Several examples in a Japanese survey made during the period 8 December 1941 to 31 October 1943 show how information was obtained by the Japanese because of lack of security precautions on the part of U. S. personnel. The document states:

"It may be seen in the accumulation of battle lessons which follow that making use of enemy communication is of great value in operations. In addition to perfecting our own communication security, we must do our utmost to develop our own operations advantageously by obtaining enemy intelligence through the use of radio.

"It is well to have a separate enemy communication section attached to each command which has a direct part in the operation. Specialists should be made of interception personnel, to train them for fixed duties and to avoid changing their assignments. The following are examples of advantage being taken of enemy communications.

"The movement of enemy planes and air bases in the Aleutian Archipelago was in general inferred by variations of signal strength. This was used to advantage in operations.

"At the time of the air attack on Dutch Harbor, the utter confusion of the enemy's movements was realized immediately by the enemy communications section on the flagship and important data was obtained.

"In the battle of the Coral Sea the frequencies of shore-based and carrier aircraft were well known, since the greater part of the enemy communication was in plain language."

Another part of the Japanese survey gives examples of their gaining valuable information from U. S. transmissions in clear text:

"In the battle of the Coral Sea plain-language communications which were used by the enemy (generally scouting planes communicating the discovery of our ships) were frequently intercepted, and we obtained material of considerable value in the conduct of operations.

"In the same naval battle, the Australian and American air forces communicated to their base by plain language every movement made following discovery of Japanese units. We were thus able to forecast the attacks of enemy planes through the communications, and to deduce the movements of enemy task forces.

"When enemy planes raided Kiska, we were generally able to forecast it from the reports of enemy weather scouting planes prior to the attack."

Interrogation of Japanese intelligence officers a few months ago brought to light a number of useful facts about the nature, extent, and success of enemy efforts in the field of communication intelligence, especially traffic analysis. One of the officers was a Commander Hideo Ōsawa and the other was Lt. Commander T. Satake. Both held key posts in the radio intelligence section of the Japanese Naval General Staff during most of the war.

Ōsawa was the center of the activity described by Ōsawa and Satake. Here Allied transmissions were intercepted, copied, and sorted by areas. There were seven of these areas - the west coast of the United States, the Indian Ocean and five different sectors of the Pacific. Several officers were assigned to each area. Though usually unable to decide whether transmissions came from ships or shore stations, enemy analysts used direction finders to determine the point of origin.

Taking Okinawa as an example, Satake made a statement as follows: "A month before Okinawa, NAMS • • • had a notable increase in transmissions. Ten days before your Okinawa operation, there was a marked increase in submarine reports. These are easy to spot because we could get good direction-finder fixes as they closed in. When submarines changed from routine operational communications to urgent, we deduced that perhaps an air strike or landing might be in the offing, depending upon the tactical situation.

Ōsawa, when asked what was the greatest success of naval radio intelligence in predicting future operations, named the Marshalls operation. "We got the word to the garrisons in time to be of some help that they should prepare for an attack," he stated. Regarding the basis of the prediction, he explained as follows:

"Bombing grew intense. Both ship and aircraft volume of radio transmissions rose to a peak, and we were able to pick up a few plain language broadcasts. I remember one saying General Olds would arrive shortly."

Our aircraft often gave away their plans. When B-29s prepared to take off "there was much adjusting of radio frequencies."

A

~~CONFIDENTIAL~~

The following clear text message, logged by a radio security officer in Italy, is a shining example of how plans may be revealed to the enemy: KNA V XDM....MESSAGE FOR YOU....BRITISH WILL BE FIRING FROM 12 TO 12:45 TODAY AT FOLLOWING POINTS 908-145, 893-141, 894-150....REQUEST YOU DO NOT FIRE THESE POINTS AT THIS TIME....DID YOU GET THAT....OVER. Another incident early in the Anzio campaign illustrates the waste of supplies through the compromise of locations by misuse of communications. An advancing tank battalion radioed back in the clear that an enemy counterattack was under way and asked that all traffic be stopped at a specified town behind the lines. German intercept notified its air force and within an hour a squadron of planes was strafing a long column of traffic halted on the road. Many trucks, jeeps, and cars were wrecked beyond repair, but more important still was the number of men killed.

~~CONFIDENTIAL~~

N

Often during the war violations of radio security on aircraft circuits provided the enemy with valuable information. An outstanding example of this occurred after the first air raid on Tokyo in April of 1942. The HORNET and the ENTERPRISE had been sighted. It was important to the Japanese to know what they would do next. Would they return to Pearl Harbor to refuel or might they steam southward to the Coral Sea?

For several days silence surrounded the carriers. As they approached Pearl Harbor, however, and began to launch planes, the air was enlivened with unnecessary and unauthorized conversation which disclosed the presence of the carriers. It was known that important information concerning the carriers was reaching the Japanese, and an examination of aircraft circuit logs at about this time showed that disclosures had been made by pilots. The frequencies then in use were favorable to long-range interception.

Corrective action was taken and the pilots learned their lesson well. When the carriers left Pearl Harbor and headed toward the Coral Sea, the radio silence of their planes was undisturbed and hope ran high. Perhaps the carriers could get to the Coral Sea area before the next Japanese push which seemed to be shaping up. Then patrol planes noticed the departure of the carriers and began talking. The information offered by the patrol planes may not have helped the Japs in making their plans, but the HORNET and the ENTERPRISE arrived too late. The patrol planes received some superheated advice regarding radio silence and the desirability of reporting only enemy ships.

~~CONFIDENTIAL~~

During the Salerno campaign, a regimental commander ordered one battalion to relieve another at 2300. Unfortunately, the battalion being relieved spent most of the afternoon discussing the details of the move on the battalion command net.

Just before 2300 hours, at the critical moment when the battalion holding the front line was due to move off and the incoming battalion was marching up from the rear to take over the position, the Germans launched a heavy attack with two assault companies brought up especially for the purpose. Since neither battalion was prepared to meet the attack, the Germans won initial successes, and it took three days of heavy fighting to restore the situation.

Prisoners of war afterwards said that the attack was made as a result of interception of our radio traffic.

A

During the battle of Germany, Nazi intercept operators were particularly on the alert for Allied reports revealing that certain areas inside Germany were not mined. Following interception of this intelligence, those areas were mined immediately, and into these traps walked United States infantry men.

N

[redacted]

In the latter part of 1944, a United States infantry division became increasingly careless about its radio procedure. Enemy interceptions of transmissions containing operator "chat", characteristic sending, and plain language had revealed the identity of all regiments within the division. Early in December 1944, the division launched a major attack. The enemy was listening as usual, and messages sent by the American division revealed the time of attack and other pertinent information. These transmissions were intercepted in time for the enemy to take effective countermeasures and arrange favorable artillery emplacements. The American attack was beaten back with heavy losses.

[redacted]

N

In the latter phase of the Allied offensive in Europe, a reconnaissance plane spotted a concentration of enemy vehicles between two German cities. The pilot instructed his operator to transmit this intelligence to his base requesting immediate air support. Unthinkingly, the operator sent this request in the clear. Enemy interception quickly assimulated this information and acted to correct an awkward situation by rerouting the vehicles to a new location. The American attack, directed at the previous location, was fruitless.

A

As the security of cryptosystems has improved, so has the "know-how" of cryptanalysts, both our own and enemy. An incident early in the North African campaign illustrates this point. An enciphered message was sent between two British units. The message was intercepted and broken by the Germans, who enciphered the result in a German system and rushed it to Berlin. The British intercepted the German message, and they broke it. They discovered, much to their chagrin, that the Germans were reading their supposedly secure cipher, and of course changed it in a hurry. All of this took place within a 24-hour period.

The contents of messages may often be a source of danger in operations, or the lack of sufficient information contained in messages. During 1943, an enemy submarine was able to sink one of our ships and escape from American waters because of incomplete messages, and failure to send a message at all. The submarine might have been destroyed before it could do damage had not any one of the following errors occurred: A plane reported rescue of survivors but failed to give the time of the attack, the position of the attack, the course of the sub, or its condition; another plane neglected to make an amplifying report and wasted time asking a question to which it should have known the answer; a third plane failed to give the position of the sub or to communicate with a plane which was in a position to assist. It failed also to make amplifying reports promptly, in sufficient detail, and in plain language instead of code. Speed was vital, and the information was of little value to the enemy.

In another case complicated by the lack of clarity in a message, during the final month of the War in the Pacific, a task group made radar contact with an unidentified submarine. All efforts at recognition failed, visibility was poor, and the submarine gave indications of being hostile. At this point one of the destroyers in the task group received a message from the task group commander which was understood to state: "Close target evaluation is enemy attack and destroy". The destroyer attacked and the target disappeared. Later it was discovered that the sub was one of our own. What the message actually said was, "Close target and if evaluation is enemy destroy it".

Repetition of message elements is a source of much insecurity, as the defenders of Corregidor found during the Japanese conquest of the Philippines. On the Cavite shore about ten miles southeast of Corregidor were batteries of Japanese artillery which shelled Corregidor and the fortified islands intermittently. During the air raids of the next few months a special code word was adopted to warn vessels of the inshore patrol when an air raid was expected. The defenders of Corregidor discovered, after a while, that the Japanese batteries on Cavite would begin shelling Corregidor every time the code word for air raid was broadcast to the inshore patrol. This shelling was erratic, but it harassed the gun crews of the anti-aircraft batteries enough to impair their effectiveness. Use of the code word was discontinued, and the vessels of the inshore patrol were required to listen for the sirens on Corregidor or else maintain their own lookouts for air raids. The shelling from the Cavite shore during air raids decreased except when bombers approached from the southeast, thus passing over the enemy gun positions.

N

At times the method of processing messages has produced compromise situations, the methods used being conducive to error and therefore faulty. In one office, for example, it was an established custom for the plain text of a message to accompany the cryptotext all the way to the teletype operator, who transmitted the cryptotext and late filed both versions separately. One day an inexperienced teletypewriter operator who was doing his best to keep up with heavy traffic transmitted both the encrypted and the plain-text versions of one of the messages, and it was subsequently relayed by radio. The method of processing was abruptly changed, but the communication officer, who was experienced but had been stationed at that headquarters only three days, received an official reprimand because he had not acted before a compromise could occur.

In another instance an inexperienced and relatively untrained communications officer was acting as control and handling nearly 10 times the normal amount of traffic. Decrypted messages were brought to the radio shack to be typed. One day a decryption which was not properly marked, either as a classified message or as a decryption, found its way by mistake into the radio files and was later transmitted in response to a request for a repetition.

A

Taking a page from the enemy's notebook, we may derive a lesson in maintaining the security of U. S. cryptosystems. The following extracts from the translation of a captured Japanese document make it clear that the Japanese expected their own cryptographed messages to be attacked by cryptanalysis, and by implication, that they were expending considerable effort to break U. S. cryptographed traffic.

"Many years of study have gone into the compilation of our latest army code books, which embody special original systems, and we can be confident of achieving security in the face of increasingly determined scientific espionage.* If we have any unproved suspicions based on doubtful information, these should be thoroughly investigated and care taken not to cause needless anxiety to higher authority. In all countries scientific espionage will go to any length and bring to bear the utmost intelligence in order to break into a code, taking immediate advantages of even the slightest flaw, and then by concentrating every energy on this, will break the code. For this reason we must spare no effort to obtain definite concrete proof. . . .

"Just as ants may enter through one hole and destroy everything within, so even a trifling error may lead to the loss of a whole army. Therefore, it is expected that henceforth code discipline shall be maintained in use of codes, so that by allowing absolutely no errors to creep in, the security of the codes can be preserved. . . .

"It is of the utmost importance that we should make continuous progress with our codes, so that persistent enemy scientific intelligence may not catch us up,

*Japanese term for enemy cryptanalysis.

and that we should recognize the necessity for uninterrupted research endeavors under all circumstances. If we interrupt our studies in this direction in the belief that our present standard is adequate, even temporarily, the enemy will outwit us by scientific intelligence methods and we will be liable to suffer undesirable results. Since first-rate mathematical research is required for theoretical study of these matters, we must redouble our efforts and naturally make full use of mathematicians of high standing. In this direction, all countries are energetically turning their attention. However, our codes have of late made great strides forward and while they seem to have reached the peak of perfection in this matter, under the circumstances mathematical study must be increased and our codes set on a secure scientific footing. Striving after new and original cryptographic methods, we may expect that our codes will lead the world and thus achieve the most important factor in signals security. . . .

"Since we must anticipate that even our best technical schemes will at once be surpassed by the enemy's technical offensive, we must be victorious in the keenly contested decisive battle of science and once and for all secure over the enemy a position of domination in technical matters. . . . Equipment has not as yet attained the desired objective, either because of a low standard of concealment or because of reluctance to put it into general use throughout the Army. The National Army will henceforth redouble its efforts in the technical field to overcome difficulties that appear insuperable, and will preserve its pre-eminent position in a science peculiarly Japanese in nature. It is of the utmost importance at present that in this matter we should thus surpass the enemy and contribute to the ultimate perfection of our arms. . . ."

It is interesting to note that the Japanese feared their codes would be broken, yet insisted that those codes were secure. They seemed mildly

hysterical on both points. The U. S. Army's attitude is that its cryptographic systems, when used according to instructions, provide adequate security for the type of communications for which they are authorized.

Moving cautiously ahead during mop-up operations on Kwajalein, a coral atoll of the Marshall Islands, a U. S. Marine stumbled across the body of a dead Jap. This in itself was no unusual occurrence for that hot day in January 1944, but the fact that the marines eye was attracted by a water-soaked sheet of paper lying next to the body started a chain of circumstantial evidence which clearly demonstrated the importance of reporting all possible losses of cryptographic documents. It developed that the paper was a cryptographic document extensively used in the Pacific area at the time, and Japanese writing on the document was later translated to read "Received 3 January 1944".

Subsequent investigation revealed that the document had originally been issued in bulk to the Chief Signal Officer for redistribution to the Army Air Forces for use in the Pacific area. The particular document was traced to a certain bomber command involved in the Kwajalein campaign. Further investigation narrowed the search down to a specific squadron of the bomber command, and eventually it was found through questioning the squadron commander that one of the Liberator Bombers in his squadron had been shot down in shallow water near the beach where the water-soaked document had been discovered. The squadron commander, seeing the Japanese capture the plane and its crew, reported the loss of the plane and assumed that higher authority would take care of the document, since it was carried on all the planes of that mission as a part of the equipment.

The fact remains that no one reported loss of the document until it was too late. The Japanese had received the document on 3 January, and the dead Jap was not found until 8 January. This means that it is very likely the Japanese were reading our tactical air-ground messages, and any other messages sent in that particular system, for a period of five days at the height of a critical campaign. ~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

A

Sworn statements reporting that specific cryptodocuments have been inadvertantly destroyed by burning and requesting release from accountability are frequently received by accounting headquarters. One such message was received from the security officer at a certain Port of Embarkation, announcing the loss of a document containing a list of types of installations using a cryptosystem used by the Army. The document was subsequently removed from accountability after a routine investigation, and the case was forgotten. A few months later the document reappeared mysteriously and the puzzled port security officer reported that fact and wanted accountability resumed.

All the employees of the signal office were questioned by investigators, and it was learned that a woman employee of the establishment had taken the document home with her; she claimed she wanted to study the document to learn all the establishments in this country using the cryptosystem, so she could apply for a job elsewhere. An investigation of the woman's past record revealed that she had originally been "cleared" at Bolling Field, and subsequently dismissed for "suspicious actions," and that two other air force installations had dismissed her for the same reason, although nothing was ever "pinned" on her.

The woman was dismissed from her job at the port signal office, but the FBI requested that she not be prosecuted, as the Inspector General recommended, as they desired to keep her movements under surveillance.

~~CONFIDENTIAL~~

A first lieutenant in charge of a code room in Canada owed his freedom and relatively honorable reputation to the clemency of the President. Visited by his wife one day, he "pulled rank" on a security-minded sergeant, who protested the violation of security regulations, and permitted his wife to enter the code room. He showed his wife one of the chief crypto machines in use by the Army, and let her encipher messages as she pleased. The sergeant, who had covered everything in sight, left and returned with the post intelligence officer, who placed the lieutenant under arrest under the eyes of the wife he was trying to impress with his importance. The officer was found guilty at the court-martial which followed, and was sentenced to four years at hard labor, and a dishonorable discharge. In reviewing the case, the President commuted the sentence to a reprimand and subsequent transfer to another station.

A Major at an ordnance plant is now fully conscious of security regulations as a result of two bitter experiences. After being charged with losing a cryptographic document for which he could not account, the Major requested that his account be inactivated. He was "through" with cryptography. The authorities obliged, requested the return of certain materials and the destruction of the rest. The Major, who had been severely reprimanded for his first violation, replied at some length on the destruction of some forty or fifty documents. The case was forgotten.

A routine investigation of the Major's files, some time later, conducted by a carefully trained security officer, revealed that some twenty-five of the documents reported burned were still on file. The Major and a captain who had "witnessed" the burning of the documents, were charged with false swearing, and were heavily fined under the 104th Article of War.

A

At the height of the invasion of Saipan, a Japanese intelligence report was picked up which stated in effect that Japanese intelligence was having considerable success reading the American traffic encrypted in a certain system in use throughout the Pacific area. It was not known whether or not the enemy cryptanalysts were having phenomenal success with the messages, or if some physical or cryptographic compromise was involved.

The break in the case came when a report reached accounting authorities that the 27th Infantry Division had "changed its accounting records" to show that three documents were missing! The 27th was then on Saipan, and the battle for the Mariannas was in its closing phases, after a long bloody struggle. Here obviously were two facts which could be linked, and an investigation revealed that they were more than remotely linked.

July 7th was a bad day for the 27th. On that date two command posts of the 105th regiment, both located near Tanapag Harbor, were over-run by a powerful Japanese force, who wiped out both headquarters, the personnel, the machinery, equipment, everything in sight. A signal salvage company recovered what it could, but when all the reports were in, three crypto-documents could not be accounted for in any way except that they were in the possession of the enemy. The 105th regiment reported this fact to division headquarters, which was the correct thing to do. However, division merely sent back an indorsement stating that "records have been changed" noting the loss of the documents. The missing documents were Joint Army-Navy key lists covering a period from 1 June 1944 to 31 July 1944, so the Japs undoubtedly had "considerable success" reading traffic during that period!

It is history now that the Saipan campaign went well during it's first week. The fact that 5,000 men were lost in the campaign can never be attributed directly to the captured documents, but it seems more than mere coincidence that most of these casualties were suffered through well-planned Japanese counterattacks after 7 July, the day the first two battalions of the 105th Regiment were overrun.

N

Like the lieutenant mentioned in a previous story, a commanding officer of a signal station neglected to keep information about cryptographic systems to himself. He had a group of distinguished visitors from an Allied nation as his guests. He had shown them many things about his establishment and discovered that he had 20 minutes left. Being the perfect host, he wanted to keep them entertained; so he took them to the code room, waived aside the protests of the non-com who was on guard at the door, and proceeded to give his visitors a demonstration of all that was there. Subsequently he was tried by court martial, reduced in rank from Colonel to his permanent grade of Major, relieved of his command, and sent home for reassignment.

N

CONVOY DELAYED

This glaring violation of Transmission Security happened shortly after the outbreak of the war.

A flight of B-25's was assigned to patrol duty on the West Coast. Orders read to be on the alert for submarines and to aid in convoying ships. The SOI required a report, upon return of the flight, of the position of a certain convoy, the number of ships, etc.

The flight leader sighted the convoy. Not having read the instructions in the SOI, he reported the position of the convoy, giving the course, number of ships, etc., in clear language by C. W. transmission.

For its own safety, the convoy was immediately ordered into the nearest port. The sailing was delayed for a period of 10 days - and who can evaluate the LOSS OF THOSE 10 DAYS!

A

BAD HABIT

There is no such thing as an inconsequential radio transmission. Messages sent in the clear can produce repercussions which dim the reverberations of falling bombs.

A British medical unit in the Sollum area of Egypt formed the habit of sending casualty lists in the clear, giving the arm of the service of the dead and injured: "Rifleman Adah Singh, killed at Gizah; Artillerist Arthur C. Smith, injured at Halfaya Pass."

Given enough volume of this traffic, the Germans were able to locate and identify all the major British units in that sector.

If wire had been available, this administrative traffic should have been sent by telegraph. Wire lacking, a courier should have carried the lists. If radio had to be used, the traffic should have been encoded.

TESTING TIPPED THEM OFF

Radio silence is more than golden to men who observe it strictly. To those who don't -

A division moving up into the combat zone in North Africa failed to observe absolute radio silence, and permitted its radio stations to send premature test messages in their new positions. Captured Italian intelligence reports later revealed that the enemy had intercepted the test transmissions and deduced that a new division was moving up.

A

~~CONFIDENTIAL~~

INTERCEPTED CLUE

Because of little consideration for the element of security, and some ingenious map-plotting by an alert enemy, serious obstacles were encountered by the British.

An attack on Halfaya Pass was planned by the British. Before moving their bases, the British opened radio nets at advanced points. With this clue to act upon, German and Italian intercept platoons were able to anticipate the disposition of the British troops - before they arrived at the front.

~~CONFIDENTIAL~~

A

THE GERMANS DID SOMETHING ABOUT IT

Among the violations of transmission security encountered daily is the ever-frequent case of sending important information in the clear. Take this example:

In the early days of the Libyan campaign, two officers were on the air talking about the difficulty of closing the 3-mile gap existing between their lines.

"I haven't the equipment," one commented.

"Well, I can't do anything about it," the other replied.

Not far distant a German intercept operator hastily sought contact with his superior officer. This vital bit of information was quickly assimilated by enemy intelligence, and before the end of the day the Germans did something about it.

Radio is a direct link to the enemy.

N

U-BOATS ESCAPED

This significant story is told by an NCO in charge of an aircraft warning station on the coast of South America.

"In the latter part of 1941 it was common knowledge that enemy submarines were operating in South American waters. From our recently established location, occasional observances of submarines, presumably German, were reported.

"We had been operating at this location for about 6 months when war was declared. Immediately, the submarine activity became more noticeable and several reports on enemy submarines were sent by radio. Through carelessness, some of these reports were sent in the clear . . . and without fail, the reported submarined would leave the vicinity, having ample time to do so, as the nearest troops were 2 hours flight away."

N

QAC

This incident has to do with IMPROPER RADIO PROCEDURE. From this story it can be seen that serious consequences may attend those who fail to observe it.

About 1 year ago, at Miami, Fla., a plane was sent out on an anti-submarine patrol, using special equipment. During the course of the flight an important part of this equipment became inoperative. The pilot instructed the radio operator to send a message back to the air base stating they were returning because the _____ was out of order.

If the correct procedure signal had been used, with no mention of the faulty equipment, the transmission would have been in order. Instead the message was sent in the clear. When the ship landed there was an escort of M.P.'s waiting. Both the pilot and the radio operator were court-martialed.

This leak was VITAL. Until then we had every reason to believe that the enemy did not know this particular equipment was being used in antisubmarined warfare in that locality.

MISSION NOT ACCOMPLISHED

Incidents that stress the hazards of SENDING IN THE CLEAR cannot be recounted too frequently.

A formation of B-25's took off somewhere in Tunisia during the early part of the North African campaign. Swiftly they climbed, and soon they were half way to the designated objective. Then . . . a message was received from their air base instructing the flight leader to abandon the assigned target and proceed to another area. The information, including the name of the new target, was transmitted in the clear.

When the formation approached the new objective a superior number of enemy planes intercepted the flight. The mission was not accomplished, and the degree of carelessness took a corresponding toll in men and planes.

A

[redacted]

TRAFFIC WAS DELAYED

Prompt distribution of SOI's within a net is always an important factor, as this story clearly shows.

In the combat zone where this particular net was in operation, transportation was at times slow and very uncertain. The only means of transportation in this area were by water and air.

SOI's were made up by headquarters in the rear echelon, about 1,500 miles distant. The majority of stations were so removed from headquarters that from 1 to 3 days' travel by air was necessary to traverse the distances. Call signs were changed periodically and frequently, but not always did distribution of SOI's include the forward stations.

Personnel of the rear echelon station, not realizing the situation, would, on the appointed hour, change over to the new call signs and refuse to answer the old ones.

This caused considerable delay in handling traffic.

It is well to remember that because of slow traffic - MESSAGES THAT ARRIVED TOO LATE - battles have been lost.

[redacted]

A

WAS THE ENEMY LISTENING?

Radio chatting is always music to the ever-listening ears of the enemy. Here is another story wherein the desire to talk paid poor dividends.

Somewhere in North Africa, a pilot was returning from a reconnaissance mission successfully completed. It might have been elation over a job well done or a general sense of relaxation which caused the officer to indulge in chatting.

During the ensuing chat this officer mentioned that a large formation of aircraft had landed at a certain air base. Was the enemy listening? Obviously he was, because in a few short hours the air base was bombed and almost totally destroyed.

~~CONFIDENTIAL~~

N

RADIO OPERATOR TALKS

Transmission security cannot be effectively obtained without a STRICT PERSONAL CENSORSHIP on the part of the operating personnel. A report recently received in Washington clearly illustrates this.

The report read: "Captain _____ and I were notified in confidence that we were to take a plane to Krehwon and stand by for passengers. We were notified we were to leave _____ Field secretly. Within 30 minutes the rest of the crew reported to us and said that they had heard from a radio operator that we were to leave in a few hours. We were soon besieged with requests from Army and other personnel who wanted to ride with us."

[redacted]

PRESUMABLY BONA FIDE ORDERS

Radio deception is frequently practiced by the enemy in an attempt to gain an objective. This story should serve as a lesson in the importance of AUTHENTICATION. Here is shown how failure to authenticate results in an effortless victory for the enemy.

During the German campaign against Norway, plans were made by the invader for an easy occupation of Bergen. On 9 April 1940 the Germans sailed troop and supply ships, along with escorting cruisers and destroyers, into the harbor. Several hours before this task force arrived, the Norwegian officers at Bergen had received presumably bona fide orders by radio to abandon the fort. Since the Norwegians made no effort to authenticate these messages, they fell easy prey to the Germans' ruse.