RESTRICTED

NOTES ON COMMUNICATION SECURITY

Revised: 1943

Prepared by

COMMUNICATION SECURITY SECTION
DIVISION OF NAVAL COMMUNICATIONS
OFFICE OF VICE CHIEF OF NAVAL OPERATIONS

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1943

Foreword

The primary purpose of this pamphlet is to provide all naval personnel who prepare, handle, and transmit classified information with a convenient booklet written to show how security practices originated and why they are necessary. Its preparation was encouraged by innumerable requests for copies of an older publication of the same name which has for many months been obsolete.

In modern warfare it is particularly important that the principles of communication security be known and applied. Experienced officers and personnel need to review these principles frequently. Thousands of inexperienced persons have entered the field of naval communications and other posts of responsibility. These facts intensify the need for a booklet of this nature.

NOTES ON COMMUNICATION SECURITY is therefore designed for wide distribution in the hope that it will help to make and keep all naval personnel security-minded. Understanding the reasons and experiences behind the rules should help everyone concerned to apply them intelligently and with unremitting alertness.

Material for this booklet has been appropriated from a variety of sources. For obvious reasons, some of it has been disguised to permit its publication in a restricted document.

CHAPTER I. INTRODUCTION

Importance of Communications.

Just as communications play a leading role in all peaceful activities—government, diplomacy, industry, commerce, and personal relations—they affect profoundly the prosecution and outcome of war, strongly influencing the success or failure of military and naval operations.

Communications are to the fleet what the nervous system is to the body. Without secure, rapid, effective communications the Navy could not function. It is over the unseen lines of communication that all sorts of intelligence are transmitted to the commander in chief. A mass of reports regarding the sighting of enemy submarines and raiders, contact with the enemy, weather conditions, convoy movements and other operational information is continuously forwarded to headquarters, where it is pieced together with other available information to serve in the formulation of plans. To effect the strategy so determined, detailed orders are transmitted to the units of the fleet.

In addition to operational orders, reports, and intelligence, the communication channels are used for the transmission of a mass of information relative to the administrative and staff functions of the Navy—varied activities which, although they have no direct connection with fleet operations, enable the fleet to function and keep its needs supplied.

Radio is the Navy's most important means of communication. Telegraph, teletype, couriers, postal systems, dispatch boats, cable, sound signals and visual signals are used as extensively as possible whenever their limitations do not prevent, but radio is indispensable at times. Its use should be restricted to those occasions for which it is indispensable.

Without radio the entire scheme of modern naval operations would be radically changed, for methods of communication at sea would be no more rapid than they were in the Napoleonic era. When the French

Toulon Fleet slipped through Nelson's blockading squadron, eight weeks elapsed before Nelson was notified, and then his only information was that the French Fleet had been sighted four weeks before.

Intelligence and orders are now transmitted within minutes rather than the days and weeks formerly required. The strategist must think quickly and act decisively without the long period of consultation formerly possible. All who use or handle communications must be continuously on the alert to keep from the enemy the information communicated.

Communications are playing a major role in the present war. When forces are otherwise evenly matched, victory will fall to the side with the more efficient communications. Tribute to the importance of communications in modern warfare has been paid time and again by Nazi invading forces, who with the aid of fifth columnists cripple or seize communication centers as an immediate prelude to invasion. With their means of organizing resistance taken away, defending armies are seriously weakened, and their defeat is facilitated.

Because all phases of the life of the Navy—its strength, its weaknesses, its plans—are entrusted to the communication network, security of communications is a prime necessity. No one, friend or foe, should be permitted to gain intelligence from naval communications without being entitled thereto.

Necessity for Communication Security.

> "If one could always be acquainted beforehand with the enemy's designs, one would always beat him with an inferior force."
>
> —*Frederick the Great*

One of the primary requirements in military or naval action is to obtain as much information as possible regarding the enemy. Without intelligence regarding strength and disposition of enemy forces, distance from sources of supply, morale, and, above all, his plans and objectives, any military or naval engagement is little more than a gamble. Once complete data regarding the enemy are in hand, counter-plans can be so laid and the attack so designed as to make victory almost a certainty. History has frequently proved the soundness of this principle. There are few examples of victorious engagements where the victor did not obtain in advance the necessary information on which to base his decision. Conversely, the majority of disastrous defeats can be attributed directly to lack of enemy information or to incorrect interpretation of it.

In view of this fact, most nations for years have maintained espionage organizations of varying size and scope for the purpose of ferreting out information regarding current or potential enemies. The activities of these organizations have always been one of the greatest hazards to secret communications.

Just as the totalitarian powers revolutionized warfare, however, they cast aside accepted theories of espionage. According to the new plan, originated by the Japanese and developed by the Nazis, espionage is no longer an undertaking by a relatively few isolated spies attempting to obtain military or naval secrets from high-ranking officers. It is a mass effort, carried out in all fields—military, naval, political, cultural—by thousands of unimportant persons in minor positions.

These informers are in large part sympathetic with totalitarian doctrine; in many cases they have been coerced into service through threats to relatives in the homeland or in occupied countries. Their purpose is to obtain and report as much valuable information as possible and to assist by spreading false reports, committing sabotage, directing invading forces, crippling key industries and utilities, seizing communication centers and generally cracking defense and undermining morale. The increased threat to secret communications is apparent.

As the only sure countermeasure against mass espionage, absolute national secrecy has been practiced by the Russians and the Nazis for years. Prior to the German invasion, the Russians successfully prevented the leakage of accurate information regarding their strength and preparedness; as a result, their ability to withstand aggression was wholly underestimated by the Nazis.

For years preceding the outbreak of the war no accurate news regarding progress of German rearmament was allowed to leak out of the country. The silence imposed was not limited to the Army and Navy but was extended to all factories working for national defense,

524477°—43——2

with harsh penalties for those who violated secrecy. In those countries where invasion was almost immediately successful, a large part of the invaders' success must be attributed to the wealth of information available in advance, as well as to the failure of the victims to take preventive action against the new type of espionage.

The lesson is clear. In order to combat the efforts of the enemy to gain intelligence of value, all who have access to official information must practice absolute secrecy at all times.

Obviously, the Navy is a potential source of valuable information, and unceasing attempts to exploit that source may be expected. Methods open to the enemy are many—planting agents within the naval organization, photographing or stealing secret documents, tapping telephone and telegraph lines, and questioning or overhearing naval personnel when off duty. Although bits of information obtained through these means often appear innocuous, they prove to be of real value when subjected to expert analysis along with other fragments of information from various sources. The necessity for unceasing vigilance and maximum preventive measures on the part of all naval personnel is apparent.

One of the enemy's most fruitful sources of information is the Navy's lines of communication. Not only can he obtain a wealth of information about strength and disposition of forces, ship movements, war plans and other phases of naval operations, but he may also obtain such thorough knowledge of the methods of secret communication as to make his task in translating future encrypted messages far less difficult. The enemy attempts to achieve this goal primarily through interception of messages and cryptanalysis.

Interception of messages is comparatively simple. Since much, and often too much traffic is transmitted by radio, a relatively few receiving sets are all that is required to permit the enemy to transcribe radio messages originated by the units of the Navy. Interception of landline, cable, visual traffic, and mail is more difficult but far from impossible.

The science of cryptanalysis or solution of encrypted messages without the keys has amazing accomplishments to its credit. Cardinal Richelieu, during the early seventeenth century, established in the French Government a department for the devising and breaking of forms of

secret communication. From that day forward the French Government maintained a cryptanalytic department almost without interruption; other nations were not long in following suit.

If there were doubts as to the contributions of cryptanalysts in war and peace, they were dispelled during the World War of 1914-18, when expert cryptanalysts in nearly all countries had a field day in the solution of enemy code and cipher systems, with substantial effect on the outcome of many major engagements.

Various theories have been advanced as to the reasons for the ineffectiveness of the German Navy during that war. There are some who say that the Kaiser, in fear of losing his prized ships, firmly opposed his advisers' suggestion that the entire fleet be sent out to undertake operations against the enemy. There are others who believe, with reason, that the efficiency of the Allied cryptanalysts more than any other one factor stymied the German Fleet and almost assured its defeat when it did venture forth.

When the Germans attempted surprise destroyer raids on channel shipping, the British intercepted and read their radio dispatches, learning of the plans in time to take effective countermeasures. When a German battle-cruiser force attempted a lightning raid against the Isles, the British knew of the project hours in advance, and the Germans were defeated in the Battle of the Dogger Bank. Again the Germans attempted a surprise operation, this time in the form of a trap for the British cruisers, but the British, reading their intercepted traffic, turned the tables, trapping the Germans in the Battle of Jutland.

Today cryptanalysis is firmly etablished as a science of considerable value to nations at war. Many of those employed at this work have spent their lives in attacking what to the layman appear to be insoluble ciphers or codes. Although systems of communication are more secure now than ever before, the cryptanalyst's ability to break messages has increased considerably. During the present war, for example, a message was transmitted in cipher from one British post to another. It was intercepted by the Nazi Army, deciphered, translated into German, enciphered in a German system and transmitted to Berlin. This transmission was intercepted by a British station, deciphered, translated

into English, enciphered and sent back to the point of origin. The entire process required only a few hours.

The cryptanalyst's methods of attack may be grouped into two general categories, the mathematical and the intuitive, but in actual practice a combination of the two methods is used.

Mathematical solutions are based on the fact that languages have certain peculiarities which are fairly consistent in a large amount of text. These "mechanics" of languages have been thoroughly studied and tabulated. Available to the cryptanalyst, therefore, are tables showing the frequency of occurrence of all letters for a certain quantity of text. The letter E in English, for instance, appears 126 times for each 1,000 letters of military telegraphic text, U appears 30 times and Z only once.

There are similar tables on the occurrence of letters as initials and terminals of words, on common doubled letters, and on digraphs. A mass of related information has been accumulated; the cryptanalyst knows, for instance, that the average length of an English word is 4½ letters, that 50 percent of English words end in D, E, S, or T, that about half of the words begin with A, O, S, T, or W, and that the letter U always follows the letter Q.

In pursuing the intuitive attack, the cryptanalyst makes assumptions as to the gist of a message or the plain language meaning of a particular portion and attempts to prove the accuracy of his assumption through application of his conclusions to other parts of the message. He uses as aids his knowledge of the habits of the enemy, variations in volume of traffic, assumptions as to originators and addressees drawn from message headings and, above all, habits in choice of terminology and errors in encryption. He actually needs only one or two apparently minor leads as to the thought of a message. Weighing this information in the light of other knowledge available to him, he may succeed in his attack.

Once the cryptanalyst has broken several messages encrypted in the same system, he has usually accumulated enough data to reconstruct at least a portion of the system, permitting more rapid decryption of future messages sent by the same means. Eventually, the cryptanalyst can read messages in that system as promptly as the authorized holders.

Twenty-three hundred years ago, man first employed encryption, or the art of writing in secret characters. Ancient records indicate that the Spartans made use of an ingenious plan. Their couriers transmitting secret information carried tablets inscribed with messages regarding subjects of no military significance. If taken prisoner en route, the couriers were often released, for their captors saw no harm in the tablets and failed to find evidence of secret dispatches. Around their waists, however, the couriers wore belts inscribed with jumbled letters, presumably prepared for travelers by the priests as invocations to the gods. When such a belt was fastened to one end of a baton of a certain size and wound spirally around it so that no wood showed, the jumbled letters in their new alignment formed intelligible text. The Greeks are thus credited with the invention of the transposition cipher, in which the meaning of a message is disguised by rearrangement of the letters according to a pattern.

The Romans also utilized secret writing to transmit military and political information and are said to have invented the substitution cipher. Caesar, while on his Gallic campaigns, used a simple substitution cipher for keeping in touch with Rome. For each letter of a plain language text he substituted the letter four places farther along in the alphabet.

During the Dark Ages, when reading and writing were a monopoly of the clergy, cryptography fell into disuse. It reappeared again during the age of the Italian city-states when codes, in which unrelated words are substituted for words of the plain language text, were utilized by Venice and the Papal State for secret communication with their ambassadors to other courts.

From this point onward, the popularity of secret communication grew, and by the year 1600 all courts and principalities of France, Spain, and Italy were using ciphers. No very complex systems were introduced for some time, but cryptanalysis lagged far behind, and the simple systems were effective enough. Thieves, strangely, developed a simple but safe universal code for communication with other members of the profession throughout Europe. In northern Europe a code con-

sisting of the substitution of far-fetched figures of speech for names of persons and places was developed. In France at one stage the names of flowers were substituted for commonly used words, and a little later a code system employing the terminology of the fur trade was devised.

The history of all major countries since the Middle Ages shows that secret communication has played a part in most intrigues and wars. A number of cipher messages plotting the assassination of Queen Elizabeth and purported to have been written by Mary, Queen of Scots, and her confederates, figured during Mary's trial.

During his Russian campaign, Napoleon communicated with his marshals by means of a simple cipher in which numbers were substituted for letters, names, and commonly used words. The Russians without difficulty deciphered the intercepted messages and followed Napoleon's plans.

Ciphers and codes were used by both armies during the American Civil War. A very simple word transposition system was used by the North and a far more complex system by the South. Although Northern cryptanalysts experienced little difficulty in breaking intercepted Confederate messages, the Southerners had more difficulty in deciphering the Northern messages and even printed intercepted messages in the newspapers with requests for information as to their meaning.

The Civil War and the Franco-Prussian War proved that the age of mass armies had arrived and that, since no general could keep his forces under personal observation, fast and secret communication was required. Ciphers and codes therefore were transformed from military tools of occasional use to necessities.

The Boer War indicated that codes, although satisfactory for higher units of command, were too limited in their means of expression for minor military units. As a makeshift, the British discovered that Latin, an almost unknown language to the Boers, proved a successful means of secret communication.

Arrival of wireless early in the present century emphasized the necessity of disguising all confidential radio correspondence, for enemy as well as friend could now receive it. There ensued a period of intensive study. Thefts of military, naval and diplomatic codes and ciphers were prevalent. Scandal and treason were uncovered on all

sides as nations purchased or stole each other's code books and cipher keys.

During the World War radio was still adolescent, but was rapidly coming into its majority. For the first time in history, all Army units could be in prompt and immediate communication with headquarters, and each ship with the commander in chief. But errors and failures were prevalent; scarcely an encounter took place without some breakdown in the communication system. Gradually, however, as training and experience of personnel grew, use of the newly invented methods of communication improved.

All nations meanwhile became impressed with the importance of communication security. All established cryptographic bureaus where, in the greatest of secrecy, code and cipher systems were developed and enemy systems were broken down. Serious violation of security principles was common and often victory or defeat was ordained in the code room.

As radio was perfected, methods of secret communication increased in complexity and security. Although there is little direct resemblance between modern systems and the early ones, most current systems fall into the basic categories of long ago—substitution ciphers, transposition ciphers, and codes.

The transposition cipher has nearly fallen into disuse, because of its low resistance to attack. Some of the faults of the substitution cipher have been circumvented; for instance, methods were long ago devised to eliminate substitution of the same letter for a letter of the plain language text whenever it occurs. In modern systems, the letter K may be substituted for E the first time the latter appears, N the second time, and so on. Mechanical and electrical cipher machines have been perfected and now are used by most countries.

Codes are in general use, but their limitations of expression, the time required for coding and decoding, and their lack of security often make them satisfactory only for conveying information of a specialized nature, such as weather and contact reports. One of the most secure methods of secret communication results from the substitution of code words for the plain language text, followed by encipherment of the coded version.

Purpose of Communication Security.

The term *communication security* embraces the precautions and measures taken to prevent transmitted information and knowledge of the cryptographic systems from falling into the hands of the enemy. Communication security aims to prevent the theft or unauthorized sighting of information and publications, the unintentional betrayal of official secrets through personal conversation, and the obtaining of intelligence by the enemy through cryptanalysis and study of traffic trends. Communication security has but one purpose—to hinder and if possible to prevent the enemy from obtaining any information which would be of value to him and which, in his possession, would be detrimental to the nation.

Secrecy in communications, desirable in peace, but imperative in war, ordinarily requires that messages be encrypted prior to transmission. Since this process reduces somewhat the speed with which messages can be delivered, security is in a sense purchased at the cost of speed. Modern cipher machines, however, with efficient operators, provide *security with speed* to an increasing degree. Seldom, except in combat, is security sacrificed to speed to the extent of using plain language.

Under no conditions should reliability be impaired in order to gain either security or speed. Any communication is worthless and even dangerous if the thought of the originator is changed or if the message when delivered is not intelligible.

Through long experience, a body of rules to enhance communication security has been accumulated, covering frequently employed processes and procedures and governing recurring situations. The field of communication is broad, however. Methods are increasing in complexity, and the possibilities open to the enemy are so numerous that no group of rules can ever be compiled to anticipate every contingency. The responsibility of those who deal with official communications in any form, or who have official knowledge which must be kept from unauthorized persons, is therefore weighty. Theirs is the obligation to know security principles thoroughly and to apply those principles to every situation which arises.

CHAPTER II. SAFEGUARDING OF CLASSIFIED MATTER

The term *classified matter* includes all publications, documents, cipher keys and aids, code books, letters, messages and materials which are secret, confidential or restricted. Carbon copies, paraphrases, and even rough drafts of messages or letters are considered classified matter. The classified nature of knowledge gained from studying or sighting any of this material should never be forgotten, and such intelligence should receive the same degree of care and safeguarding as the matter itself.

Too often through the unwitting cooperation of Navy personnel, the enemy obtains valuable information regarding naval communications without the necessity of employing cryptanalysis. Carelessness in the handling and stowing of publications and dispatches, and thoughtless discussion of official secrets in the hearing of those who have no right to know are more helpful to the enemy than a corps of expert cryptanalysts. Occasionally, too, an item appearing in the newspaper or broadcast over the commercial radio gives the enemy a lead of value.

Physical Safeguarding.

Because knowledge of secret and confidential communication systems and information is in itself dangerous, only a limited number of Navy personnel are authorized to handle and to use classified matter. The loyalty of other personnel in the great majority of cases is unquestioned, but, if they had knowledge of classified information, the likelihood of such information being given inadvertently to outsiders would be much greater .

The first obligation, then, of the officer or enlisted man working with classified matter is to protect that matter from being seen by any unauthorized individual, be he officer, bluejacket, or civilian. There

524477°—43——3

is no reason why officers or men unconcerned with secret matters or communications should have any access whatever to secret stowage until it becomes necessary in the proper conduct of their duties.

Close restriction of the distribution of classified material is necessary, for "too many cooks spoil the broth" either through inadvertent disclosure of information or through increasing the likelihood of capture. In one of the battles in a Libyan campaign, the Italians obtained a mass of secret documents when they captured a small advance unit of the British Army. Included was a publication listing the code names of all British units engaged in the battle. Seizure of this information revealed to the Italians that the British had thrown all forces into the battle and had no available reserves, a circumstance suspected by the Italians but not previously confirmed.

Anyone who removes secret or confidential material from the designated working space runs the risk of compromising the particular material concerned. During the German occupation of Paris in 1940, the Nazis reaped a harvest of valuable documents, duplicates and originals, which French politicians and Government officials were retaining in their homes for current work or for writing their memoirs. Although they believed that such stowage was secure, fifth columnists had spotted the homes of officials, and lightning raids prevented destruction of the documents.

Classified material should never be left unguarded, and must always be kept in the proper locked accommodation when not in use; a glance at a message or a cryptographic aid may be enough to betray the system, and a photograph can be taken with a concealed camera in a split second.

The famous Zimmerman message, in 1917, in which Germany offered Mexico several American States as her reward for declaration of war against the United States, was decoded by the British with no difficulty, for they had obtained a copy of the German diplomatic code from a young Austrian radio technician employed in the German Embassy at Brussels. The Austrian over a period of months had laboriously copied a few words a day from the code book, seizing moments when the book was unguarded, and hiding the slips about his person until he could pass them on to a British agent. Vaults, safes,

or lockers used for stowage of classified material should always be kept locked when not under the supervision of authorized personnel. Cryptographic aids and related classified matter must never leave the possession of the person to whom entrusted or the safe in which they are stored. Even then, assurance is never absolute.

On shipboard, ciphers and codes are not subject to the same hazards as on land, and even in event of capture or crippling of the ship, are not likely to fall into the hands of the enemy except through carelessness. Capture of classified matter is most likely to occur in the case of ships operating in comparatively shallow waters near enemy territory.

Capture of a code or cipher is always an extremely serious matter. Not only is the key available for deciphering current and past dispatches, but the basic style and structure of the system are apparent, giving substantial aid to cryptanalysts in the breaking of similar systems.

In the early days of the first World War, an event occurred which had a tremendous influence on subsequent naval operations. When the German light cruiser *Magdeburg* ran aground in the Baltic and was captured by the Russians, a diver was sent down who soon retrieved a pile of submerged documents from the shallow water near the ship. This recovery was of double significance for the Allies, since the books contained the current German naval code and the keys for future variations; although the Germans frequently changed the key, they continued the use of the system for two years, enabling the Allies to keep in close touch with all their naval plans.

There have been several instances in the present war of the seizure of codes from captured merchant ships before the ship's officers could dispose of them. Divers have retrieved important documents from enemy submarines sunk in coastal waters. In one case an unconfirmed report was received that eight enemy submarines were sunk at a rendezvous arranged through use of a secret code taken from a crippled submarine.

Although great care is taken in the handling and stowage of classified matter, we often forget that the materials and methods used in preparing classified messages or other matter are potentially just as dangerous as the actual messages.

Rough drafts and notes should be written on single sheets placed upon hard surfaces to avoid impressions, for chemical treatment and photography can make impressions remarkably clear. Stencils, cushion sheets, and carbon paper are almost as legible as the original, and desk blotters and backing sheets can be rendered clear. For these reasons the same care and stowage should be given materials and supplies as are given the classified matter itself.

When the usefulness of materials is past, they should be destroyed under supervision and never should be discarded in wastebaskets for ordinary disposal. If immediate destruction is not feasible, work sheets and notes should be torn to bits and stored in a safe or a guarded "burn bag" until destroyed.

Detailed arrangements should be made for the destruction of classified material in event of capture or sinking, even to the extent of destroying in advance certain files and reserve publications. While sinking at sea in weighted bags is best in deep water, it is not satisfactory for shallow water or near the shore.

Responsibility should be assigned by duty rather than by name, and the order in which publications and apparatus will be destroyed should be clearly understood. Secret publications are destroyed before confidential and restricted matter. *Documents and devices not yet made effective take precedence over those which are.* Destruction by fire is ordinarily preferred.

Restricted apparatus and equipment must be destroyed beyond repair. Secret and confidential equipment is to be destroyed beyond recognition. When time does not permit communication with the commanding officer, every person concerned must act on his own initiative.

Whenever evidence is received indicating that a code or cipher may have been broken or captured by the enemy, use of the system is discontinued and outstanding publications are destroyed, for continued use of a compromised cipher may result in defeat. Therefore, whenever anyone uncovers evidence that unauthorized personnel have had access to classified matter or that a system may have been otherwise compromised, he should report the details promptly. In event of the loss of a ship, it is essential that the Navy Department be given full

details immediately of the disposal of classified matter in general and secret and confidential publications in particular.

Personal Censorship.

"What I must keep from a
foe I do not tell a friend."

—*Confucius.*

No one knows how many battles have been lost, how many ships have been sunk, how many lives have been sacrificed because someone casually or in a moment of boasting betrayed a vital military or naval secret. Available evidence indicates that the figure would be astounding.

In time of peace it is a sound policy to shroud in secrecy methods of secret communication and general naval information in order to keep knowledge of naval progress from the unknown enemy of the future; but if secrets are betrayed, no world-shaking importance attaches to the matter. When the nation is at war, however, violation of secrecy becomes a matter of national life and death. Because the lives of thousands, the fate of ships, and the national security itself hang in the balance, absolute secrecy in war is imperative.

In January of 1916, an American businessman in Warsaw was invited to dine at the home of a German military official. The food was excellent, the wine flowed freely, and barriers of nationality were temporarily forgotten. As the conviviality increased, the officer's tongue became loosened, and before the American left he learned that the Germans had scheduled for late February a terrific offensive against Verdun, designed to crush France. The story was passed on to the Allies, who reinforced the hitherto weak defenses of Verdun, bringing up additional troops and artillery. The Germans struck on February 21, but the French guns were ready, and what might have been a knockout blow at France was turned into a bloody defeat for Germany—all because of a loose tongue.

A pilot in an English coastal town who for years had been steering merchant vessels through the difficult port waters, boasted to his cronies in the tavern of his feat in bringing into port that day the largest ship of his career—a 25,000-ton vessel. That night a squadron of Nazi

bombers appeared overhead, docks were destroyed, the loaded ship was sunk, and lives were lost.

A young naval reserve officer assigned to ciphering work devised a novel idea for entertaining his friends at a cocktail party. He passed around a sample of encipherment of several sentences as a challenge to his friends' ingenuity, pointing out that each sample was from a different key but that all were in the same parent system. It did not seem surprising that one of the guests, a refugee from a Nazi-occupied country, failed to make any progress in deciphering the sentences, although he seemed to be very much interested and asked a great many questions. Enemy cryptanalysts pray for just such an opportunity; more complicated systems of encipherment have been broken with much less information than the officer had offered.

There is only one safe conversational policy for naval communication personnel to follow when on duty—say nothing about classified matter or information to anyone who is not authorized to know. There is only one safe policy when off duty—say nothing about the work to anyone, even when in the company of authorized personnel. There are few places where conversation cannot be overheard; sometimes even the walls have ears. It must be remembered that it is human nature to pass on a secret accidentally acquired.

Through the nature of his work, the communication officer knows all secrets which come over the radio network. He frequently finds himself in the possession of information shared only with the captain. Aware of this fact, the ship's personnel look upon the communication officer as someone in the know and listen closely whenever he speaks, in anticipation of picking up some bit of hot information. In order not to betray their trust, communication personnel must be constantly on guard against a slip of the tongue which might reveal intelligence to those who have no right to know.

Official secrets should not be discussed even with members of one's own family or close friends in whom one has the greatest of confidence. Although they would never knowingly reveal information given to them, they may, in ignorance of its importance or forgetting its source, inadvertently mention a detail in casual conversation.

There are some who believe that a policy of mendacious garrulity

about their work in the Navy is more satisfactory than absolute secrecy. The tall tales they spin offer them much entertainment and prevent gibes from their friends relative to their secretiveness. Although this method may be successful in deceiving the unknown enemy, it should be reserved for experts.

To keep the silence one should, by skillful maneuvering of the conversation or by outright refusal to talk shop, decline to discuss official matters. In many cases it is desirable to plead ignorance of the subjects under discussion.

Personal censorship includes telephone conversations. A naval officer who, in the course of his duties, refers to a dispatch over the telephone by mentioning both the serial number and the gist of the message, endangers the information and the cryptographic system. An encrypted copy of the dispatch is probably available to the enemy. Telephone wires can be and are tapped, private lines being less secure than party lines because they are specifically labeled and are therefore easy to locate at junction points in the cables. Conversations may be heard at the switchboard and various other points along the circuit.

Official secrets should not be discussed over the telephone, and no information of any nature should be given by phone to a caller whose identity has not been satisfactorily proved. If the caller professes to be an authorized person, but is not positively identified, it is often wise to break off the conversation and call him back on his officially listed extension, prior to discussing professional matters.

What holds true in respect to conversation applies to personal correspondence as well. Mail can be intercepted by enemy agents, and there is no surety that information in letters will be held inviolate by the addressees, regardless of their trustworthiness.

A young soldier stationed near Sourayville during the Great War described in a letter to his mother the success of his battalion and the failure of the enemy to locate its position. "The enemy seemed to think we were in a similar clump of woods about 400 yards north of us, for he shelled it heavily several times today," he wrote. The young man put the letter in his pocket for mailing at the first opportunity. That night he was captured. Less than an hour later there came a heavy concentration of enemy fire on the clump of woods in which his battalion

was located. Over 100 of his fellow soldiers were killed and more than that number wounded.

Personal letters or gifts from questionable acquaintances, business firms or advertisers should never be acknowledged. There have been cases in which enemy agents, in an attempt to find the location of a military or naval official and perhaps the type of work he is doing, have addressed a letter to him or have sent a gift, in the hope that when it eventually reached him he would acknowledge it and his courtesy might betray some information of value. The enemy has also been known to send false personal messages and to make bogus telephone calls in an effort to learn sailing dates and routes of merchant or naval ships.

It is a temptation to jot down in personal notebooks events that occur or interesting bits of information which will make entertaining conversational material after the war. Diaries of prisoners are fruitful sources of information for the enemy.

Press and Radio Censorship.

Occasionally the enemy, through his agents, will read in the newspapers or hear by commercial radio items of information about military or naval matters or production of matériel which are of value to him and, in his hands, detrimental to the interests of the nation.

It is to prevent the leakage of information as well as to insure the loyalty of the citizenry that totalitarian countries have adopted absolute censorship of the press, whereby the newspapers and similar publications are told what they must print and what they must suppress. The democratic countries have nothing which even remotely resembles the press censorship of the totalitarians. In Great Britain, the United States and other nations subscribing to a similar form of government, the press is free to print what opinions it will and, with a few exceptions, the facts it uncovers. In time of war or other national emergency, it imposes limitations upon itself in order to prevent vital information from reaching the enemy.

Disclosure of certain types of information which would be particularly advantageous to the enemy is forbidden by the Government during time of war. Falling into this category are such items as detailed

weather reports, specific information regarding production of war materials, premature disclosure of the results of naval and land battles, and the identity, location, and movement of merchant vessels or ships of the Navy. Even with such restrictions, however, censorship in the United States is a far cry from the rigid control of the press existing in enemy countries today and from the degree of censorship which has been resorted to by warring countries in the past. During Napoleon's regime, for example, the decisive battle of Trafalgar was not mentioned in the French press until a decade after it took place.

Democratic censorship places a substantial burden of responsibility upon Navy personnel. It is the obligation of those who deal with the press to point out clearly what may be printed and what should be withheld in the interests of national security. In almost all instances of betrayal of official secrets by press or radio, the blame can be laid at the door of some government official who failed to explain the importance of secrecy or was careless in the drafting of a statement.

A magazine of sizable circulation recently printed several photographs of minor war vessels which clearly showed the display lights and aircraft identification apparatus in general use. Although the layman would see no harm in information of this nature, an enemy agent might find it valuable.

When the *Robin Moor* was sunk in 1941, American newspapers printed a statement by an American consul in a South American country to the effect that the survivors had submitted eyewitness reports of the sinking and that a summary would be telegraphed to Washington as soon as coded. With a copy of the coded message and this information as to the contents, an enemy cryptanalyst would have little difficulty in breaking the code.

Although information printed in newspapers may appear to be harmless, it often can be of considerable value to unfriendly nations. No one would expect the enemy to profit from social notes appearing in the society pages, and yet with their help an amateur cryptanalyst in a friendly country once followed a fleet maneuver by breaking intercepted radio messages. He had only two leads. One was the recurrence of the same terminal characters in many messages and the other was the social notes in newspapers of Hawaiian and United States

524477°—43——4

cities. By reference to the latter he discovered the names of ship captains present at social functions in various ports; from the Navy Directory, he learned the ships they commanded. Thus, he was able to gain enough information regarding the routes and probable missions of the ships to reach sound conclusions as to the contents of the messages.

A thoughtless word by an official or a commentator over the radio may undo months of hard work and may even cost lives and ships. A British official speaking over a radio network one evening stated that for several days no raids had been made over Germany, due to bad weather conditions there. The Germans rightly assumed that the British had successfully broken their weather cipher and immediately introduced a new system.

When the enemy intercepts an encrypted message from a commander in chief to Washington and a day or so later a statement of progress, attributed to the commander in chief, appears in the newspapers, it is not difficult for the enemy to assume that the press statement is a paraphrase of the intercepted message. Knowledge of the thought of a message may be but a few steps removed from the breaking of the system.

SUMMARY

If official Navy information is to remain out of enemy hands and if systems of secret communication are to continue uncompromised, Navy personnel must at all times exercise maximum care in the handling and stowage of classified material, in their personal and official conversation, and in their statements to news-gathering agencies.

CHAPTER III. PREPARATION OF DISPATCHES

Naval communications may be roughly segregated into three categories—reports, letters, and messages. Reports are official statements in written or printed form, presenting detailed facts regarding a particular operation, condition, or procedure. Letters are written or printed communications, generally expressed in some detail and transmitted by mail or, within a particular unit, by messenger. Letters are rarely encrypted.

A message is a communication expressed in very brief form, and may be one of three types—a signal, a procedure message or a dispatch. A signal consists of one letter of the alphabet or a combination of several letters with predetermined meanings, transmitted by visual means, special sounds or radio. Procedure messages are brief communications between radio operators relative to the handling of traffic and radio operation. All other messages are classed as dispatches and may be sent in plain language or may be encrypted.

Dispatches are released by officers in positions of command at sea or in shore stations. The originator of a dispatch specifies the desired precedence and classification, using mailgram or airmailgram service if possible. It is his duty to draft the dispatch properly. Communication officers and others may suggest improvements in drafting or changes in classification and precedence, but they have no authority to institute revisions; only the originator or his superor may do this.

Unnecessary Messages.

The originator's first task is to determine whether it is imperative to send the message he has in mind. Unnecessary messages cause countless hours of work in encryption, transmission and decryption,

and take the time of officers in responsible positions. They burden the lines of communication, delay the delivery of important messages, and add to the volume of intercepted traffic available to the enemy cryptanalyst.

Much of the confusion of the Germans and the Allies during the early days of the World War was caused by unnecessary radio messages. As the Germans marched to the Marne, the air was filled with radio traffic—French, British, Belgian, German; often several stations were working the same frequency, jamming one another. Entire messages were lost, improper transmission spoiled some, others had to be repeated as much as a dozen times, and many of the most important communications failed to get through.

At Mons the British escaped a well-planned trap because the Germans failed to receive the orders from their high command in time; at Guise the French slipped from another trap when the Germans did not understand their orders to encircle. Through French interception and deciphering of high-command dispatches which the German armies failed to receive, the French were able to delay the two main German armies before the latter had time to join forces, and the British, reinforced by another French army, struck between. The Battle of the Marne was the result, scotching the German plan to eliminate France from the war.

The magnitude and intricacy of modern warfare require that the minds of participants be freed from consideration of matters not directly pertinent. Messages reporting trivia during operations distract the attention of seniors from matters of great importance; communications passed from higher authorities to subordinates, with no change except the addition of detailed instructions, swamp the subordinates with information which they do not have time to digest. A trivial dispatch may provide the enemy with a clue to the structure of a system, enabling him to extract valuable intelligence from important messages enciphered in the same system. Successful naval communication, therefore, necessitates the sifting of information and the elimination of all messages which are not absolutely necessary.

The originator should always determine, then, that a concrete and constructive goal will actually be realized if his message is transmitted.

If he cannot satisfy himself on this point, the dispatch should not be sent. He must remember that unnecessary messages during war jeopardize communication security and overload circuits.

Selection of Means of Communication.

The volume of naval communications is so great that no one means is physically able to carry the entire load. All naval personnel consequently share the responsibility of channeling traffic so that no type of communication service is called upon to carry a greater load than it can handle efficiently.

Radio is frequently taxed beyond its physical limits, and in a great many cases communications which could well be transmitted just as efficiently by some other means are thrust upon the radio network. On land an originator has access to the telegraph, regular mail, air mail, and courier service; in harbor, dispatch boats and visual signals may be used; at sea, visual and sound signals are available; and across oceans are the international cables.

Radio fails to distinguish between the receiver of friend and foe. Developments in radio direction-finding equipment during the past few years now enable the rapid and fairly accurate location of any radio transmitter in operation. These characteristics make it imperative that radio be used only as a last resort, when other means of communication are not available or, for some good reason, are unsatisfactory.

The primary purpose of naval communication service is the dissemination of operational orders and military information. Communications of an administrative nature necessarily fall into second place. It logically follows that the more rapid methods of communication, radio and telegraph, should be reserved insofar as possible for military purposes and that the mail services should be used for administrative traffic. Only when the time element makes the use of other means impractical should radio or telegraph be used for administrative communications.

Because alternative methods of communication are far more numerous on land than at sea, personnel in naval shore establishments should make particular effort to reduce radio and telegraph traffic to

a minimum. Mail rather than radio should be the common land method of communication.

Mailgrams, which are dispatches transmitted by mail or airmail, offer many advantages. They are given the same internal handling by communication personnel as are radiograms, and they need not always be encrypted. Therefore, they are sometimes more rapid than radio or telegraph because of the hours lost through encryption, decryption, and occasionally through transmission errors. In one recent instance, an enciphered telegram was sent to a destination 450 miles away. Due to delay and garbling in transmission, it did not reach the addressee in translated form until 43 hours later, whereas a mailgram would have been delivered in half the time.

If military necessity requires the transmission of an administrative communication by radio to the action addressee, it is often feasible to send it to the information addressee by mailgram. Time is saved and security is enhanced. If there are many information addressees, the dissemination of the message is concealed by reducing the number of circuits on which it is transmitted.

It must not be overlooked that other means of communication are also subject to interception by the enemy, although not nearly to so great an extent as radio. Evidence during the present war has indicated interception and deliberate garbling of cable messages to confuse addressees. Telegraph messages have been routed through enemy territory by enemy agents rather than over more direct lines through neutral territory. Mail has been intercepted, and even teletype lines have been tapped. If there appears to be likelihood of interception, dispatches should be encrypted.

Constant vigilance is required to insure that plain language visual messages at sea or in port are not subject to undesired interception. In the Battle of Jutland, the Germans intercepted British visual recognition signals and flashed them at night when contact was made with minor units of the English Fleet; with the time so gained, they blew up several British destroyers before the latter could damage the German ships or warn the rest of the fleet.

In port, the maximum use of mail and dispatch boats should be made whenever time and circumstances permit. In many cases mail

sent by special boat is more expeditious than encryption, transmission by visual, and decryption would be.

Precedence.

If the originator, after weighing the advantages and disadvantages of available means of communication, decides that a dispatch must be transmitted, he considers next the *precedence* necessary. The term indicates the preference to be given a dispatch in order of transmission. The higher the degree of precedence, the more expeditious will be the handling and delivery.

It is an unfortunate tendency of originators to designate the highest possible degree of precedence in order to eliminate any delay in the delivery of dispatches. The time differential in delivery of messages in different precedence brackets, however, is a matter of no more than a few hours. The top degrees should be retained for a few extremely urgent dispatches. To specify high precedence when a lower degree would serve decreases the value of high precedence on dispatches meriting such expeditious handling. In many cases a high designation may be required for the action addressee, whereas the lowest degree will suffice for the information addressees. As a general rule the high degrees of precedence must never be used for administrative traffic.

Classification.

After designation of the means of communication to be utilized and the precedence to be given, the originator should select the secrecy classification warranted by the subject matter of the dispatch. Three degrees of secrecy are prescribed in the United States Navy.

Information, the disclosure of which would endanger the national security or would be prejudicial to the interests or prestige of the nation or of any Government activity, is classified as *secret*. A secret document or message is very closely regulated in distribution. Only a few officers in position of command and a limited number of other officers whose immediate duties require that they have such knowledge, are permitted to see and to handle secret matter.

Information, the disclosure of which would be prejudicial to the interests or prestige of the nation or would endanger some Govern-

ment activity but would not necessarily threaten the national security, is classified as *confidential.* The distribution of confidential matter is closely limited to those responsible persons who need the knowledge in connection with their work. Confidential information thus is available to a much larger group of naval personnel than is secret information.

Information or matter which can be used by all naval personnel but which cannot be made available to the general public is classified as *restricted.*

Unclassified matter consists of publications and information the distribution of which is not limited.

The originator of a dispatch or the officer who releases a letter or a report always assigns the desired classification. Prior to transmission of a dispatch, if another officer believes that the classification should be changed, he may suggest this revision to the originator, but no one other than the originator or his superior can make the final determination.

Classification of dispatches does not define the degree of security of the particular cipher or code used but designates only the restrictions to be placed upon the information.

Secret, confidential, and restricted dispatches are always sent in encrypted form when transmitted by radio. Unclassified messages are never encrypted, though they may be encoded for condensation.

The classification of dispatches has an indirect bearing upon the security of the system. If dispatches are indiscriminately classed as secret, the systems available for encryption of secret dispatches are burdened with an undue volume of traffic, and their security is endangered because of the large amount of traffic available to interception and cryptanalysis by the enemy.

The demarcation between the degrees of secrecy classification is not clear-cut, and no particular type of information will always, without variation, be classed in the same category. Only through actual experience can an officer arrive at a keen understanding of the various degrees and develop the ability to designate the proper classification.

In determining the classification to be given a particular dispatch, the originator should ask himself a number of questions. First, he

should determine the number of individuals who must have the information. Secondly, he should estimate the threat to the national security should the information become known to the enemy. Thirdly, although he may believe that the information should be classed as secret, he must ask himself whether it is possible that *it is and can be kept truly secret.*

Once a dispatch has been transmitted under one classification, that same dispatch should not be reclassified. If, for example, the addressee of a confidential dispatch determines that the subject matter warrants only a restricted classification and changes the classification downward, retransmitting the dispatch to certain units under his command, two cryptographic systems will have been used in the transmission of the same dispatch. Progress made by the enemy in breaking one system could then be applied to the other.

One of the most secure ciphers used by a great power in the current war was compromised in just that manner. A dispatch was given the highest secrecy classification and transmitted in a secure cipher. Along the route, its classification was lowered, and the same dispatch was retransmitted in a less safe cipher. The enemy, who had already broken the second cipher, read the dispatch with ease, applied the translation to the intercepted message as first transmitted and so broke a system which up to that point had withstood cryptanalytic attack.

Theoretically, information once transmitted in a secret system should remain secret forever; normally, all subsequent dispatches on the same subject should be transmitted in the same classification. This is not a hard-and-fast rule, however. During war, information regarding a particular subject occasionally is classified downward. Assume, for example, that an operation is carried out against an enemy base. In the planning stage, information regarding the proposed operation is kept in the greatest secrecy and is known only to the highest ranking officers involved—probably only the most responsible authorities in the Navy Department, a commander in chief and the commander of a task force.

Once the plans have been formulated, operation orders are issued to the task group commanders. The proposed operation is still secret, but more persons are now aware of it. In the execution stage, when

524477°—43——5

instructions are distributed, information regarding the operation reaches unit captains and certain members of their staffs.

When the operation is in progress, all personnel involved become acquainted with the objective; and finally, after the operation has been completed, an account is issued to the press and is disseminated throughout the nation. Although information regarding a general subject is thus classified downward during war, an individual message should not be reclassified.

During time of war there is a dangerous tendency to overclassify dispatches, arising from a sincere desire for maximum secrecy. Such a tendency is illustrated by a report recently circulated in the Navy Department. The report, consisting of nothing more than photostats of two newspaper articles and a copy of a brief Navy Department press release concerning a round-up of Axis agents and radio transmitters, was classified as confidential, although all of the information was known to anyone in the United States who had troubled to read the newspapers.

The story is told that some years before the war an admiral wished to issue an order to his captains. Since the utmost secrecy was imperative, he was anxious that no detail should come to the attention of unauthorized personnel.

"It's maddening," he said. "Everything gets known here, especially by those who ought not to know."

"Don't mark it secret and then no one will look at it," advised a member of his staff.

According to the tale, the admiral followed this advice; no one whose duties did not compel it took any interest in the order, and secrecy was attained. Regardless of the truth of this story, it illustrates a recurrent danger.

Ordinarily underclassification is more harmful than overclassification but not nearly so common. Care should be taken to specify as high a classification as is warranted, in order to prevent betrayal of secrets through possession of information by too many persons.

One other consideration should be kept in mind. If information which is destined soon to appear in the press is classified and encrypted in a dispatch, it might be easy for the enemy to link the dispatch with the information and achieve an entry into the cryptographic system.

Transmission by a method which does not require encryption is preferable in such a case, if circumstances permit.

A reply to a message is now classified on its own merits. Ordinarily it is given the same classification as the message to which it replies and is normally sent in the same system, but this is not an iron-clad rule.

When a dispatch refers to a previous dispatch, it may be sent unclassified only if the reply consists solely of a reference or a reference plus one of certain authorized expressions. "Compliance effected your secret 152016" may be reworded and sent in plain language as "Your 152016 affirmative."

Drafting.

The only purpose of communications is to convey information or instructions. If a dispatch is ambiguous, poorly worded or incomplete, this purpose is lost, and the addressee might be better off had it never been sent. Regardless of how speedily or how secretly it is transmitted, if a dispatch does not say exactly what the originator intended, it is not only without value but dangerous. Catastrophe may follow closely on the heels of misunderstood orders. Brevity, clarity, conciseness must be the first aims of anyone who drafts a message.

Dispatch preparation would be comparatively simple if the job of the drafter stopped with the realization of these goals, but his task goes much further. Since every message may be intercepted by the enemy and every dispatch by radio is likely to be intercepted, the originator must word his dispatch so that the enemy can gain little information of value. Unless he is alert, the odds are in favor of the enemy. When time is limited, drafting must be done in a hurry, whereas the effort to break an encrypted dispatch will always be made by experts with unlimited time at their disposal.

If the message is to be sent in plain language, it must contain no information or clues to information which, in the hands of the enemy, could cause harm. A plain language dispatch should have meaning for the addressee but should be meaningless for the interceptor or should give him no information which is not already public knowledge. "Your 231910 affirmative," transmitted in plain language,

would be of little value. To the addressee, on the other hand, it might mean that the authority he requested in his dispatch 231910 was granted. This rule may be relaxed if the dispatch is to be sent by a channel secure against interception, but it can never be disregarded if the dispatch is to be sent by radio.

When a dispatch is to be enciphered and transmitted by radio, the tendency often is to assume that encipherment guarantees security, regardless of the physical make-up of the text. No theory could be more fallacious. Although current methods of encryption are the product of years of scientific study and extensive experience, no practical system of encipherment yet devised can resist attack forever except a one-time pad. The best machine ciphers are considered almost impregnable provided the rules are followed scrupulously. If properly drafted and enciphered, a dispatch in a less secure system will resist cryptanalytic attack until the information has lost its value to the enemy.

Though never at the risk of clarity, phraseology should be chosen with a view to forestalling attempts of the cryptanalyst to break a message by intuitive methods. Proper drafting is no guarantee against mathematic cryptanalysis, for many rules of language construction apply regardless of the wording used, but proper drafting defeats the enemy's attempts to break an encrypted message by guessing at the sense of a particular portion. In attempting to arrive at the meaning, the cryptanalyst relies heavily on what he believes the originator has said; through sheer guesswork coupled with a wealth of experience and knowledge of the originator's habits, he often is successful.

Habit in communications and especially in drafting is a boon to the cryptanalyst. During the World War of 1914–18 German slavery to method in the field of communications proved a never-failing source of aid to the Allies. The British usually knew in advance, for instance, when a Zeppelin raid on London or some other English city was under way. Because of the hazards attending raids of that nature, the Zeppelins carried on board only one code, not their most confidential. Prior to leaving their hangars, the Zeppelin commanders reported by radio that they had "Only H. V. B. on board," "H. V. B." being the term for a less secure code.

Unfortunately there is a general tendency for military or naval terminology to fall into a set pattern, readily exploited by the enemy to his own advantage. This tendency must be resisted by originators of dispatches. Varying one's phraseology helps to keep the enemy's cryptanalytic processes off balance and to force him to waste time and effort, a result as desirable in communications as in fleet operations. Unless the enemy can guess successfully the thought of a dispatch and the terminology used in expressing that thought, he is doomed to failure in his attempts to break the message rapidly.

Often dispatches must be written, enciphered, and transmitted in haste. The originator will not always have time to draft and redraft at leisure until he has achieved the maximum of clearness and the minimum of helpfulness to the enemy. It is therefore important to practice drafting at every opportunity and to take the same pains with plain language as with encrypted dispatches until proper drafting becomes second nature.

Stereotyped Phraseology.

During the years immediately preceding 1914, when all Europe was seething, absolute secrecy in diplomatic and military affairs was zealously sought by the great powers, and it was considered a tremendous achievement for one country to obtain, through breaking or theft, the code of another. The greatest coup of all was the work of the Viennese cryptanalysts, one of whom noticed that the diplomats of every great European power used a certain opening in their plain language dispatches—"I have the honor to inform Your Excellency—" or its equivalent. It occurred to him that the same introductory phraseology might also be used in coded diplomatic telegrams, and with this clue the Austrian cryptanalysts attacked the intercepted communications of all foreign representatives in Vienna.

The supposition was correct; eventually, aided by several other weaknesses in the code structures, the Austrians succeeded in reconstructing the diplomatic codes of most European countries. Blinded by confidence in the security of their secret systems, and unaware of their bondage to habit, the foreign ambassadors blissfully continued the use of the compromised codes, to their own detriment.

The lesson learned by the European ambassadors is directly applicable to naval communications today. It is not an exaggeration to estimate that at least half of the time when an originator takes pen in hand to draft a dispatch, the first words which spring to his mind are the words which the enemy expects him to use. If he wishes authority from a superior to carry out a specific task, he is tempted to write "Request authorization—." If he is confronted with an unusual situation requiring enlightenment, he is likely to begin with "Request advice—." If he believes that a required procedure may be improved, he writes "Recommend—." When he wishes to get information from a junior, the first word which occurs to him is "Report—." If he needs details regarding the effectiveness of a new item of equipment, his first inclination is to write "Submit—."

Stereotyped phraseology within the body of a dispatch is often as valuable to an enemy cryptanalyst as at the beginning. When he locates the word "practicable," he assumes that the phrase "as soon as" precedes it. When the word "earliest" is found, the chances are that "at" precedes and "opportunity" follows. If he recovers the word "please," which is understood but should not appear in naval dispatches, he is probably right in his conclusion that "advise," "report" or "submit" follows. It is common to end messages with the word "comply," "advise" or "expedite"; and frequently the phrase, "details will be forwarded by mail," appears.

The originator might substitute, for example, "at first feasible time" for "as soon as practicable"; "present particulars" instead of "submit details"; "needed immediately" in place of "urgently required"; or "Can you now answer my 271642" instead of "Request reply my 271642."

No forms of expression should *habitually* be used by an originator. This applies to the unusual method of expression as much as to the stereotyped phrase. Once a drafter falls into the *habit* of substituting a certain phrase for a common one, he has stereotyped the unusual phrase and may expect the enemy soon to realize this. In drafting, *any habit is a bad habit.*

A stereotyped message, whether necessary or unnecessary, can be of great value to the enemy. In 1917, the Germans were following the

practice of changing their military ciphers every few days, but prior to putting a change into effect, they often radioed a test message in the new cipher in order to ascertain that the system was understood. These test messages simplified the work of the British and French cryptanalysts, for there was little originality in their texts. Proverbs were most popular, and of these "A bird in the hand is worth two in the bush" was the outstanding favorite.

Routine messages which follow a prescribed pattern or outline present a problem in drafting which requires resourcefulness and common sense. The form for daily fuel reports is an example. In the hands of a literal-minded communicator it may start off with "paren able paren" and the amount of fuel on hand, followed by "paren baker paren" and the number of gallons expended, and so on. One day's traffic similarly drafted contained "dash" nearly 400 times in 2,000 groups, making a total of 300 unnecessary groups and exposing the system to almost certain compromise. Other instances of smaller magnitude could be cited.

The words "dash" and "paren" are unnecessary and should be omitted. Moreover, the order of the items may well be varied. Item "able" need not always come first or "baker" second. The danger of misreading certain of the phonetic equivalents should not be overlooked, however.

Length.

Brevity must ordinarily be the goal. The originator who uses 50 words to write what can be said in 25 causes needless work along the entire line of communications and runs the risk of being misunderstood. The longer the individual message, the greater the amount of traffic available for interception; the more traffic the cryptanalyst has to work with, the more likely is he to succeed, and the shorter the life of the system.

Unless one is continually alert to avoid superfluous and redundant phraseology, he will unconsciously include many unnecessary words in his dispatches. A submarine on patrol in the eastern Mediterranean recently transmitted a radio message in which the words "north" and "east" were used 18 times. All 18 words could have been omitted, for

it is impossible to confuse north and south latitude and east and west longitude in the Mediterranean, except in the far western portion.

Articles, prepositions, and conjunctions are among the first values recovered by cryptanalysts, often giving clues to the words preceding and following. They should, therefore, be deleted unless absolutely necessary for clarity. Officially recognized abbreviations should be used whenever possible.

Given an unusually long message, the cryptanalyst seeks first of all to locate repetitions and to apply his mathematical knowledge to the breaking of the text. If an encrypted radio dispatch, even though concisely drafted, is still unusually long, it may be better to break it into two or more dispatches of dissimilar length, with all outward evidences of linkage between the parts eliminated. Experience has indicated that 100 groups is the safe maximum for a single message in a flat strip cipher.

Extreme brevity is dangerous. With a message of two or three enciphered groups, the cryptanalyst can restrict the probable meaning to a very few possibilities, and in the majority of cases will find that one of his assumptions is correct. Five groups, exclusive of indicators, therefore, constitute the minimum desirable length of a dispatch.

Substitution of uncommon expressions for stereotyped phraseology may at times justifiably increase the length of a dispatch. Use of verbose language to extend the length to or even beyond the minimum of five groups is likewise permissible. In no other instance is there excuse for lack of brevity.

Repetitions.

It is a common fault in preparing a dispatch to repeat a word, perhaps an uncommon one, several times. Often the nature of a message demands repetition of certain technical words or phrases, but repetition should be avoided whenever possible.

A vicious habit, but a common one, is repetition for emphasis. The originator probably believed he was lending clarification and stress when he transmitted, "New direction-finding equipment not repeat not received." Such redundancy is totally unnecessary and is dangerous.

References.

References to date-time groups of previous messages are always a source of danger. Numbers are the easiest words to recover. The enemy interceptor who successfully locates the reference, knows that the two messages are related and, if he has made any progress in deciphering the first dispatch, can apply his knowledge of the subject matter to obtaining the meaning of the second.

The ideal solution would be to avoid all references in encrypted messages, but this is impossible, since references are often necessary for clarity and brevity. Whenever it appears that a reference is not necessary or that it can be omitted through minor rewording of the text, it should be avoided.

When use of a reference appears necessary, it should not be placed at the beginning, for this is the place where a cryptanalyst expects to find it. It should be worded to avoid repetition of numbers, if possible. One is tempted to write "your 070700" as "your zero seven zero seven zero zero" without realizing how this might help the enemy. "Your zero seven hundred yesterday" would be much better.

Punctuation.

Punctuation in a dispatch is a weakness, for cryptanalysts are quick to search out values for expressions of punctuation. Once these are located, the remaining task of the cryptanalyst is simplified, since the message can then be divided into its component sentences and clauses.

A properly drafted dispatch needs very little if any punctuation. When it is used, the marks will seldom need to be spelled out; the single letter X should be consistently used for comma, period, and other marks. The word "stop" should not be used, and obviously there is no need for either the word "end" or an X at the end of a dispatch. There should be very rare occasion for use of "quote," "unquote," "dash," and "paren."

In referring to task organizations in dispatches, the word "point" is usually used to separate the component numbers. Task Unit 4.1.2 is in most cases expressed as "four point one point two." In order to avoid repetition, it would be well to use "decimal" or "dot" part of the time.

Dates.

In the solution of an intercepted message, dates and the names of days and months are particularly helpful. The cryptanalyst may assume that the current month is mentioned somewhere in the text; he may also expect reference to previous or future days and months. If he can locate one of these values, he is assisted in arriving at the meaning of at least a portion of the dispatch.

It is well, therefore, to eliminate reference to dates whenever possible. Instead of using "September 10," one may say "day after tomorrow" or "yesterday" or "tomorrow" or "three days ago" as the case may be. There is no reason for writing "tomorrow Tuesday," as is so often done, or "arrived August 30," when the date-time group shows that the dispatch was originated on August 30.

Names of Addressees and Originators.

The concealment of the addressee(s) and the originator of a message is as important as concealment of the subject matter. If the enemy is aware of the originator and destination of a message, he is part of the way toward guessing the contents. Furthermore, the identity of units at sea must be protected. For this reason, call sign ciphers are provided and are used under certain circumstances with both plain language and encrypted traffic.

This necessary secrecy may be defeated, however, when the name of the originator or the name of an addressee appears in both heading and text of the message. Compromise of either would lead to breakdown of the other. If, under certain circumstances, it becomes necessary to mention an addressee or the originator *in an encrypted message,* the title and not the call sign should be buried in the text.

Information Addressees.

The Japanese, it is said, through some inherent fear of offending, include in their dispatch headings the call letters of any activity which could be even remotely interested in the text. The practice might keep certain officers from losing face, but it increases the possibility of their losing their heads.

Experienced radiomen who know the originator, action and information addressees of a particular message, can often guess at the content. It would be foolhardy to assume that the enemy can do less. A dispatch from an aircraft carrier at sea addressed to the Bureau of Aeronautics and the Bureau of Ordnance is likely to concern aircraft gunnery. If the message were addressed only to the Bureau of Aeronautics, the text could include a request that Ordnance be informed, and interceptors would have less information as to the contents of the message.

Addressing messages to a large number of activities for information, without serious consideration as to whether they must have knowledge of the dispatch in question, is a burden to the addressees and to the communication system. Information addressees should be reduced to a minimum consistent with effective action.

Frequently it is not necessary that information addressees receive a dispatch as promptly as the action addressee. It is well in that event to forward copies of the dispatch to the information addressees by mail rather than by radio.

Acknowledgments.

Acknowledgements to encrypted messages must be cut to the bare minimum. They increase the volume of traffic, burdening communications when attention should be concentrated on important operational messages. If acknowledgments are sent by radio, they give the enemy information regarding the echelon of command, the call sign cipher, and the movements of ships at sea.

The reliability of the Naval Communication Service, offering assurance that messages will be delivered to the addressees without fail, precludes the necessity for acknowledgments except in the most unusual cases.

Frequently, although acknowledgment may be requested, a prompt reply to the dispatch will eliminate the need for a separate acknowledgment. When separate acknowledgment is necessary, it should be made by mail if at all practicable.

Acknowledgments, when made, should be in plain language. To send a radioed acknowledgment in cipher would endanger the system, because the dispatch would contain only the reference numbers of the acknowledged message, values easily assignable by the cryptanalyst.

During war, acknowledgments should never be requested of ships at sea, since the breaking of radio silence is very dangerous. Messages transmitted by the broadcast and intercept methods should never be acknowledged.

☆ ☆ ☆

SUMMARY

The aim in preparing a dispatch should always be to express oneself clearly and without ambiguity, avoiding the common method of expression and any possible linkage of the enciphered version with the plain language text.

CHAPTER IV. PROCESSING OF DISPATCHES

Once a dispatch has been drafted and then released, the communication personnel take charge. It is their duty to encrypt where necessary and to transmit the message.

In most activities, carelessness redounds to the detriment of the responsible individual. In communications, however, the direct result of error is often the defeat of well-laid plans, frequently accompanied by unnecessary loss of ships and lives. The individual at fault too often escapes unharmed.

Communication Personnel.

On shipboard, the communication officer is at the head of a division which is responsible for the operation and maintenance of radio, underwater sound apparatus and visual signaling equipment, the proper handling of all correspondence, and the custody of classified matter.

In addition to his technical duties, the communication officer is ex-officio head of the coding board—an organization consisting of personnel assigned to the encryption and decryption of dispatches. At sea where the complement may be too small to permit adequate numbers to perform coding board duties exclusively, the coding board will include all officers assigned to communication duty and certain others whose routine duties are not pressing during operations and who therefore are available to assist when most needed. At least one member is on hand for cryptographic duties at all times, and more if the volume of traffic requires.

It is the communication officer's responsibility at intervals to conduct practice drills covering encryption, decryption, rectification of errors, clearing of garbles, and preparation of paraphrases. All members of the coding board participate.

No one in sound mind would attempt to drive an automobile

without learning the rules for its care and operation and observing them. Yet relatively few who drive cars understand exactly how the manipulation of levers starts a car or keeps it under control. In the same way, the coding officer may not fully understand the purposes of the rules he is asked to observe, but if he follows them faithfully and intelligently the ciphers will carry out successfully the job they are expected to perform.

The security of a cryptographic system is governed by the manner of its employment. Developed after years of study, the rules for use of each system are based upon sound security principles. Each rule closes a gap in the defenses; if it is ignored, a breach appears in those defenses. The result of years of labor and the product of the most experienced minds in the field may thus be lost through a minute of carelessness on the part of a coding officer.

Use of a compromised cryptographic system obviously must be discontinued immediately. Unfortunately, *compromise through misuse* often does not come to light until a long period has elapsed, during which the system may have been used frequently. Combating compromise, therefore, is like dealing with unknown fifth columnists; a misused cipher or code may long remain in effect, trusted and unsuspected but a source of intelligence to the enemy.

Communication and coding personnel have no authority to determine the secrecy classification and the degree of precedence of a dispatch or to alter its phraseology. Because of their familiarity with the principles of proper phraseology and classification, however, they should be quick to uncover violations in these fields on the part of the originator. Whenever it appears that improper phraseology has been used in the drafting of a message or that the classification should be altered, the communication officer or the coding officer may suggest to the originator that a change be made, provided that the time so lost is not a matter of serious importance.

Since coding officers are more familiar than any other naval personnel with the work of encryption, they are more likely to uncover flaws in current systems and to discover means of strengthening communication security. By submitting their suggestions for improvement in code and

cipher systems and in security factors, coding officers can make a substantial contribution to the Navy's methods of secret communication.

Plain Language Dispatches.

Although radio dispatches during war or a national emergency are generally transmitted in cipher or code, there are certain circumstances under which such dispatches need not be encrypted. Such plain language messages may give no indication of the originator, the addressees, or the names of ships, in order to avoid the possibility of call sign compromise or betrayal of the location of fleet units.

In some cases, plain language replies may be made to encrypted messages. Only certain words are permitted. Thus the plain language message, "Your 172309 negative," is acceptable in reply to a secret dispatch. The number of permitted expressions is small lest any be included which the enemy could exploit deceptively and with disastrous results. "Cancel," for instance, is one of those *excluded.*

If a proposed dispatch consists primarily of information which need not be enciphered but also includes some information of a classified nature, it may be feasible to segregate the classified information from the other, sending the former in cipher and the latter in clear. Reference may be made in the encrypted dispatch to the plain language message, but there must be no evidence of linkage in the latter.

Under no conditions should a message which has once been transmitted in cipher be retransmitted in plain language or vice versa, regardless of whether or not the dispatch should have been encrypted in the first place.

In 1914 at the outbreak of war, the Russians replaced their peacetime cipher with a new system. Through error, only one of the two main armies advancing on Prussia received the key and destroyed the old cipher. Close coordination between the two armies was imperative, but all attempts to communicate secretly were fruitless, for neither had the system held by the other. Finally, in desperation, the Russians repeated their radio dispatches in plain language, giving the Germans not only the means to break the new system but information on which to plan a counterattack, carried to success in the battle of Tannenburg.

Choice of System.

To distribute the traffic load over the available cryptographic systems and to provide means for secret communication between sundry units and activities of the Navy, a system of cryptographic channels has been developed. A naval unit has available certain cryptographic aids, each of which is held by a number of other units. All the holders of one system form a channel of communication. The Navy Department is the only activity holding all naval cryptographic aids; other units usually are members of a number of channels, but to some units only one channel is available. It is the job of the coding officer to select the particular channel to be used.

Normally, the cryptographic system with the narrowest distribution including all addressees should be employed in the encryption of a dispatch. If a system of wider distribution were used, that system would carry an unnecessary load, thereby shortening its life. The channel organization is delicately balanced with the reasonable expectancy of traffic volume and the estimated life of the cryptographic aids concerned.

Special-purpose systems should always be used in place of general-purpose systems in encrypting dispatches for which they were designed. They have been devised for the peculiar requirements of certain functions or operations, and are adapted to give maximum speed and security when used as intended.

A message is rarely sent to two correspondents in two different cipher keys or systems, and then only by a senior officer when all addressees do not hold the same system. In such a case padding would be used to conceal the otherwise identical length of the two messages.

Violation of this principle enabled the "American Black Chamber" to break the Spanish diplomatic code in 1918. A circular telegram of identical text had been entrusted to four different codes for transmission to a number of addressees. Since the key to one of the codes was known, breaking of the others became only a matter of time and patience.

Encryption.

In his efforts to extract intelligence from naval communications by cryptanalysis, the enemy relies heavily on two aids—improper drafting and faulty encryption. Of the two, faulty encryption is probably the greater source of compromise. A poorly constructed cipher used by a careful coding officer observant of all the rules may actually be safer than a more secure cipher used carelessly. It must be remembered that violations of security can cause greater loss than incompetent navigation.

Since the rules for the use of different cryptographic aids vary even within a family group, the coding officer must be ever on guard against applying the instructions for one system to his use of another. He must review instructions at intervals and keep up to date as changes occur. Cryptographic systems of allies often differ basically from those of the United States, increasing the need for complete understanding before use.

Accidental inclusion of a line of plain language text in an encrypted dispatch may well result in rapid decipherment of the rest of the message and compromise of the system. Yet it sometimes appears as a result of thoughtlessness.

One can imagine the German coding officer's embarrassment, immediately prior to the Battle of the Dogger Bank in 1915, when the message, "Main fleet and destroyer flotillas will come as soon as possible" and signed "Commander High Seas Fleet," was transmitted. The entire message was sent in plain language with the exception of "as soon as possible," which was encoded. Prevention of such an error is certain if ordinary alertness is manifested.

There is only one sure method of determining that a dispatch has been properly encrypted. Another member of the coding board should decrypt it prior to transmission, checking to ascertain that all rules have been obeyed. Only through pursuit of this policy can errors be corrected before they have caused trouble.

If a dispatch is unusually long or beyond the limit prescribed for the system employed, it should be divided into two or more parts of unequal length, to be encrypted and transmitted as separate messages. Different date-time groups and internal indicators should appear, and every

effort should be made to avoid any *external characteristics* which will permit an interceptor to realize the connection between the parts. If possible, parts should be encrypted on different days.

Padding: Dummies and Nulls.

In a properly drafted dispatch, there is no need for the addition of *dummy* words at the beginning or end of the text. In the case of unavoidably stereotyped dispatches, padding may serve two purposes: it may disguise stereotyped beginnings and endings and it may increase a dispatch to the minimum desirable length. When used, padding must be applied to the *plain language* draft, then encrypted.

As an example of too brief a message, assume that the coding officer receives for encryption the following dispatch: "Arrive sixteenth." If encrypted and transmitted exactly as submitted to the coding officer, the dispatch might readily be translated by an interceptor. The encrypted version would consist of fewer than five groups of text, exclusive of indicators, and the phraseology is exactly what the enemy would expect the originator to use if he were reporting the date of arrival.

Since the dispatch as submitted is stereotyped and short, the coding officer might suggest to the originator improvements in wording and an increase in length, or he may, through the use of dummies, increase the length and bury the stereotyped terminology. The first course may be more satisfactory, but the second is far more practical.

There are several dangers which must be avoided in the use of padding. The dummy words which are selected must be so foreign to the text as positively to prevent misunderstanding by the addressee. In addition, they are separated from the text by one or two infrequently used consonants.

If the dummy words are linked in meaning to one another, they will aid the cryptanalyst in assigning remaining values after he has successfully translated one of the dummy words. Suppose the phrase "cats and dogs" is used at the beginning of a dispatch and "Happy New Year" at the end. If the enemy solves *one* of the words in each group, he can readily guess at the true meaning of the others. The same principle applies to continuity of padding at the beginning and ending. "Now is the time for" at the beginning and "all good men" at the end

would not long stump the cryptanalyst once he acquired an entering wedge.

Several short, unconnected words are more satisfactory as dummies than one long word. It is often easy, after two or three letters of a long word have been given values, to guess accurately at the remaining letters. Also, to keep the cryptanalyst's scientific approach off balance, it is well to vary the length of the padding used.

Nulls are meaningless letters a common use of which is to complete the last enciphered group of a message. Since each group must contain five letters, there are few messages which normally end with a complete enciphered group. If the plain language draft of a dispatch contains 67 letters, three nulls must be added before encryption.

When the same nulls are consistently used by the coding officer, a series of X's or XYZ, for instance, the nulls themselves become stereotyped, and the enemy may be expected to translate them with little effort. No letters should be consistently used, but nulls should be selected at random, preferably from such infrequently used consonants as J, K, M, P, Q, and V. Alphabetical series such as K L M should be avoided. Care must be taken to make sure that the null or nulls selected cannot be considered as the close of the last word or an additional word in the dispatch, perhaps in this manner changing the intended meaning; for this reason vowels should usually be avoided.

Retransmission.

Frequently it becomes necessary to retransmit a dispatch which has already been enciphered and transmitted by radio.

Through errors in enciphering and occasionally in transmission a dispatch may become so garbled as to be unintelligible to the addressee. It has been said that fully one-third of the radio dispatches intercepted by the British in the first World War were garbled. In a count of traffic on a Mediterranean submarine patrol, 30 out of 127 dispatches received were found to be corrections to previous messages.

Garbled messages not only perplex addressees but, because of the need for retransmission, increase the volume of traffic, overloading cipher systems, crowding radio circuits, and aiding enemy cryptanalysts in their search for the meaning of intercepted dispatches. Observance

of the ciphering rules and thorough checks prior to transmission will eliminate many garbled dispatches.

An able coding officer who receives a garbled dispatch can often locate the source of the trouble without requesting a repetition of the message. Errors of transmission usually result in single-letter garbles, which are readily cleared through close inspection. Prior to requesting a repetition, every effort should be made to detect the error and to arrive at the correct wording.

Unfortunately, in some of the more complicated cipher systems, an error in encryption will render the balance of the message gibberish, making solution almost impossible without repetition. When a dispatch appears hopelessly garbled, a verification should be immediately requested, but this is no reason for casting the dispatch aside to await the retransmission. Frequently, with a little ingenuity, the coding officer may be able to unscramble the garbled message before the correction has been received.

Sometimes a coding officer is asked to repeat only a portion of a dispatch which was unintelligible due to garbling. He occasionally will need to transmit enciphered corrections to the original message in the same cryptographic system; but he must not make corrections in such a way as to repeat the correct portion of the dispatch with different cipher values.

If the letters in the group KBLAD, for instance, had been accidentally transposed and transmitted as BKDAL, a correction could be transmitted, if no succeeding cipher groups were thereby changed. If, however, a word was omitted in the original transmission or some other error has occurred which results in change of the cipher values in the remainder of the message, corrections would not be permissible, and a new message should be originated with different padding, a new date-time group, and a different internal indicator. It should contain a cancellation of the previous message.

The reason for this is clear. Enciphered variants of the same word are a tremendous help to the cryptanalyst in reconstructing a system. If he can discover that a word is enciphered as HCDON on one occasion and FJIKB on another, he will be a step along the road toward rebuilding the system.

Occasionally a dispatch is enciphered in a cryptographic system not held by the addressee. When this occurs, the dispatch is lengthened by padding and the sentences are rearranged before encrypting it in the correct system and retransmitting. All external evidence of linkage must be removed.

Failure to do this, thus giving the enemy obviously parallel texts of the same dispatch encrypted in different systems, would encourage a recurrence of the German experience on the Champagne front in 1918. The Germans had planned a devastating drive on Champagne in July, and in their pains to keep the proposed attack absolutely secret, issued a new cipher to all units. In answer to certain orders encrypted in the new system, one unit replied, "New cipher not yet received. Please repeat message in old cipher." The message was repeated in the superseded cipher, which the Allies had already broken. Soon the Allies were reading all traffic encrypted in the new system; adequate countermeasures were taken against the contemplated attack and the drive turned into a serious reverse for Germany.

When the recipient of a dispatch wishes to pass a message along to others who should have the information, he may retransmit the dispatch to them *exactly as received,* provided, of course, they are holders of the system utilized. In passing a message to an addressee who does not hold the same system, the procedure is the same as in other instances where reencryption becomes necessary. The length may be altered by insertion of a statement such as "This is forwarded for your information."

Paraphrasing.

The term *paraphrasing* as used in the Navy is the process by which the sentence structure and language of a message are altered without changing the meaning. An encrypted naval dispatch must be thoroughly paraphrased whenever its content is made public or otherwise given distribution outside the Navy.

Paraphrasing is an evil which sometimes risks more in misunderstanding than it gains in security. Since a paraphrased message must not change the sense of the original, the process is difficult even in the hands of experienced officers. *It should not be undertaken lightly.*

At best it is only a makeshift method which, if properly performed, hinders linkage of the paraphrased and encrypted versions of a dispatch. It merely makes the task of the cryptanalyst more difficult.

While the simple process of reducing numerals or expressions like "Communication Security Publication" to "CSP" or vice versa is sometimes called paraphrasing, this really is not a correct use of the term. Such changes are a routine part of preparing a message for internal distribution after receipt and decryption.

A quotation from a newspaper, a periodical, a letter, or even from conversation should be paraphrased before including it in an encrypted message. It should always be assumed that the enemy has available at his fingertips these sources of information; to lift even a brief quotation and to transmit it verbatim in a cipher might give him an adequate lead to the reconstruction of a system. Although paraphrasing in this case is the task of the originating officer, communication personnel should be alert to suggest its use when this appears desirable, and should be prepared to assist the originator in the actual mechanics.

Cryptanalysts attacking a multialphabet system once uncovered in a message of low security a long quotation regarding a diplomatic conference, which had been lifted from a secret dispatch. The day on which the dispatch was received was also mentioned. Without difficulty the secret message was located in the intercepted dispatch files, and the quotation applied. A sizable portion of the system was in this manner reconstructed. Paraphrasing of the quotation and elimination of the date of receipt would have protected the system of high security.

The same principle holds true in connection with information issued to the newspapers or otherwise given broad distribution. If information received encrypted is translated and issued unaltered as a portion of a communique, it would not require a very clever enemy to break the system through application of the published translation to the dispatch he has already intercepted.

An example of paraphrasing may be helpful. Suppose that the commander of a task force has transmitted the following dispatch to his commander in chief:

UNKNOWN CRUISER TENTATIVELY IDENTIFIED AS GOEBEN CLASS ATTACKED CONVOY XRAY NINE AT SEVENTEEN HUNDRED TODAY X RAIDER SUPPORTED BY TWO DESTROYERS X TWO MERCHANT VESSELS DAMAGED X ONE SERIOUSLY BY SHELLFIRE X NO DAMAGE TO ESCORT FORCE X AT APPROACH OF ESCORT DESTROYERS ENEMY IMMEDIATELY RETREATED UNDER COVER OF NIGHT TAKING SOUTHWESTERLY COURSE

Paraphrase may best be performed in successive stages, as follows:

1. The order of sentences should be altered. Sentence number three may be placed first, one second, five third, two fourth, and number four last. Any other unconfusing arrangement of sentences would be acceptable, provided each sentence is moved from its original position.

2. Transitive verbs should be changed from the active to the passive voice and from the passive to the active, reversing subjects and predicates. At this stage in the process, the dispatch might read:

SHELLFIRE DAMAGED TWO MERCHANT VESSELS ONE SERIOUSLY X CONVOY XRAY NINE WAS ATTACKED AT SEVENTEEN HUNDRED TODAY BY UNKNOWN CRUISER TENTATIVELY IDENTIFIED AS GOEBEN CLASS X AT APPROACH OF ESCORT DESTROYERS ENEMY IMMEDIATELY RETREATED UNDER COVER OF NIGHT TAKING SOUTHWESTERLY COURSE X TWO DESTROYERS SUPPORTED RAIDER X ESCORT FORCE WAS UNDAMAGED

3. Where possible, the location of clauses and phrases should be changed within each sentence and the order of words in series should be altered.

4. Synonyms should be substituted wherever practicable, making sure that no misunderstanding is likely to result.

When the last two steps have been carried out, the dispatch might appear as follows:

PROJECTILES CRIPPLED ONE MERCHANT SHIP SOMEWHAT IMPAIRING ANOTHER X AT SEVENTEEN HUNDRED TODAY CONVOY XRAY NINE WAS SHELLED BY UNIDENTIFIED CRUISER BELIEVED TO BE OF GOEBEN DESCRIPTION X IN DARKNESS ENEMY ESCAPED SOUTHWEST WHEN OUR DDS CAME UP X TWO DESTROYERS ACCOMPANIED ATTACKER X OUR SUPPORTING SHIPS UNHARMED

5. Unnecessary words should be eliminated. The phrase "at seventeen hundred today" may be briefed to "seventeen hundred," which will be clear to the addressee as the time of the raid, occurring "today" unless another date is given.

6. The length of the dispatch should be varied from 15 to 25 percent as compared with the original version. In most cases, the preceding steps in paraphrasing will have changed the length substantially so that no further adjustment is necessary. If the length has not been changed sufficiently through this process, phrases, clauses and word-synonyms of different length may be substituted.

7. All external evidence of linkage with the original dispatch must be removed from the paraphrase. If the dispatch is to be retransmitted, a new date-time group should be substituted. If necessary, the originator and time of origin may be buried in the text.

After completion of the paraphrasing process, the dispatch shows a minimum of linkage to the original and yet retains the same meaning:

PROJECTILES CRIPPLED ONE MERCHANT SHIP SOMEWHAT IMPAIRING ANOTHER X SEVENTEEN HUNDRED XRAY NINE SHELLED BY CRUISER BELIEVED OF GOEBEN TYPE X IN DARKNESS ENEMY ESCAPED SOUTHWESTWARD WHEN OUR DDS CAME UP X TWO DESTROYERS ACCOMPANIED ATTACKER X OUR SUPPORTING SHIPS UNHARMED

Once the methods of paraphrasing have been mastered, the steps given above need not be performed separately but may be accomplished in one operation. With experience and care, paraphrasing can be performed competently with little delay.

SUMMARY

Communication and coding personnel have a heavy responsibility in processing messages. They must be conscientious, up to date, and well practiced in performing their duties. They must be alert for possibilities of compromise and ready to suggest changes in precedence, classification, or phraseology when this seems warranted.

CHAPTER V. RADIO INTELLIGENCE AND SECURITY

Widespread use of radio as the primary tool of naval and military communications has inspired the development of a new phase of espionage—radio intelligence. While this activity concerns communication personnel only directly, except as it includes interception and cryptanalysis, an understanding of it is valuable in a variety of ways.

The Enemy Is Listening.

This warning is never more pertinent than when applied to radio communication. Today, each message sent by radio is open to reception by any friend or foe who has the necessary equipment and is within the reception range. *Unauthorized interception must be expected whenever a transmitter is placed in operation.*

How does the enemy profit from his clandestine observance of naval radio activity? What are his methods of gaining useful intelligence? In the first place, the enemy copies the traffic intercepted by his listening posts. This is then forwarded to the black chambers for classification and expert cryptanalytical attack. If the volume of traffic enciphered in any one system is great enough and there are sufficient errors in drafting and encryption to aid solution, the likelihood of success is strong.

In most cases, if a message is drafted and encrypted in full compliance with the principles of cryptographic security, cryptanalysis, if successful, is so delayed that the information has lost its value to the enemy. Data as to the structure of the system, which the cryptanalyst acquires through breaking a few messages, will usually improve his efforts to break future messages.

A second phase of radio intelligence, which may be fruitful to the enemy even when his cryptanalysts fail him, in analysis of the volume of radio traffic. The peaks and valleys in the numbers of dispatches

transmitted are frequently excellent indications of contemplated major operations on the one hand and routine activity on the other. When hitherto little-used circuits suddenly crackle with transmissions, the enemy cannot be far wrong in assuming that something unusual is afoot.

The British, for example, were forewarned of an impending naval action by the German Fleet in late May 1916, when the radio waves were suddenly burdened with enemy traffic. Regardless of the success of their cryptanalysts in solving the dispatches, the traffic peak was enough to put the British on their guard and lead them to expect some move by the German Fleet. The Battle of Jutland took place a day later.

During one phase of the Battle for Libya, Italian radio intelligence agents were warned of an impending British move by the suddenly increased daily traffic between sundry army units as they moved into position.

Traffic peaks, in this manner, may prevent the success of proposed operations. The effectiveness of a plan frequently is lost when the enemy becomes aware that an operation is impending. In many cases the method of attack can be deduced, but at very least the enemy, being forewarned, becomes more alert and holds his forces in readiness. In view of the advantages, it is logical to expect the enemy to keep accurate statistical records of the number of messages handled over the various circuits and to interpret the lows and highs in traffic volume scientifically.

The enemy may also draw conclusions as to impending operations through observing the direction of traffic flow. If, for instance, within a short period of time, a radio dispatch is transmitted from point Baker to Queen, another to Victor, another to a unit of the fleet operating off William, and a fourth to a unit off Oboe, the enemy may logically assume that a convoy from Baker to Queen is being planned and that provisions are being made for its escort. The intelligence experts are almost certain to draw this conclusion if their traffic records indicate that seldom are messages transmitted to the four addresses almost simultaneously and that previous coincidences of this nature were followed by the arrival of a convoy at Queen.

Traffic flow may also indicate the organization and composition of forces at sea. If a particular unit at sea directs dispatches to several ships and the latter in turn transmit to still other units, with return messages following the same channels, the enemy may be able to construct in outline form a particular task force organization. Future messages may give him the details to fill in his tentative chart or may indicate previous assumptions incorrect.

One of the important phases of radio intelligence concerns the locating of ships through radio direction finding. Direction-finding equipment has reached such perfection that any radio transmitter in use for more than a few seconds at a time may be located rapidly and with fair accuracy. A valuable navigational aid during peacetime, radio direction finding during war is turned to the locating of ships for purposes of attack or evasion.

Directional wireless was a substantial help to the British in locating the position of units of the High Seas Fleet whenever they ventured from harbor. Stations scattered along the coasts of the British Isles submitted frequent reports of intercepted call signs of German submarines and the direction from which the signals were coming. When plotted on a central chart, the reports of several differently located stations indicated the approximate position of the U-boat transmitter. With the location of the submarine known, convoys were routed to avoid the enemy's effective striking area.

Direction finding played a part, albeit a minor one, in the location of the German battleship *Bismarck* during the chase of May 1941. Equipment on submarines for direction finding has been so perfected as to reveal the location of merchant ships by means of bearings taken on oscillating receivers.

Another phase of radio intelligence consists of basing assumptions on what one fails to hear. The Battle of Coronel in 1914 provides an example of the dangers connected with conclusions arrived at by this means. A small British squadron cruising northward along the Chilean coast intercepted a number of messages from the *Leipzig*. Since no other radio calls were heard and the *Leipzig* was apparently not transmitting to naval vessels, the British concluded that she was on a lone raiding mission. The English ships thereupon scattered to bear down

upon the German from several directions. A short time later, when the British force was badly dispersed, the *Leipzig,* accompanied by a numerically superior German squadron, was sighted. The Battle of Coronel followed.

Radio Security.

Just as for every poison there is an antidote, for every new tool of warfare there is an effective countermeasure. To prevent the enemy from learning the truth through 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 discipline is, primarily, intelligent adherence to existing instructions. Unless rules for the use of radio are continuously observed, not only will the communication system fail to function properly, but it will betray its secrets to the enemy at a time when intelligence in unauthorized hands may result in loss of lives and ships.

The radio operator's manual covers a variety of instructions, the need for which has been proved by long and often bitter experience. Operators are required to keep logs, to avoid unauthorized transmissions, to use correct procedure at all times, and to report violations of instructions which they have noted. They must use radio calls properly and observe strictly the rules for the use of plain language.

Radio transmitters should always be calibrated accurately and tuned to the proper frequency. Every precaution should be taken to give a transmission enough power to reach the addressee *and no more,* in order to reduce the interception radius to a minimum. Operators must be prepared to shift from the current working frequency to the standby frequency whenever interference requires.

Radio discipline requires more than blind obedience to the rules. The good operator develops an active imagination which explores the possible deductions the enemy might make from the manner in which he uses his radio; he does everything within his power to prevent the enemy from learning the truth about the messages he transmits. Continued alertness is coupled with intelligent observance of instructions.

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 whenever British ships left their base.

In view of his familiarity with the technical potentialities and limitations of radio, the operator is frequently in a position to suggest changes in procedure and to make intelligent recommendations along many lines.

It would be well for a shift of operators to take place when radio frequencies or call signs are shifted. An experienced interceptor becomes familiar with the idiosyncrasies of an operator's technique and has little difficulty in recognizing his transmissions. The purpose of changing either frequencies or call signs, therefore, is defeated unless the radio operator is changed also.

Radio silence.—Most effective counteragent for radio intelligence is absolute radio silence. If the radio is never used, the enemy can gain no intelligence. Unfortunately, however, naval communications cannot revert to the methods of Trafalgar. Since radio performs a vital service and is essential for modern fleet operations, the only sound solution of the problem is to minimize its use. Radio silence, therefore, becomes the rule at sea.

Although general rules are dangerous, this formula is usually applicable: When it is reasonable to assume that the enemy is unaware of the presence of a unit of the fleet or does not anticipate a specific, planned operation, radio silence must not be broken; when it appears that the enemy does anticipate the ship movements or when contact has already been made, radio silence may be broken, provided the need is imperative and no other means of communication will suffice.

Through extensive employment of the broadcast and intercept methods of transmitting traffic to the fleet, ship transmissions are reduced to a minimum. As a result, shore stations transmit over 90 percent of naval radio traffic and fleet units at sea seldom have to break silence.

In order to compensate for the lack of radio during operations, detailed orders must be obtained and thoroughly understood prior to leaving port. At sea, communication between units is carried out by

visual signals. Receivers should be kept open to intercept broadcast schedules; needless to say, such messages must not be acknowledged. When battle is imminent or in progress, the picture changes entirely, and security gives way to speed.

Radio deception.—Just as the Germans prior to the Battle of Coronel used their radio to deceive the British and draw them into a trap, radio may frequently be used as a strategic weapon designed to misinform the enemy, to encourage him to draw the wrong conclusions, to force him into difficult situations, and generally to throw him off balance, thwarting his offensive and undermining his defense. Such use is for experts only, because of the danger that deception may backfire disastrously.

A most practical use of radio deception is in connection with a justified breaking of radio silence. For example, a task force well off the coast of northwest Africa receives a dispatch from a merchant vessel reporting the presence of enemy fleet units to the westward. Since pursuit of the enemy necessitates a change of original plans, two destroyers are detached from the task force with orders to return in the direction of Gibraltar and, after sailing 150 miles, to transmit a radio message advising of the alteration in the course.

If bearings should be taken by the enemy on this transmission, the position and course of the main force would not be betrayed, and the speed of the destroyers would enable them to evade attack directed on the basis of the direction-finder bearings.

Radio deception may also take the form of bogus messages purporting to be genuine orders but transmitted to confuse the enemy and disrupt his plans. British expeditionary force units in France received a message, transmitted under an official call and using a general headquarters frequency, ordering that radio silence be observed by all units in a particular sector; the message had been originated by the Nazis at a time when radio silence would have frustrated British operations.

In 1915 two German ships were stationed at Constantinople but were rendered useless by the presence of the Russian Black Sea Fleet. When the Russians put to sea, a German cruiser, interposing herself between the fleet and the Russian base, transmitted a message in Russian code to the admiral, ordering him to transfer his fleet immediately

to the far eastern portion of the sea. While the Russians sailed eastward, the German ships played havoc with coastal shipping and shore establishments.

Traffic peaks may be hidden from the enemy or false peaks may be created through careful rearrangement of radio traffic from shore activities. Routine administrative traffic, which has a tendency to form highs and lows on certain days of the week, may be artificially spread out over the entire week. Other, evenly scattered administrative traffic may be delayed for one or two days and then suddenly released, creating a traffic peak likely to confuse the enemy. Dummy messages may be transmitted at intervals, either to fill traffic depressions or to create artificial peaks.

Dummy messages must have all the earmarks of legitimate traffic. Failing to realize this, the Russians, in order to cover up the withdrawal of two corps from the Eastern Front in 1916, simulated false radio activity but introduced each message with some such wording as "Do not be alarmed; this is a deception." The Austrians, who had broken the Russian system, read the messages and were not deceived.

The practices of radio deception are almost limitless. Transmissions from a few naval or merchant ships can simulate the activity of a busy fleet in a remote sphere of operation; naval units may lure enemy warships into ambush with the use of compromised merchant codes; and enemy radio dispatches, not heard by the addressees, may be answered. It is because transmissions could be canceled by deceptive messages that the word "cancel" is not permitted as a plain language reply to an encrypted dispatch.

Since radio deception is such a valuable weapon, its principles are often woven into the patterns for fleet movements and missions. Stratagems carefully planned in advance and developed at crucial moments can contribute substantially to the success of naval operations. Ingenuity and meticulous attention to detail are necessary attributes of the radio deception expert, but he performs only on approval or instigation of high authority. Every precaution is taken to prevent misunderstanding by other units of the fleet.

Authentication is a defense against deception. While the British reserve authenticators for use with plain language messages chiefly,

they are used more extensively in this country. Authenticators are used when a station begins to transmit or when there is suspicion of enemy deception.

In radio telephone conversation, the authenticator consists of a password. This may be obtained from a registered publication or it may be an informal challenge, such as a request that the person calling "talk Brooklyn." Frequently, however, a voice may be recognized without authentication, and voice deception is difficult for the enemy to attempt successfully.

Radio interference.—Radio interference, or jamming of the enemy's frequencies, may be a useful weapon, provided it is practiced by experts. If the enemy is allowed to communicate without interference during the early stages of a combat operation and then at a critical point his frequencies are jammed, the resultant confusion and lost orders may spell the difference between victory and defeat.

Interference has been utilized in the present war in jamming airplane and tank radio frequencies and in some cases in naval engagements. In each instance, jamming was withheld until a decisive phase of battle had been reached.

For effective interference, maximum power and an interrupted signal are used. The possibility of jamming by the enemy necessitates readiness at all times on the part of the operator to shift to the standby frequency when interference disrupts his use of the working frequency.

☆ ☆ ☆

SUMMARY

The field of radio intelligence and radio security is one of enormous potentialities. As yet it is relatively undeveloped. Its possible contributions to naval strategy and operations are almost unlimited, offering a continuous challenge to those who deal with naval communications to devise new methods and stratagems. The techniques of radio deception and interference, however, must be prescribed only by those of highest authority and must not be attempted by inexperienced personnel.

CHAPTER VI. COMMUNICATION SECURITY CHECK LIST

For reference purposes, the following summary of the principles of communication security should be useful

I. Safeguarding of classified matter

- A. Physical safeguarding
  1. Prevent any unauthorized person from sighting or using classified matter.
  2. Minimize the number of authorized individuals.
  3. Don't remove classified matter from designated working space.
  4. Don't leave classified matter unguarded.
  5. Keep classified matter in its assigned stowage when not in use.
  6. Don't put plain and encrypted versions of a dispatch on same sheet or even in same file.
  7. Destroy or sink all classified matter when capture is imminent.
  8. Afford rough drafts, notes, stencils, cushion sheets, typewriter ribbons, carbon paper, and blotters the same care and stowage as classified matter.
  9. Write classified data only on hard surfaces; don't use a pad.
  10. Store discarded classified matter and work materials in a "burn bag" or safe until burning is possible; don't throw into wastebaskets.
  11. Report evidence of possible compromise immediately.
- B. Personal censorship
  1. Don't discuss classified information with anyone who not need to know.

2. In social conversation, either refuse to talk shop or plead ignorance.
3. Don't discuss classified information over the telephone.
4. Never link the reference number and content of a dispatch over the telephone.
5. Beware of incoming telephone calls; never discuss any official matters over telephone unless identity of caller is established.
6. Never mention classified information in personal correspondence.
7. Don't acknowledge personal letters or gifts from unknown individuals or business firms.
8. Don't mention classified information in personal notebooks.

C. Press and radio censorship
1. In issuing statements for the press, distinguish clearly between classified and public information.
2. Scrutinize even the most innocuous-appearing photographs and releases to the press for information of possible value to the enemy.

II. Dispatch preparation

A. Unnecessary messages
1. Never send any message unless it is absolutely necessary.
2. Don't report trivia to higher authorities.

B. Selection of means of communication
1. Use radio only when speed and urgency demand it and circumstances permit. Use mail whenever possible in preference to telegraph or radio.
2. Mailgrams are often equally rapid and sometimes faster.
3. Don't send administrative dispatches by radio or telegraph, unless no other means will serve.
4. Send dispatches to information addressees by mail, unless immediate delivery is essential.

C. Precedence
1. Don't designate high precedence unless seconds count.

2. Use lowest precedence for bulk of administrative matters.
3. Designate lowest precedence for information addressees whenever priority of delivery is not essential.

D. Classification
1. Classify a dispatch according to content and in light of requirements; avoid overclassification.
2. Don't classify information to be released to public within near future, if this can be avoided.
3. When feasible, rewrite proposed dispatches to eliminate classified information or references to classified dispatches.

E. Drafting
1. Strive for clarity and conciseness.
2. Avoid the habit of having habits in drafting.
3. Apply good drafting principles to plain language messages as well as to encryptions.
4. Avoid stereotyped beginnings, endings, and phraseology.
5. Use language the enemy does not expect you to use, but never sacrifice clearness.
6. Vary length, phraseology and sequence of parts in a series of stereotyped messages.
7. Eliminate unnecessary words and strive for brevity; use official abbreviations if meaning will be unmistakable even though a slight error in transmission occurs.
8. Send unusually long dispatches as two or more separate, seemingly unconnected messages.
9. Five groups is the minimum length of a dispatch.
10. Avoid repetition of words and phrases where possible, particularly unnecessary words like "dash" and "paren."
11. Never repeat for emphasis.
12. Avoid references if possible.
13. Bury necessary references in text; don't consistently place at beginning.

14. Vary means of expressing reference numbers.
15. Minimize punctuation used.
16. Seldom spell out punctuation marks; use X for every value.
17. Never use "stop" or "end" or X at end of dispatch.
18. Avoid mention of dates if possible; substitute other equivalent expressions.
19. Never mention current date in text.

F. Information addressees
1. Minimize information addressees.
2. When addressees *must* be numerous, conceal routing instructions in text.
3. Never mention in dispatch hearings addressees receiving dispatch by mail.

G. Acknowledgments
1. Don't request acknowledgment unless vital.
2. Never request acknowledgment from ships at sea.
3. Reply promptly if possible, eliminating the need for separate acknowledgment.
4. Use mail for acknowledgment as a general rule.
5. Never encrypt acknowledgments, except as part of an encrypted reply.

III. Processing of dispatches

A. Communication personnel
1. Master the principles of encryption and decryption.
2. Participate in frequent coding drills.
3. Review and obey the specific rules for each system.
4. Report possible compromises promptly.
5. Suggest improvements in systems and security factors.
6. Make suggestions to originator regarding phraseology, precedence and classification when this seems advisable.

B. Plain language dispatches
1. Send in plain language only those dispatches of no possible value to the enemy.

2. If dispatch contains some classified matter but is primarily unclassified, either encrypt all or divide into two messages, one to be encrypted and the other sent in clear.
3. Never send in plain a message once encrypted.
4. Transmit in clear when security *must* be sacrificed for speed in combat or other emergency.

C. Choice of system
1. Normally use system of narrowest distribution including all addressees.
2. Select area system in preference to world-wide.
3. Use special-purpose system for special-purpose dispatches.
4. Sending identical messages in two systems should be avoided as far as possible.

D. Encryption
1. Encrypt classified messages whenever there is fair possibility of interception—even in case of mailgrams, letters, and visual signals.
2. Master the rules before attempting to use any system.
3. Follow the rules with common sense.
4. Don't blindly apply the rules of an old system to a new one with which you are not familiar.
5. Never mix cipher and plain language in the same dispatch.
6. Always check the entire encryption by decrypting before transmission.
7. Divide unusually long dispatches into unequal parts and transmit as separate messages.
8. In encrypting two or more parts of same message, use different date-time groups and different internal indicators; bury linkage in text.

E. Padding
1. Use dummy words to protect stereotyped terminals.
2. Use dummy words to increase length of short dispatches.
3. Avoid relation between padding and text.

4. Select unconnected words as padding.
5. In separating padding from text, use consonants, preferably of low frequency, but avoid habitual use of any.
6. Avoid X's or XYZ as nulls; select from other seldom-used consonants.
7. Avoid use of vowels, and of consonants open to linkage with adjacent words.

F. Retransmission
1. Attempt to clear garbles prior to requesting retransmission.
2. Continue attempts to clear after retransmission has been requested.
3. Don't attempt to transmit correction if different cipher values would so be assigned to more than one group of text. Reencrypt the message.
4. Before reencrypting, either because a correction is necessary or the dispatch was originally sent in the wrong system, alter padding and insert cancellation of the original message. The length, internal indicators, and date-time group of the new message should be different.
5. In passing a dispatch to other units, either transmit exactly as received or lengthen, eliminate linkage as explained above, and send in appropriate system.

G. Paraphasing
1. Paraphrase quotations prior to encryption.
2. Paraphrase thoroughly any information from encrypted dispatches which is to be made public.
3. In paraphrasing, retain the original meaning *without change*.
4. In paraphrasing, alter entire make-up of dispatch as much as may be necessary: Vary the order of paragraphs, sentences, clauses, words in series; substitute synonyms; eliminate unnecessary words; vary over-all length; and eliminate all other evidence of linkage.

IV. Radio security

A. Radio discipline
1. Master and intelligently observe existing radio instructions.
2. Shift operators when frequencies or call signs are changed.
3. Intercept and record all transmissions feasible.
4. Be alert to make logical deductions from interceptions.

B. Radio silence
1. Use radio as seldom as possible.
2. Never use radio at sea if it can be avoided.
3. Obtain and thoroughly understand operation orders prior to leaving port.
4. Use visual signals in preference to radio for communication between units at sea, except at night in enemy waters.
5. Be alert to intercept messages transmitted from shore by broadcast and intercept methods.

C. Radio deception
1. Scientifically rearrange traffic to disguise lows and highs of volume.
2. Give dummy messages all earmarks of genuine messages.
3. Be alert for dummy messages originated by enemy.
4. Be alert to devise and suggest methods of deception.
5. Never employ radio deception unless ordered by high authority.
6. Use authenticators when suspicion of deception exists.

D. Radio interference
1. Never practice jamming except by specific order of commanding officer.
2. Be prepared to shift to standby frequency when enemy utilizes jamming.

○