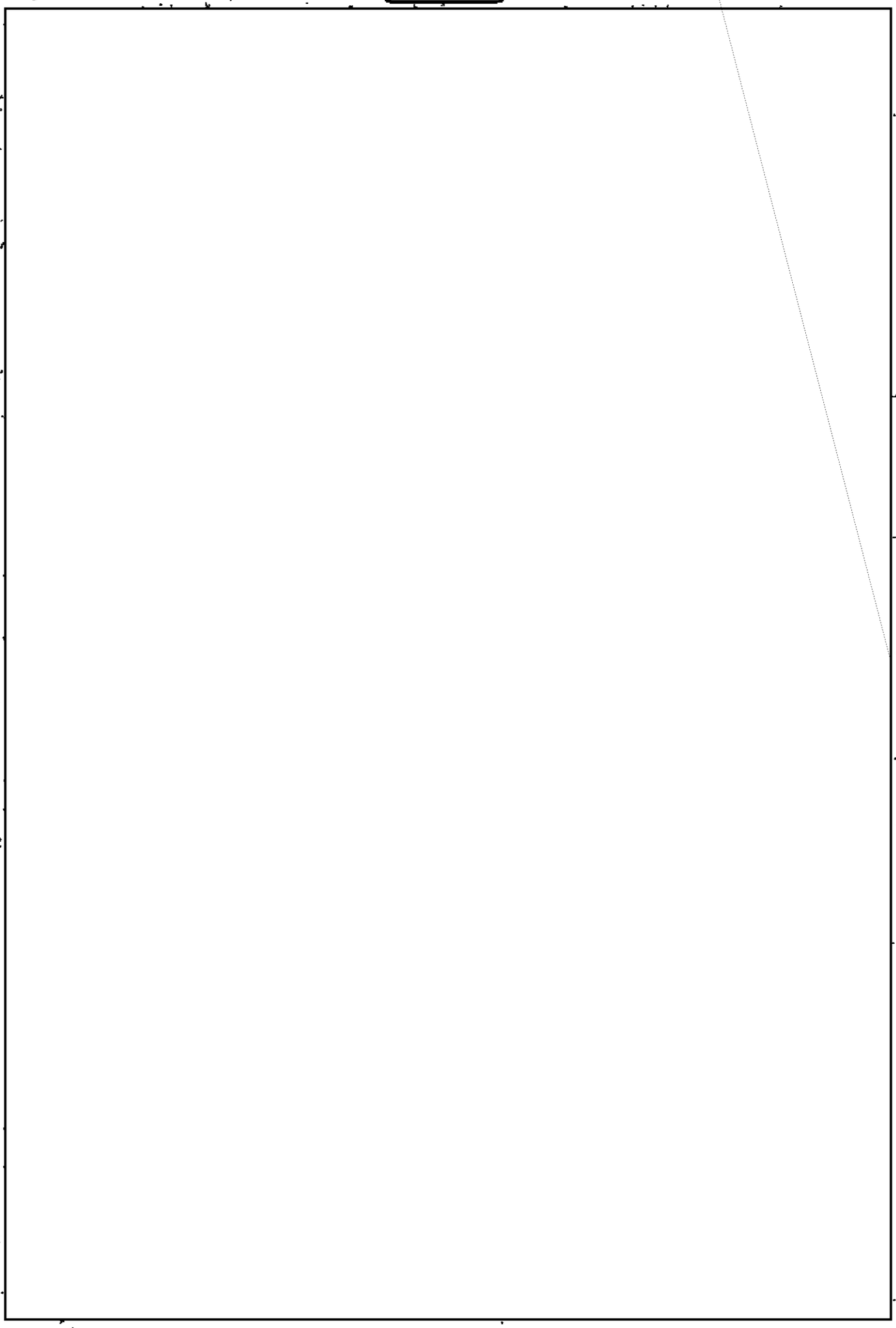
But it still has
It has, for one thing, the very serious weakness [redacted]

they
as I've explained [redacted]

If time permitted I could
In order to show you how easily this is done, but you'll just have to take my I will go through the steps. First

word for it. [redacted]

— the whole setting of the machine is not at all



Now for We are going to proceed with a quick review of the development of what we call electrical-rotor machines. The first one I show--also a product of the Hagelin company which was headed by Mr. Hagelin when his father bought out a Swedish cryptograph company in Stockholm--was not a real rotor device of the type we know today but I don't want to go into details. I merely want to show the device, which The device is now connected to a Remington electric typewriter, so that instead of writing down letters one by one you can make much more speed by having a printed record. Up to that time devices of this sort were only of the lamp- indicator-type of machine. You press a key and a light would light; you would have to write down the letter flashed on the light bank and then the cipher wheels would step.

The next slide shows a better picture of this machine controlling a Remington electric typewriter. The next forward step was taken step, of course, was made by Mr. Hagelin when Hagelin made the printing mechanism an integral part of the machine itself. Here is the keyboard, the printing mechanism, in here, and now the whole assembly is very much smaller and more compact.

Now I show a German machine known as the Enigma, a commercial model, invented and put on the market in about 1923-24. It comprised a keyboard, a light bank,

or contact on a fixed entry plate or stator into

and a small dry cell for power.

a set of electric wheels called rotors, In this case the enciphering-deciphering circuitry is more complicated; it goes from a key of the keyboard, ~~and~~ then through stepping these rotors and, by means of a reflector or reversing rotor, back through the ceiphar rotors to one of ~~back through them to~~ a bank of lights, ~~whereon it lights a lamp~~. This reflector or reversing ~~wheel~~ rotor is a very important feature of this machine. ~~Now~~ The stepping ~~everytime you press a key, one of these rotors steps forward and the stepping~~ of the rotors is such that the machine ~~has~~ had a rather ~~very~~ short cycle as such things go, less than ~~about~~ 26^3; it was a little less than 23^3 ~~that on account~~ because of certain factors into which it isn't necessary to go. ~~Now~~ I'm not going to take the various developments of that machine through World War II. At the moment, and in period of time to anticipate German developments in this field, I want to go directly to the American developments in ~~these~~ rotor machines. First ~~For this purpose~~ I show a picture ~~of a man named~~ the late Mr. Edward H. Hebern, a Californian, who seems to have independently, ~~I think,~~ thought of rotor machines. I asked Mr. Hebern one day how he happened to get started on such ~~work~~ things and he said, "well, you see I was in jail". I said: "In jail, what for?" He said, "Horse thievery." I asked him: "Were you guilty?", whereupon he said: "The jury thought so." It was while he was in jail, then, that Mr. Hebern conceived the idea of a cipher machine. Here is his very first model, It is possible that he built it as an item of occupational therapy while in jail but I think it more likely that he built ~~presumably~~ it after he got out of jail. It has a keyboard, a left-hand stator, that is, a ring of 26 stationery contacts, to one of which the current goes when a keyboard key is depressed; arranged in a circular fashion, a rotor of 26-points, and an exit stator of 26 contacts on this side. It is important to note that there was no reflector rotor; the type here is what we call a "straight through" rotor machine. You press a key and a lamp lights. ~~Just~~ There was just one rotor ~~was~~ in his first model, which he built in 1922 or 1923 for the Klu Klux Klan. Here is the first printing model made by Mr. Hebern--still a ~~one-wheel or~~ one-rotor machine--with a keyboard and now an electric typewriter connected

thereto. I have among my treasures in my library a brochure which went with this thing and it's a very curious document. Now, one interesting thing about Mr. Hebern's rotors is worth noting. He didn't have absolutely fixed wiring, as in the German Enigma rotors, for these are detachable wires, and this next slide shows 13 leads on one side and 13 on the other, showing that he conceived at an early date the idea of variable connections in rotors. This is an extremely important feature of any kind of a rotor machine. This shows his next step. Now we have three rotors in cascade. This, too, was a very important step--the cascading effect was a great advance in connection with rotors. Here I show his next development--a 5-rotor machine. Here are the rotors removed from the machine to show you what they look like. They were still variable--you could take wires and rearrange them, connection changers as and when you pleased. there was a keyboard and still a light bank. There is an interesting story connected with that model. The Navy Department was very much interested in cipher machines much more so than the Army in those days, because for these were things they absolutely had to have for speedier communications, from Washington to the Fleet Commanders and, of course, for intra-fleet communications. The Navy was very anxious to have a suitable machine and thought this Hebern model a Hebern machine seemed like a good bet. This was the machine they thought they would like to buy. They got an appropriation for the purpose, a large sum of money for those days, $75,000, and they proceeded then to negotiate with Mr. Hebern. I was asked by the President of the Naval Board that had been appointed to study the Hebern machine to give him my personal opinion At that time, in the code and cipher section, there was a cryptanalyst of parts, who happened to be a lady, and she was quite able. She was the one of its security. I had no machine and the Navy had only two, both who got Mr. Hebern ready to move from a three-wheel to a five-wheel machine; undergoing service tests. and when he finished the development of the latter and he seemed to be on the

point of getting a good-sized order from the Navy Department, he offered and she accepted an attractive offer to come and join the Hebern firm in California. I apologize for introducing the first person singular so much, but the fact is that I became interested in this machine as a result of a personal inquiry from the President of the Naval Board that had been assigned to study the machine and I persuaded the War Department to purchase a machine from Mr. Hebern. I sat and studied it for some weeks--three or four weeks. The whole of my outfit consisted of myself and a World War I veteran, an ex-prize fighter, with pug-nose crossed-eyes and cauliflower ears; the only thing he could do was to type, and I may say that he could copy from draft letters or cipher text with absolute accuracy, but that's all he could do. The rest of it was up to me. As I say, I studied the Hebern machine until an idea for a solution came to me, whereupon I went over to the Navy Section, which was then in charge of a Lt. Struble, who now is Vice Admiral Struble, Retired, with an enviable service record. I said to Struble, "Lieutenant, I don't think that machine is quite as safe as you think it is." He said: "Oh, you're crazy!" I said: "Does this mean that you challenge me?" whereupon he said, "Yes." So I said: "I accept." He asked: "Well, what do you want in the way of messages?" I said: "How about ten messages put up on your machine?" He gave me the ten messages and with some typing help from that ex-prize fighter I worked on them until I got to a place one day, at the close of business, when I had reduced the text of one of the messages to monoalphabetic terms. By this I mean that I'd reduced it to its simplest terms: I knew that in the first line of the text of that message the

letters which were the same but I didn't know what the letters actually were. Let us say, for instance, that the first, the seventh, the ninth letters were the same, whatever they were; the second, the seventeenth and the twenty-third were the same, and so on. That's all I had when I left for home that evening. We were going to some sort of a party, and I had these letters in my mind, at least the ones that were identical and their positions. As I was tieing a black tie, it suddenly came to me, and I can't tell you to this day just how or from where, but the whole line of text fell into place with all the repetitions in the proper place: "President of the United States." I could hardly wait to get to the office in the morning, and to my intense gratification I found that my subconscious guess was correct. I reconstructed the ten messages, turned them over to Lt. Struble, and there was a considerable amount of excitement after I showed him how I'd reasoned out a solution. The Navy Department cancelled the order that they had placed; the Hebern Company, which had been selling stock on the basis of great prospects, went to pieces, the ex-Navy Department lady who joined the Hebern firm lost her job, and begged to be taken back. Mr. Hebern, trying to recusitate what he could from his unfortunate encounter with an unknown cryptanalyst, bought stock in the Southern part of California at 4¢ and sold it in the northern part of the state at about $2.$$. The California Blue Sky Laws didn't like that sort of conduct and Mr. Hebern spent a year in prison.

I hope you won't think I am vain by shewing this—I saved the paper which

had the text of the first message which I was ever able to solve in that sort of a machine, and by the way, I hope you will forgive me if I say that the methods I had to were devised at that time for the solution of rotor machines and rotors in cascade are practically the same today as they were over thirty years ago. Despite my solution we thought the Navy decided that the Hebern principle was still a good one and went ahead with Mr. Hebern after he got out of prison. Here's a picture of the last machine built for the Navy. Hebern

As regards the purely mechanical factors the Navy wasn't satisfied with the power drive and the hand drive; but the crypto-principles seemed satisfactory, but the cautious Navy asked the Army's help in evaluating the security afforded by the machine. It had a different kind of stepping motion in which the Navy had put a great deal of faith. It was a good motion but nevertheless it had weaknesses that we found we could exploit, and we solved challenge messages put up by the Navy. Here's a picture of the last machine that Hebern built for the Navy. He wanted to get paid for it, naturally, but there was a hitch — just one — the machine wouldn't work and when this was pointed out to him that the machine didn't work, he said: "Show me where it says in the contract it has to work", and when they couldn't, he was paid off. The Navy then decided that they had had enough of Hebern and went into research and development themselves. They had a laboratory established in the Navy Yard, with a very able young man named Seiler, now a Captain in the Navy, who did some excellent developmental work. Years later the Hebern heirs brought suit in the United States Court of Claims against the United States for $50,000,000, believe

it or not. The case has been pending for a number of years and the last I knew of it, which was about a month or two ago, a settlement was in prospect for about $35,000. That's quite a discount. I might say that, ~~except for these challenges and acceptances of challenges~~, there was very little collaboration between the Army and the Navy cryptologic organizations in those days before Pearl Harbor. Each Service had its own secrets--which was really too bad, but the situation was mended later, as we will have occasion to learn.

Now, I'm going to show you a few slides of the Army developments in crypto-machines. This, after the debacle I've told you about, was the first shot that we in the Signal Intelligence Service in the Office of the Chief Signal Officer, had at developing for the Army a machine in Washington. It had a keyboard, a light-bank, 5-rotors, and now an interesting feature--an external keying mechanism--Because ~~Lately in this field~~ I had come to the conclusion that internal control mechanisms for stepping rotors had a fundamental weakness. I felt that you must not make the rotors depend upon themselves for the stepping, and I conceived the idea of having an external key, for example, a teletype tape, which would step along and control the stepping of the rotors in random fashion. These tapes were composed of a sequence of random characters so that the rotor stepping was quite erratic, and that was our first shot at it. I think the principle is still quite sound, especially if the tapes are not overburdened in usage. This is another view of the same machine--here is the tape transmitter, the rotors, the keyboard, an electromatic typewriter etc. ~~This was a slow machine, entirely too slow because it didn't print the results.~~ Next we had a printing model

~~Here it is, connected with an electromatic typewriter.~~ not I think this was one of the very early models, ~~but it was still a five-rotor cryptograph controlled by a tape transmitter.~~ For the tapes we had boxes of ~~[illegible]~~ Key about 150 tapes from which you could make the selection for the day according to the keying document. ~~The latter also told the various starting places on those tapes.~~ The fatal weakness, of course, was the production and the distribution of the tapes. This was quite a headache and the tapes (soon when we used specially heavy paper for they) would break after they had gone through ~~say thirty or forty~~ a number times. ~~The Army developments continued and here is the next one, Converter M-134. Here you see a side-by-side arrangement, keying mechanism with the typewriter.~~ We had about 75 of these manufactured by a concern in New Jersey that was not particularly gifted in the typewriter art. The machines functioned all right but before even ten of them had been produced we had hit upon a new principle for the control of the rotor stepping. I tried my very best to get the Signal Corps to change the development right there and then, and shift to the new type of control. I was practically thrown out of the office of the chief of the division with the remark, "Go back to your den--you inventors are all alike. A new and better idea every day. If we always listen to you, we never get anything out." So we put the idea on ice, that is, in secrecy. I will switch now to the Navy MARK I ECM, the electric cipher machine, designed, developed and built by the Navy without any help from Mr. Hebern. It had a new type of control mechanism for rotor stepping, based upon the use of Bowden, or flexible cables. They were tricky and gave rise to a lot of difficulty

but over and beyond that the machine had a fatal security weakness. It had a key length of tremendous length but with only 15 different starting points. You'll remember what I said about such a situation a few minutes ago. How this came to be the case I do not know, for there wasn't any coordination or collaboration in those days with Army cryptologists--we didn't even know that there was such a machine had been built by Navy. Each service went its own way. When there came a change in command in the Navy code and signal section the new head decided that that development had gone far enough and he wanted some help from the Army if he could get it. He came to see me one day and told me that they were in difficulty and needed new ideas if we had any. I said: "Well, we have a good idea but it's secret." He asked: "Well, what do you have to do to tell me?" I told him: "I'll have to get permission from the Chief Signal Officer", which I proceeded to do. I mention this specifically and ask that you believe that this was the situation in those days--there were Army secrets and Navy secrets, and never the twain did meet. When I told the Chief Signal Officer what Navy wanted, he promptly said: "Of course, let them have it". So I told the Navy about the Army idea for rotor control; I showed them the circuitry and after some delay the thing was adopted. The delay was caused by Navy doubts that sufficient currents could be obtained through sets of 10 or more rotors--they were having contact troubles with their rotors to do what electrical work had to be done. But the machines were built by the Teletype Corporation, a very competent organization, and were highly successful. Here is a picture of the MARK II ECM, Navy terminology, or the SIGABA, Army terminology. If it hadn't been for the fact that we got together before we became belligerents in World War II, it would have been extremely

difficult for the Army and the Navy to have had in World War II any inter-communication at all. The only thing that we had for a good many years was a very slow, ~~was a disreputable~~ hand-operated cipher using pencil and paper, which had been adopted way back in 1930 ~~by direction of the Chief of Staff of the Army and the Chief of Naval Operations, and that's all there was.~~ The strip cipher device was then ~~could have been~~ adopted for all joint communications until ~~just wasn't. Fortunately,~~ the ECM-SIGABA came into use, just in good time, and it was used with great satisfaction on both sides, ~~I am very happy to say~~. I might add, in closing that incident, ~~by saying~~ that, to the best of my knowledge, this is the only gadget that was withheld from our British Allies. Although they knew that we had a machine of this character and although we knew all about their type of machine, in fact, the Navy was using it for communication with the British and neither side was ~~with which neither they nor we were~~ at all happy, it was our policy on the highest level of the Army and Navy, to withhold ~~this~~ their machine from the British. There was a struggle for several years on this point until the recalcitrant people high up in both services began to see the light. The trouble was that when the technicians assured them that messages put up by this machine couldn't be read without having ~~the rotors and~~ the current key list--that we ourselves, in Army as well as Navy, had tried very hard to do so and failed--they just wouldn't believe it. One reason ~~is, of course,~~ for this adamant policy was that they were daily getting the decrypts that were being produced from German, Italian and Japanese messages and they just didn't feel like taking any chances. "How ~~could~~ can the technicians be so sure as they say they are?" they asked over and over again. I don't know how many millions of dollars were spent needlessly in establishing means for inter-communication with the British. By this I mean that we had to make an adaptor for this machine so

that it could inter-communicate with the British TYPEX and the British had to make an adaptor for their machine to inter-communicate with the ECM-SIGABA. It was a wholly unnecessary expense, I think, but by the end of 1953 we were able to convince the authorities that it would be all right and finally the British were allowed to have our machines until they could complete their developments and be on their own. I think ~~even at the present time~~ they still have some of our machines, but they're supposed to turn them back in due course. I can explain the basic principle of the machine. Here are ~~the~~ its essential elements: ~~in the machine:~~ a set of five ciphering rotors here, and another set of five control rotors here, making a set of ten altogether. Since the ~~These~~ rotors are all interchangeable, ~~as you see that~~ to ~~begin with~~ there can be a great number of permutations from a primary set of ten rotors. It's greater than 10! because the rotors can be inserted right-side up or upside down; in fact, the number is 20×18×16...×2. And if you have a set of [illegible] from which you can select 10, as is now the case, the number becomes very much greater. Now there are four inputs in this row of control rotors and their output ~~goes~~ governs to control the stepping of the five cryptographic rotors in a very erratic manner. This ~~so that the stepping of these rotors is very erratic according to the output of the control rotors. Here is another~~ set of ~~rotors,~~ five small rotors ~~ones, which are used to~~ permute the output of the control rotors, adding an additional valuable keying element.

We know of no case of solution of this machine and system ~~at all~~ throughout the war, and it is still in service as a high-grade off-line machine. During its use in World War II there was one possible compromise and it raised quite a storm at the time. The 28th Division bivouacked for the night in a small city in France and the vehicle containing the cryptomaterial and the SIGABAs was stationed in front of the place where the Signal Officer and his entourage were quartered for the night. Unfortunately no guard was posted to safeguard the van. In the morning that

vehicle was missing. Warning messages were sent instantly to Washington and there was a great to-do. The Army set up blockades on all the roads, the idea being to make sure that the truck wasn't being carried off by some German outfit, but nothing turned up. The Engineer Corps even diverted a river and sure enough all found the cipher machines and the cryptomaterial in the river. The van had been stolen by Frenchmen purely for the vehicle; its contents were of no interest to them. The episode was one which caused the Signal Officer to be tried by court martial, as were several others. We had very strict rules indeed about safeguarding this gadget, and in mentioning this point I should say that we weren't worried by the thought that our messages could be read if the Germans would capture one. We were worried by the thought that they would learn how good it was and would copy it--thus cutting off our COMINT. One of the funny things about our not giving the machine to the British when they needed it so desperately I can hardly refrain from telling you. I mentioned the strict rules about safeguarding it--who could see the thing, who could service it, and so on, and we saw to it that these rules were followed. But there came a time in North Africa when our maintenance men were knocked off and there was nobody to service the machines. However, there was a very skillful British Officer, an electrical engineer, He serviced and maintained our SIGABAs there for a while. When he got back to London, he built a machine based upon the ECM-SIGABA principle!

I want to show you next the Enigma, the cipher machine used very extensively by the German Armed Forces in World War II. This was a modification

of their commercial Enigma machine but an important modification, I think you can see it better on the next slide. Here are the rotors--they are exactly the same physically as they are on the commercial model, but with different wirings of course. Now let's see what the modification was--the addition of a plug board by means of which one could change the connections between the keys of the keyboard and the lamps on the lightbank. There were 13 plugs and jacks and this number was not chosen by accident; they apparently had mathematicians figure out absolutely the best number of plugging arrangements for this particular machine. There were certain weaknesses in the German Military Enigma but the absolutely fatal weakness was that they couldn't, or at least they didn't, change their rotor wirings at all throughout the war. Without the rotor wirings we couldn't have done anything with their traffic; but with them we were able to read practically all of it. ~~The Germans tried to make a printing model with eight wheels but it wasn't a success. We captured this model in 1945.~~ I'll come back to the Enigma in the next period. The Naval Enigma was much like the Army and Air Force machine except it had one more wheel and the rotor wirings were different.

Now we come to the development of cipher machines for teleprinter communications. With the ever-increasing speed of communications, it was necessary to speed up this business of protecting the contents of messages by cryptography. This was recognized a long time ago. In 1919, for example, the A.T. & T. Company engineers, in collaboration with the Signal Corps, devised this modification of the then standard printing-telegraph machine to make it a printing-telegraph

using circular key tapes of random characters.

cipher machine. This is the way it was done. Here is the keyboard for punching out the plain-text message; here is an ordinary tape transmitter, which took the plain-text tape and put the signals on the telegraph line; but here there were two additional transmitters through which key-tapes were passed. These were composed of random-punched characters, the tapes being joined at their ends to form two circular tapes, and they were of different diameters. To begin with the A.T. & T. started out with one tape 1,000 characters in length and the other 999, so you can see if the tapes start at an initial point, they would not return to the original pair of starting points until the shorter tape had made 999 revolutions, the longer one 1,000, that is, the interaction of the two tapes produced a key that was 999,000 characters in length. So there were three tape transmitters interacting, one for the plain-text tape, two for the key tapes. Great faith was placed in this machine but it was not put into use until the war was over. By that time I had come back from France, rejoined the Riverbank Laboratories and accepted a challenge to solve this kind of cipher system. It's too long a story to go into right now but as a result of the solution the Army dropped the project. I think it was in a way too bad, and I suppose some of the responsibility lies on my shoulders, because when we had a need for teleprinter ciphering in the early days of 1942 we actually went back to this ting. The big trouble of course was the production and distribution of the key tapes, and it is a ~~manufacturing key tapes is one~~ problem of which is still with us. Here's an early model

of a machine for making key tapes. We improved such machines very greatly in the next year or two, so that we could produce hundreds of thousands of good tapes in a hurry. Our modern key-tape manufacturing apparatus uses a key generator for producing electronically the random impulses for punching the tapes.

Next I show another commercial development for teleprinter ciphering, one by the I. T. & T. Co., who employed Colonel Parker Hitt after he had retired from the Army in about 1925. The machine presumably was to incorporate a very secure principle, since Colonel Hitt was well acquainted with cryptology. But I am sorry to tell you that it wasn't a secure principle that he employed. A demonstration equipment was installed in the State Department and the Army cryptanalysts were asked to test its security. Some messages prepared by the State Department's Chief of Communications were solved in a hurry. I had the unpleasant task of telling Colonel Hitt that I wasn't at liberty to tell him what the trouble was. This was our fixed policy in the Office of the Chief Signal Officer, and I think it was an understandable one. If we undertook to tell all inventors what the trouble is with their inventions we would never get anything else done but look into their successive modifications. We would this bring them up-to-date in cryptanalysis, too, and this is certainly not advisable as regards the run-of-mine or would-be inventors of crypto-apparatus.

This is the device which the Army developed in 1942-43, a rotor machine, the SIGCUM, and used very successfully to encipher teletype communications. ~~We called it the SIGCUM, and modifications of it are still in service.~~ It uses not perforated tapes but rotors, meters which step

in an erratic fashion but not as erratic as in the ECM-SIGABA. The SIGCUM and its successors had weaknesses; every once in a while, when we discovered cryptanalytic techniques, new ways of doing things, we found that SIGCUM had weaknesses which could be exploited; whereupon we would proceed to tighten up things by changes in the method of usage or the method of stepping the rotors, and so on. Here's a picture of the entire SIGCUM unit with the teletype-signal mixing unit--the big set here--most of which was unnecessary. The mixing apparatus takes the signals from here and mixes them with the SIGCUM, then putting the enciphered signals out on the line.

Now we have to say a few words about certain other types of ciphering apparatus. For example, it is necessary to send weather maps, situation maps, and other types of maps important for successful military operations, and so it was desirable to have a machine which would encipher and decipher facsimile. The generic name we gave to machines for ciphering facsimile was cifax. Here is one such machine that was developed by Army for the purpose, called SIGMEW. We also had need for machines that would impose security protection upon telephone conversations, machines with the generic name ciphony equipments; here's the first shot at it--a development by the Bell Telephone Laboratories, called SIGJIP. It was a gyp in a way--it gave you much more feeling of security than was warranted by the circumstances. Conversations enciphered by means of that thing could be read very readily and we all knew this but it was only an interim piece of equipment. The Telephone Company proceeded with its work, in collaboration with engineers from the Signal Intelligence Service and the Signal Corps,

and a very high-grade ciphony system which became known as SIGSALY was finally developed. Each terminal cost over a million dollars and there were a total of seven of them. ~~This is just one piece of apparatus--~~The two ends of the circuit were kept in synchrony by means of a very-very high grade record-playing mechanism. The SIGSALY turned out to be extremely useful.

Now in addition to cifax and ciphony we tried to develop practical cipher machines for other purposes, such as recognition, identification, IFF, callsign machines, etc. This is a war-time callsign machine developed by the U.S. Navy. It was based upon an algebraic principle described in a paper in one of the American mathematical journals; it appealed to me but I could never get the Army to go in for callsign changes in a big way. The Navy did, however, and this principle was incorporated in a call-sign ciphering machine for Navy communications. A good machine was developed and I think it is still in service.

Sooner or later--and I think the sooner the better--we will have to have ciphering apparatus for protecting telemetering signals, television signals, homing beacons, etc.--for anything in the way of a signal is going to have to have means and mechanisms for security protection.

The professional cryptologist is always amused by the almost invariable reference by the layman to "the German code", "the Japanese code","the U.S. code, etc. To give an idea as to how fallacious such a notion is, I will say as I said once before, there are hundreds of systems in simultaneous use in the communication services of all large governments.

This slide shows the number of cryptographic systems in effect on 7 December 1951 until October 1945 in the U.S. Army alone. There were literally hundreds of them. The next slide shows the number of holders of cryptographic materials during the same period, December 1941-October 1945, and, mind you, this is U.S. Army and U.S. Army Air Corps alone. It does not consider U.S. Navy, which had as great or perhaps greater distribution, nor the State Department, the Treasury, and the many other agencies that use cryptography.

Keeping track of crypto-material and accounting for it is a big headache. There is no way of getting around this that I know of and it is important that the rules for the protection of the material be followed absolutely to the letter. ~~I'm going to show you as my wind-up two slides.~~ The Japanese also had very ~~definite and~~ detailed rules for accounting for crypto-material. They were supposed to burn the codebooks, the cipher keys, the cipher tables, and so on. They were enjoined to scatter the ashes and then make a certificate, witnessed by a fellow officer, as to the complete destruction of the material. Occasionally these certificates were sent by radio and then we would find a case like this, where two chaps had certified the destruction, by burning and the scattering of the ashes, but one chap was observed by binoculars when he took a spade and dug a hole, dumped the codebooks and the tables in that hole, and poured in some water. ~~In that hole.~~ Well, in due time, some of our people sneaked out, dug into the hole, got out the material and brought it in. And there it is, being dried out. This recovery of crypto-material helped a great deal because it saved us an enormous amount of time and labor to reconstruct that particular code and set of tables. There were

instances of this sort every now and then. By the way, the Japanese were worried about this business of their security. They sensed that something about their secrecy systems was wrong and the only thing that they could imagine was that there were spies all 'round them. There were messages all the time requiring the commands to go through their quarters and look under the beds and into all closets, hunting for spies. Of course, that wasn't the case at all; we were solving their codes and ciphers because they were not secure.

You have seen the important World War II developments in crypto-apparatus and now it's time I showed you a bit of the new ones. In general the trend has been toward these things: making the machine more manageable as to size and weight, by miniaturization, the use of transistors and other solid state components, and by better packaging; next, by making the machines more secure, by incorporating better or more advanced crypto-principles, and particularly by simplifying the procedures. The aim of this last set of improvements, simplification, is accomplished wherever practicable, by eliminating as many features and procedures which, because of operators' errors, lead to crypto-security weaknesses. That is, we've been trying to make the machines as nearly automatic as is possible and practicable as regards their keying and functioning, so as to eliminate weaknesses caused by human error. We must take into account the fact that the machines have to be operated by human beings and human beings occasionally and inevitably make mistakes; they are prone to errors of omission

and commission. Experience has proved that in the past it has been these errors and not so much technical weaknesses in the cryptosystems and machines themselves that have made solution on a regular basis possible. This sort of practical experience means that the keying procedures should be made simpler, and, if possible, entirely automatic so far as concerns the human operator and user of the machine and system. Complexities can be introduced, incorporated, or applied at NSA, where there are extremely well-trained and experienced crypto-engineers and their helpers.

You understand, I'm sure, that we depend for crypto-security not on keeping the construction or design of the machines deep secrets. This means that even if copies of them fall into enemy hands, by capture or otherwise, the machines must be based upon crypto-principles such that without possession of the exact key for the day, the period, or the messages themselves, the enemy cannot learn the contents of the messages--ever, or at least for a very large number of years--by cryptanalysis. At the same time there is a real point in keeping the machine, apparatus, or system itself in a classified status as long as possible, because in the case of well-designed crypto-apparatus if you don't even know what the machine looks like, or its general principles of ciphering, you can't even make a start at cryptanalysis, or, to be more accurate, it will take a considerable length of time and more or less involved study to ascertain what you must know before you can make an attack on the messages with some hope of success. In a nutshell, then, we keep the machines in a classified status

as long as possible in order to delay the enemy's real attack on the traffic enciphered by the machines. But, of course, there's the other reason I've already mentioned: to prevent a potential enemy from copying our machines and turning our own weapons against us.

Now let's see pictures of some of the new apparatus.

Here's a machine designated the KW-3. It is an off-line teleprinter cipher machine but it has all the conveniences of an on-line machine and eliminates some of the weaknesses of the latter. The machine generates the key as well as the indicators for messages. All the operator has to do is to type the address, punch a starting key on the machine, and then proceed to type off the plain text of the messages, whereupon a cipher tape is produced, which can be put on any teleprinter circuit for transmission. At the receiving center the operator puts the cipher tape into a reading head, the start button is pushed, the message sets up its indicator and key, and the tape produced is the plain text of the original message. The KW-3 is becoming the real work-horse of our Armed Forces high-command cryptocommunications.

Next I show the KW-37 designed for Navy Fox or broadcast transmissions, a machine which embodies a teletype printer and uses an IBM card for keying purposes. So far as the communication center aboard ship is concerned, the operators don't even see the cipher--the messages arrive there in plain language. The ciphering is done elsewhere on the ship. This system is a synchronous one, meaning that both ends of the circuit are constantly and automatically kept in step; also, and related to this fact is the fact that the system is such that the intercepting enemy can't tell when a message is being transmitted and when the circuit is idling, giving what we call "link security," a very important element in communication security.

Insert

For field use we now have in place of Converter M-209 a small off-line high security machine designated the AFSAM-7. It has a keyboard and prints the cipher text. For electric power it uses any 24-volt source. This machine is now the work-horse for tactical cryptocommunications, and, by the way, several thousands of them have been issued to our NATO allies.

Next we have the KY-3, a ciphony or telephone security equipment. It has very high security and excellent quality, and is not a push-to-talk machine. It's range is 10-15 miles but this can be extended with good repeaters.

Here's the KY-8, a smaller version of the KY-3, occupying less than one cubic foot space and weighing between 10 and 15 pounds. It's for air-to-air and air-to-ground talk with high security.

Next we see the KY-9, a great improvement over its predecessors, one of which was the SIGSALY I mentioned a few minutes ago. It uses the vocoder principle, which yields talk that is intelligible but of poor quality. What it lacks in that respect it makes up by having excellent reliability. Moreover, you can use it on any commercial telephone circuit in the U.S. or circuits of equivalent quality abroad. For comparison as to size I show you again a SIGSALY terminal of World War II days, which cost over $1,000,000. The KY-9 gives equal security and costs only about $60,000.

Finally, I show you the KY-11, the crypto-portion of a microwave telephone system. We have this between Fort Meade and our former headquarters at the Navy Security Station in Washington where our COMSEC operations are conducted, and where also is located the Navy Security Group. The telephone micro-link is rented from the telephone company. We also have a similar link between the Navy Security Station and Arlington Hall Station where the headquarters of the Army Security Agency are located.

But with all these modern improvements I don't think the day has yet dawned when the human factors that make for crypto-insecurity have been altogether eliminated. Perhaps it's true that at the moment it can be said that cryptographic COMSEC technology is ahead of COMINT technology; but with ever-increasing speed of electronic analytic apparatus the gap can and perhaps will be closed, unless the COMSEC engineers keep pace with that apparatus. In short, it is the age-old battle between armor and armor-piercing projectiles. In the meantime, communicators must keep their guard up and enforce the rules supplied them for operating this crypto-equipment. In closing this period let me remind you of that introductory slogan: "Don't learn your COMSEC rules by accident."

In what I've just showed you'll notice the emphasis placed on telephone security devices and systems, and on automatic teleprinting systems. The days of hand-operated devices is over, and those of semi-automatic off-line cryptographic machines are drawing to a close. And, last to be mentioned, NSA crypto-engineers are doing development work in civision systems--enciphered television--which will doubtless come into use within a few years.