

TB SIG 2

WAR DEPARTMENT TECHNICAL BULLETIN

THINK NEXT TIME

War Department, Washington 25, D. C., 15 December 1943

INTRODUCTION.

THESE ARE NOT JUST STORIES—the factual incidents related herein were taken in substance from data furnished by men in army communication units and illustrate a few of the violations of Transmission Security occurring daily. Attendant results from these breaches of security, or “leaks,” are given in some cases; in others, the story is terminated on the note of what might have happened.

To an enemy staff of traffic analysts every breach of radio procedure bears a telling significance. Special attention is given to each violation, glaring in nature or otherwise. It does not matter whether the violation tells a revealing story; the information imparted may be infinitesimal, but its “straw-weight” may break a communication system locally. It is wishful thinking to assume that some casualties, some delays, and some absences of the element of surprise are not directly attributable to an alert enemy organization making prompt use of information furnished through “leaks” provided by deviations from prescribed radio procedure.

~~RESTRICTED~~

The Admiral Ordered Continued Radio Silence.

Here is a story of General Clark's headquarters ship, taken from a stirring account of the Salerno invasion, which portrays fully what major issues hinge on the principles of Transmission Security.

"Late on that flaming Saturday afternoon the *Ancon's* radio room reported the interception of an important enemy message. Many enemy messages were intercepted that afternoon.

"But this one message was too pointed for comfort. *It was a pinpoint location of the headquarters ship, together with an order to sink her at any cost.*

"Admiral Hewitt decided to move the *Ancon* from the Salerno area. At dusk the ship heaved anchor, and, escorted by two destroyers, sailed out to sea. Strict radio silence was ordered. Under a full moon the ship moved out of the battle area. Most of us turned in for the first good sleep in 4 nights.

"At 3:30 a. m. the alarm bells clanged. General quarters! A wave of uneasiness swept the ship. For the first time since the expedition started we were without the ack-ack protection of big naval units. Our location was a secret even from our own fighter cover.

"Up on deck all was ominously quiet. Gunners were at their posts, the human ammunition chain was in position; but there was no order to fire. A slight sea haze diffused the bright moonlight. We could hear, faintly, the drone of planes.

"Down in the wardroom a tense conference was being held. The ship's detecting apparatus had a grim story to reveal: bombers on our port side, bombers on our starboard, all within a 6-mile radius, searching the seas for the *Ancon*.

"Should we break radio silence to ask for air help? Or should we sit tight and quiet? Admiral Hewitt was awakened. He ordered continued radio silence.

"For an hour the crews stood by their guns. We moved nervously about the deck pondering the Admiral's grand gamble. The drone of plane motors grew louder, then receded; revived, and finally was heard no more. The sea haze had saved us from certain destruction.

"In the morning we were back in Salerno Bay. The armada was intact. The bridgehead's first landing field was in operation. Our fighters were thick over the the area. The luftwaffe had failed."

(Reprinted from North American Newspaper Alliance)

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 conveying 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 SOL, 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?

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 G. 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.

The enemy is often furnished VITAL INFORMATION BY PLAIN TEXT TRANSMISSIONS.

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.

DON'T BREAK RADIO SILENCE until ordered to do so by competent authority.

AN ADVANCED ALASKA BASE, April 20.—An Army colonel tells this one:

"One of my 'fist fakers' (a telegrapher who can imitate another's touch) who knows Japanese practiced for months to imitate the 'fist' of a Domei news radio operator who relays daily news to the Kiska garrison.

"One evening, as the Domei sender was almost through tapping out the 'good' news from Tokio to the Rat Island defenders, we jammed the program so that Kiska did not hear his sign off.

"After this 'jam session' our 'fist faker,' imitating the Tokio man's every sending peculiarity, cut in:

"Domei news deeply regrets that Admiral Yamamoto is discredited in imperial circles because he has lost too many valuable ships. The defeat of our naval forces at Coral Sea, Midway, the Solomons, and now our 22-ship convoy to New Guinea has saddened the imperial household."

"Next our operator sent: 'Due to the lack of critical materials, baseballs in Japan have been reduced to the size of golf balls, golf balls to the size of peas, and there are no more peas so we do not play golf any more. Thank you, Kiska, that is all.'

"The Kiska operator, in precise Morse, acknowledged: "Thank you, Domei, for the excellent news. This is radio Kiska signing off. Good night.'"

(Reprinted from Associated Press)

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.

Failure to observe Transmission Security measures makes VITAL INFORMATION available to the enemy.

For Official Use Only.

Numerous infractions of the proper use of radio reflect extreme foolhardiness on the part of some operators. Such is this case.

In February 1942, a radio operator in Charleston, S. C., transmitted the following message in the clear, "German Submarines Sighted in Charleston Harbor." This adolescent trick aroused high authorities, and immediate steps were taken to check the authenticity of the transmission.

The moral in this minor incident is that our communication facilities are for OFFICIAL USE ONLY and should at no time be used for the transmission of foolish traffic or personal messages.

The Enemy Was Also Willing.

In this story a radio operator actually talked with the enemy, and raised his own colonel out of bed.

Apparently the radio operator had for some time harbored a desire to "chat" with the enemy. Late one night while scanning the bands he picked up an enemy station and established contact. The enemy was also willing to chat, so back and forth via C. W. flowed a stream of conversation—until the radio operator realized with a start that he was committing a very serious breach of Army discipline, as well as radio discipline.

Without discontinuing the conversation he dispatched a message to the colonel, who roused himself in all haste to notify G-2. Direction finders were put on the enemy signal and the location was spotted.

Isn't it logical to suppose that the enemy SPOTTED OUR STATION?

Outcome of Individualism.

Occasionally a radio operator finds in the temporary absence of normal restrictions an opportunity to indulge an old, lax habit of batting the breeze. This story is an instance.

When our forces first began establishing outposts on islands in the South Pacific, the radio operations were taken over by skeleton crews who developed small dynasties. Radio procedure was more or less what the men themselves established, and it was common practice to bat the breeze, or transmit in the clear.

Staff Sergeant X, an operator with a speed of 45 to 50 words per minute, was the head of a dynasty with an unbroken record for no services on messages transmitted. He held undisputed

sway until after the battle of the Coral Sea. Then followed an increase in personnel and a heavier volume of traffic.

Very little time elapsed until reminders in the form of quotations from Army Regulations were issued pertaining to transmission security violations, especially sending in the clear.

Staff Sergeant X was resentful of interference—even of Army Regulations. After a month of asserting his belligerence and repeated warnings, he was demoted to buck sergeant. Another month passed with no change in his attitude. The outcome of his continued individualism was a court martial. He was reduced to the rank of private and relieved.

A fast radio operator is still NOT A GOOD OPERATOR unless he follows prescribed procedure.

So Much Confusion.

The demoralizing situation related below is an interesting example of radio deception. If the net-control station had followed the rules of Transmission Security, it would not have happened.

During maneuvers, the artillery in a Blue division dropped the use of authenticators. The radio operator of a Red division passed himself off as the Blue net-control station. He received locations of units, plans of fire, and future movements; he directed fire into an empty field and along an unoccupied ridge; he persuaded the receiving operator to ignore the frantic calls of the real net-control station, and finally created so much confusion and mutual distrust among Blue stations that radio communications broke down completely.

Think of the disaster that would have resulted from a similar situation in combat!

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.

I Was Not Supposed to Comply.

The following incident illustrates a violation of radio-net procedure as told by a station operator.

"UR3 was the net-control station of an artillery net in the Hawaiian Islands. When one of the operators, identifiable by his 'characteristic fist,' remained continually off the air, it was apparent that he had been transferred elsewhere. Sure enough—in a few days I received a call, transmitted by the 'telltale fist,' from a neighboring island. He was unable to establish communication with UR3 in our net, and wanted me to let UR3 know that UR3-7 was calling.

"I went ahead and gave UR3 a call and, shortly after, UR3 and UR3-7 established communication and began exchanging greetings and personal problems. This was obviously a violation of transmission security but as I was not a net-control station, I stood by and listened.

"The following day I learned that a radio intelligence operator had copied my transmission to the unauthorized station UR3-7 and also UR3-7's transmission to UR3.

"UR3-7 made up his own call sign to call a personal friend at UR3. He included his new post in his transmission, thus releasing military information. UR3-7 was not supposed to be working on that frequency, as he held up messages from other stations authorized to operate in the net. I was NOT SUPPOSED to comply with UR3-7's request before making a challenge and receiving a satisfactory answer. The call sign UR3-7 was foreign and NOT in the SOI issued me."

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 submarine would leave the vicinity, having ample time to do so, as the nearest troops were 2 hours flight away."

Don't show your hand by **SENDING IN THE CLEAR!**

Breezy Story.

Here is a story apparently insignificant—and yet the actions of one man failing to do his job in a remote section of the Alaskan Territory could, and probably did, impart to the enemy a fair idea of the use of our procedure signals.

This man, a radio operator, was on duty at his post handling a mere trickle of traffic. To lessen the tedium and amuse himself, he began transmitting a "breezy story," punctuating it with regular procedure signals. During that same period, an intercept operator, policing the bands, tuned him in and discovered this obvious violation of transmission security. Our operator had picked up the offender—**BUT SO HAD THE ENEMY!** And the enemy also had picked up a fair idea of how our procedure signals fit into a message.

Send Over Some Beef.

Here is an example of a striking violation which occurred in the Asiatic Theater.

Our forces were in an extended position, and the proximity to the enemy necessitated the establishment of several outposts. One of these was to be an island outpost about 10 or 12 miles distant from headquarters. To this point were sent radio operators to set up a station.

Then, for approximately a week, came calls in the clear, such as: "Send over some beef, I am ham happy"; "We're all out of water, get some over here"; and other similar transmissions.

The enemy, by listening in for a few days, could have determined the number of men on the island and the tactical disposition—**AND MOST LIKELY DID.**

Oddity of the War.

If there are any doubts existing as to the amount of intelligence gleaned by the enemy from varied sources, here is a story which should quickly dispel any such illusions.

A TWA plane pilot heard a strange radio call one day in mid-Atlantic. A crisp, clear voice in English advised the pilot that he was using the wrong code of the day. And he was! The voice identified itself as belonging to a German submarine commander.

Somehow, somewhere, there had been one leak or several in our communications. Make sure that such leaks do not result from violations of transmission security.

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 antisubmarine 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.

Disastrous results from transmissions erroneously sent in the clear cannot be evaluated.

REF ID: A71866

Enemy Notified.

Frequently, information is imparted to the enemy by an untrained radio operator. The following incident occurred in one outfit, and probably has in numerous others.

The scene of this short story is a combat zone where violations of transmission security may be measured quickly in terms of casualties. Pfc Y was an untrained radio operator who unwittingly notified the enemy as well as the stations within his net, of the call signs to be used the following day, by first identifying each one with the current call sign.

Obviously, the call signs were compromised even before they had been put to use.

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.

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.

No matter how strong the temptation—DON'T CHAT!

Bull Sessions.

Too often the security of a post or station is jeopardized by LAXNESS IN MONITORING the net. The following situation could have been quickly corrected.

The net-control station was located at a post that was, we had reason to believe, unknown to the enemy. As this net linked the post with outposts in the Pacific and Bering Sea, the maintenance of circuit discipline was highly important.

The staff sergeant in charge of the station was an excellent and highly trustworthy operator. As time passed, with only routine messages constituting the traffic, he grew lax, and decided that conversation with one of the other operators would not be harmful.

At 1145 and again at 1200 of each day, stations would be coordinated by the NCS.

The intervening time was used by the staff sergeant for his "bull sessions."

This continued for about 2 weeks until, by chance, the nearest AWS station happened to be listening on the frequency used by this NCS, and heard this transmission: "Yes, Larry left with supplies for the OP at Ybor on the *Stark* yesterday . . ." etc. The staff sergeant was severely disciplined.

MONITORING is a necessary function of Transmission Security.

Suspected Espionage.

Chatting always helps the enemy in one way or another. In this instance it was a means of distracting for several nights the functions of a "spotter" net.

The incident took place overseas in an aircraft-spotter net charged with monitoring both friendly nets and enemy spy stations, and with goniometric activities.

On goniometric operations it was necessary to use radio for communication to Control as the base lines were from 350 to 500 miles distant. Selecting frequencies for 24-hour communication, with available equipment, presented something of a problem. It finally became necessary to use frequencies close to other radio channels of our forces.

In a nearby outpost net there were two radio operators in the habit of passing the night hours by chatting. To escape detection they would shift their frequency. One night, this shift of frequency landed them on the channel of the aircraft-spotter net.

Immediately the spotter net grew alert. Could these be new espionage stations using informal conversation to transmit ship movements to German submarines? Bearings were taken for several nights to determine the locations accurately. An investigation brought the solution—the two radio operators were uncovered as the suspected “espionage” stations.

CHATTING, like crime, NEVER PAYS.

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 Erehwon 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.”

In this particular instance, proper action was taken immediately and no damage was done.

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.

REMEMBER—FOLLOW AUTHENTICATION INSTRUCTIONS TO THE LETTER.

CONCLUSION.

TRANSMISSION SECURITY is an effective countermeasure against enemy efforts to obtain intelligence by an analysis of our transmissions.

If the serious consequences of violating Transmission Security are understood by communication personnel, prescribed radio procedure will be more closely followed.

Maintenance of circuit discipline is dependent upon close supervision by the net-control station, the agency responsible for its enforcement.

Authentication is an effective means of defense against forms of radio deception practiced by the enemy.

ALL VIOLATIONS ARE DANGEROUS. The foregoing stories are intended to provide communication personnel with the form and identity of certain frequent violations.

DON'T ENDANGER YOUR UNIT by—

Transmitting in the clear without proper authorization.

Chatting.

Breaking radio silence.

Sending unauthorized communications.

Using improper radio procedure.

[A. G. 300.5 (27 Nov 43).]

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
Chief of Staff.

OFFICIAL:

J. A. ULIO,

Major General,

The Adjutant General.

DISTRIBUTION: