JANP 143

COMMUNICATION SECURITY

Published by the authority of the

JOINT COMMUNICATIONS BOARD

Washington 25, D. C.

April 1947

FIRST EDITION (7 APRIL 1947)

Original

I

THE JOINT CHIEFS OF STAFF

Washington 25, D. C.

Joint Communications Board

COMMUNICATION SECURITY
(Short Title: JANP 143)

1. This publication is effective on receipt.

2. JANP 143 is a restricted non-registered publication and shall be safe-guarded in accordance with current instructions for the safeguarding of restricted documents. Periodic accounting is not required.

3. JANP 143 may not be carried in Aircraft for use therein.

4. Approved in principle by the Joint Deputy Chiefs of Staff and published by the authority of the

JOINT COMMUNICATIONS BOARD

Washington 25, D. C.

April 1947

E. H. PIERCE
Captain, U.S. Navy

GERALD CARLISLE
Lt. Col., Sig. C. U.S. Army

JOINT SECRETARIAT

Original

JANP 143

RECORD OF CORRECTIONS

Change, Dispatch, Letter or Memorandum No.	Date	By whom entered (signature, rank or rate, name of command)

Original

RESTRICTED

RECORD OF CORRECTIONS - Continued

Change, Dispatch, Letter or Memorandum No.	Date	By whom entered (signature, rank or rate, name of command)

Original

LIST OF EFFECTIVE PAGES JANP 143

(All numbers are inclusive)

Section	Page	Change No.	Section	Page	Change No.
	I to VIII	Original			
1	1 - 1Ø	Original			
2	11 - 16	Original			
3	17 (reverse blank)	Original			

INTRODUCTION

Intelligence is an offensive weapon, one which searches out the vulnerable points in a nation's armor, and attacks strong points again and again, until they, too, are made weak. The only defense against intelligence is security and no form of security is more important or more effective than communication security.

In the words of Frederick the Great, "If one could always be acquainted with the enemy's designs one would always beat him with an inferior force." And, in the words of a German of more recent vintage, a prisoner of the past war, "If U. S. troops win the war it will be in spite of their communication security and not because of it."

The establishment and maintenance of communications security is a function of command, a function that unfortunately is not always understood, not always correctly performed. This pampblet will attempt to bring home to all officers their past deficiencies in communication security and the steps recommended to correct them.

Original

CHAPTER I

THE COMMANDER'S RESPONSIBILITY--COMMUNICATION SECURITY

Every commander, regardless of echelon, must be vitally concerned with security in all its phases, for every commander is constantly receiving and disseminating classified information. Without a secure communication system the commanding officer of a modern armed force cannot safely transmit information to, or receive information from, commanders of other units.

The measures that a commanding officer employs to prevent compromise of the traffic handled by the systems of his unit constitute communication security. His responsibility in this regard is shared to a certain degree by his cryptosecurity and communication officers but because of the highly important relation of security to tactics, the commanding officer himself has the final responsibility.

SECURITY IN STAFF WORK

Communication security is definitely an item for staff consideration and understanding. The commander should take communication problems into the conference rooms as an operational part of command. He should require his security personnel to make periodic reports of how much information has been exposed to the enemy. This information should be considered when making military decisions. The status of security of communications should be coordinated with various staff sections, particularly operations.

It is obviously adverse diplomacy for a junior officer to tell his senior officer what he can, can't or must do. However, it is the duty of the junior (staff officer) so to inform his superior (commander) regarding communication security that the commander decides and acts with knowledge and not in ignorance of risks involved. Completed staff action in this case is a definite "must," and the commander should demand it.

The final responsibility of command for communication security cannot be delegated. However, it is an unwise commander who attempts to do all the work of his staff. Regulations permit him to appoint an officer of his staff as the security officer, cryptosecurity officer, Top Secret control officer, or communication security officer. This officer then is responsible to his commander for the execution of his appointed task. The importance of his job cannot be overemphasized. Perhaps the most important job of an officer in this position is that of cryptosecurity. Actual examples of insecure cryptographic practices point out the necessity for strict control of means of communication.

1. Failure to Report Loss of Codes or Ciphers

   For eight days a military code was used after it had fallen into the hands of the enemy, because compromise was not reported immediately, as required by instructions. Fortunately, it was a special-purpose code not ordinarily used for secret traffic, but the damage might have been very great. There is no way of knowing how great it actually was.

2. Discretion in Destruction

   A naval vessel was engaged in a running battle with enemy craft in the English Channel. Considering the relative position of ship, enemy, the rocky French coast, and other circumstances, the commanding officer decided that to jettison the registered publications was a necessary

Original

1

precaution. When the order to jettison was given, one sack of pub-
lications landed on a submerged rock. The sack broke open and a swift
tide scattered the publications far and wide. Subsequently, many of the
publications were recovered through the efforts of other naval vessels.
Some were picked up by French fishing vessels, others were found along
the shore. Some were never found and supersession of many publications
was necessary. While it is difficult to criticize acts committed under
such circumstances, it must be pointed out that both instructions and
good judgment require that jettisoning be done in deep waters. Had the
publications been put over the side earlier, considerable inconvenience
to allied communications and the expense of replacement of compromised
publications might well have been avoided.

3. __Use of Superseded Publications__

Because a superseded code was used to transmit a warning, an Army
bomber group in the China-Burma-India Theater nearly came to disaster
during the war. The group was on its way toward Kyushu in Japan and
had been gone about two hours when the Navy reported a sudden hurricane
off the Japanese coast. All fields were ordered to establish communic-
tion with their planes and change the target to Shanghai. Each base
notified its planes without incident except for one base, which encrypted
the hurricane message in an obsolete code. The planes operating from
that base copied the message readily enough, but reported that they could
not decrypt it. The crypto officer at the base was not in the crypto-
room, and the nature of the difficulty could not be determined at once.
By the time the message had been encrypted correctly it was too late.
The planes were beyond the range of communication. Unwarned, they rode
into the hurricane, narrowly escaped destruction, and had barely enough
fuel to return to a China base. By just one error in the use of a crypto-
system the lives of 300 airmen were thus jeopardized and the efforts of
2,000 men expended uselessly.

4. __Loose Handling of SOI'S__

Two bombers crashed into the sea while on a training flight. Each
carried a nearly complete set of signal operation instructions. As a
result, the SOI's issued by the bomber command were compromised for a
period of several days.

A pilot returning from a training flight discovered that a portion
of an SOI folder was missing. The radio operator was of the opinion
that the portion was not in the folder when it was handed to him. How-
ever, it was necessary to report that the missing SOI possibly had been
compromised, since no check of the contents of the folder had been made
prior to the flight by the issuing officer or the operator.

Certain signal operation instructions contain information of extreme
importance to the enemy. Therefore, crew members on tactical flights are
permitted to carry ONLY those extracts of SOI's which are necessary for
pursuance of immediate tactical operations. Precautions which are neces-
sary for tactical flights should be observed during the training period
and commanders must assure a realistic approach to all security practices
during training exercises.

5. __Use of Unapproved Codes and Ciphers__

It is an obvious truth that precautions must be observed in consider-
ing plans for operations. Without security it would be impossible to
achieve surprise in attack. Codes and ciphers are furnished to a com-
mander so he can achieve surprise and control his forces, without his

Original

intentions being known to the enemy or to those parts of his own forces which should not know future operations. The pressure of war may force us to use less secure cryptographic systems. The commander therefore should be aware of the weaknesses in those systems upon which he may be forced to rely. He should prevent the use of locally produced crypto-graphic schemes. Nothing can lead to more trouble than relying on a crypto-aid which cannot stand before an enemy expert. Only approved codes should be used within the services.

SECURITY IN THE USE OF MEANS OF TRANSMISSION

Because commanders are forced for the most part to rely on electrical communications to effect the dissemination and receiving of classified in-formation it will be well to determine just how private these means are in order that the information which has been encrypted, and even the crypto-systems themselves, may accomplish the desired purpose and not become in-effective through disclosure or compromise.

Wire transmission is rightly considered to more secure than radio, but only because interception of radio transmission is so much easier, not because wire lines are free from interception.

Interception on wire lines is a frequent and important source of in-telligence. Wire tapping often may be discovered through physical examin-ation or from transmission irregularities, but interception by induction can escape detection completely. A supposedly secure communication circuit of a physically checked wire may still be intercepted by use of a concealed coil of wire placed as far as six feet from the communication line -- even if the six feet consist of reinforced concrete.

During the war the Germans consistently used many clever tricks to intercept communications and to conceal the fact that interception was going on. They placed carefully hidden taps on wire lines which they were abandon-ing and which they knew advancing Allied troops would use for their own communications. In one instance the Russians found a communication system in splendid condition in a village evacuated by the Germans, but careful exam-ination showed that something had been added. A buried cable extended from each end of the village circuit. They learned later that the Germans had made a large arc with the village line as the center, the buried cables form-ing the ends of the arc well within the German defenses.

The use of radio to a point where it has become the prime means of electrical communication has had a profound effect upon communication security. The speed, range, and versatility of radio have kept communications apace with the mobility of modern warfare. But the use of radio has also exposed communications to their greatest danger--radio transmissions can be inter-cepted by friend, neutral, and foe alike. The mere fact that a radio station is on the air is a source of information to the enemy. The extensive use of intercept stations and direction finders enables the enemy to record every transmission that is made and to log the place of its origin, thereby giving him an opportunity to follow troop movements and to learn the identity, strength, plan or tactical disposition of a military force.

A single electrical impulse may indicate the existence of a unit. Upon one occasion during the North African campaign, several aircraft were sent on a mission and every precaution had been taken to conceal the size of the flight. While enroute a radio operator on one of the planes carelessly tapped his key. Another operator thoughtlessly responded by tapping his key twice. The remainder of the operators in the flight eagerly entered into the "game," each adding a "dit" to his response. All previous efforts to conceal the

Original

3

JANP 143

flight were lost since this "harmless" game disclosed to the listening enemy the exact number of aircraft in flight without a message being sent. <u>The mission was unsuccessful and serious losses resulted</u>.

LOCATION BY RADIO

Direction finding today is more effective than many officers realize. Although radio silence can be carried too far, it has lost none of its importance. Tests of captured equipment show that it is possible at a distance of 100 miles to locate accurately by direction finding a 50 watt VHF transmitter. Forward observers and naval gunfire liaison officers reported that the Germans possessed effective D/F equipment and were able to locate key radio stations and subject them to fire in a matter of seconds, according to an official report from one sector. Beach patrols thought it expedient not to use their radios until after German batteries had been driven out of range.

In the North African campaign, a U.S. tank destroyer battalion was moving into postion to attack, and radio silence was ordered. After several hours, a detachment from the battalion realized it was lost and broke radio silence to verify its position. That enemy direction finders were on the alert is evidenced by the fact that a subsequent air attack wiped out the entire detachment.

Naval vessels also suffered as a result of ill-advised use of radio. Over-use of radio was given as one reason for the loss of ten Allied submarines in the Mediterranean during the early months of the war against Italy. PT boats were often bombed by float planes immediately after radio transmissions although the planes had previously passed overhead several times without attacking. Submarines operating in the Pacific noticed on several occasions that use of radio brought a patrol boat or plane to search in the vicinity the next day. One submarine reported that a radio transmission led to both aircraft and surface interception within 17 hours. "Numerous close Jap radio stations seemed to D/F the submarines quite accurately," one report declared.

A vessel in the European Theater broke radio silence to report a rudder casualty. This report could have been cleared later by visual methods. In another case, radio silence was broken to report a small hole in the ship's side, well above the waterline, the sea being quite calm at the time. The operation plan specifically stated that strict radio silence was to be maintained and that submarine and other enemy contacts were to be reported by visual methods.

Under some circumstances radio silence may be less important for planes than for surface ships. Failure to observe radio silence, however, may disclose a flight which would otherwise surprise the enemy, and insure for the planes a deadlier reception while performing their mission than they would otherwise encounter.

RATIONALIZING RADIO SILENCE

Although it is one of the most effective components of communication security, radio silence can be carried to the point where it becomes a handicap rather than a protection. When it is reasonable to assume that the enemy is unaware of the presence or precise location of a task force or ship and does not anticipate the operation which is about to commence, the breaking of radio silence must be ordered only as a calculated risk. However, when it is certain that the enemy knows the location or anticipates the movements of a ship or task force, or when contact has been made, there is little to gain by radio silence. Dispensing with fighter direction in order to preserve radio silence was given officially as one of the factors contributing

Original

to the loss of a United States cruiser early in the war. Observance of radio silence upon the occasion of a positive enemy contact shows a lack of appreciation of the offensive action expected of units of the fleet and jeopardizes the safety of all other units in the vicinity.

A JAPANESE COMMENT

Eloquent testimony on the subject of radio silence was offered in a Japanese broadcast beamed to the United States from Batavia in the Netherlands East Indies during the war. It read in part as follows:

"If the Americans are so eager to fight the Japanese Navy, why do they dive into a complete radio silence as long as they understand that the Japanese Navy will come out and meet them? If one may believe the Americans, there were not many Japanese ships at Truk when they attacked there. Notwithstanding the fact there were only small units of the Japanese fleet, and notwithstanding the fact that the Americans announced the attack on Truk as a crippling blow, they kept a complete radio silence as long as they were within the reach of Japanese forces in Truk."

SUCCESSES OF JAPANESE INTELLIGENCE

Interrogation of Japanese intelligence officers 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 Commander Hideo Ozawa and the other was Lt. Comdr. T. Satake. Both held key posts in the radio intelligence section of the Japanese Naval General Staff during most of the war.

Owada was the center of the activity described by Ozawa 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.

Traffic was analyzed according to call signs, cryptosystems, plain language, total volume, procedure signals, and precedence. Volume and precedence were plotted on a chart, one for 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.

United States operators were often identified by individual peculiarities in sending. As a rule ships could not be traced, however, presumably because radio silence prevailed quite generally. The enemy analysts were not able to estimate the strength of our forces in various theaters. If a force broke radio silence, the enemy would start a new search in the area.

It was realized that a peak in traffic represented "a crisis." The interpretation "was completely dependent upon the tactical situation," however, and the Owada officers "could not tell where that crisis would materialize."

Taking Okinawa as an example, Satake made a statement translated as follows: "A month before Okinawa, BAMS***(Radio Broadcast) had a notable increase in transmissions. Ten days before the Okinawa operation, there was a marked increase in submarine reports. These are easy to spot because we got good direction-finder fixes as they are close 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 on the tactical situation."

Original

REF ID:A71913

Ozawa, 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." Aside from "some minor success in predicting the Iwo Jima landing," Ozawa claimed little or no success in other operations.

Air-to-air and air-to-ground coded information was received and "we were able to interpret much of it," but "the rapidity with which aircraft codes were changed caused confusion to us," Ozawa stated. Our aircraft often gave away our plans. When B-29s prepared to take off "there was much adjusting of radio frequencies." Moreover, "weather reconnaissance planes which preceded large strikes gave an indication of the large strike by the volume of data sent back to its base." Ozawa claimed 50 percent success in making predications based on weather reconnaissance flights.

It may have been due largely to our defensive measures against traffic analysis and also against interception and direction finding that the enemy did not learn more and was seldom certain of the deductions that he felt justified in making.

USE OF RADIOTELEPHONE

In this treatment of radio security a particular and separate emphasis must be placed on the proper use of radiotelephone. During the second world war its incorrect usage constituted one of the most vulnerable spots in the security armor of communications. Too much emphasis cannot be placed on the need for extreme security consciousness in the use of radiotelephone, for the fact that such equipment can be operated by other than trained personnel increases the need for adequate control and complicates the problems of good circuit discipline, correct procedure and strict adherence to all security precautions.

The security of voice codes is comparatively limited even though they are prepared by experts and offically approved. This is due to the necessity for simplicity. However, the outstanding difficulty encountered in the security of voice codes can be attributed chiefly to the so-called private organizational codes. This was clearly demonstrated in operations in Sicily and Italy. Information obtained from prisoners indicated that the Germans were usually able to figure out these private codes rather easily. Veiled language is scarcely more difficult for the enemy to understand than for the person being addressed.

Use of a foreign language does not provide any measure of security as a rule, although U.S. forces are said to have used Choctaw and Navajo Indians as telephone talkers quite successfully. The British used Latin as a makeshift during the Boer War because they knew the Boers were not familiar with it, but the Boers would certainly have found someone who was if the British had depended on Latin very long.

The mistaken idea that voice radio transmissions are more secure than keyed transmissions is one of the most treacherous illusions in the field of electronic communication. The insecurity of VHF transmissions was not generally realized during the early years of the war. This fact explains in part the tendency to use voice radio circuits too much and to transmit information which should not have gone out on the air, even in a voice code. In 1945 a headquarters ship on a two-week voyage from Iwo Jima to Pearl Harbor was able

Original

6

to log each day VHF transmissions from Iwo, the Ryukyus, or the Philippines for several hours a day until the day before it arrived. The maximum range at which solid signals were picked up was 3700 miles. The more a commanding officer knows about radio wave propagation at various frequencies, the more discreet and judicious he is likely to be in his use of voice radio. His is the direct responsibility for its secure use.

VHF, UHF, and SHF designate specific bands of "very high," "ultra high" and "super high" frequencies (30,000 to 30,000,000 kc) which are employed for the very reason that their normal range is limited roughly to "line of sight." Instances continue to accumulate, however, of verified reception at distances of several thousand miles. Thus, even though higher frequency bands normally provide more limited range characteristics than the lower frequencies, they are not secure enough to justify use of plain language which on lower frequencies would have to be encrypted. Voice transmissions on any frequency are, in reality, less secure than CW on the same frequency because anyone can understand them--without knowing the telegraphic code. Carelessness on VHF leads to carelessness on MF and HF voice circuits.

The fact that radio is the least secure of the means used for transmitting messages makes it necessary for anyone using radiotelephone to be thoroughly versed in radio procedure. Radio procedure is formulated to insure a rapid and accurate method of transmitting and receiving messages in a brief, definite and uniform language. In the interests of security, no variations, elaborations or short cuts on the prescribed procedure should be authorized.

In order to prevent the enemy from gaining much information from his observation of radio activity, the principles of radio security have been developed. These principles are grouped into four categories: Discipline, Silence, Deception and Interference.

RADIO DISCIPLINE

Radio transmission security embodies the maintenance of circuit discipline and the suppression of all superfluous transmissions. That component of radio transmission security which includes the maintenance and proper use of radio equipment, the adherence to prescribed procedure when operating and the employment of remedial action when and where necessary by the net control station or other responsible agency is known as circuit or radio discipline. Corrective measures taken toward the suppression of excessive transmissions are formulated on the basis of procedure analysis of monitored material. Security monitoring logs are analyzed for deviations from prescribed procedure to determine trends in violations. Analyses indicate the nature and extent of corrective action to be taken within the units concerned. Radio transmission security is attained by the following:

1. Training radio operators in the principles of circuit discipline.
2. Monitoring transmissions of our forces.
3. Instituting remedial action for security violations when and where necessary.

Radio discipline requires more than blind obedience to the rules. It includes active imagination on the part of anyone using radiotelephone in order to deny all information to the enemy which may help him analyze the message intercepted. It should be impressed that continued alertness must be the watchword of all communication personnel. It was an alert German operator who noted, during the first world war, that the shore station at Scapa Flow broadcast weather reports only when Grand Fleet units were at sea. He thus could advise the German Admiralty when British ships left their base.

Original

There are basic rules that should be remembered and followed by anyone using radiotelephone. While these rules and many more should be instilled in trained radio operators, these should be of particular concern to the officer who, on occasion, used radiotelephone.

1. LISTEN BEFORE SPEAKING. Failure to do this causes loss of time and makes additional transmissions necessary.

2. SPEAK CLEARLY. Clipped speech and ₄jammed-together words are difficult to understand.

3. SPEAK SLOWLY. Must be slow enough to be copied without "repeats."

4. SPEAK EVENLY. Not in a monotone.

5. KEEP THE DISTANCE FROM MOUTH TO MIKE THE SAME AT ALL TIMES. Inexperienced perronnel often fail to realize the importance of this detail.

6. MAINTAIN A NATURAL RHYTHM. Group words and phrases in a normal manner. Transmit phrase by phrase, not word by word, avoiding "er's" and "ah's."

7. USE STANDARD PRONUNCIATION. Standard speech without sectional peculiarities is most easily understood.

8. KEEP TRANSMISSION TO A MINIMUM. Avoid crowding circuits with excessive call-ups, receipts, tuning, testing, and unnecessary repetitions.

9. USE STANDARD PHRASEOLOGY. Continuea use has made its meanings unmistakable. Nicknames and fancy language are confusing and less brief.

10. INCLUDE SUFFICIENT INFORMATION. Messages omitting necessary information are worthless.

11. DO NOT COMPROMISE VOICE CODES.. Never state in plain language what has just been transmitted in voice code.

12. USE PLAIN LANGUAGE WITH THE GREATEST DISCRETION. Future operations have sometimes been discussed on voice circuits. An instance at Tarawa gave the enemy advance warning of landings planned at other points subsequent to the initial landing.

13. DEMAND AUTHENTICATION WHENEVER THERE IS CAUSE FOR SUSPICION. Do not allow enemy attempts at deception to succeed. He can speak excellent English when the need arises.

SILENCE

As stated previously, radio silence is the primary defense against interception and direction finding. Both interception and direction finding are now effective on nearly all frequencies. A transmission of only a few seconds duration is sometimes sufficient for obtaining a bearing. Avoid all unauthorized transmissions and unnecessary testing.

DECEPTION

Although adaptable to any means of communication, deception is employed chiefly in connection with radio. There have been many instances in which the enemy has attempted to disrupt communications to prevent a message from being delivered, divert our forces or draw them into a trap. Enemy methods

Original

include answering call-ups and offering to accept traffic, receipting for messages which our stations have not been able to copy, transmitting false orders by voice or radiotelegraph in plain language and originating messages pieced together from parts of intercepted messages.

The greatest defense against enemy attempts at deception is the correct use of authentication. Incorrect authentication undermines communications and invites deception, especially in combat when seconds count. Even an occasional error far from the scene of action is a serious matter. It delays traffic and encourages operators to distrust or disregard an important means of protection. A vital message may be disregarded.

An incident illustrates quite clearly what could happen in actual combat: "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 location 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 the Blue stations that radio communications broke down completely." Unless radio operators are thoroughly instructed and well-trained in the use of authenticators THEY WILL MAKE MISTAKES. In order not to forget about authenticators it is necessary to review instructions and PRACTICE them.

Japanese deceptive ingenuity in obtaining information from AAF radio operators was revealed by reports from the Central Pacific. A B-29 which participated in a mission over Japan gave its altitude, course and speed in response to a radio query, apparently from a plane that had become detached from the formation. Immediately the formation experienced intense and accurate antiaircraft fire. This could have been avoided by proper authentication. Another B-29 on a later mission, in reply to a similar query, gave inaccurate information with the result that antiaircraft fire became "intense and accurate" at an altitude far below the B-29 formation.

Appropriate training manuals contain measures designed to prevent enemy interference from succeeding. Listed below are some of the more important ones to be remembered by commanding officers as well as radio operators.

1. Improve procedure and circuit discipline. These should attain such perfection as to nullify any attempt by an enemy to imitate procedure.

2. Demand authentication whenever there is call for suspicion. Plain language is more vulnerable to deception than encrypted traffic. A request for authentication will usually expose and silence the most determined effort of deception. All personnel using radio must be able to authenticate PROMPTLY AND ACCURATELY.

3. Keep accurate logs. These will be useful in studying suspicious transmissions. Much can be learned from them.

4. Do not reveal the precedence of messages awaiting transmission if this can be avoided. Doing this may invite interference if the precedence is high. The enemy may try to accept the message, receipt for it or jam the transmission if all else fails.

5. Keep procedure messages and service messages at a minimum. These help the enemy to learn our procedure and meanings of operating signals, thus making imitation comparatively easy.

6. Respond promptly on call-ups. Long call-ups are an invitation to the enemy to come in on a circuit.

7. Report all irregularities at once. This may help in discovering

Original

whether the interfering station is genuine or not. If it is not, this
might also help destroy it.

"During the Tarawa operation, a Japanese operator took over the
the call of the commander of one of the transport divisions and
and gave orders to land troops and supplies to the westward of a
certain pier. The position of Jap automatic weapons at that time
was such that this was the worst place to land. The operator was
alert and suspicious. He demanded authentication. When this was
not forthcoming, an urgent was broadcast to disregard this deception
and the Jap attempt failed. This illustrates the necessity for
constant use of authenticators during such periods."

8. In regard to radiotelephone, remember the two basic assumptions that
must always be considered whenever radiotelephone or wire circuits are
used.

   a. All telephone calls over a circuit which has a radio link
       will be heard by the enemy.

   b. All telephone calls over wire circuits may be heard by the
       enemy.

"A telephone circuit which had a radio link was monitored for three
hours. Headquarters Third U. S. Army disclosed that during this brief
period sufficient material was provided 'to enable friendly monitors to
establish a fairly complete personality file for this headquarters,
almost the complete order of battle for our higher echelons, and the
exact coordinates of this headquarters advance command post one day
prior to its opening.'"

Having treated the command functions in regard to signal security it
would be well now to turn to the originator and determine his position in the
over-all pattern of secure and efficient communications.

Original

10

CHAPTER II

THE ORIGINATOR AND COMMUNICATION SECURITY

The mission of a military communication service is to provide reliable, rapid and secure communication to command. The most direct, and often the only, contact that many officers have with communications is in the capacity of originators or addressees of messages. It is essential that those who use this service are aware of and observe the relatively few basic rules which will assist materially in the accomplishment of this mission.

Messages which make the grade on security counts will usually be found satisfactory by any other communication standard. Communication security begins with the originator. His skill in drafting a classified message has an important bearing on the security of the ciphers used. If he has learned the secrets of brevity, his message will take less time to encrypt, transmit, and decrypt. The net result of similar skill on the part of all originators will make a surprising improvement in the speed with which messages are transmitted and delivered. Clearness and exactness also pay dividends. A message which is not clear causes misunderstanding or necessitates a service message. If the messages are classified, security suffers, and in any case the over-all speed of communications is reduced proportionately.

MUST IT GO BY RADIO?

It is obvious that if no messages are originated no security problems exist. This happy state of affairs cannot now be anticipated. It is possible, however, to keep a large proportion of communications out of the most rapid, yet most insecure methods of transmission. The first responsibility of an originator is to specify another but more secure means of communication than electrical whenever circumstances permit. He can thus cooperate in keeping overloaded circuits clear enough for maximum speed when minutes are really important. By such cooperation he will use messenger service in the field in preference to electrical communication whenever practicable. At sea he will make maximum use of dispatch boat, message drop, or visual means, depending on the length of his message, weather conditions, radio silence requirements and other factors. On shore he has a fast mail service of unlimited capacity at his disposal, at least in the United States; or he may employ guard mail or air courier services and sometimes diplomatic pouch if he is in a foreign country.

U.S. mail service frequently equals the speed of a low precedence message. In continental United States no two points are more than a day apart for mail planes, and the U.S. postal system is sufficiently secure for most confidential and secret communications.

Before using radio or any other electrical means of communication, therefore, an originator should invariably ask himself, "isn't there some other way of getting this message to the addressees which will serve just as well and is at the same time _more_ secure?" Sometimes methods other than radio are faster. This has been the case with visual methods more than once during landing operations, and the same has proved true for mail plane service in advanced areas as well as in the United States.

WHO NEEDS TO KNOW?

The second responsibility of all who draft or release messages is to keep addressees at a minimum. Unnecessary addressees lengthen the text or the heading unduly, and often make it necessary to relay a message on more

Original

circuits than would otherwise be required. Sometimes a more widely held and therefore less secure cipher must be employed because a remote outpost is addressed.

Failure to include an addressee who needs the information a message contains can be potentially more harmful to security, however, than unnecessary addressees. The reason is that it may be necessary to re-encrypt the message in a different cipher for an addressee whom someone thought of too late. The dangers of re-encryption are well known. Any progress an enemy may have made in breaking one of the systems can be applied to the other when a re-encryption is detected.

The tendency toward including too many addressees is international. The following statement was found in 1944 in the notebook of a Japanese officer:

> "The purposeless designation of addressees on a grand scale complicates the exchange of communications and leads to an increase in the number of messages."

Truer words were never spoken. Here again it is the originator to a large degree who determines the speed and efficiency of his servant, the communication system.

HOW SOON MUST IT BE ACTED ON?

A third responsibility connected with the drafting of messages is judicious use of precedence. Time and again during the war high precedence messages, requiring the utmost speed were delayed by other messages which had been assigned equally high precedence merely because the persons who drafted them thought their own messages the only really important messages being originated, and overlooked the need for economical use of existing circuits. In one case, which caused widespread comment and brought vigorous action, a red-hot operational priority dispatch from the Commander-in-Chief of the U.S. Fleet was delayed 6-1/2 hours and arrived too late to serve its purpose. That same afternoon as it turned out, there were 110 other operational priority dispatches waiting to be transmitted, most of them barely lukewarm. Subsequent investigation showed that scarcely a dozen were of sufficient urgency to justify the precedence carried. Another case involving the misuse of precedence occurred at and army headquarters. A message with priority precedence came in addressed to two officers who were not at that headquarters. It was necessary to go back to the originator in order to find out whether the message had been addressed correctly. "Sit on the message," the originator replied. "The two officers are on their way and arrive in a couple of days."

In many cases a high precedence may be required for the action addressee, but a lower degree will suffice for information addressees. If message drafters make a habit of assigning a lower precedence to information addressees when practicable, communications will be able to function more rapidly when speed is required.

The following considerations are also of great importance in the intelligent use of precedence:

1. Precedence begins when a message is drafted. It is only fair to expect originators and releasing officers to handle it with the same speed they expect of communications.

2. Precedence is a guide for communication personnel, not addressees. It is better to ask whether the text alone requires prompt action than to insist on speed of transmission, since high precedence gains speed on

Original

the circuits only and does not require prompt action on the part of the
addressee.

3. <u>Time zone differences have an important bearing on precedence.</u> For
example, routine precedence may be too high for a westbound message and
too low for an eastbound message. It is not intelligent generalship nor
admirable naval tactics to assign a precedence which results in delivery
during the night when no action is necessary until the following morning.

<div align="center">DOES IT SAY WHAT YOU MEAN?</div>

Drafting the text with completeness, clearness, and brevity is never easy.
Patience, practice, and resourcefulness are needed. The first try is not likely
to be satisfactory unless the drafter has had thorough training and consider-
able experience. A dictated message is almost certain to be wordy and there-
fore very unmilitary. If it doesn't contain too many words, it probably con-
tains long, pompous ones which are out of place in message texts.

<u>Completeness</u> is the first requirement of a well drafted message. If it
does not give all the necessary facts, it may be little better than no message
at all, especially when combat is imminent or in progress.

During 1943 the enemy was able to sink one of our ships and escape un-
harmed from American waters because of incomplete messages and failure to send
a message at all. One plane reported the rescue of survivors but failed to
give the time or position of the attack, or the course of the enemy submarine.
Another neglected to make an amplifying report. A third plane failed to give
the position of the submarine or to communicate with a plane which was in a
position to assist; it also failed to make adequate amplifying reports and used
code when speed was vital and plain language would have been of little value to
the enemy. Accuracy is also of vital importance. Downed aviators were some-
times lost during the war because reporting planes in their eagerness to hasten
a rescue gave incorrect positions. Later corrections did not always get
through. Numerous instances could be cited.

<u>Clearness</u> is another major factor in message drafting. A message which
does not say exactly what the originator intends to say or one which can be
read with two quite different meanings is likely to lead to confusion and
disaster. This fact was forcefully stated in a CINCPAC-CINCPOA report of
operations in the Pacific:

> "A little thought will show that the dispatches one sends may be
> more vitally important than anything else he is likely to do in
> the battle; and that however great the stress of the situation,
> one must apply to their contents and phrasing the same cool, cal-
> culating judgment that he would use in spotting salvos, launching
> bombs or torpedoes, or maneuvering his ship or plane against the
> enemy.

> "Let us suppose (for the emphasis of comparison only) that one of
> our ships or planes should desert in the face of the enemy and seek
> safety in flight, or that its personnel should be so flustered by
> danger as to be ineffectual in the battle. The very thought is
> abhorrent to us; and yet if this thing should happen, the harm done
> might not be serious. It would be only one unit failing; and others
> of sterner stuff could be counted on to make up for it.

> "But a single inaccurate or misleading dispatch, though drafted
> by someone of impeccable loyalty and courage, can easily work far
> greater harm than the foregoing suppositious defection, since it
> may be the cause of error or delay in the action taken, not merely

<div align="right">Original</div>

by one plane or ship, but by whole groups or forces. Thus, from the standpoint of the results, a force thirsting for combat with the enemy, but hunting for him in the wrong place because of a too-hastily worded dispatch may fail as badly as though it had little stomach for fighting at all ....".

Lack of clearness affects communication security as well as operational security in a very definite way. If time permits, each addressee must ask for clarification. The resulting exchange of communications may not be completed during the day on which it began, and in wartime call sign ciphers or cryptosystems which change daily will be linked, thus facilitating compromise.

CAN IT BE MADE SHORTER?

Studies indicate that messages can be clear and complete yet considerably shorter than the average military message now is. Here are five ways in which brevity can be achieved:

1. <u>Kill unnecessary amplifying details</u>. Strike, search and intelligence reports were frequent offenders during the war. Only information of operational value was needed. Reconnaissance and situation reports from secondary areas were over-written 25%-75%.

2. Strike out superfluous words such as <u>number</u>, <u>following</u>, and <u>dated</u>, before submitting a message for release, thus:

As Sent	Recommended	Saving
reurser <u>number</u> 981	REURSER 981	43%
answers request <u>contained</u> in your	ANSWERS YOUR	62%
urltr <u>dated</u> six July	URLTR SIX JULY	29%
CNO <u>dispatch</u> 292359 June	CNO 292359 JUN	43%
<u>following</u> items needed colon	NEED	84%
<u>accomplish</u> repairs	REPAIR	65%
to <u>effect</u> repair of	TO REPAIR	50%

A submarine in the eastern Mediterranean in one instance used <u>north</u> and <u>east</u> 18 times in a single message. Neither word was needed more than once for clearness.

3. <u>Use shorter words and phrases</u>. Request expressions are among the worst offenders. For cryptosecurity as well as brevity the following substitutions are preferable:

As Sent	Recommended	Saving
Request reply	ANSWER	50%
Request following items	SEND	81%
Request shipment five spares	SHIP FIVE SPARES	44%

In all such expressions <u>please</u> is understood.

<u>Report</u> and <u>advise</u> are two other words, which, like <u>request</u>, occur too often. <u>Advise earliest practicable shipping date</u> might well be replaced with the simple question HOW SOON CAN YOU SEND.

4. <u>Use authorized abbreviations</u>. They are well known, and their use saves time and trouble. When an abbreviation is very short and a garble of one or two letters of the abbreviation may be represented by their phonetic words--unless the word itself is shorter than the phonetics for its abbreviation. A/C apart from identifying words might give trouble,

Original

but ABLE SLANT CHARLIE is twice as long as AIRCRAFT.

5. <u>Avoid unnecessary use of phonetics</u>. They only waste space in expressions like UNCLE SUGAR MIKE CHARLIE, but they serve a useful purpose in LOVE SUGAR TARE when used apart from the name, number, or other iden- ·tification. The following is an extreme example of phonetics gone beserk, all of the expressions having appeared in a single message of medium length:

CHARLIE OBOE MIKE DOG TARE NAN YOKE DOG for COMDT NYD
SUGAR OBOE NAN YOKE DOG for SUPOF NYD
UNCLE ROGER SUGAR SLANT ROGER apparently for URSER
ROGER YOKE EASY XRAY PETER BAKER SLANT LOVE apparently for
       RAILWAY EXPRESS BLADING
ITEM NAN VICTOR apparently intended to mean INVENTORY

This little orgy lengthened the message by 18 groups or about 20%, and the message would have been 10 groups shorter than it was <u>if all of these words had been fully spelled</u>.

Other useful ways of achieving brevity include the deletion of unnecessary punctuation. Telegraphic style has small place for it, and its use should be severely limited. Combining reports is another important way to reduce traffic. Fuel and ammunition reports for example, may serve their purpose equally well if required less frequently.

                    DON'T QUOTE

Quotations from another message or almost any other source are a security hazard. The danger is much greater with some cryptosystems than others, but an originator has no way of knowing which cryptosystem will be used. The rule is therefore very simple: restate in different words if necessary, but <u>avoid verbatim quotations</u>.

                 WHAT ABOUT THAT REFERENCE?

References are security hazards if they appear too often at the beginning of a message. They should be buried in the text. Plain language references to encrypted messages are dangerous in that they often reveal the subject of referenced messages. For this reason plain language references to encrypted messages are limited to those which consist of the date-time group reference plus one or more of the following words - Affirmative, Negative, Interrogatory, Comply, or Letter.

               DOES IT AFFECT THE NATIONAL SECURITY?

The final responsibility of the drafter, once he has assigned a reasonable precedence and drafted the text securely is to classify realistically. Over-classification on a large scale undermines respect for the higher classifica-tions, overloads the secret keys to cryptosystems, and encourages laxity in handling and safeguarding documents and the information they contain. Under-classification is dangerous but much less common. Frequent reference to the definitions of Top Secret, Secret, Confidential, and Restricted in Army or Navy Regulations will help all drafters of messages to find the happy medium between underclassification and overclassification.

                                                Original

                          15

CHAPTER III

COMMUNICATION SECURITY IN PEACETIME

The continuing importance of communication security cannot be over-emphasized. Since the cessation of hostilities a large volume of classified information has been downgraded; however, a tremendous amount of information remains classified and of vital interest to the national security, and is constantly being added to by current developments. In addition, potential enemies will have more leisure in which to attempt penetration of our security barriers.

It is essential that the elements of communication security be understood and provided for at all levels. Those who use the communication service must learn and practise the drafting of clear, complete, concise messages, and assign realistic classifications and precedences. Physical security must be considered. Efforts to steal, copy, photograph, or otherwise obtain cipher keys and specifications of our cryptographic equipment are not likely to diminish during peacetime. Many of our ciphers will be less exposed to capture, but infiltration of enemy agents may actually be facilitated by the unsuspecting nature of Americans. Security of thought, word, and action are requisites. Public places and desk telephones do not provide the secure conditions necessary for the discussion of top secret matters by high-ranking officers or others.

Security is one of a commander's best defensive weapons. It is also one of his prime responsibilities. The <u>successful</u> officer will know the rules and procedures designed to provide security, and he will follow them.

Original