THIRD 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 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 think the slogan useful as a sub-title for my talk but I'll modify it a little--"Don't learn your COMSEC laws by accident." I begin my talk by reading the Webster Dictionary definition of the word "accident". I know, of course, that perhaps only a few of you will ever be directly concerned with COMSEC duties, but as potential future commanders of fighting units the definition of the word "accident" should be of real interest in connection with with 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."

I will now make the definition relevant by reminding you of a minor
~~Having defined the word, I will now proceed to make the definition~~

but nevertheless quite
~~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, accompanied by a good many VIP's, journeyed several times half-way around the world to attend special conferences. They apparently could go with safety almost anywhere . They met with no accidents. 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/ maybe it was Jimmy Walker, then Mayor of New York City, but it is decidedly applicable in this case: "Accidents don't happen, they are brought about". U.S. Navy communications intelligence experts were quite regularly reading practically all the Japanese Navy's messages because its crypto-systems were not secure In the case of Yamamoto's inspection trip our Navy had his schedule down pat to the day, hour and very minute

They also knew what his air escort would be, and so on. It was relatively easy to bring about the "accident" Yamamoto was to suffer, and it's obvious that his death was no accident in the dictionary sense of that word--it was brought about because his communications were insecure. 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 <u>Forrestal Diaries</u>, 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 realise why and how what had happened to them had come about, and recently published books by Japanese

Navy 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 as an aside what Wenger told as to disbelief in decrypts.)

It is hardly necessary to tell you that with the advances made in the invention and development of ~~[illegible]~~ weapons of warfare, including communication systems, the old so-called "pencil-and-paper ciphers", the hand-operated small cipher devices, and the codes ~~[illegible]~~ of former days became ~~[illegible]~~ 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 or electronic apparatus, speed in crypto-communications would at least begin to approach the ever-increasing speed of electrical communications. ~~[illegible]~~ 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 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 in addition~~ Greater security was needed because ~~the weapons of~~ cryptanalysis had been made much more effective by advances in that science, aided 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.

45. Aside from the much earlier Scytale used by the ancient Greeks, the earliest cipher device known to history is the cipher disk, first described by an Italian cryptographer named Alberti, who wrote a treatise on ciphers in Rome about 147Ø. ~~His is the oldest tract on cryptography that the world possesses.~~

45.1 The next slide shows a similar sort of wheel which appeared many years later in a book by another Italian cryptographer, Porta, who recommends the use of the cipher disk with keywords. I have the Porta Book with me.

45.4 The next slide pictures the U.S. Army Cipher Disk, which was used in the period 1914-1918, and which follows exactly the same principles that Alberti recommended. It seems to have taken a long time for the Signal Corps to get caught up with Alberti!

47 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.

48 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 187Ø. It is not just a simple cipher disk. 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 44 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 can now be made variable mixed sequences, whereas before, in the original Wheatstone, only the inner alphabet could be varied. In fact, a good many were just about to be issued to field units, not only Britisn 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 and they were withdrawn. I had something to do with demonstrating the insecurity of the device and when I reached American GHQ in France about three months later I found I wasn't a bit popular with certain British, French and American cryptologists. Reliance continued to be placed in codes.

444 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 20 letters at a time (because there are 20 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 never got anywhere in his attempts to get the Army to adopt any of his ciphers.

160
160 1 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/the interesting items in my collection. Here is a better model, one he
50.4 made in 1915, with the paper strips mounted on wood--wooden sliders. That
159 device was brought to the attention of the then Signal Corps Major Mauborgne 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. Am here's
50.3 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, used by the Army, the Navy, the Coast
Guard, and the Treasury. A couple of years after the M-94 was put into service
a friend showed me a write-up of something he'd come across more or less accidentally
in the Library of Congress, among the papers of Thomas Jefferson. Jefferson was
the first to invent the cipher cylinder principle, and he anticipated the Frenchman,
50 Bazeries, by a century. Here is the first page of his description of his device,
50.1
which he called "The Wheel Cypher." 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
cryptologists soon came to the conclusion that security would be much increased
by the use of changeable instead of fixed alphabets. Among other versions, I had
one made which used metal rings on which we could mount slips of paper and fasten
them; thus we could change the alphabets as often as was felt necessary. Navy
tried other versions. That was the beginning of the various forms of strip
cipher devices used by the Armed Forces, and later by the State Department and
50.11 the Treasury Department. Here is a picture of the final Army strip cipher device.
The strip ciphers carried an enormous amount of traffic.

54 Next we come to a machine called the Kryha, invented by a German, in about
the year 1925. According to its inventor the Kryha was the last word in the way of
mechanical cryptographs, and he tried to interest various governments in his
machine. There isn't time to explain the machine, but

~~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

55 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 nothing or 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 same sequence of alphabets, producing a condition which the cryptologist calls "depth". When this is the case he proceeds to solve the set of messages vertically, column by column, and when he's finished he can read the messages horizontally. ~~and~~ eureka! the business is successfully ~~terminated~~. When known alphabets are used the trick can be done with just two messages.

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 high-security, electrically-~~operated~~ machine for ~~mean echelon~~ high-command use. Let us take up the first of these two types and see what happened.

171 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 ~~unable~~ not permitted even to know what

was being built until the final model was completed and ready to be delivered to us. 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. There's the machine, take it with you." The Colonel never was given the opportunity to improve his model, ~~[illegible]~~ because the crypto-principle was very faulty and the laboratories development ~~[illegible] but he never was given the opportunity to carry out that plan, because~~ came to a sudden and ignominious end. The whole development represented a loss ~~the crypto-principle was very faulty; it didn't take very much time to read~~ which wasted what little money we had for such business. ~~test messages put up by my chief himself, and the laboratories development came to an ignominious end. The whole development represented a loss of time and energy and moreover, it wasted what little money we had for such business. But I'm glad to say that that chief of the laboratories was an unusual Colonel; those who came later were much more inclined to take advice from persons experienced in the field of cryptology.~~

171

Now we come to a development which is of considerable interest to us.

164. 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 all the services used 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 ~~simply accepted it.~~ It turned out, ~~I think,~~ that my superiors were right, for our troops at least had something 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, or the strip cipher device--all too slow.

Now just a bit about Mr. Hagelin. He did what I best describe as a hysteron-proteron. That'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 not at all a poor sort of hysteron-proteron if you're going to do one.

63 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. ~~It is a very interesting device.~~ From that prototype he built better models and interested the Signal Corps in them. As a consequence we built in America, for World War II, this six-wheel Hagelin machine, which many of you no doubt know as Converter M-209. ~~[illegible]~~ We built the M-209 according to American inch-measurements and specifications, and with American tools, rather

than European metric measurements and tools, and we built an astonishing number of them--over one hundred and ten thousand.

[illegible]

Many of you may know that the M-209 had a serious, a very serious security weakness, about which I'll say a few words later. This is a picture of one

70 3 of the Hagelin machines as modified by some of our GI's in Italy. The M-209 has no printing mechanism and you know how resourceful GI's can be. A couple of them scrounged parts here and there and improved their machine to make it a printing model. See, here's 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 will the damned thing work?"

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

I60.1 of one of his latest models--the CX-52. It prints not only the plain text but also the cipher text, and it incorporated a much improved ciphering mechanism, because the wheels, instead of being permanently fixed upon the shaft, are demountable and can be rearranged in 720 different ways. The stepping motion for these wheels is complicated [redacted]

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

for it. When there are several messages [redacted]

That is the fatal weakness of machines of the type of the M-2Ø9 and is the big problem in connection with the use of what we call key-generator types of devices. A cipher machine which has been built and proposed for use by the Marine Corps is a double M-2Ø9 machine, and it is an improvement security-wise over the single M-2Ø9, but I'm sorry to say that it too has the [redacted] I think we will have something better very soon, and I've brought a model to show you. It doesn't have the weakness of the M-2Ø9, and has a much higher degree of security. Moreover, it requires no source of electrical power--not even a dry cell--and it produces a printed record.

I'll show you a picture of it later.

Now for 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 in Stockholm--was not a real rotor device of the type we use today but I don't want to go into details. I merely want to show the device, which is 59 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'd press a key and a light would light; you'd have to write down the letter flashed on the light bank and then the cipher wheels would step.

The next forward step was taken when Hagelin made the printing mechanism 65 an integral part of the machine itself. Here is the keyboard, the printing mechanism is in here, and now the whole assembly is very much s.aller and more compact.

57 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, a set of electric wheels called rotors, and a small dry cell for power. In this case the enciphering-deciphering circuitry is more complicated; it goes from a key of the keyboard, then through a contact on a fixed entry plate or stator into these stepping rotors,and by means of a reflector or reversing plate, back through the cipher rotors to one of a bank of lights, so that the current goes through the rotors twice, which complicates things a good deal. ~~This reflector or reversing rotor is a very important feature of this machine~~ Each time a key is depress'at least one rotor steps forward and the stepping of the rotors is such that the machine has a rather short cycle as such things go, less than 26^3; it was a little less than 23^3 because of certain factors into which it isn't necessary to go.

I'm going to take the various developments of rotor machines 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 rotor *11 machines. First, I show a picture of the late Mr. Edward H. Hebern, a Californian, who seems independently to have thought of rotor machines. I asked Mr. Hebern one day how he happened to get started on such things and he said, "Well, you see I was in ,ail". 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
172 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 it after he got out of jail. It has a keyboard,
a left-hand stator, that is, a ring of 26 stationery contacts arranged in a
circular fashion to one of which the current goes when a keyboard key is
depressed; 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. There was just one rotor in his first model, which he built in
1922 or 1923 for the Klu Klux Klan. Here is the first printing model made by
711 Mr. Hebern--still a one-rotor machine--with a keyboard and, now, an electric
typewriter connected thereto. 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, showing that at an early date
71.2 he conceived the idea of variable connections in rotors. This is an extremely
71.3 important feature in any kind of a high-security rotor machine. This shows his next step.
712 1 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
72 show his next development--a 5-rotor machine. Here are the rotors removed
73 from the machine to show you what they look like. They were still variable

connection changers--you could take wires and rearrange them as and when you pleased. 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 they absolutely had to have secure means for speedier communications from Washington to the Fleet Commanders and, of course, for intra-fleet communications. The Navy thought this Hebern model a suitable machine and they got an appropriation for the purpose, a large sum of money for those days, $75,000. 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 of its security. I had no machine and the Navy had only two, both undergoing service tests. But 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 crossed-eyes, pug-nose 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 test of one of the messages to 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

~~letters which were the same but I didn't know what letters. 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, 165 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 Navy Department clerk 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 40¢ and sold it in the northern part of the state at about $2.00. The California Blue Sky Laws didn't like that sort of conduct and Mr. Hebern spent a year in prison, / giving him lots of time and opportunity to think up improvements on his machine. ~~I saved the paper which had the text of the first message~~

~~I hope you won't think I am immodest by showing this. I saved the paper which~~

Despite my solution we thought that the Hebern principle was still a good one and Navy went ahead with Mr. Hebern after he got out of prison. 172.1Ø Here's a picture of the last machine he built for the Navy. Hebern wanted to get paid for it naturally, but there was just one hitch--the machine wouldn't work and when this was pointed out to him 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, a laboratory being established in the Navy Yard. Years later the Hebern heirs brought suit in the United States Court of Claims against the United States for $5Ø,ØØØ,ØØØ, which was settled last summer at a considerable discount, $3Ø,ØØØ.

I'm going to show you now a few slides of the Army developments in rotor-type 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, in Washington had at developing a machine for the Army. It 17Ø. 7 had a keyboard, a light-bank, 5 rotors, and now an interesting feature--an external keying mechanism. I had come to the conclusion that internal control mechanisms for stepping rotors had a fundamental weakness; that is, 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 safe, especially if the tapes aren't overburdened in usage. [~~This is another view of the same machine. Here is the tape transmitter, the rotors, the keyboard, an electromatic typewriter, etc. I think this was one of the very early models.~~] We had boxes of about 100 key tapes from which you could make the selection for the day according to the keying document. A serious practical weakness, of course, was the necessity for production and distribution of tapes. 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 listened to you inventors we'd never get anything out." So we had to put the idea on ice, that is, in secrecy.

172.4 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 wires 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 ~~[illegible]~~ produced a key sequence ~~[illegible]~~ 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 such a machine had been ~~[illegible]~~ 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 or I have to do to get it released so that you can 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 current ~~[illegible]~~ 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. 173 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 any inter-communication at all in World War II. ~~The only thing that we had for a good many years was a very slow, hand-operated cipher using pencil and paper, which had been adopted way back in [illegible]. The strip cipher device was then adopted for all joint communications until the ECM-SIGABA came into use, just in good time, and it was used~~ The ECM-SIGABA came into use just in good time, and it was used with great satisfaction on both sides. I might add, in closing that incident, 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, ~~[illegible]~~ ~~although it was our policy on the highest level of the Army and Navy to~~ it was U.S. policy on the highest level in both the Army and the Navy to withhold our 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 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 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 chance. "How 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, perhaps entirely needlessly, ~~needlessly~~ in establishing means for inter-communication with the British. By this I mean

that we had to develop, produce, and use an adaptor for our machine so that it
177 could inter-communicate with the British TYPEX, and the British had to do the
same for their machine to inter-communicate with the ECM-SIGABA. 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 it would be nice if
there were time to explain the crypto-principles of the ECM-SIGABA but suffice
it to say that we know of no case of solution of this machine and system
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 which raised
quite a storm when it was discovered that some Frenchman had liberated a U.S.
Army truck and trailer--the latter carrying all the 28th Division's HQ cipher
machines and materiel. But the stuff was soon found where it had been dumped
by the Frenchmen--in a nearby river. The episode was one which caused the
Signal Officer and other officers to be tried by court martial. We had and
still have 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. I can hardly refrain from telling you one of the funny
things about our not giving the machine to the British when they needed it so
desperately. 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 strictly enforced. But there came a time in North Africa when all our maintenance men were knocked off and there was nobody to service the machines. However, a very skillful British RAF Officer, an electrical engineer was pressed into service and he maintained our SIGABAs there for a while. I'm sure you won't be astonished to learn that when he got back to London he built for the RAF a machine based upon the ECM-SIGABA principle!

I want to show you next the cipher machine which was used very extensively
74 / by all the German Armed Forces in World War II. This was a modification of their commercial Enigma machine but an important modification, introduced when Hitler came into power, at which time the commercial model was withdrawn from the market. [redacted]

[redacted] Here are the rotors--they are exactly the same physically as they were 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. [redacted] The Naval Enigma was much like the Army and Air Force machine except that it had one more wheel and the rotor wirings were different. [redacted]

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 56 the then standard printing-telegraph machine to make it a printing-telegraph

cipher machine, using circular key tapes of random characters. 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, because when we had a need for teleprinter ciphering in the early days of 1942 we actually had nothing except this thing. The big trouble of course was the production and distribution of
258 these key tapes, and it is a problem 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.

178
179 This is a rotor machine, the SIGCUM, which the Army developed in 1942-43 and used very successfully to encipher teletype communications. It uses not perforated tapes but rotors which step in an erratic fashion but not as erratic as in the ECM-SIGABA. But even while in service, it had weaknesses; every once in a while, when we discovered new cryptanalytic techniques, 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. The machines are still in use, doing valiant service because we were able to incorporate more and more improved features in it. Its new designation is KW-2.

Now we have to say a few words about certain other types of ciphering
apparatus. For example, it is necessary to send, with security, weather and
situation maps, and so it was desirable to have a machine which can 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,
183 called SIGMEW. We also had need for machines for enciphering telephone conversations,
machines with the generic name *siphony* equipments; here's the first shot at it--
185 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
siphony system which became known as SIGSALY was finally developed and was
extremely successful. Each terminal cost over a million dollars and there were
seven of them.

The professional cryptologist is always amused by the almost invariable reference by the layman to "*the* German code", "*the* Japanese code", "*the* U.S. Navy code", etc. To give an idea as to how fallacious such a notion is, I will say that there are hundreds of systems in simultaneous use in the communication services of all large governments. You not only have to have different kinds to meet specific types of communications but you have to divide up the traffic for two reasons;

first, so as not to overload one system beyond the safety limit, and second, so that not everybody can read everybody else's messages, even in the same family. The Midway leak happened primarily because this last principle wasn't in effect at that time in U.S. Naval communications.

23b 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 number of holders of cryptographic materials was almost 6,000, -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. 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. Well, in due time, some of our people sneaked out, dug into the hole, got out the material and brought it in and 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, conceived, developed and in some cases produced by the now centralized cryptologic agency of the Armed Forces, the National Security Agency. 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 ~~as~~ 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 the machines must be based upon crypto-principles such that even if the machines fall into enemy hands, by capture or otherwise, without possession of the exact key for the day, for the period, or for each individual message itself, the enemy can never learn by cryptanalysis the contents of the messages, or at least he can't for a very large number of years. 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, which will soon be ready for issue.

For field use we now have in place of Converter M-209 a small off-line KL-7 high security machine designated the K$\overset{L}{\text{W}}$-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.

K- 7 Next we have the KW-9, an on-line or off-line teletype encipherment machine that uses rotors instead of key tapes and is very much safer than the old SIGCUM KW-26 or KW-2 I showed you. Here we have the new KW-26, which is in fact becoming the work-horse of fixed station teletype long-range communication systems. It is an on-line synchronous teletype cipher system with link-encryption, that is, so far as enemy intercept is concerned it is impossible to tell when the circuit is idle and when it is carrying a message.

This and the next slide are a bit out of order but I didn't have glass slides for them and have to use the small 35 mm. ones. This one showing the (KL-36)KL-36 is the one I mentioned before as having been developed for the Marine Corps. The next one is the pneumatic rotor machine that we think would serve the needs (KL-17)better than the KL-36 and be far safer.

X-27 Here's a machine designated the KW-3, now undergoing test. 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 will become the real work-horse of our Armed Forces high-command cryptocommunications.

X-28 Next I show the KW-37, designed for Navy Fox or broadcast transmissions, and now undergoing service test. It is a machine which embodies a teletype printer and uses an IBM card for keying purposes. So far as the ship is concerned, the radio operators aboard won't even see the cipher--the messages within the communication center aboard will be in plain language; the ciphering is done elsewhere on the ship. The 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.

X-29 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

X-30 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.

X-31 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
X-33 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.

X-32 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.

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.

But with all these modern improvements I don't think the day has yet dawned when it can be said that human factors that make for crypto-insecurity have been altogether eliminated. Perhaps it's true that at the moment COMSEC technology can be said to be 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 their crypto-equipments. In closing this period let me remind you of the following: (1) that the establishment and maintenance of communications security is a responsibility of command; (2) that there aren't any short-cuts to achieving communications security; and (3) that the rules of COMSEC must be followed to the letter by everybody connected with COMSEC but most especially by crypto-operating personnel. If these reminders are followed, the chances are good that you won't learn your COMSEC rules by accident!

With the foregoing remarks I bring to a close my talk on COMINT and COMSEC. If there is any last word or impression that I would like to leave with you let it be that, in my opinion, COMSEC, though less spectacular and less interesting than COMINT, is by far the more important of the two. There are two reasons for this opinion. The first is that secrecy in the conduct of modern large-scale military operations, ground, sea, air, and para-military, is of the highest importance to their success; without secure communications there can be little or no secrecy, and without secrecy nearly every such operation is doomed. The second reason is one that is not so obvious. It is that your COMINT successes will soon be eliminated unless the communications over which the traffic and the final results must pass to reach those who can use them are secure. Therefore, COMSEC is doubly important, once and first, to protect our own plans and movements, and once again, or second, to protect our COMINT product and sources. I'd therefore like to present for your consideration and rumination the following statement of what I'll immodestly call Friedman's Law--something patterned after Professor Parkinson's Law: Your cryptologic coin, like any other coin, has two faces. If you're up against equal or even superior forces, and if the COMINT face of the coin is bright and shiny, your chances of winning are good--maybe and at times excellent; but if you let the COMSEC face of your coin become tarnished and dull, you'll sure as hell lose.

In thanking you for your patience in listening to my rather lengthy discourse and for your courtesy in paying such careful attention to what I have presented for your information, let me invite those of you who care to examine some of my exhibits to come up to the table here and we can look at them as long as you wish.