Physical, Transmission, & Cryptographic Security

Major W. N. Hamilton

~~(Confidential)~~

We recently wrote in the Review regarding the information to be gained from security lapses in the enemy's communications nets. While our intention was to drive home the importance to our nets of communication security, the article itself was written from the Japanese point of view, to show how the failure to maintain security in our nets aided the Japanese in anticipating our actions in the South Pacific area.

No doubt the Japanese radio intelligence service was very clever and added a few new wrinkles to the game of interception and traffic analysis. But they were beginners compared with the larger, more prosperous Western nations who had developed the radio from the beginning.

This time, let us look at the question of communication security from the point of view of the German radio intelligence service. As has been told elsewhere in the Review the Germans had an extensive service of this sort. But while much has been said about their activities directed against foreign agents and partisan radio stations, not much has been told concerning their work against our military forces.

Insecure Message Handling

At times, cryptographic compromises have resulted from insecure message-handling practices employed in some of our message centers. In one office, for example, it was an established custom for the plaintext of a message to accompany the cryptotext all the way to the teletypewriter operator, who transmitted the cryptotext and later filed both versions separately. One day early in World War II, an inexperienced teletypewriter operator, who was doing his best to keep up with heavy traffic, transmitted both the encrypted and the plaintext versions of a message, and it was subsequently relayed by radio. The method of processing was abruptly changed. The communications officer, however, who was experienced, but had been stationed at that headquarters only 3 days, received an official reprimand because he had not acted before a compromise could occur.

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

The two cases cited above are outstanding examples of why operating procedures must be good, without weaknesses, and must be followed explicitly. The failure of the Control Officers to follow operating procedures or to prescribe secure operating procedures brought about these compromises of cryptographic security.

Incident at Ordnance Plant

A prime example of a breach of physical security concerns a Major at an ordnance plant. As a result of two bitter experiences, he is now fully conscious of security regulations. After being charged with losing a cryptographic document for which he could not account, the Major requested that his account be inactivated. He was "through" with cryptography. The authorities obliged, requesting the return of certain materials and a report of the destruction of the rest. The Major, who has been severely reprimanded for his first violation, replied at some length on

ASA REVIEW - March-April 1951, pp. 2-4

Physical, Transmission, & Cryptographic Security

Major W. N. Hamilton

~~(Confidential)~~

We recently wrote in the Review regarding the information to be gained from security lapses in the enemy's communications nets. While our intention was to drive home the importance to our nets of communication security, the article itself was written from the Japanese point of view, to show how the failure to maintain security in our nets aided the Japanese in anticipating our actions in the South Pacific area.

No doubt the Japanese radio intelligence service was very clever and added a few new wrinkles to the game of interception and traffic analysis. But they were beginners compared with the larger, more prosperous Western nations who had developed the radio from the beginning.

This time, let us look at the question of communication security from the point of view of the German radio intelligence service. As has been told elsewhere in the Review the Germans had an extensive service of this sort. But while much has been said about their activities directed against foreign agents and partisan radio stations, not much has been told concerning their work against our military forces.

Insecure Message Handling

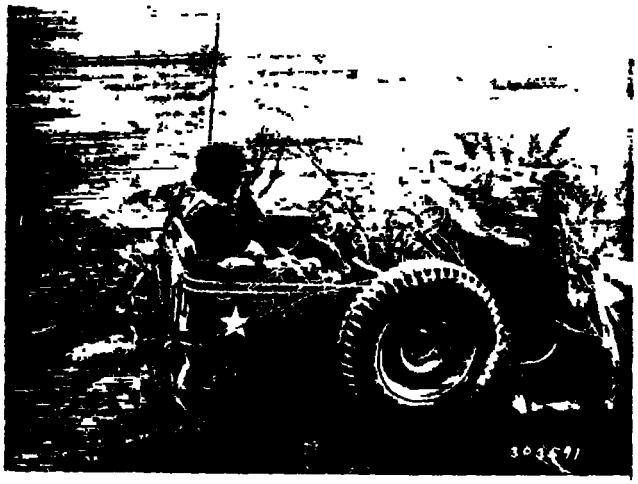
At times, cryptographic compromises have resulted from insecure message-handling practices employed in some of our message centers. In one office, for example, it was an established custom for the plaintext of a message to accompany the cryptotext all the way to the teletypewriter operator, who transmitted the cryptotext and later filed both versions separately. One day early in World War II, an inexperienced teletypewriter operator, who was doing his best to keep up with heavy traffic, transmitted both the encrypted and the plaintext versions of a message, and it was subsequently relayed by radio. The method of processing was abruptly changed. The communications officer, however, who was experienced, but had been stationed at that headquarters only 3 days, received an official reprimand because he had not acted before a compromise could occur.

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

The two cases cited above are outstanding examples of why operating procedures must be good, without weaknesses, and must be followed explicitly. The failure of the Control Officers to follow operating procedures or to prescribe secure operating procedures brought about these compromises of cryptographic security.

Incident at Ordnance Plant

A prime example of a breach of physical security concerns a Major at an ordnance plant. As a result of two bitter experiences, he is now fully conscious of security regulations. After being charged with losing a cryptographic document for which he could not account, the Major requested that his account be inactivated. He was "through" with cryptography. The authorities obliged, requesting the return of certain materials and a report of the destruction of the rest. The Major, who has been severely reprimanded for his first violation, replied at some length on



Radio-Equipped Jeep

Soldier at Junction Box

the destruction of some forty or fifty documents. The case was forgotten.

Later, a routine investigation of the Major's files, conducted by a carefully trained security officer, revealed that some 25 of the documents reported burned were still on file. The Major, and a Captain who had "witnessed" the burning of the documents, were charged with false swearing, and were heavily fined under the 104th Article of War.

In the above cases no one but the enemy knows if use was made of these compromises. Interception of just the right message-the clear text of a coded message-or the chance look at some classified material-the "destroyed" crypto material-is enough to start a chain reaction of events. The thwarting of laboriously conceived plans, the counter attack at a weak sector, the destruction of vital supplies, and, coincident with all of these, the death of many good men and women.

In the following cases we do know what action the enemy took and how thankful the German signal intelligence service was for our lack of communication security.

Regain Our Message

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

We must assume that clear-text transmissions of important classified messages are intercepted by the enemy. If this information is in any way useful to him, you may be sure that he will make use of it. The intercept effort of the enemy provides one of his most prolific sources of information about us and our Forces and our actions.

The following clear-text message, logged by a radio security officer in Italy, is a shining example of how plans may be revealed to the enemy: KHA V XIM...MESSAGE FOR YOU...BRITISH WILL BE FIRING FROM 12 TO 12:45 TODAY AT FOLLOWING POINTS 908-143, 893-141, 894-150...REQUEST YOU DO NOT FIRE THESE POINTS AT THIS TIME...DID YOU GET THAT...OVER. Another incident early in the Anzio campaign illustrates the waste of supplies through the compromise of locations by misuse of communications. An advancing tank battalion radioed back in the clear that an enemy counterattack was under way and asked that all traffic be stopped at a specified town behind the lines. German intercept notified its air force and within an hour a squadron of

planes was strafing a long column of traffic halted on the road. Many trucks, jeeps, and cars were wrecked beyond repair, but more lamentable was the number of men killed.

And how they must have licked their chops over something like the following. During the early part of the breakthrough in France a staff officer heard a familiar warbling tone on his tactical radio set. It was irritating but not enough to hinder seriously his contact with the battalions in his unit. But in one of his transmissions to a battalion he said, "Looks like the Krauts are trying to jam us." Within minutes the warbling shifted frequency to cover completely that net frequency and the bag pipes stopped all transmissions until a shift could be made to a new frequency.

Land Mines Result from Intercept

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

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

Information which, although classified, cannot be acted upon by the enemy within the time the action is to take place can usually be transmitted in the clear. In some situations, speed is more vital than the security of the information to be transmitted. By the time the enemy has intercepted these clear-text messages, and has passed the information to where it can be acted upon, the action has taken place and the information is no longer valuable to him.

Denying the Enemy Information

The efforts to develop secure cryptosystems, the adopting of procedures which lend themselves to speed of message-handling and the following of procedures for safeguarding and using cryptographic material are all done with a view toward denying the enemy information.

Continued efforts to develop more secure cryptosystems, the adopting of operating procedures which lend themselves to speed of message-handling and the strict adherence to authorized procedures for the safeguarding and use of crypto-material are all for the purpose of denying the enemy classified information. Failure to adhere strictly to authorized procedures for the safeguarding and use of crypto-material will assist the enemy a great deal in his efforts to compromise our crypto-systems and gain access to vital military information of a classified nature. Or as the Germans said "FIEND HORT MIT."

View of buildings in area assigned to ASA School at Fort Devens

ers. Guest houses on the Post are available for visitors.

Adequate Facilities Provided

The post has adequate facilities which include clubs for officers and noncommissioned officers, a service club, a post exchange, and, in addition to the golf course mentioned above, tennis courts, and two small lakes with excellent swimming and fishing. The vicinity of the post includes a number of these small lakes, or "ponds" as they are called in New England. The communities of Fitchburg (12 mi. from the post) and Leominster (9 mi. from the post) and the big manufacturing town, Lowell, population 195,000, are fine shopping centers. It is not far across the New Hampshire border to Nashua. Winters are cold and snowy, Springs damp,but pleasant, and Summers moderate to hot. Autumn is the best part of the year. It is the countryside made familiar by the poet Whittier; south Europeans have taken over many of the farms.

Fort Devens, built at a cost of $44,000 000, total in World War I and II, occupies 10,000 acres. During King Philip's War in 1671 the house of Major Simon Willard,situated where the main gate of the Fort now stands, was burned to the ground by Indians, and the settlers of the area were forced to flee. The camp was named after Major General Charles Devens who served in the War between the States and later became Attorney General of the United States. When it was constructed early in 1917 a total of 9,000 civilians in nine weeks erected more than 600 buildings, built 200 miles of roads, laid 25 miles of sewer and water pipes, strung 400 miles of telephone and electric wires, and dug a 3,000,000 gallon well - all for $6,000,000. In the autumn of that year an additional $13,000, 000 was spent for 800 additional buildings. Expansion during World War II, totaling $25,000,000, included a nine-fold increase in area, the leasing of 325,000 acres for training purposes, and the erection of 1,200 buildings.

In World War I when it was occupied by the 76th Division, the Commanding Officer was Major General Harry F. Hodges. Also the Camp housed the 12th (Plymouth) Division under Major General Harry P. McCain; during World War I, 800 persons died there of Spanish Influenza. The 26th Division, which fought at St. Mihiel, was demobilized there.

Became A Fort In 1931

The status of Devens was changed from that of Camp to Fort in November 1931. Dur-

(Continued on page 19)

A 8-6 (1)

Importance Of Transmission Security

~~(Confidential)~~

by Major William M. Hamilton

Transmission security plays an important role in military communications. In peacetime as well as in war, communicators must guard constantly against disclosing information which would be beneficial to the enemy.

A survey made by the Japanese during the period 8 December 1941 to 31 October 1943 indicates that they were able to obtain vital information through the nonobservance of communication security precautions on the part of United States personnel. The survey states in part:

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

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

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

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

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

The interrogation of two Japanese intelligence officers, Commander Hideo Ozawa and Lt. Commander T. Satake, brought to light a number of useful facts about the nature, extent, and success of enemy efforts in the field of communication intelligence, especially traffic analysis. Both officers held key posts in the radio intelligence section of the Japanese Naval General Staff during most of the war.

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

Taking Okinawa as an example, Satake made a statement as follows:

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

Ozawa stated that the Marshalls operation supplied the greatest amount of radio intelligence and allowed the Japanese sufficient time to notify the garrison of the impending attack. Regarding the basis of the prediction, he explained as follows: