STANDARD FORM NO 64 ~~SECRET~~ MATERIAL ATTACHED

Office Memorandum • UNITED STATES GOVERNMENT

TO Chief, TNG Division DATE 5 May 1954

FROM DD/COMSEC

SUBJECT Lecture to be Given at Armed Forces Staff College

Attached for your information and file is a copy of the presentation I will give at AFSC on 6 May 1954. This is in accordance with our recent conversation concerning TNG as a central file and reference point for such material.

Declassified and Approved for Release by NSA on 05-08-2018 pursuant to E.O. 13526

F. E. HERRELKO
Colonel, USAF
Deputy Director,
Communications Security

Incl:
a/s
Copy furnished: cc: Daily File
A1

LECTURE ON COMMUNICATIONS SECURITY
GIVEN AT THE ARMED FORCES STAFF COLLEGE ON 6 MAY, 1954

BY

Colonel Frank E. Herrelko, USAF
Deputy Director, Communications Security
National Security Agency

1. The easiest way for me to define Communications Security, or it's short title COMSEC, is in terms referring to the lecture you have just heard on Communications Intelligence. Communications Security is the defense against Communications Intelligence. Thus, it involves the protection given to communications to prevent the derivation of intelligence by unauthorized persons, either through cryptanalysis, physical recovery, or traffic analysis. Therefore, Communications Security resolves itself into three basic components--cryptographic security, physical security, and transmission security.

2. ~~Let us talk first of cryptographic security.~~ Cryptographic security is maintained by the provision of sound cryptosystems together with appropriate instructions for their use. Cryptosystems are developed primarily as the result of Service or Joint Service requirements for equipments or material, with specified characteristics of speed, reliability, security, and perhaps others such as weight, size, and power requirements to meet a particular communications problem. These requirements are submitted to the National

Security Agency which then determines whether existing materials will fill the requirement, or whether new equipment must be developed.

3. If a new equipment is developed, it is turned over to the Services for testing. Results of Service tests are used to modify the equipment as necessary; then full-scale production is begun.

4. As most of you know, most cryptosystems consist of a single basic operating method made secure through the introduction of variable elements. These variable elements, usually rotors, are produced at or provided by NSA. Rotors consist of wheels containing random electrical circuits which can be arranged in a great number of ways to perform the actual process of encipherment. With these variables go key lists which tell the operator how the rotors are to be set up for the particular messages he is to encipher.

5. Once a new equipment and its associated materials are placed in use, the Services are responsible for insuring that established rules are properly followed. To insure that proper action is taken when serious mistakes occur, a reporting procedure has been established which requires that all mistakes which might affect cryptosecurity be reported to NSA. There, cryptanalysts evaluate each case and inform holders of the system what action must be taken. NSA is responsible for determining the effect of a violation, for determining whether a cryptosystem need be superseded because of

mis-use, and for correcting procedural deficiencies and clarifying existing instructions. Action to prevent recurrence of error, improve training and ~~improved~~ supervision, take disciplinary action, and the like are purely Service responsibilities. As an example of the cryptoviolation reporting procedure, I will tell you of an interesting incident which occurred a few years ago.

6. An operator inadvertently included a few groups of plain text in the middle of a cipher message. This was reported by the recipient and a copy of the text involved was forwarded to the National Security Agency. The fragment of plain text was recognized as a direct quote from the The Light List, a standard navigational guide. The remaining text was therefore recovered, the basic key reconstructed using matched plain and cipher text, and the entire cryptosystem required supersession.

7. Before I leave the general picture of cryptosecurity, I should say a little [redacted] about its adjunct, physical security. The National Security Agency establishes the minimum standards considered necessary for the protection of various types of cryptomaterial while in storage, transit, or use. This includes determination of the types of guards, facilities, accounting, and clearances necessary. In most cases, the Services may institute more restrictive physical security safeguards if they so desire. Physical loss of material is not particularly rare, especially if it is of the type used in aircraft or at forward echelons. However, I'd like

to tell you of one or two of the more unusual cases to give you an idea of the variety of problems which may some day confront you in the ComSec business.

8. One day, a few years ago, a warrant officer assigned to the Military Attache's office in Kabul, Afghanistan, was walking to his office after a leisurely lunch and stopped in a fruit store to buy some grapes. Paper was an acute shortage there and he was idly amused as he watched the vendor make a sort of paper bag out of a sheet of paper which looked like scratch paper. When he got outside in the light he looked closer, and almost dropped dead when he saw that the scratch paper was an official classified message addressed to the Military Attache. He ran back to the office, told the Attache. This officer grabbed up all the blank paper he could find, reams of it, and ran back to the fruit shop. Here he made a trade with the astonished storekeeper--piles of nice clean paper for all the "dirty old stuff" he had. In the "dirty old stuff" the Attache found all but three items that, the last he knew, had been in his classified message file. What happened? Presumably, the message file had been dropped accidentally into a waste basket and was a bonanza for a janitor there, who was adding to his wages by peddling scrap paper to merchants around town.

9. That was an accidental thing, but there have been many cases somewhat similar. Worse of course are the intentional cases,

and the worst of these are those which involve personnel defections. We do have them. You may recall the case of the American enlisted man who had worked in the Attache cryptocenter in the Embassy in Moscow, was fully exposed to all U.S. cryptographic information, was often alone there at night, unsupervised, and who suddenly disappeared, leaving a letter to the effect that he'd become a Communist and was going to stay in Russia.

10. There was another case of a disgruntled crypto-repairman, caught in the act of selling diagrams of one of our top cipher machines to a Russian agent. Fortunately for us, and thanks to the alertness of some other enlisted men, the Russian agent turned out to be an agent of the ONI.

11. Personnel security has been one of our biggest headaches and probably will continue. It thus becomes one of the commander's chief tasks to insure the unquestioned continued loyalty of men assigned to cryptographic duties.

12. The administration of techniques to insure cryptosecurity and physical security is truly a Joint enterprise. General procedures and specific systems are jointly used. All interested Services join in the expression of requirements and test equipments to determine their applicability in aircraft, on shipboard, or on the ground.

13. This is as true in the transmission security phase of COMSEC as it is in the cryptographic and physical phases. To more closely define "transmission security," let's say that it is the taking of all me

measures necessary to protect our communications from unauthorized interception, traffic analysis, and imitative deception. Since prevention of unauthorized interception is often impossible to insure, what we really mean in our definition when we use the phrase ~~in our definition~~ "measures necessary to protect our communications from unauthorized interception" is the taking of steps to make that interception as difficult as possible. "Imitative deception" may be a new term to some of you. It consists of the introduction of fraudulent transmissions into our communications. The purpose of this deception may be nothing more than to create a nuisance by causing confusion, but on the other hand, it may be carefully planned, have all the appearance of authenticity, and have the purpose of forcing action on the part of our tactical organizations, causing them to carry out faked orders and fall in line with the originator's idea of a helpful tactical situation.

14. Transmission security techniques differ from those used to maintain physical and cryptographic security in several important respects. Remember that cryptographic security is a sort of business in itself and uses special facilities and specialists to do the work. Encryption is often quite distinct from transmission. But transmission security deals with protective measures during the act of communicating. Therefore, there cannot be a distinct body of regulations and procedures; rather, communications operating instructions must themselves incorporate the necessary transmission security procedures. This how it works:

15. The National Security Agency publishes a book titled "Fundamentals of Transmission Security" which establishes basic policy and doctrine. Using this as a guide, the communications procedure people develop communications instructions which incorporate means of complying with the established doctrine. For example, NSA doctrine might state that "Rotation of frequencies is the most effective means of preventing station identification through frequency." Appropriate panels of the JCEC then translate the doctrine into effective instructions in ACP's and JANAP's by giving detailed procedures as to how frequencies should be rotated.

16. Since virtually all communications procedures are now considered to have Joint applicability, the JCEC is the body which prepares and publishes them. Panels of the JCEC are staffed by communications personnel of the three Services. The Methods and Procedures Panel and the Call Sign Panel are the two which have most to do with the translation of transmission security policy into operating methods.

Thus you can see that although cryptographic security and transmission security are closely related, they receive quite different treatment.

17. To continue the story of the conduct of the transmission security phase of COMSEC, let us talk for a moment of monitoring, which is merely the act of intercepting one's own communications.

The Services monitor their circuits for policing and counter intelligence purposes. For purposes of economy and greater efficiency, the monitoring is usually done by the simple method of obtaining copies of messages as received at communications centers. There is also some, but a small amount, of actual interception performed.

18. NSA monitors communications from the standpoint of developing improved security practices through study of current procedures, thereby locating faults and omissions in the rules established. In this way we determine what traffic analysis of our circuits is possible, in spite of the rules and procedures in force, and thereby determine what additional security practices are necessary. In this way we also build up a large amount of data for use in future communications cover and deception planning.

19. On the other hand, the Services conduct their own monitoring programs for the purpose of determining violations of or deviations from prescribed communications procedures.

2Ø. That covers the conduct of COMSEC from the standpoint of what is done. Now a little bit about the overall organization to perform the job.

21. At the top of the pyramid sits NSA. As I have said, NSA provides the basic doctrine, policy, and instructions for COMSEC, manufactures or procures all the material necessary, and distributes it to the parent users. Then it acts as a judge and jury concerning the use that the material gets. However, it is by and large a wholesaler, and even its policing function stops far short of punitive action.

22. The Services are the retailers and the real police force. All the material is turned over to the Service Cryptologic Agencies in bulk. These are the Naval Security Group in Washington, the Army Security Agency in Arlington, Virginia, and the Air Force Security Service in San Antonio, Texas. Here the material is packaged and distributed to the Services' main issuing offices around the world. The Navy issuing agencies are called Registered Publication Issuing Offices (RPIO's), and are located in each Naval district and at major overseas commands. Some of the larger ones are in Pearl Harbor, London, Yokosuka and Guam. The Army and Air Force use what they call "Command Issuing Offices" (CIO's) in overseas commands, but distribute directly from Arlington and San Antonio to users in the United States. Air Force CIO's are at locations such as Elmendorf Air Force Base, Alaska, Hickam Air Force Base, Hawaii, and in Tokyo, Japan, and Burtonwood, England. The Army's are at such places as Fort Shafter, Hawaii, London, Tokyo, Fort Richardson, Alaska, and Quarry Heights, Canal Zone.

23. On the policing side there are COMSEC detachments assigned to most of the major commands. The Navy assigns them to commands ashore and afloat. For example, one COMSEC activity is on the staff of ComSixthFlt. Others are located at major shore stations around the world, there being approximately 13 such at the present time. The Army and Air Force follow the same practice, assigning COMSEC detachments to major Army and Air Force commands.

24. The function of these organizations is to maintain communications security in the commands to which they are assigned. This they do through monitoring and policing, and reporting to the command all violations or bad practices, so that prompt and effective corrective action can be taken.

25. Within each command, no matter what its size, there is at least one officer who has been assigned, by his commander, the responsibility for cryptosecurity. He is the cryptosecurity officer, assigned in accordance with established joint directives. In addition, there must be an officer assigned the duty of cryptocustodian, with responsibility for the receipt, proper accounting for, and safeguarding the command's cryptomaterial. In the smaller commands, these two functions are sometimes assumed by one man.

26. There we have a statement of the conduct of COMSEC and a brief outline of the manner in which the business functions. What is the effect of all this, especially the effect on staff and command?

27. If there is one disheartening word in our language, that word is compromise. A compromise is defined as occurring when facts make it necessary to assume that thru physical loss of a piece of cryptomaterial, or thru operational errors which permit successful cryptanalysis of message or messages, intelligence is revealed. We think we know the type of error which could conceivably lead to compromise. Further, we have a very elaborate system devised whereby we can get information concerning loss or cryptographic errors quickly, evaluate that information, and take necessary corrective action. In other words, we think we know how to take care of cases that we know about. What causes us to lose sleep is the case we do not know about. Of necessity then, we put great faith in all communications security officers everywhere, relying on them to get fast and accurate information for us. That is the essence of the compromise reporting system.

28. It is an indication of a well operated and supervised communications security organizations when a command timely reports itself guilty of an infraction. If someone else must detect and report the infraction, the commander is then in the position of wondering just how secure his communications are. That is the point at which that COMMANDER may begin to lose sleep.

29. When the report is received at NSA it is evaluated immediately and the answer is either that no compromise has in fact occurred, or that it is necessary to assume that one has. In the latter case, if the event is such as to require that current cryptomaterial be considered compromised, action to replace it is started at once. This will prevent any more damage from being done; however, all messages already sent are suspected of being compromised. In other cases there may not be any need to supersede a system, but messages sent during a given period must be considered compromised. These two types are the ones which cause the real headaches. Cryptosecurity officers are required to gather together all messages involved and show them to the commander or proper staff officer saying that the messages are considered compromised. The commander must then decide what to do about it. If the messages contain plans originated by him which can be changed, he should change them. If they contain plans received from higher authority, he must inform higher authority of the compromise and they must decide what to do. In either case it's a mess, but fortunately, it doesn't happen very often.

30. Compromises are usually the commander's or staff officer's first intimate brush with communications security and it's a hard way to learn, especially if the compromise was caused within his command. So, without waiting for that kind of a lesson, the

commander or staff officer should know what he can do to prevent compromises and bad security practices.

31. The first step is the old standby, good training. You will get, if you're lucky, trained cryptographic and communications personnel. But you can't always rely on it. Rules and procedures change, new systems are placed in effect, and the training a man received in a school somewhere may become obsolete. On-the-job training is a must, and it's particularly important in small commands where traffic is light.

32. Another very valuable security tool is the monitoring service I've referred to earlier. Commanders should avail themselves of this service and take prompt and effective corrective action when required. A good many of the procedural discrepancies which a monitoring service may turn up will appear trivial and minor. Nevertheless, they will be indicative of misunderstanding of the rules, or of a slackening in security discipline, which could easily and quickly lead to much worse things. Other yields from monitoring may be far from small. A case in point occurred last summer in Korea when a monitoring unit plugged into a Division switchboard heard an officer on a phone circuit tell another officer the coordinates of his headquarters. This information was relayed to the Commands concerned, and unfortunately, the risk was considered too small to warrant movement of the headquarters.

Within a short while, artillery zeroed in on the headquarters and inflicted [redacted] casualties.

33. A third key to good security, and probably the most important, is the selection of good, competent officers for assignment as custodians and communications security officers. There is no better way to maintain security than to have good men running it for you, and as far as possible, such duty should be primary duty. Too often it happens that some junior officer is assigned the function together with a number of others. While this cannot always be avoided, perhaps it can be minimized.

34. Last, and of equal importance, is maintenance of contact with the higher [redacted] echelon. Get in the habit of questioning apparently outdated or burdensome rules and procedures. Communications security is a business which should be participated in, and not just tolerated with a sort of resigned acceptance.

35. Communications security has changed a lot in the last few years. Primarily, the function has broadened. You might even say that the U.S. has, to a certain extent, lost a good part of its cryptographic sovereignty. By that I mean that we used to keep most cryptographic secrets strictly to ourselves, except for a few we shared with the U.K. Now, however, we're in the business of

sharing a good deal of our secrets with the member countries of the North Atlantic Treaty Organization. ~~Really, it's~~ Actually, it is a matter of our supplying COMSEC material, cipher machines, procedures, and the like, for there is very little we can get in return. This of course is of great importance to us, and very necessary, because so many U.S. secrets are now being revealed to NATO, and must be communicated by member countries in messages, that much of our own security would be jeopardized by insecurities in the communications of our NATO allies.

NSA50X6

NSA50X6

[redacted]

There is also a cryptographic coordinating agency, in Paris, which is a board set up to provide us with coordinated crypto-requirements for European nations and commands. The commands themselves have internal arrangements very similar to the American plan, and there is an especially good COMSEC organization as part of the Signal Division at SHAPE.

37. During the rest of my time I will briefly discuss some of the new developments in communications techniques, and in communications security equipments and procedures to go with them. But first, to obtain an understanding of the enormous problem involved, let me quote the definition of the word "Tele-communications"---"Any transmission, emission or reception of sign, signal, writing, images and sounds or intelligence of any nature by wire, radio, visual, or other electromagnetic system." There, in broad terms and definition, are the means available to the commander for transmitting intelligence electromagnetically. There is also the problem of COMSEC. Any and every means used by the commander must be made secure. Generally speaking, our research and development of new communications security systems may be thought of as progressing along six parallel but inter-related lines. All of these fields of investigation stem from the users requirements to provide better, more secure, and faster methods of handling classified information over the available communications facilities. The first category, literal cipher machines, is the oldest and probably the most familiar to you. Whenever you have the ability to send a message to another person by wire, radio, messenger, carrier pidgeon, or any other way, we must assume that the enemy has the capability, under certain conditions, to intercept and read this information. The logical means to deny this capability to the enemy is to disguise or encrypt the intelligence contained in the message so that, if intercepted, the enemy cannot understand the meaning of the message. Code books and present

encrypting machines have been too slow, bulky, or insecure to serve the present day requirements of the military for rapid and secure communications down to and between low echelons. Yet, such coordination is essential in modern warfare. An example of a new machine, designed in its final form, by the National Security Agency to provide faster more secure communications in this category is the AFSAM 7. This machine is a keyboard operated, tape printing cipher machine which encrypts literal text and numerals and is about the size of a portable typewriter. Incidently, I will have some photographs and brief descriptions of some of the newer COMSEC equipments for you to look at during the break, if you're interested.

38. Another field of communications in which security must be provided is that of teletype. As you are aware, the vast majority of military communications is carried by means of teletypewriter. Since speed is essential in this type of communications, the time spent in encryption and decryption should be a minimum. We are working toward a zero time loss in the COMSEC field. This goal will assure that the only limiting factor in speed of secure communications is that of the communication system itself. An example of a machine which will automatically encrypt or decrypt standard teletype signals is the AFSAM 9. This device is a non-synchronous teletype security equipment designed primarily for forward area use. It weighs about 50 pounds and is about 15" by 16" by 7" in size and uses rotors to encrypt the teletype signals. However, techniques are already developed to encrypt, by electronic means, as many teletype signals at any desired speed as may be required.

39. A third field of communications for which security must be provided is that of voice. The method of securing these communications is known as CIPHONY. For a long time there has been an urgent requirement to transmit classified voice conversations. This is particularly true where it is essential that advantage be taken of opportune tactical or stategic developments. In the past, since techniques were not available to provide security to this type of transmission, the commander was forced to assume the risk that the enemy could not act fast enough to take advantage of the classified information which they intercepted. To assist the commanders in exchanging information, a piece of Ciphony equipment, the AFSAY 8Ø6, is being field tested, and a light weight, airborne, VHF Ciphony system is presently being developed. Development models of VHF Ciphony Equipment were used successfully at the recent Atomic Bomb tests in the Pacific for ship-shore control use.

4Ø. Another field of interest is the transmission of classified maps or photographs. Encryption of these transmissions is known as CIFAX. Equipments are being developed which will make it possible to make these transmissions secure. An example of this type of equipment is the AFSAX 5Ø3 which the Air Force will test out later this year. We are also working on a Cifax device which will encrypt not only black and white, but will allow encryption of various levels or shades of gray to be transmitted. This will allow classified photographs, suitable for bomb assessment damage, to be sent over radio or wire circuits.

This information will then be secure from enemy interception.

41. A fifth very broad field is that of COMSEC support ancilliary equipments. These are the equipments required to assist in the encryption of decryption of messages, but are not in themselves cryptographic in nature. They do not contain cryptographic principles. An example of ancilliary equipment is the AFSAZ 7315. This device is designed as a single channel, synchronous equipment which provides traffic flow security between messages encrypted on the AFSAM 9, the non-synchronous teletype security equipment.

42. The sixth and last field I will mention is that of "Special Purpose". In this field will be found all those devices, methods, and procedures which do not constitute a major means of communications, but which are essential to the transmission of communications. Examples of such means and methods include authentication, IFF, and data transmission. These techniques are extremely important to the commander in the solution of his operational problems involving communications and security. Provision of security to all of these techniques has not yet been accomplished. The requirements are recognized and research and development is under way.

43. I have outlined only a few typical examples of equipment, problems, and recognized fields in which the National Security Agency, assisted by the consumers, is taking steps to solve the problems of secure communications. There are many other equipments being

simultaneously developed to provide the tools to the commander for fast secure communications. We are striving to develop and push to completion a dynamic, balanced, and integrated program which will provide insurance that classified information will remain secure in transmission. As new techniques, concepts, methods, procedures, and devices are developed for the transmission of intelligence, there must be concurrent development of new security measures.

44. Automatic switching equipment now designed, and in some cases available, will accomplish the following: It will check incoming channel continuity numbers, recognize message precedence and routing information, and automatically transmit messages via cross- office circuits to the correct outgoing circuit.

45. Communications security complicates all this, for cryptographic equipment associated with the relay equipment must provide an equal degree of automaticity. The principle of "link encryption" has been adopted. This means that a message, automatically encrypted at its point of origin, is automatically decrypted, routed to the proper outchannel, and reencrypted at each relay point. When a message is placed on the system, everything, heading and all, is encrypted. Thus, we have arrived at an almost perfect answer to traffic analysis. The only basic improvement which need be made is the constant transmission of an enciphered signal, whether intelligence is being passed or not. This, too, is possible. On circuits such as these it will be impossible for interceptors to detect the existence of messages, and the

first traffic analysis tool, volume count, disappears.

46. There is now in being, a multipurpose cryptographic equipment which can be used for the encryption of teletype channels, all channels of a 4 or 8 channel multiplex, or for the encryption of facsimile transmissions. Particularly in its latter use will this equipment open up new communications concepts, for it will be possible to transmit securely, at the rate of 1000 elements per second, a 9 x 12 picture in about 15 minutes. It is called the AFSAJ 700.

47. The problem of increased security at the lower echelons is being helped by the provision of a good, fast, cipher machine which can be used wherever there is power, can be used within battalions and for air-ground communications. This is the AFSAM 7. There is also the AFSAM 9, coming along rather well, which will provide field teletype security. And some progress is being made in the development of secure low echelon speech equipments.

48. Together with these new developments will come something which will make the cryptographic business much more enjoyable. We are trying, as we increase inherent security in our systems, to decrease complexity of operation. Much of our older equipment has been on the market - so to speak - too long. Cryptonalytic techniques have caught up with them and , as a result, we have had to keep them "jacked up" by inflicting cumbersome, burdensome procedures. If any

of you were connected with the COMSEC business during the past two years, you will remember the frightful procedures we had to impose, for security reasons, on the Combined Cipher Machine (CCM). Fortunately, we were able to simplify these procedures by equipment modifications.

49. I have tried to give you, in brief outline, a definition of Communications Security, the many facets of this broad definition, and some of the concepts by which the problem is being approached. In addition, I have attempted to give you some specific examples of what has been done to resolve certain problems, and what is being done to resolve other problems presently facing the commander in his operational communications. I have pointed out that new, and as yet, not fully developed, techniques of communications are recognized, are being studied, and steps are being taken to make them secure from enemy translation.

5Ø. That's what communications security is. I hope that this very broad picture has been a little bit enlightening------THANK YOU