First draft with handwritten changes.

When General Twining invited me to address the staff and students of the Senior School of the Marine Corps on the subject "Communications Intelligence and Security" it was with pleasure ~~and alacrity~~ that I accepted the invitation because ~~it is to be~~ I assumed that the objective of such an address is to give you some background ~~orientation and~~ information about the field to which ~~these~~ those two subjects matters belong, namely, the science of cryptology, ~~and to~~ Suppose I propose to tell you something about how ~~it~~ that science developed; and ~~then~~ to indicate the manner in which it can and has been employed as a vital military weapon.

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

First, then, for historical background.

I opened my remarks by referring to the science of cryptology as a vital military weapon, but it has not always been regarded as a weapon, let alone a vital weapon. I am here reminded at this point of a story that I came across in an old book on cryptology, a story which is probably apocryphal but which I give for what it may be worth.

It seems that about two thousand years ago there was a Persian queen named ~~whose name was~~ Semiramis, ~~who~~ who took an interest in ~~cryptography~~ cryptology. Whether it was because of that interest or for other unnatural reasons, ~~circumstances~~ such as curiosity about what people call secrets, the record doesn't say, but anyhow it was reported that she met an untimely death. Presumably she went to Heaven, or perhaps to the other place, but she having left instructions ~~as to the disposition~~ that were to be placed in a golden sarcophagus within ~~of~~ her earthly remains, ~~they built for her~~ an imposing mausoleum, ~~in which her sarcophagus was placed.~~ On the outside of ~~the mausoleum~~ which, on its front wall, there was to be carved a message, ~~which said~~ reading:

> Stay, weary traveller!
> If thou art footsore, hungry, or in need of money—
> Unlock the riddle of the cipher graven below,
> And you will be led to riches beyond all dreams of avarice!

Below this curious message was a cryptogram, and ~~I'm sorry I can't show you what it looked like.~~ For several hundred years the possibility of sudden wealth served as a lure to many ~~all the~~ experts who tried their hands at deciphering the message, ~~but~~ they all were without success, until one day along came a long-haired, be-whiskered, and bespectacled savant who, after working at the project for a considerable length of time, solved the cipher. It gave him detailed instructions for finding a secret entry into the tomb. When he got inside, he found an instruction to open the sarcophagus, but he had to solve another message in order to do so. Possibly it involved finding the correct combination to a 5-tumbler lock! Well, he solved that one too, after a lot of work, and this enabled him to open the sarcophagus, in which he found a box. In the box was a message in plain

language, and this is what it said:

> O, thou vile and insatiable monster! To disturb these poor bones!
> If thou had'st learned something more useful than the art of deciphering,
> Thou would'st not be footsore, hungry, or in need of money!

Many times in the course of the past forty years I've had occasion to wish that I knew the old gal's address so that I could write her, as a first indorsement to her basic communication, the single word "Concur." Well, anyhow, it's been an interesting life!

The title of my talk, this, the final parcel of, 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 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.

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 note incidents of both types and we may start with an incident of the first type, one in which lots of first-class COMINT was available. 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.

This being a TOP SECRET lecture it will appear a bit incongruous that I should begin by reading from a source which you'll all recognize--TIME magazine. I'll read from the 17 December 1945 issue, and ~~I must~~ will preface the reading by reminding you that by that date the war was all over--or at least V-E and V-J days had been some months before. You'll remember the celebrated ~~case that there was a~~ loud clamor on the part of certain vociferous members of Congress who had for years been insisting upon learning and disclosing to the people of the United States the reasons why we had been caught by surprise in such a disastrous defeat and calamity as the Japanese had inflicted upon us at Pearl. This clamor had to be met; the matter could no longer be hushed up, they contended, by the need for military secrecy. So there were investigations--a half dozen or more of them and more there were to be a ~~winding up in the~~ grand finale Joint Congressional Investigation into the Attack on Pearl Harbor. It was this investigation which not only itself brought into the open every detail and exhibit uncovered by ~~the~~

~~presented~~ in its own lengthy investigation and hearings, but also it disclosed to America and to the whole world everything that had been said and shown at all the previous Army and Navy investigations--about a half dozen of them.

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

"U.S. citizens discovered last week that perhaps their most potent secret weapon of World War II was not radar, not the VT fuse, not the atom bomb, but a harmless little machine which cryptographers painstakingly constructed in a hidden room in Fort Washington. With this machine, built after years of trial and error, of inference and deduction, cryptographers have duplicated the decoding devices used in Tokyo. Testimony before the Pearl Harbor Committee had already shown that the machine known as 'Magic' was in use long before December 7, 1941, had given ample warning of the Japs' sneak attack if only U.S. brass hats had been smart enough to realize it (TIME - Dec. 18). Now General Marshall continued the story of 'Magic's' magic. It had:

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

"Given the U.S. full advance information on the size of the Jap forces advancing on Midway, enabled the Navy to concentrate ships which otherwise might have been 3,000 miles away, thus set up an ambush which proved to be the turning-point victory of the Pacific war.

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

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

And then TIME goes on to give more details of that story. We shall return to it later in this talk.

It is hardly necessary to tell you how carefully Magic was guarded before, during, and after the war. It is still very carefully guarded. Even the fact of its existence was known to only a very few persons at the time of Pearl Harbor--that is an important element in any attempt to explain why we were caught in such a devasting surprise attack. Let me read you a bit from page 261 of the Report of the Majority in the Joint Congressional Investigation of the attack: "The Magic intelligence was pre-eminently important and the necessity for keeping it confidential cannot be overestimated. However, so closely held

and top secret was this intelligence that it appears the fact the Japanese codes had been broken was regarded as of more importance than the information obtained from decoded traffic."

TIME says, in connection with this phase of the story of Magic during World War II: "So priceless a possession was Magic that the U.S. high command lived in constant fear that the Japs would discover the secret, change their code machinery, force U.S. cryptographers to start all over again."

Now I don't want to seem to over-emphasize the importance of COMINT in the Pearl Harbor affair but I think it warranted to read you what the Majority said about it in its Report. ~~of the Joint Congressional Committee on the Investigation of the Pearl Harbor Attack.~~ The following comes from p. 232:

" ... all witnesses familiar with MAGIC material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

General Chamberlin, who was MacArthur's G-3 throughout the war in the Pacific, has written: "The information G-2 gave G-3 in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." I hardly need say that we can't put a dollar-and-cents value of COMINT in the saving of lives; but we can make an estimate of what COMINT meant in the way of shortening the war by two years means. I made a calculation and found that $1.00 spent for COMINT is worth $1,000 spent for other activities and materials.

In short, when our commanders had COMINT they were able to put what forces they had at the right place, at the right time. But when they didn't have it--and this happened several times--their forces often took a beating. In one famous or infamous case, the Battle of the Bulge, 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 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 75,89# men, of whom 8,6#7 were killed, 47,139 wounded, and 21,144 missing Over 8,##8 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:

"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.'

"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, the word "MAGIC" was used to refer to the information that came from the solution of German, Italian, and Japanese secret

communications. MAGIC, 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 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; (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 (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.

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.

A bit of history is always useful in introducing a subject belonging to a special and not too-well known field, so I'll begin by giving you some background information about COMINT. COMINT, which is based upon the science of cryptanalysis, has a long and very interesting history which is inextricably bound up with the history of the science of cryptography, upon which COMSEC is largely based. The two are but opposite faces of the same coin, for progress in one inevitably leads to progress in the other. Hence, my talk will deal with both COMINT and COMSEC. Now, because of the secrecy or cloak of silence which officially surrounds the whole field of cryptology and especially cryptanalytics, it is obvious that authentic information with reference to the background and development of the science in foreign countries is quite sparse; and although after World War II we learned much regarding the accomplishments in this field of work by our enemies, security rules prevent my saying very much in detail about how good or bad they were in comparison with us. Suffice it to say that we looked pretty good; together with our principal ally, Britain, we won the war, though we seem to have lost the peace somewhere.

I can only give a fairly good account of U.S. cryptologic activities up to a certain point of time, and even then I will not be able to say very much about them simply because the story is too long to give in a lecture or even a series of talks. In the course of my talk I will present a number of illustrations of

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

Now, because of the curtain of secrecy which officially surrounds etc p. 11