Second Period

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

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

~~But before leaving~~

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

Before showing you a few of our newer machines I want to switch to another projector and this gives me a chance to show a few slides related to intercept work. Here's an antenna
I-1 field at Hof, Germany showing two types of masts and mobile intercept vans.
I-2 Next, an intercept operating position at a Navy station on Skaggs Island and
I-3 one at Bremerhaven. Practically all the equipment is specially designed and developed by or for NSA, and a great deal of the intercept is taken in record form, on magnetic tape as a rule.

Looked at from a purely philosophical or logical point of view, COMINT operations and activities should be, and in the U.S. Navy they are, conducted within ~~[illegible]~~ Naval Communication commands and by Naval Communications personnel. I think this is logical because they ~~and by and large,~~ ~~[illegible]~~ are certainly ~~operations and activities~~ the same ~~generically~~ as those conducted by any large organization for providing communications systems, that is, systems and means for getting messages from certain people to certain other people — we call them originators and addressees. The only and the principal difference between this ordinary type of communications and what goes on in the production of COMINT is that we interpose ourselves between the actual originators and intended addressees of the messages, that is, without their permission and often without even their knowledge, ~~in short we~~ we put ourselves on their distribution list. Of course, we're not furnished the keys and cryptomaterial ~~that~~ the ~~actual originators and the~~ intended addressees are provided with (to make unbuttoning the messages a direct and easy process; we have to find or work out the keys, and this is often very difficult but it has been done in the past and will probably be done again in ~~the~~ future wars. Lastly, there's the job of translating the messages — this usually involves making the necessary corrections and explanatory notes, sometimes. There is an important corollary to what I'm saying here and it is that the real key to success in the production of COMINT is excellence in our own communication systems. Unless we can get the traffic quickly and accurately back to where it can be worked on by the analysts and unless we have rapid and secure communications among the various analytical stations and also to those authorized to receive the final COMINT, you're conducting ~~an~~ were exercise, not a real operation.

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

Insert attached >

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

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

I'll now show a few of our newer machines, which
for the most part are specially designed high-speed
X-1 electronic digital computers. Here's one called ABNER II,
which uses a mercury tank for storage or memory. Next
X-2 is ALWAC III which is one of a set of ~~four~~ machines
remotely controlled so that four ~~different~~ analytic units can
call ~~upon~~ the machine into action to solve the same or different
but already programmed-for problems. This is a machine which can be used
when a job is too big for hand work and too
small for one of our ~~sea~~ large machines built to
handle really big and complex jobs, such as
X-3 ATLAS 2, Serial 1, which has a magnetic-drum ~~and~~ also an
electrostatic-tube storage system, the former for high-speed memory operations.
A newer ATLAS using magnetic cores for memory is
now under construction. In this next slide you'll
X-4 see how the substitution of solid state diodes such
as ~~transistors and~~ magnetic cores permits miniaturization. The slide shows ATLAS and alongside it BOGART, which does everything that ATLAS does but is much smaller and faster. ATLAS will be the last of the old style
machines using electronic tubes, ~~although our newer
machines will be faster and smaller because of
the elimination of nearly all tubes~~. Here's a larger view of
X-5 BOGART, and next I show you DUTCHESS which
X-6 does certain quite complex matching and crypt-

analytic operations with 5-digit code groups at the
rate of 50,000 groups per second. Next I show
X-9 you SOLO, a transistorized machine which has the
general capability of ATLAS and can operate at
megacycle speed — a million pulses a second.
I may add that NSA has, of course, a number of
other types of computers, including IBM's 704; in
fact, NSA has the largest collection of electronic
computers and data processing machines in the
world. It must have them in order to handle the
very large and complex analytical problems which
it is expected to handle.

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

With the foregoing remarks I bring to a close my talk on COMSEC and COMINT. If there is any last word or impression that I would like to leave with you let it be that in my opinion the former, though far less spectacular and interesting than the latter, is the more important of the two. There are two reasons for my opinion. The first is that secrecy in the conduct of military operations is of the highest importance to their success, and without secure communications there can be little or no secrecy. The second reason is one that is not so obvious. It is that your COMINT successes will be eliminated unless the communications over which the results must pass to reach those who can use them are secure. Therefore, COMSEC is doubly important, once for itself and once for COMINT protection. 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: A commander may win if he has good COMINT; but he will surely lose if he has poor COMSEC.

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

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

With the foregoing remarks I'll end my talk on COMSEC and COMINT. If there is any last word or impression that I would like to leave with you let it be that, in my opinion, the COMSEC ~~former~~, though ~~far~~ less spectacular and less interesting than ~~the latter~~ COMINT, is by far the more important of the two. There are two reasons for ~~my~~ this opinion. The first is that secrecy in the conduct of modern large-scale ground, sea, air, and para-military, military operations, is of the highest importance to their success; ~~and~~ 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, ~~for~~ itself and once again, or second, to protect our COMINT product and sources. ~~for~~ COMINT protection. 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: Substitute ~~A~~ Attached ~~commander may win if he has good COMINT; but he will surely lose if he has poor COMSEC.~~

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

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.

COMMUNICATIONS INTELLIGENCE

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

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

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

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

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

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

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

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

I have reference here to the Battle of the Bulge, wherein a serious catastrophe was barely averted because our G-2's had come to rely too heavily on COMINT, so that when it was unavailable they seemed to lack all information or at least they felt that way. I said that a serious catastrophe was barely averted but even so the losses were quite severe, as can be seen from the following:

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

What happened? Why?

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

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

Further on Baldwin notes that:

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

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

In what I read from TIME in the first period, the word "MAGIC" seemed to refer only to the machine that we reconstructed for solving Japanese Foreign Office communications. In reality the word MAGIC was used as a sort of code name among the initiated and indoctrinated persons who were entitled to receive the highly secret information that came from the solution of German, Italian, and Japanese secret communications. The term was introduced to us by the British when we began to play together in the cryptologic gardens; we found it useful and adopted it, too. Later on we came to use other secret words to designate this sort of intelligence and to change the words from time to time, for security reasons. Currently, COMINT is composed of three types or categories of intelligence, and by far the greatest part of it comes from intercepting, recording, and studying enemy radio traffic. The three types or categories are: (1) Special intelligence, which comes from the solution and processing of the encrypted messages themselves and the result is information of highest reliability because it comes, so to speak, "right out of the horse's mouth". (2) Traffic intelligence, which comes from the study of what are called "the externals" of those messages, data applicable to such things as their callsigns, the frequencies employed, the direction or routings, and so on and from this comes information from which inferences can be drawn; and (3) Weather intelligence, which comes from the study of the enemy's weather messages, which in wartime and even in peacetime to a certain degree, are encrypted. In this audience it's hardly necessary to mention how important a role the weather plays in the conduct of war. Recently NSA has also been assigned over-all responsibility for ELINT, or electronic intelligence, but I won't go into that in this talk.

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

It was in response to this third and last objective of COMINT that World War II gave a brilliant answer. I'm sure you would find the detailed story of the successes of Navy, Army, and Army Air Corps cryptanalysts, and of their opposite numbers in the British Services on German, Italian and Japanese messages in World War II highly interesting but there just isn't time. I think the contents of the Marshall-Dewey letter, from which I read a bit in the first period, will have to suffice. However, it in itself is sufficient to give you a pretty good idea of the contributions COMINT made toward our winning World War II. It is unfortunate that General Marshall's letter was disclosed during the Congressional Hearings for it's now in the public domain and its contents are undoubtedly now known in all the important chanceries and war offices of the world. General Marshall, you'll remember, in his letter to Governor Dewey, sent during the hot political campaign of 1944, was asking the Governor not to use certain information Dewey got by surreptitious channels. Here are some excellent illustrations of the manner of employment of COMINT:

> "Now the point to the present dilemma is that we have gone ahead with this business of deciphering their codes until we possess other codes, German as well as Japanese, but our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government. These are still in the codes involved in the Pearl Harbor events.
>
> "To explain further the critical nature of this set-up which would be wipted out almost in an instant if the least suspicion were aroused regarding it, the Battle of the Coral Sea was based on deciphered messages and therefore our few ships were in the right place at the right time. Further, we were able to concentrate on our limited forces to meet their advances on Midway when otherwise we almost certainly

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

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

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

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

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

* * * * * * * * * * * *

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

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

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

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

The next step after interception is traffic analysis, that is, the reconstruction of the radio nets of the enemy and the location of their transmitter stations. This gives very important information on two counts. First of all, establishing or reconstructing the nets gives you order of battle which is very important. The reconstruction of the networks is not an easy thing for when the callsigns and frequencies are changed rapidly. It is a curious thing that the Germans seemed to be able to change their callsigns and frequencies without too much trouble--it gave us and the British a good deal of trouble and we had to keep a good many people working at it all the time.

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

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

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

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

Now I will go back to COMINT processing and give you some information about cryptanalytic techniques and gadgetry. I venture to say that you all know the mental picture the average citizen has of a cryptanalyst, for the picture is a very old one, like the one I now show you, of Trithemius, whom I mentioned before. He's a long-haired egg-head; he wears thick spectacles, has long whiskers, with crumbs in them, he has grimy fingers and finger nails, and so on. This chap goes into a huddle all by and with himself and the cryptogram and sooner or later he comes up with the answer, shouting Eureka! Well, that picture is far from the truth these days, for cryptanalysis and COMINT is "big business" now--very big business indeed, because we're spending well over half a billion dollars on it every year now.

Cryptanalysis of modern crypto-systems has been facilitated, if not made possible, by the use and application of special cryptanalytic aids, including the use of high speed electronic machinery and digital computers, some of which I'll show in slides to come. Some are standard machines, but mostly we device and use modifications of them. More importantly, we have recently gone into the invention, development, and production of highly specialized electronic cryptanalytic gadgetry. At this point I must take a few moments to clarify the picture and in simple language tell you what gadgets do for us. As I said before, the mere number of permutations and combinations afforded by a cryptosystem <u>per se</u> isn't too significant; it's what they amount to or involve in terms of cryptographic meaningfulness and complexity. In modern cryptanalytic attacks on the crypto-communications of knowledgeable governments what you are up against are usually quite complex cryptosystems which generally involve, for their solution, the making of a great multiplicity of hypotheses each of which must be tested out, one after the other, until you find the correct one. The job of the cryptanalyst is to devise short cuts for testing the hypotheses, short cuts often based upon the use of statistics and statistical theories having to do with the relative frequency of letters, pairs or sets of letters, words, sets of words, and so on. Once having devised the proper test or tests for each hypothesis, or for several concurrent hypotheses, human labor could be set to work making the millions of tests in order to find the correct hypothesis or to cast out the vast majority of incorrect ones. When each test is complicated, or lengthy, it is obvious that you'd have to have, as we used to say, factorial n Chinamen to do the job, or else the job would take eons of time. But it is our experience that every test which can be made by hhand can be mechanized, and it is further our experience that in most cases it is practicable to build machines which will make the tests. I don't have to tell you that machines don't tire as rapidly as humans, they don't need much sleep, or time out for meals, or for recreation or for such things as shopping, love-making, etc.-- in short, the "care and feeding of machines" is a relatively much more simple matter than the "care and feeding of human beings." So, we have cryptanalysts who devise the tests; then we have cryptanalytic engineers who mechanize the tests, then devise, invent, develop, and produce the machines to perform the tests at high speed. We have to have maintenance engineers to keep the machines in good working order; and the cryptanalytic assistants who examine the output of the machines and who are usually able to take the correct hypothesis or few correct ones and go on with them to the final stage where a key is recovered. Next we may have to have other machines which apply the recovered keys to specific messages and produce the plain texts from them. But in all these steps, let me emphasize, the machines can do only one thing: they can only perform, at a high rate of speed, processes which the human brain and hand can perform but only at a much slower rate. Let me emphasize that these machines don't, they can't, replace the thinking processes involved in cryptanalysis.

This may be a good place to read a paragraph or two from a very recently published book by retired General Albert C. Wedemeyer to show you what misconceptions about cryptology can be entertained even on the highest levels. General Wedemeyer states, in connection with his discussion of U.S. culpability in the Japanese attack on Pearl Harbor,[1] that President Roosevelt had ample time to broadcast a warning, and he goes on to say:

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

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

[1] <u>Wedemeyer Reports</u>, Henry Holt & Co., New York, p. 438.

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

Now, I want to show you what some of these machines look like. Here is a highly-specialized World War II machine for deciphering messages; we call it an "analog" because although it does what the enemy's cryptosystem does, any resemblance between it and the enemy's machine is purely coincidental. To explain, I'll say this: In a cryptanalytic processing center, we try to duplicate with a few people what thousands of people on the enemy side are doing, for it takes thousands of soldiers to encipher and decipher the messages of the many headquarters involved in intercommunication. All these messages, or most of them are intercepted, they all flow into one place, and you can only have a certain number of people to process them. If you have the key or keys, then it becomes a problem of production-line deciphering; so we devise special machines to decipher the messages. As I said before, the machines may not have any resemblance whatsoever to the enemy's cryptographic machines, but they duplicate what their machines do, and do so at a high rate of speed. Here's a picture of such a device. In this next slide you see a tabulator, a standard tabulator with a special attachment devised by our own engineers susceptible of doing what we call "brute force" operations, where you are trying to solve a thing on the basis of repetitions which are few and scattered over a large volume of messages. Well, if you've got millions and millions of letters, or code groups, the location of those repetitions is a pretty laborious thing if you have to do it by hand, so we speed the search up. A machine of this kind will locate these repetitions in, say, one-ten-thousandths of the time that it would take to do it by hand. Here is a specialized machine, again a tabulator, with an attachment, here, that is used for passing the text of one message against the text of another message in order to find certain similiarities, or perhaps differences, or maybe homologies, and it does it automatically. These relays are set up according to certain circuitry; you start the machine, and low and behold, it produces a printed record of the message repetitions or what not.

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

We now have more modern and much faster machines, and I'll now show you a few of them.

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

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

I want to say a few words about the great importance of coordinating COMINT activities with other intelligence operations and with the tactical situation. Although COMINT is the most reliable, the most timely and, in the long run, the most inexpensive kind of intelligence, it must, as I've said before, still be evaluated, collated, correlated and coordinated with intelligence coming from other sources, if for only this reason: to provide data for cover and protection of COMINT sources. When a decision has been made to take action based on COMINT, careful efforts must be made to insure that the action cannot be attributed to COMINT alone. This is very, very important. When possible, action must always be preceded by suitable reconnaissance and other deceptive measures, otherwise the goose that lays the golden eggs will be killed. I am going to give one example of what is meant by COMINT cover.

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

Of course knowledge and experience point to the necessity of exploiting every possible advantage a tactical situation affords, and the temptation is naturally very great, in the heat of battle, to use COMINT whenever and wherever it is available. This may lead to carelessness which quickly jeopardizes COMINT sources. Of course, the full value of COMINT cannot be realized unless operational use is made of it; however, when action based on it is contemplated, possible compromise of source must always be borne in mind and the danger of compromise weighed against the military advantages to be gained. A minor military advantage is never alone sufficient grounds for risking the loss of the source--this is a cardinal principle.

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

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

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

With the foregoing remarks I bring to a close my talk on COMSEC and COMINT. If there is any last word or impression that I would like to leave with you let it be that in my opinion the former, though far less spectacular and interesting than the latter, is the more important of the two. There are two reasons for my opinion. The first is that secrecy in the conduct of military operations is of the highest importance to their success, and without secure communications there can be little or no secrecy. The second reason is one that is not so obvious It is that your COMINT successes will be eliminated unless the communications over which the results must pass to reach those who can use them are secure. Therefore, COMSEC is doubly important, once for itself and once for COMINT protection. 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: A commander may win if he has good COMINT; but he will surely lose if he has poor COMSEC.

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.

COMMUNICATIONS INTELLIGENCE

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

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

→ Insert here attached

Sometimes the course of history is materially changed by the amount and quality of the COMINT and COMSEC available to field commanders and also how well they use these offensive and defensive weapons. Sometimes it is materially changed by the absence of COMINT and COMSEC where it had previously been in existence and used. We ~~shall~~ have already noted incidents ~~of both types and we may start with an incident~~ of the first type, ~~one~~ those in which lots of first-class COMINT was available, including the COMINT available before the attack on Pearl Harbor. ~~I need only mention the name Pearl Harbor, and many of you will no doubt think that I'm going to go into that still controversial and disastrous episode in this talk, but I'm not. I will, however, use it as a jumping-off point for what will follow in the talk.~~ We may now take note of an incident of the second type, one in which the consequences of a lack of COMINT plays the most prominent role.

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

indent | Any examination etc. p. 55 to that word "silent" in 9th line of para.

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

[Story about General Montgomery if there's time.]

~~When our commanders had COMINT they were able to put what forces they had~~ ~~[illegible] places at the right [illegible] But when they didn't have it--and this happened several times--their forces often took a beating. In one famous or infamous case~~, I have reference here to the Battle of the Bulge, wherein a serious catastrophe was barely averted because our G-2's had come to rely too heavily on COMINT, so that when it was unavailable they seemed to lack all information or at least they felt that way. ~~that lack.~~ I said that a serious catastrophe was barely averted but even so the losses were quite severe, as can be seen from the following:

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

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

What happened? Why?

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

> "Intelligence deficiencies and an astigmatic concentration upon our own plans with an almost contemptuous indifference for the enemy's, set the

stage in December, 1944 for the German successes in the Battle of the Bulge--a case history in the 'dos and don'ts' of intelligence."

~~* *~~

Further on Baldwin ~~said:~~ notes that,

"Another and more basic failure was the inadequacy of collection; we just did not get all the facts that were available. There was a variety of reasons for this.

"In General Sibert's words, 'we may have put too much reliance on certain technical types of intelligence, such as signal intelligence . . . and we had too little faith in the benefits of aggressive and unremitting patrolling by combat troops. ~~We had no substitute, either, for aerial reconnaissance when the weather was bad; and when we cam up to the Siegfried Line, our agents had great difficulty in getting through, particularly in the winter.'~~

e/

✓ "Dependence upon 'Magic', or signal intercepts, was major, particularly at higher echelons; when the Germans maintained radio silence, our sources of information were about halved."

~~I hope I've not tried your patience by such a lengthy preface to the real substance of my talk, so it's about time I got down to brass tacks, that is, to the technical aspects of the talk.~~

In what I read from TIME, in the first period, the word "MAGIC" ~~was used~~ seemed to refer only to the machine that we reconstructed for solving Japanese Foreign Office communications. In reality, the word MAGIC was used as a sort code name among the initiated and indoctrinated persons who were entitled to receive the highly secret information that came from the solution of German, Italian, and Japanese secret communications. ~~MAGIC,~~ It was, of course, ~~simply was a sort of code word for~~ COMINT. The term was introduced to us by the British when we began to play together in the cryptologic gardens; we found it useful and adopted it, too. Later on we came to use other secret words to designate this sort of intelligence and to change the words from time to time, for security reasons. ~~Now Magic or~~ Currently, COMINT is composed of three types or categories of intelligence, and by far the greatest part of it comes from intercepting, recording, and studying enemy radio traffic. The three types or categories are: (1) Special intelligence, which comes from the solution and processing of the encrypted messages themselves, and the result is information of highest reliability because it comes, so to speak, "right out of the horse's mouth"; (2) Traffic intelligence, which comes from the study of what are called "the externals" of those messages, data applicable to such things as their callsigns, the frequencies employed, the direction or routings, and so on, and from this comes information from which inferences can be drawn; and (3) Weather intelligence, which comes from the study of the enemy's weather messages, which in wartime and even in peace time to a certain degree, are encrypted. In this audience it's hardly necessary to mention how important a role the weather plays in the conduct of war. Recently NSA has also been assigned overall responsibility for ELINT, or electronic intelligence, but I won't go into that in this talk.

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

It was in response to this third and last objective of COMINT that World War II gave a brilliant answer.

I'm sure you would find the detailed story of the ~~cryptanalytic~~ of Navy, Army, and Army ~~Air~~ Corps cryptanalysts, and of their opposite numbers in the British Services, successes on German, Italian, and Japanese messages in World War II highly interesting but there just isn't time. I think the contents of the Marshall-Dewey letter, from which I read a bit in the first period, will have to suffice. However, it in itself is sufficient to give you a pretty good idea of the contributions COMINT made toward our winning World War II. It is unfortunate that General Marshall's letter was disclosed during the Congressional Hearings for its contents are now in the public domain and its contents are undoubtedly now known in all the important chancelleries and war offices of the world. General Marshall, you'll remember — etc p. 42 of A to middle of p. 43.

* * * *

It will be helpful to list in sequence the steps involved in the production of COMINT. First, [at [illegible] on p. 14 of E to point shown on p. 14]

The interception of the traffic is not only a complicated but also a very ~~costly~~ expensive enterprise, costly in numbers of personnel

ludes]

n. You

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

The next step after interception [etc. on p.15 of "E", continuing on p. 16 + 17 to point marked]

Now I will go back to COMINT processing and ~~It's time I~~ give you some information about cryptanalytic techniques and gadgetry. I venture to say that you all know the mental picture the average citizen has of a cryptanalyst, for the picture is a very old one, like the one I now show you, of Trithemius, whom I mentioned before. He's a long-haired egg-head; he wears thick spectacles, has long whiskers, with crumbs in them, he has grimy fingers and finger nails, and so on. This chap goes into a huddle all by and with himself and the cryptogram and sooner or later he comes up with the answer, shouting Eureka! Well, that picture is far from the truth these days, for cryptanalysis and COMINT is "big business" now — very big business indeed, because we're spending well over half a billion dollars on it every year now.

Cryptanalysis of modern etc. p. 38 of A + continue on p. 39 to bottom, adding the handwritten matter attached to p. 39, then continue with p. 40 of A, then p. 41 to place marked.]

[Then continue with new para:

~~There are~~ We now have more modern and much faster machines, ~~now~~, and I'll now show you a few of them. ~~pictures~~

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

Each Service [etc. p. 20 of F.

~~The next step after interception [etc. on p.15 of E~~
~~continuing on p. 16, 17.]~~
~~[Then go to bottom of p.4 of "F"~~

"F"

requires the services of large numbers of communications and specially trained personnel. In order that the product may be ~~xxxd~~ useful operationally and not merely historically interesting, the intercept traffic must be forwarded most expeditiously to the processing center and after processing the final results must be transmitted promptly to the ~~xxxxxxxxx~~ evaluators and other intelligence personnel and in some cases directly to field commands by fastest means. The scheme, the system, by means of which this was done was beautiful in the Navy, in the Army and in the British Services. Great protection, special crypto-systems, special security officers, so that there was no slip-up. Thus a large processing center is necessary now because of the complexity of modern crypto-systems, most of them cannot be solved in the field. You can solve low-grade, perhaps traffic analysis problems. Some COMINT processing can be accomplished in the field as I said before in order to meet certain immediate needs of field commanders but as these systems get more and more complicated, Iam beginning to be very doubtful about that. [Each Service provides for its own special needs in this category

Begin

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

I want to say a few words about the great importance of coordinating COMINT activities with other intelligence operations and with the tactical situation. Although COMINT is the most reliable, the most timely and, in the long run, the most inexpensive ~~in the long run, the most inexpensive~~ kind of intelligence, it must, as I've said before, still be evaluated, collated, correlated and coordinated with intelligence coming from other sources, if for only ~~one~~ this reason: ~~alone~~, to provide data for cover and protection of COMINT sources. When a decision has been made to take action based on COMINT, careful efforts must be made to insure that the action cannot be attributed to COMINT alone. This is very, very important. When possible, action must always be ~~is~~ always preceded by suitable reconnaisance and other deceptive measures, otherwise the goose that lays the golden eggs will be killed. I am going to give one ~~or two~~ example~~s~~ of ~~this~~ what is meant by COMINT cover.

On a certain day in November 1944, an enciphered code message was sent by a certain Japanese staff section to a certain Japanese Air Force unit, requesting air escort for two convoys carrying troops to reenforce the Philippines. The message gave the number of ships, tankers, escort vessels, date of departure, port and route, and noon positions for the next seven days. The message was solved in Washington. Two days after the convoy left, one report, in a message which was also intercepted and solved, stated that it had been sighted by a B-29, with strong indication, that the other convoy had also been sighted. A few hours later, messages from these convoys reported losses as follows: six ships definitely sunk, one disabled, one on fire. Later we learned from another source, that ~~in addition~~ one aircraft carrier was also sunk. But did you happen to notice that message about the B-29?

It just didn't happen to be cruising around there, but it sent there to be observed.

Of course knowledge and experience point to the necessity of exploiting every possible advantage a tactical situation affords, and the temptation is ~~of course~~ naturally very great, in the heat of battle, to use COMINT whenever and wherever it is available. This may lead to carelessness which quickly jeopardizes COMINT sources. Of course, the full value of COMINT cannot be realized unless operational use is made of it; however, when action based on it is contemplated, possible compromise of source must always be borne in mind and the danger of compromise weighed against the military advantages to be gained. A minor military advantage is never alone sufficient grounds for risking the loss of the source--this is a cardinal principle.

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

Finally, another aspect of coordination is that between the operations ~~people~~ offices and the COMINT ~~people~~ officers. The COMINT ~~people~~ authorities should be carefully oriented to give the optimum coverage for operations in progress. There are just so many facilities and personnel available, and only a part of the enormous amount of traffic can be obtained and processed. Therefore it is essential that the COMINT ~~field~~ producers be constantly informed of current and planned operations so as to direct attention where most needed. This was a very, very important point to get across; it was a difficult one to get across because ~~the~~ commanders, ~~people~~ in charge of ~~very important~~ large-scale operations are naturally ~~were very~~ leery of telling any outsiders ~~of~~ what they were planning to do, and the how, ~~and~~ when, and where of the impending operation. ~~But as we went on,~~ Mutual confidence must be ~~was~~ established, so that ~~and~~ the COMINT producers learn ~~people got to know~~ what the operations staff is ~~people were~~ planning; ~~and~~ they ~~both~~ support~~ed~~ each other.

With the foregoing remarks I bring to a close my talk on COMSEC and COMINT. ~~and CRYPTOLOGY.~~ If there is any last word or impression that I would like to leave with you let it be that in my opinion the former, though far less spectacular and interesting than the latter, is the more important ~~than the latter~~ of the two. There are two reasons for my opinion. The first is that secrecy in the conduct of military operations is of the highest importance to their success, and without secure communications there can be little or no secrecy. The second reason is one that is not so obvious. It is that ~~of~~ your COMINT successes will be eliminated unless the communications ~~the~~ over which the results must pass to reach those who can use them are secure. Therefore, COMSEC is doubly important, once for itself and once for COMINT protection. 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: a commander *may* win if he has good COMINT, but he will surely lose if he has poor COMSEC.

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.