REF ID:A74823

A3-81-160912 cy 1

TOP SECRET

MINUTES OF MEETING ON THE LABORATORY SECURITY OF AN/GSQ-4

Held 24 September 1946

PRESENT

Dr. A. Sinkov, Chairman
Mr. F. C. Austin
Mr. H. L. Clark
Mr. R. A. Dibos
Dr. S. Kullback
Mr. M. M. Mathews, Jr.
Mr. Leo Rosen
Mr. A. W. Small
Mr. C. R. Summers
Captain W. C. Washcoe
Mr. C. C. Wright

Captain Washcoe opened the meeting by stating that it came about at the request of Mr. Wright. He reported that a paper entitled "Evaluation of Security" had been prepared in Security Division and was about to be coordinated within Security Division and would later be circulated throughout the Agency. R & D Division has stated that the over all problem of security is a bit broad for them. The immediate problems for discussion were set forth by Mr. Wright in the announcement of the meeting (TAB A), and the meeting was turned over to him.

Mr. Wright opened the discussion by stating that the main question was "What is security?", realizing, of course, that security isn't the same for each echelon. Laboratory security is R & D Division's only concern. They are responsible for the development of the equipment only.

Captain Washcoe suggested that Mr. Small tell the group of his experiences with regard to laboratory and field security. Mr. Small said he had found that after a war has been going on for about a year, and the fronts are more or less stabilized, a first approximation is a one to one ratio. When the next war occurs, ciphony will have advanced to where very nearly laboratory conditions will be provided in the field in each corps area. For instance, the 5th Army Group in Italy had its own intercept radio and analysis groups within an area of 25 or 30 miles from the front. Various Signal companies were combined, working in 2 or 3 trailers, and the equipment in the trailers was modified to suit their various conditions. In answer to paragraph 2, Mr. Small estimated that a good unit for reference would actually be 3 or 4 trailers of equipment and probably 40 men, with 5 or 6 different tents. Dr. Kullback then stated that if a SIGJIP were supplied to each company, the amount of traffic carried would certainly tie up a lot of enemy personnel. It was pointed out that if we intercepted traffic of this sort we would have to determine what it was worth--a large crew or a small crew. Security depends on these factors. Dr. Sinkov said that if all other factors are equal, the enemy attacks that system which

TOP SECRET

requires less people; however, the enemy would not hesitate if it needed the information. Mr. Small emphasized that we must either take the position that the enemy is limited in personnel or else take the position that he has unlimited personnel, and he felt that Security Division should take it for granted that we assume he is unlimited. If we were fighting defensively and being pushed back, security would come "snowballing downhill" and this is a danger that we must foresee.

Mr. Rosen said that in the laboratory solution you have two irreducibles--men and length of time. The more people--the faster the solution. Therefore, the transfer to the field amounts to additional people and a faster solution. Mr. Small added that it would depend on the state of the war. Mr. Austin further added that machines are susceptible to human errors and that this must also be considered in setting the hours of security. Mr. Wright replied that rules are set up to take care of the latter; but, nevertheless, the ratio of laboratory to field security has now been reduced to less than one.

Mr. Wright reported that on the basis of the request R & D Division made of Security Division regarding use of the TDS principle, R & D Division is now devising a method of determining how the scrambler is to be made, its weight, its security in length of time, etc. A 10-unit scrambler is presently being used, and it has been decided that 100 units would be the maximum that could be utilized. The problem now is to choose the proper value between 10 and 100 elements and still maintain the 15 pounds.

Dr. Kullback said he thought the best guide for development on the AN/GSQ-4 would be some definite indication from the people for whom it is being developed whether they would prefer more security or less weight. Dr. Sinkov stated that the Ground Forces have been complaining that they have had no indication of what progress we have made on the cryptographic plan (SIGIRA). He suggested that they be provided with a statement of the difficulties on the AN/GSQ-4 and advised that we can give them increased security if they will permit the weight limitation to be raised. Mr. Small added that we still would not be able to state the security. Captain Washcoe brought up the fact that the question of weight is governed by AR 850-25. The military characteristics are what someone would like to have, we strive toward them, and one of the three following results is obtained-- (1) We can fully meet military requirements; (2) Military requirements are met only fairly well, but the result is much better than anything presently known; or (3) We can be so far from military requirements that they will have nothing to do with it. Mr. Small replied that all we can do is to give the user an estimate of the security if the field conditions are "such and such," and that under special conditions, the security will not be as great.

Mr. Small also asked if the use of TDS could be eliminated. Mr. Mathews then raised the question of whether we are going to do anything and whether we are going to spend more money if it will never be any good. Dr. Sinkov asked if the TDS and converter equipment combined would be secure. Mr. Mathews replied that the two dimensions, frequency and time position, are more or less unrelated in the two best equipments.

Dr. Sinkov said that what we are searching for is some equation or weighting method, so we can arrive at some number for designating security. At the moment we have no sure-fire method of determining it, as there are all kinds of factors tending to invalidate any result. Mr. Wright stated that most of the variables had been eliminated, and Mr. Small replied that this is the best that can be done. Mr. Small then asked if there isn't some agreement that could be reached between the two divisions, to permit reaching some sort of conclusion. We must consider security against the seemingly best enemy, and we must assume that he has equipment as good as ours. If that is so, field security can never be greater than laboratory security.

Captain Washcoe stated that we have nothing now that is suitable for the AN/GSQ-4, and asked if the SIGJIP is good enough in the meantime. The Ground Forces do want equipment, and in the event of another war, we must have some device to use. Captain Washcoe further stated that he considers the SIGJIP a failure because it does not work, rather than because it does not provide enough security. Mr. Austin raised the question of whether we should make the SIGJIP better or design a new machine.

Captain Washcoe continued that we have to think--"Would this device give them something or would they be better off without it?" The information handled by the device, transmitted under proper controls and proper rules, would be tactical information not having long range value. It might, however, offer information which would later be transmitted in a higher security system, thus giving a break into the higher system. Information transmitted by low echelons would be of a nature that would not require a long period of security.

Mr. Austin brought up the question of conferences between regiments, companies, and platoons in battle. Captain Washcoe stated that a net would be set up enabling this to be done. Mr. Wright asked for a definition of "radio net." Captain Washcoe replied that a net consists of several stations, one being the central station. "A", the central station, can talk with "B" and "C", and "B" and "C" can talk with each other. The point was brought up that if the latter is true, it actually is a conference. Dr. Sinkov replied that if "B" and "C" couldn't talk to each other, operation would be very limited.

Mr. Wright brought up an entirely different problem, involving the factors in a. and b. of paragraph 3. The inherent security of the AN/TRA-16 is in the technique of transmission, provided that the enemy is not in the line of the transmission beam. Mr. Small said that the Germans had estimated two years security on beam teletype, but we were able to collect the traffic and read it to great advantage. It was stated that the problem in the AN/TRA-16 is the recording of the material. The only way the traffic can be interpreted is by listening to the plain text. Any security evaluation will have to be made when the problem of recording the traffic is solved. Mr. Mathews stated that there was no point in discussing 3a. and 3b. on the basis of the foregoing discussion. Mr. Small added that line of sight transmission beamed on the horizon would be out of the question unless it was infra-red.

Dr. Sinkov drew the following conclusions: R & D Division has within the laboratory a method of making a statement regarding the ratio involved in considering the security; Security Division must have something to provide the Ground Forces in the way of equipment in the near future; we will do the best we can to meet military characteristics and give the best security we can. Mr. Clark added that no matter what decision was made now, we would still be faced with the same problem with the Air Forces. The Air Forces very definitely have a transmission problem.

Captain Washcoe stated that integrated equipment directly ties together the security and transmission elements. The AN/TRA-16 is in itself an integrated piece of equipment. An opinion had been expressed by Mr. Friedman that an integrated equipment could be described as an equipment with all its parts functioning as a unit in such a way that the complete equipment would cease operating if the cryptographic feature were removed. The Air Forces disagree with this interpretation because they do not want to consider radio equipment as cryptographic equipment. Nevertheless, this is the ASA definition as it now stands, and Staff is defending it. Mr. Mathews stated that the AN/TRA-16 would not function without the key generator, but that it could be modified so as to make possible a key setting which would reduce the effect of the crypto-mechanism to zero. Captain Washcoe added that a plain wafer could also be thrown in and that it would produce the same effect.

Mr. Wright closed the meeting by stating that the only solution is to do the best we can on the SIGJIP. Dr. Sinkov said the whole problem of field versus laboratory security would be set aside, and Captain Washcoe added that R & D Division could go through with their estimates and indicate the laboratory security afforded.

R. A. DIBOS
Technical Staff
Security Division

TOP SECRET

TAB A

CONFERENCE 0900 Tuesday, 24 September 1946, Room 1010-A

Requested by Mr. Wright of R & D Division

1. Object is to obtain a criterion of sufficient security for low and medium grade ciphony and cifax systems.

a. General - Set up tentatively a policy sufficiently definite to give us a first approximation for correlating "laboratory security" with "field security". It is realized that in the final analysis, specific equipments will have to be considered individually.

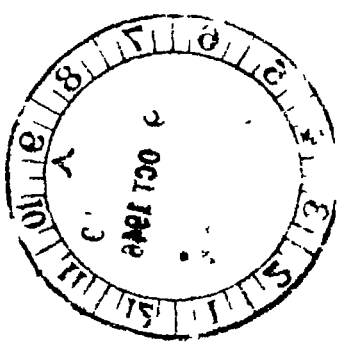
b. At present, we badly need a definite minimum "laboratory security" requirement for AN/GSQ-4.

2. We would like to standardize the unit used in stating "laboratory security." We feel that this unit might well be defined in terms of a normal field group which would be assigned to solving the traffic from properly recorded intercept. i.e. 2 men and 1,000 lbs. of equipment might be a reasonable unit.

3. Considerations which must necessarily be considered to determine the correlation between "field security" and "laboratory security".

a. Suppose the equipment was limited exclusively to very high frequency radios by its design and therefore transmission would always be line of sight except in very unusual instances.

b. Certain types of modulation, notably pulse modulation, might greatly increase the problems of recording and playing back intercept. This comes about because of the high speed recording medium necessary and the need for accurately timed recordings to make playback possible.



TOP SECRET