[redacted] DECLASSIFIED

NRL REPORT NO.R-3170

[redacted]

THE ATTAINMENT OF SECURITY IN IFF

[redacted]

NAVAL RESEARCH LABORATORY

Washington, D.C.

NRL REPORT NO.R-31

THE ATTAINMENT OF SECURITY IN IFF

by

L. S. Schwartz

August 1947

Problem No. 34R03-06

Approved by:

Dr. J. M. Miller
Superintendent
Radio Division I

Commodore H. A. Schade, USN
Director
Naval Research Laboratory

NAVAL RESEARCH LABORATORY

Washington, D.C.

DISTRIBUTION

	Copy No.
BuShips Attn: Code 910B(918)	1-5
ONR Attn: Code N482	6-9
CNO Attn: Code Op-413 Attn: Code Op-20D	10 11
BuAer Attn: Code EL-83. Electronics Division	12-16
BuOrd Attn: Code Re9 Attn: Code Re4f	17 18
CO, ONR, Boston	19
OpDevFor, U. S. Fleet, Norfolk	20
USNEL Attn: Dr. R. O. Burns	21-22
SNLO, USNELO, Ft. Monmouth	23
OinC, NRL Field Station, Boston	24
CG, AGF, Pentagon Attn: STSGE	25
CG, AAF, AC/AS-4, Pentagon Attn: Mr. Harry Mulkey, Res. and Eng. Div.	26
CO, AMC, Red Bank Attn: WLENA (Via ALO, NRL)	27
ANEESA	28
CG, AMC, Wright Field Attn: TSELR, Engineering Div. (Via ALO, NRL)	29-30
CO, AMC, Cambridge Field Station Attn: Dr. O'Day (Via ALO, NRL)	31
Deputy Cdr. for Res and Dev., Signal Corps, Bradley Beach Attn: Dir., ESL for Mr. Stokes (Via ALO, NRL)	32
RDB Attn: Library Attn: Navy Secretary	33-34 35
Science and Technology Project Attn: Mr. J. H. Heald	36-37
NRL, Code 187B	38-50

CONTENTS

ABSTRACT

It is pointed out in this report that primary emphasis in the development of a secure IFF system must be given to the introduction of a coded transmission which will satisfactorily prevent the enemy from appearing as a friend and that only secondary emphasis should be given to the means of preventing the system from being used as a cheap radar by the enemy.

Six factors affecting the security are discussed: (1) coding on the interrogation and reply path, (2) reply to any of several interrogation codes radiated at the same time, (3) the length of the coding cycle, (4) random changes of the interrogation and reply codes, (5) the duration of each code and the number of codes and (6) prevention of prediction. It is shown that these factors serve as a basis for evaluating the security of any coding proposal.

It is concluded that no particular gain in security accrues from the use of multiple modulation modes or unusual transmission characteristics. It is further concluded that efforts to uncover "new" and startling principles of operation are unlikely to result in techniques capable of improving security.

AUTHORIZATION

This report covers one phase of the study assigned by the Bureau of Ships Problem S1234X-S (now designated as 34R03-06).

PROBLEM STATUS

Work is continuing on other phases of this problem.

THE ATTAINMENT OF SECURITY IN IFF

INTRODUCTION

This report discusses the factors upon which a valid estimate of the security value of an IFF coding proposal depends. The procedure is: (1) to give an account of the points of difference and the points of similarity between communication and IFF security, (2) to use this account to pave the way for a statement of the basic criteria of IFF security, (3) to state the criteria and to illustrate their application as guides to a solution of the problem of preventing the enemy from using the IFF system to appear as a friend, and (4) to draw the conclusions against which any IFF coding proposal can be evaluated.

In IFF operation it has been generally agreed that it would be desirable to include functions of a limited tactical and informational nature in addition to the primary function of recognition and identification. These would encompass the transmission of such information as personal identity, squadron leader designation, limited intelligence, and a distress signal. Each function would be assigned a particular code. This paper will be concerned with the transmission of the security code only, and no mention will be made of the other functions.

GENERAL PROBLEM

The problem of coding for IFF is distinct from that encountered in communications. In the latter, complex and involved intelligence must be transmitted frequently in messages of considerable duration. In IFF, except for certain supplementary functions of an informational or tactical nature, the operator is concerned with the transmission of very simple intelligence in the form of the question: "Who are you?" and the answer: "I am a friend". The same transmission is repeated in talking to one target or to many, and the very simplicity of the message allows the use of any arbitrary signal for challenge and reply. By the employment of cryptographic measures in communications, one seeks to deny the enemy access to the information which is transmitted over a message link and to prevent his use of that link to convey false information to friendly formations. In other words, it is presumed that the enemy does not know the information that is being sent, and the problem is to prevent him from finding out. In IFF, on the other hand, the enemy knows very well what the message is, and the problem is to prevent him from saying it in the agreed-upon way, thus appearing as a friend. Moreover, an additional problem in IFF is to prevent enemy use of the system to interrogate friendly units, thereby securing their recognition and location.*

In the case of communication systems, the impossibility of indefinitely preventing the enemy from satisfactorily breaking a particular code is recognized. It is expected rather that for a given code a limited security only can be achieved which is measured in periods of hours or days at most. Although very secure codes, which for years

---

* C. E. Cleeton, Coding and Security of Electronic Recognition and Identification Systems, NRL Report R-2972, 12 September 1946

baffled the most ingenious methods of cryptographic analysis, have been devised, they lacked the flexibility and simplicity needed in military operations. An example is the use of a book selected at random in which the number of the page and of the word on the page are transmitted as cipher elements. It must be remembered that speed in encipherment and decipherment is desirable, and often urgent, and that the conditions of military action are conducive to maximum error. Hence, it seems that a basic requirement for an "ideal" or "perfect" military code is simplicity. This is not in contradiction to the demand for security if the concept of security is extended to include the factor of time. A code is employed for a given period and then is changed, the period of its transmission being short enough in the case of communications to insure against the collection of sufficient data to break the code and in the case of IFF to insure against breaking the code before it is changed.

During the past war the Bell Telephone Laboratories, under NDRC project C-43, investigated the security of several speech privacy systems.† The results of this study appear to indicate that the maximum security obtainable with very elaborate and well designed apparatus could be measured in terms of hours at best. It is necessary to emphasize, however, that this is true only where specialized apparatus for decoding, including the unscrambler itself, is available; otherwise the security of the apparatus would be much higher. A further conclusion derived from this study is that, while a particular speech privacy system may have small security when analyzed by experienced personnel with a laboratory full of equipment, this same system might possess a high degree of security if the necessary decoding apparatus and experienced personnel were not available. Under combat conditions, only higher military echelons could be expected to maintain a full complement of decoding equipment, but by the same token the lower echelons of combat formations, both the enemy and friendly, would be restricted to the simpler coding devices and the simpler codes. This implies that the encoded messages could be decoded by less specialized means. Nevertheless, the experience with project C-43 seems to support the view that the "cracking" installation becomes complicated at a more rapid rate than the scrambling and unscrambling system itself. Two more lessons brought out by the Bell Laboratory study are that cryptographic security is greatly increased (1) by use of an essentially non-recurrent cycle and (2) by code changes which are random. These lessons have been learned from a study of speech scrambling methods, but they are equally applicable to IFF. The only difference is in the comparative simplicity of the IFF problem.

These observations conclude the comparison between communication and IFF security. An attempt will now be made to examine and assess the factors which promote the latter.

Basic Factors in Security

Before discussing the primary factors which are believed essential to the security of an IFF system, it is desirable to be clear on the type of IFF operation envisaged for the future. Current thinking has the question "Who are you?" raised by an interrogator which may be air-based, ship-based, or ground-based. The answer in the form of the reply, "I am a friend" is given by a respondor or transpondor which also may be air-based, ship-based, or ground-based. The reply is received and interpreted by a unit called a responsor which is integral with the interrogator. In the succeeding discussion it is assumed for convenience of description that the interrogator and responsor are surface-based and that the transpondor is air-based. Any conclusions so derived are, however,

---

† W. Koenig, Final Report on Project C-43, Parts I and II, Bell Telephone Laboratory Report, October 12, 1944

general and are not restricted to this situation.

A satisfactory means for preventing the enemy from using the friendly IFF system as a "cheap radar" has not as yet been evolved. Although a solution to this problem is desirable, it does not seem as imperative as the prevention of enemy use of the system to appear as a friend. The reasons for this are as follows. The enemy cannot rely on the friendly IFF system to inform him at all times of the presence of hostile units. Hence, he must have his own radar for the periods when friendly IFF is inoperative. In that case he is likely to depend for his means of detection almost exclusively on his own radar. Although it is admitted that the friendly IFF system would afford him a positive means of identification, it would be dangerous for him to depend on this, since our elements may not use their IFF over or near his territory, and furthermore, we may attempt deceptive measures by means of it. It is clearly to the enemy's interest, therefore, to have his own identification system as well as his own radar.

For these reasons the principal effort must be directed towards the introduction of a means of coded transmission which the enemy would be unable to duplicate with the intention of appearing as a friend. In order to be clear in regard to how this effort can be made productive, it is necessary to consider the merits of coding on the interrogation path, on the reply path, or on both. For practical reasons there is a limit to the number of interrogation and reply codes that can be built into a system. Hence, any particular code would inevitably be repeated, enabling the enemy to determine the codes in use by monitoring methods. In the case of interrogation coding, once the enemy has resolved all the codes, he can adjust his transpondor to reply correctly to all interrogations. But in the case of reply coding, even though he knows all of the reply codes, he must ascertain which one to use at any given time. If, however, false interrogation codes are interspersed among the true, the enemy must at any time discover which codes are true, so this is equivalent to reply coding from the security standpoint. But there are several operational and technical disadvantages to the use of false codes.‡ One point bears particular emphasis. It is a major task to coordinate radar and IFF information. It is expected that it would be an even more difficult task to coordinate replies to false codes in addition. Consequently, since an increase in system complication would result from the use of false codes on interrogation, and since their use would not afford a gain in security over that from reply coding, the latter is to be preferred.

Nevertheless, coding on the interrogation path is important because the time required by the enemy to determine the replies by interrogation is directly proportional to the number of interrogation codes. Furthermore, the probability of the enemy's furnishing appropriate replies by chance is reduced in accordance with the number of interrogation codes. Moreover, it is desirable to employ a multiplicity of interrogation codes at any one time in any operational area, since this would force the enemy to run through all the interrogation codes to find the corresponding reply code.

Finally, coding on both the interrogation and reply paths is desirable because an additional coding element would be introduced by varying the relation between the interrogation and the reply codes. For example, suppose one is limited by design considerations to a maximum of five codes on each path. If the relationship between the interrogation and reply codes is held fixed, the total number of possible code combinations is 5. But if this relationship is varied, the total number of possible code combinations is 5 factorial or 120.

---

‡ Cleeton, Op. Cit.

It is believed that there are four basic factors which promote IFF security: (A) the length of the coding cycle, (B) the randomness of code change, (C) the frequency of code change, and (D) the complexity of the code. Before a detailed discussion of these elements is begun, it should be understood that a customary assumption is made: the enemy is in possession of captured units of the friendly IFF system, and/or he has constructed his own counterparts.

Length of Coding Cycle

The coding cycle should be as long as practical, ideally of sufficient length to obviate the need of repetition during the life of the system in order to discourage attempts at prediction. Also, care must be taken to insure against the inclusion of tell-tale sub-cycles within the coding cycle.

Randomness of Code Changes

Security is improved by arranging for one code to follow another in a random sequence, both in the interrogator and in the transpondor. This prevents prediction. Moreover, it is equally important that the code changes in the interrogator and the transpondor be random with respect to each other. This may be done manually or automatically by chronometer control. The importance of mutually random code changes is seen in the anticipation that both the interrogation and reply codes will be monitored. Obviously, the job of monitoring will be much more difficult if it is possible to correlate replies with interrogations only during comparatively short intervals of time.

The Frequency of Code Change

The time devoted to each code should be minimized. Consequently, a means must be provided for synchronizing the reply code changes in order that all of them can be changed at the same time. This may be accomplished by a chronometer carried with each transpondor. But the limitation on how rapidly the code can be changed seems to depend upon the tolerance in the chronometer setting because it fixes the interval of uncertainty regarding the position in time of the next code. Thus, in a recent Army-Navy Aeronautical specification§ for aircraft clocks the tolerance on time is, under the conditions of test, more than a minute in a period of 24 hours. If errors in IFF interrogation and reply are not to be made, the time interval devoted to each code must be at least as long as this, unless it is agreed that codes adjacent to the desired code are also acceptable.

But, as will be seen, a code time of the order of a minute may not be short enough, so a means of reducing it may have to be found. Two possibilities are suggested: (1) to reduce the clock tolerances by perhaps a factor of ten or more through improvements in the clocks themselves, and (2) to synchronize the clocks at short time intervals by signals sent from shore or ship stations where accurate time is kept, thus limiting the maximum clock error. It seems clear that the former is preferable because the radiation and reception of synchronizing signals require additional ground and airborne installations. Furthermore, these signals may be jammed by the enemy and can be used by him to synchronize captured equipment. An additional point is that the enemy may radiate false timing signals. On the other hand it may not be practical to devise a chronometer with the accuracy necessary to allow the desired rapidity in change of code; hence, the arguments

§Army-Navy Aeronautical Specification Clocks; 1-7/8 Inch Dial, AN-C-99a, 16 March 1945

against the synchronizing system might be outweighed by the consideration of greater frequency of code change attendant upon its use.

As it is unlikely that the synchronizing signals can be made worldwide, it is expected that friendly aircraft would, under certain conditions, fly beyond range of the signals for hours at a time. The implication of this needs to be examined. Given the tolerance on aircraft clocks and the maximum expected duration of aircraft missions, one can assign the minimum time interval between synchronizing signals. This interval must be sufficiently large to eliminate the possibility of any chronometer's being positioned to the incorrect setting because, during the course of an extended aircraft mission beyond the range of the synchronizer, the chronometer has drifted more than half way in time between two timing signals. For example, suppose that the tolerance on clock time is one minute in 24 hours and that the expected maximum duration of any mission away from friendly territory is also 24 hours. Then the minimum time interval between two synchronizing signals must be greater than two minutes. On the other hand,one has to consider that, during the first two minutes of the return flight over territory covered by friendly radar, a plane could respond with incorrect IFF replies; and this time might be sufficient in which to initiate defensive action against it. Obviously, therefore, the time between synchronizing signals must be short enough to prevent such an occurrence. A reduction in this time could be accomplished only by paring of the chronometer tolerance.

The Complexity of the Code

A coding system can be devised which would have only two code elements, M and N, for example, and which would satisfy the requirements postulated under A, B, and C. That is, the length of the cycle can be made as long as desired, the change from M to N or N to M can be made random, and this change can be made in the shortest possible time set by the chronometer or by the synchronizing signal tolerances. A little study will show that the three criteria just postulated though necessary, may not be sufficient, since there are two distinct methods of breaking the IFF code which can still be tried by a determined enemy: (1) the method of percentage risk and (2) the method of monitoring.

The percentage risk method. It is assumed that the enemy has captured a certain number of our transpondors or has modified his own to answer correctly to each of our interrogations. In an effort to break our IFF system he could do the following things. First, he might equip one plane with as many transpondors as there are codes, with each unit set to reply on a different code. Under interrogation at least one of his replies would be certain to be right. Second, he might have each of several transpondors set up on different codes and placed in different planes, the planes being spaced relatively close together and operating as a single group. The responses would appear to come from approximately the same position in space. Conceivably, these situations could be readily handled by means of anti-coincidence circuits which would cancel or eliminate any indication when both false and correct codes originate from the same point in space. There is, however, a danger in the use of anti-coincidence circuits. If an enemy plane can fly toward a friendly base in company with a close formation of friendly planes (an "intruder operation"), he can successfully blank out the correct replies from the friendly planes by the mere device of radiating one or more false codes. The friendly craft would then be identified as enemies. It seems clear, therefore, that if anti-coincidence circuits are used, they should not be positive in their action. That is, correct replies, unlike the false, must be blocked from coming through. The function of the anti-coincidence circuits should be to warn the equipment operator of the presence of false replies among the true, so that steps can be taken to ascertain the real situation. For example, warning of the

intruder's presence might be radioed to friendly craft if possible. The third imagined contingency is more difficult to cope with because the planes are presumed to be separated widely in space, as in a coordinated attack on a ship from various directions. In this case anti-coincidence circuits could not be used to aid in the identification of the enemy targets. With a single interrogation code there would be no means of indicating whether a given plane, which by chance had the correct code, was in fact an enemy or not. One could hope to unmask him only after a shift was made to the next reply code interval which, unless he had broken the security of the system, he would be unlikely to anticipate properly.

The third contingency provides a strong argument for the use of more than one interrogation code in any reply code interval and/or for a rapid change of reply code. An example may show this. It was said earlier that without synchronizing signals the minimum time for each code interval is equal to the tolerance on the clock time. Actually, if a timing signal is not employed, it may prove necessary to have an interval which is several times this tolerance in order to avoid ambiguity caused by the reception of overlapping transpondor codes. Suppose the interval is five minutes. It is foreseen** that by 1960 airplane targets may attain the enormous speed of 1,500 nautical miles per hour, traversing a distance of 125 nautical miles in the 5 minute interval. If the enemy were flying at an altitude of 5,000 feet, he could transmit friendly indication from the radio horizon to the radar position without defensive action being taken against him, and he could accomplish his mission. If the attacker were unwilling or unable to send a number of planes equal to the number of reply codes against a friendly objective, his probability for success would be diminished accordingly, but he still might be willing to send some planes if his chances were sufficiently favorable. It is clear that this could be combated by a rapid change of reply code which could be achieved in two ways: by a large reduction in clock tolerance and/or by means of synchronizing signals.

It may be useful to consider what could be done to circumvent the enemy in regard to percentage risk if it should prove impractical to employ more than one interrogation code in any reply code interval or to shorten this interval as much as necessary. The question naturally arises as to the ultimate ceiling on the number of planes which the enemy would care to equip with transpondors in a risk venture. One might think of the following operational situations.

1. The enemy has complete control of the air in which case he probably would not attempt to break the friendly IFF system.
2. The enemy does not have complete control of the air but can send a sufficient number of planes to saturate the defense of a particular installation, in which case also he probably would not try to break the friendly IFF system.
3. The enemy does not have sufficient planes to saturate the defense, so it is in his interest to endeavor to break the system.

It appears from the foregoing possibilities that, in order to cope effectively with percentage risk if only one interrogation code is used and if the reply code interval is too long, a sufficient number of code combinations is needed on the reply channel to oblige the enemy to attack with enough aircraft to saturate the defenses. Category (2) then applies, provided the enemy has the planes.

**An analysis of the Problems of Location and Destruction by Gunfire of Future Aircraft Targets (Gunfire Control System Mark 65), by Bell Telephone Laboratory Report, Feb. 1947.

Monitoring methods. The second mode of approach to the problem of breaking the IFF code is now considered. It is assumed that the enemy has acquired not only one or more friendly replying units but an interrogator as well and that the friendly system does not use synchronizing signals. If the enemy were trying to monitor friendly transmissions, it is believed that he would, during any code interval, play through the interrogation codes, and catalog the appropriate replies he receives from hostile transpondors. If the number of interrogation codes is small, this could be accomplished in a short time and it could be done manually. One reason, therefore, for considering more complicated systems of coding is to force the enemy to employ a longer time for monitoring than is available in a code interval. The ultimate objective is to prevent the enemy from manually setting his transpondors in the time allowed, thus forcing him to adopt an automatic means for analyzing and evaluating the code. In addition to having a large number of codes as a means for the prevention of successful monitoring, one sees the need for a rapid change of reply code in order to combat automatic scanning of the code sequence. For example, the enemy's decoder must first determine the interrogation and reply codes and relate them. Then it must provide the transpondor with the appropriate receiver and transmitter settings. All this takes time. If the hostile interrogator and transpondor codes should change relative to each other within one period of rotation of an interrogator directional antenna pattern, incorrect responses might be given during part of the period. In other words one should force the enemy to be ready to emit any or all of the reply codes at any instant. The underlying thought is that his decoding equipment would then be more complex than the IFF system, since his equipment would be required to indicate any of the codes at any time. In the IFF equipment the same circuit could be used over and over again, with minor modifications, to generate and decode new programs, but in the enemy's decoder the number of complete circuits must equal the total number of codes radiated by our units, if the enemy is to achieve automatic and instantaneous decoding.

It seems that with careful preparation, a determined enemy should be able to handle a fairly large number of code combinations by manual means alone. For example, if the coding program involved the use of trains of pulses, an analysis of the transmission could be made by an "A" scope with multiple sweep presentation, each sweep corresponding to a given reply channel. The reply channels could be determined by triggering a transpondor with a succession of interrogation codes. Having correlated, by means of a chart prepared in advance, the patterns on the scope with the relevant circuit settings in the transpondor, the enemy would be in a position to emit the correct reply to our interrogation. As a guess it would seem that the whole procedure involved in manually decoding and adjusting the transpondor for proper reply might not, with experienced operators, require more than a minute.

It has been pointed out that if frequent changes of reply code are to be made, chronometers are probably necessary. Having granted the need for chronometers, one is concerned about the advantage in combating monitoring methods to be gained by increasing the number of codes. If the enemy attempts decoding by manual means, it is believed that the chief gain would be to force him to increase the number of his people involved in the decoding effort. For example, if only two or three codes were used on interrogation and reply, it is possible that one of the crewmen in the enemy aircraft might do the monitoring in addition to his other duties; if more codes were used, it might be found that one man would have to be detailed full time for monitoring and setting up the equipment. If still more codes were used, it might be necessary for two additional men to be employed for monitoring them. Thus, the number of men required for monitoring increases proportionately with the increase in the number of codes.

It is clear then that the number of codes should be increased. It must be realized, however, that this increase would result in a departure from simplicity in design with the consequence of reduced equipment dependability, increased size and weight, and increased input power requirements. It is possible that, for a given degree of security, it would be more economical to keep the number of codes small and to decrease to a practical minimum the time assigned each code. This possibility should be carefully evaluated. If the assigned time is to be short enough, it appears that improved aircraft clocks would be needed, and/or synchronizing signals controlled by accurate time pieces must be used to minimize the tolerances in aircraft clocks. It is conceivable that the timing signals would allow the code time to be reduced to the order of seconds or even a fraction of a second, thereby forcing the enemy to employ automatic means in his monitoring efforts.

Let us consider in further detail the problem of code complexity. That it need not be complex if one considers the problem from the probability point of view alone is readily seen from the following example: It is assumed that there are only two codes, M and N, and that the simultaneous radiation of both codes has no particular advantage because of anti-coincidence circuits. If the selection of either one is random and if the code time is 5 seconds, the probability that the correct program would be radiated for one entire minute without error on a trial and error basis is $(1/2)^{12}$ or 1/4,096. Furthermore, if the enemy were unable to complete monitoring and setting up before the next code is transmitted, two codes should certainly be enough because in that case he would always be out of step. It must be clear, however, that by automatic means he may still be able to decode a friendly transmission as fast as it is changed. The last remaining recourse in this event is to increase the number of codes beyond the point at which the enemy's decoding installation becomes excessively complex. This would be determined for both, but it is hoped that it would impair the enemy's operation more. It is difficult to guess the number of codes that might be required, but it seems that the number need not be large. It is probable that a specific number can be supplied only after a careful study of design and operational considerations.

It should be pointed out that it is not necessary for the enemy to capture interrogators or to construct his own for monitoring purposes. It is technically possible, although more difficult, for him to correlate interrogations and replies by synchronizing the scan of his monitoring scope with one of our interrogators in order to receive transpondor replies.

GENERAL OBSERVATIONS

The Prevention of Successful Prediction

The likelihood that the enemy might capture airborne transpondors in working condition is not to be neglected. If the basic coding mechanism should fall into his hands, he might be able to determine the complete output curve from which successful prediction may be possible, so it would be a distinct disadvantage to have the mechanism in the transpondor. Instead, the code generators should be maintained at surface stations and only that portion of the code cycle which is appropriate for the day should be sent aloft in transpondors. To do so, perforated tapes or cards, or film on which the code of the day has been inscribed, could be employed. A scanning head in the transpondor could be used to convert the perforations or marks into the appropriate code. The enemy, in possession of such a transpondor, would have insufficient information on which to base a successful prediction, provided, of course, that the code cycle were very long. He could, at most, utilize the transpondor for the remainder of that day, but without

monitoring it would be of no use to him on succeeding days. The only way to prevent his using it for even part of one day would be to employ adequate destructor devices. It is likely that eventually the enemy will capture the basic coding mechanism in any case, although of course the likelihood is greatly reduced if the above-mentioned precaution is taken. To guard against the eventuality of ultimate capture, it will probably prove necessary to change the initial starting point of the code generators at predetermined times.

There is another advantage in the use of tapes and similar devices. If the enemy captures the basic coding mechanism, he also can employ it; this is to be avoided, especially if it is superior to his own.

Complex and Unusual Transmission Characteristics and "New" Principles of Operation

As has been seen, security in coding is obtained by the rapid and random variation of an operating characteristic. The characteristic may be frequency, phase, or pulse pattern. Security rests not so much on the nature of the characteristic which is changed but rather on the speed and randomness with which the change is made. Aside from operational and technical considerations, there is no particular advantage in using one kind of modulation as opposed to another, nor in mixing them, as for example, interrogating by means of frequency modulation and replying by means of amplitude modulation. Although the mixing of modulations or principles of operation may be expected to complicate the enemy's problem in "breaking" the system, it may also be expected to augment our problems of construction and maintenance of stable operation.

Another point which deserves emphasis is that very little security is afforded in adopting a new principle of operation primarily because it is new, if it is assumed, and it is the only sensible thing to assume, that one will be dealing with a determined and technically advanced enemy. In this connection it is of interest to note that during World War II the Germans devoted considerable effort to IFF and their thinking showed marked similarity to thinking on IFF in this country. For example, intelligence reports state that at the close of the war they had under development a system (The Neuling) with provisions for:

1. Continuous presentation of IFF signals on all types of early warning radar,
2. Ground-controlled interception,
3. Air-to-air recognition,
4. Twelve alternative pairs of frequencies, each pair to consist of an interrogating and response frequency.

Also, the Germans planned to combine this system with high discrimination radars by the addition of a centimeter receiver to the IFF transpondor so that the IFF response would occur only over the narrow arc of the radar.

CONCLUSION

The primary emphasis in the development of a secure IFF system must be given to the introduction of a coded transmission which will satisfactorily prevent the enemy from appearing as a friend. Only secondary emphasis should be given to means of preventing the system from being used by the enemy as a "cheap radar"

The security of any new IFF proposal can be evaluated from the standpoint of the six following points and failure to comply with any of them should be cause for

rejection of the proposal:

1. Coding should take place on both the interrogation and the reply path.
2. The system should be capable of replying to any of several interrogation codes radiated at any one time.
3. The length of the coding cycle should be at least as long as the anticipated operational use of the system.
4. Interrogation and reply code changes must be individually and mutually random.
5. The duration of each code should be as short as possible, perhaps not exceeding a few seconds, in order that the number of codes can be held to a practical figure. The number of codes, however, must be adequate to render efforts at automatic decoding impractical.
6. The coding system should be so designed that only a portion of the coding cycle would be sent aloft in an airborne transpondor.

It is concluded that no particular gain in security accrues from the use of multiple modulation modes or unusual transmission characteristics. It is further concluded that efforts to uncover "new" and startling principles of operation are unlikely to result in techniques capable of improving security.
