Third Period

"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."

omit

~~Here is another comment from Japanese Naval Officer:~~

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

~~Books~~ recently published ~~in Japan by~~ former Japanese ~~military~~ naval 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.)

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 in Russian communications which let the German fighter commands know exactly when our bombers left and where they were going. When found out what the trouble was, it was too late. This incident leads me to say that when you fight a war with allies their COMSEC weaknesses are bound to affect the security of your own forces; something must be done to eliminate those weaknesses, even at the risk of jeopardizing other important things. For instance, you may have to provide them with some of your own cryptomaterial, in which case you lose control of the continued secrecy of that material.

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

what we call Cipher Device, type M-94. Now, when Major Mauborgne 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 Mauborgne 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. [redacted] When after some six or so months nobody had solved his challenge messages Mauborgne went ahead and got the thing out, and [redacted] were thousands of them made. 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 write-up of something he'd come across more or less accidentally in the Library of Congress, among the papers of Thomas Jefferson. [redacted] 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

50. 50.1 device, 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 ~~variable~~ or 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 ~~variant~~ forms of strip cipher devices used by the Armed Forces, and later by the State Department and the Treasury Department. Here is a picture of the final Army ~~type of~~ strip cipher device. 50.11 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. Omit 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, ~~at the time,~~ and Mr. Kryha, he tried to interest various governments in his machine. I think I should explain it for those who have never seen it. There isn't time to explain the machine, but

which was ever solved 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 devise at that time for the solution of rotor machines and rotors in cascade are practically the same today ~~as they were over thirty-five years~~ ago. 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. 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, ~~They had~~ a laboratory being established in the Navy Yard, ~~with~~ a very able young man 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, which was settled last summer at a considerable discount, $30,000.

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 $30,000. That's quite a discount. I might say that [redacted] 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.

Omit

Now I'm going to show you 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 had a keyboard, a [redacted] light-bank, 5-rotors, and now an interesting feature--an external keying mechanism. [redacted] 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

170

170.7

is another view of the same machine--here is the tape transmitter, the rotors, [redacted] 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 necessity for The fatal weakness, of course, was the production and the distribution of the tapes. This was quite a headache and even when we used specially heavy paper for the tapes they would break after they had gone through a number of times. 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 listened to you, we'd never get anything out." So we had to 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 wires or flexible cables. They were tricky and gave rise to a lot of difficulty

17k.9

develop, produce, and use
that we had to ~~make~~ an adaptor for ~~this~~ our machine so that it could inter-communicate with the British TYPEX, and the British had to do the same ~~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 ~~they~~ it would be nice if there were time to explain the crypto-principles of the ECM-SIGABA 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 its essential elements: a set of five ciphering rotors here, and another set of five control rotors here, making a set of ten altogether. Since the rotors are all interchangeable, 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 x 18 x 16 ... x 2. And if you have a set of 20 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 governs the stepping of the five cryptographic rotors in a very erratic manner. This set of five small rotors permutes the output of the control rotors, adding an additional valuable keying element.

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 ~~and it~~ which raised quite a storm ~~at the time.~~ The 28th Division bivouacked for the night in a small city. When it was discovered that a French civilian had liberated a U.S. Army truck and trailer — the latter carrying all the 28th Division's HQ cipher machines and material — but the stuff was soon found where it had been dumped by the Frenchmen — in a nearby river.

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 blockaded 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. There was a possibility that the van had been stolen by Frenchmen purely for the vehicle, in which case its contents would be of no interest to them. Surely they'd get rid of that hot goods at the first opportunity, which would be to dump them in the nearest river. The Engineer Corps diverted that river and sure enough all the cipher machines and the crypto-material had been dumped into the river. The episode was one which caused the Signal Officer and other officers to be tried by court martial, ~~as were several other~~. 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 ~~after VE Day~~, 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. I think

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,ØØØ 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,ØØØ, that is, the interaction of the two tapes produced a key that was 99Ø,ØØØ 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 had nothing except went back to this thing. The big trouble of course was the production and distribution of these key tapes, and it is a problem which is still with us. Here's an early model

258 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 thus 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 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

But even while in service
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 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. 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, with security, weather and situation maps, and other types of maps important for successful military operations, and so it is desirable to have a machine which can encipher and decipher facsimile. The generic name we gave to machines for ciphering facsimile was cifax. Here 183 is one such machine that was developed by Army for the purpose, called SIGMEW. We also had need for machines for enciphering 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 185 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. 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.--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. 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.

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 ~~of them~~ the machines fall into enemy hands, by capture or otherwise, without possession of the exact key for the day, the period, or ~~the messages~~ for each individual message itself, the enemy ~~cannot learn~~ can never learn by cryptanalysis the contents of the messages, ~~never~~ or at least he can't 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

on-line or off-line

Next we have the KW-9, a teletype encipherment machine that uses rotors instead of key tapes and is very much safer than the old SIGCUM, or KW-2 I showed you. Here we have the new KW-26, which is fast 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 any enemy intercept is concerned it is impossible to tell when the circuit is idle and when it is carrying a message.

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 high security machine designated the ~~AFSAM-7~~ KW-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.

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 ~~is becoming~~ will become the real work-horse of our Armed Forces high-command cryptocommunications.

and now undergoing service test. It is

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 radio operators aboard won't even see the cipher--the messages ~~arrive~~ will be ~~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.

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 the 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: ~~of that introductory~~ slogan: "Don't learn your COMSEC rules by accident."

(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!

This and the next slide are a bit out of ~~st~~ 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 is KL-36 the one I mentioned before as having been developed for the Marine Corps. The next one is the pneumatic motor machine that we think would serve the needs KL-17 better than the KL-36 and be far safer.